

**TO
THE
NEW™**



IAM and AWS CLI

Trainee Name : Chhavi Sharma

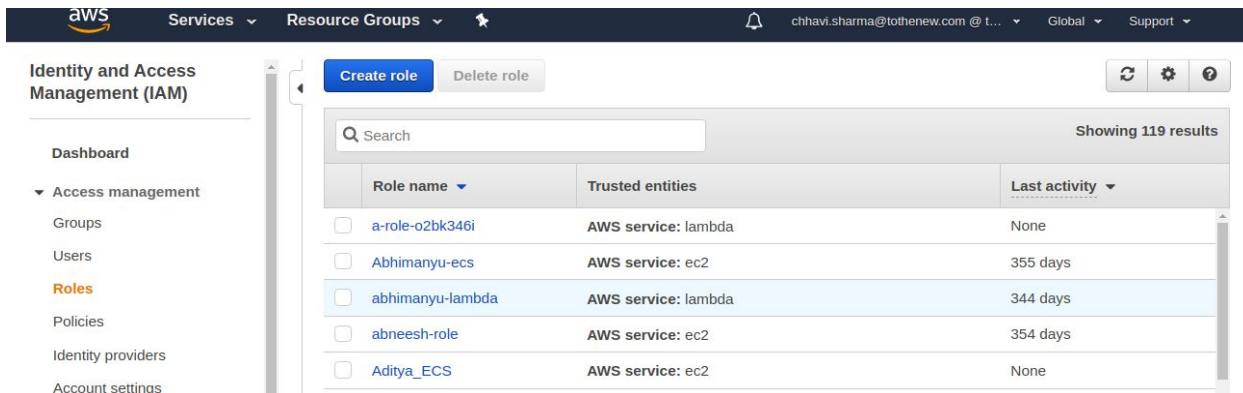
Newers ID : 4023

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.

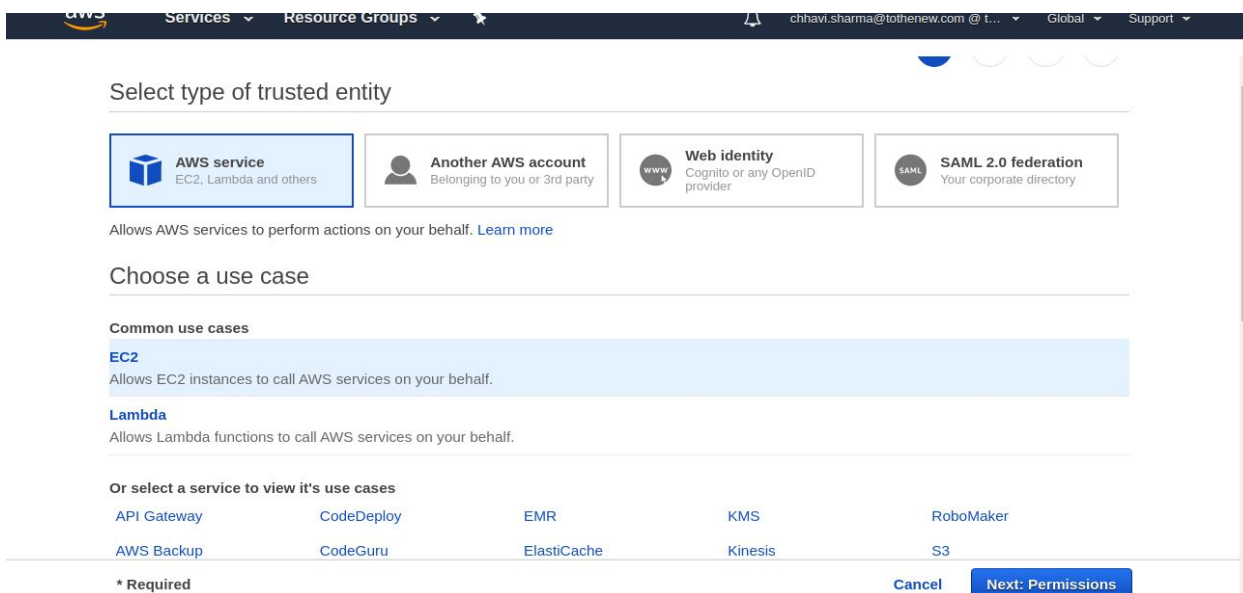


The screenshot shows the AWS IAM console. The left sidebar has a menu with 'Roles' highlighted. The main content area shows a table of roles. The 'Create role' button is at the top left of the main area.

Role name	Trusted entities	Last activity
<input type="checkbox"/> a-role-o2bk346i	AWS service: lambda	None
<input type="checkbox"/> Abhimanyu-ecs	AWS service: ec2	355 days
<input type="checkbox"/> abhimanyu-lambda	AWS service: lambda	344 days
<input type="checkbox"/> abneesh-role	AWS service: ec2	354 days
<input type="checkbox"/> Aditya_ECS	AWS service: ec2	None

Click on create role.

Select a use case.(here ec2)



The screenshot shows the 'Select type of trusted entity' page in the AWS IAM console. It has four tabs: 'AWS service', 'Another AWS account', 'Web identity', and 'SAML 2.0 federation'. The 'AWS service' tab is selected. Below the tabs, there are sections for 'Common use cases' (EC2, Lambda) and 'Or select a service to view its use cases' (API Gateway, CodeDeploy, EMR, KMS, RoboMaker, AWS Backup, CodeGuru, ElastiCache, Kinesis, S3). At the bottom, there are 'Cancel' and 'Next: Permissions' buttons.

Select type of trusted entity

AWS service
EC2, Lambda and others

Another AWS account
Belonging to you or 3rd party

Web identity
Cognito or any OpenID provider

SAML 2.0 federation
Your corporate directory

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

API Gateway CodeDeploy EMR KMS RoboMaker

AWS Backup CodeGuru ElastiCache Kinesis S3

* Required

Cancel **Next: Permissions**

Select permission : S3 full access

▼ Attach permissions policies

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

Create policy



Filter policies ▼		Q s3full	Showing 1 result
	Policy name ▼	Used as	
<input checked="" type="checkbox"/>	AmazonS3FullAccess	Permissions policy (23)	

Role Created.

entity and Access management (IAM)

Dashboard

Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

✓ The role Chhavi-S3-FullAccess has been created.

Create role

Delete role



Q chhavi

Showing 1 result

Role name ▼	Trusted entities	Last activity ▼
<input type="checkbox"/> Chhavi-S3-FullAccess	AWS service: ec2	None

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

Ans.

Step 1: Create a new role.

Identity and Access
Management (IAM)

Dashboard

▼ Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

✓ The role AssumeRole-Chhavi has been created.

Create role

Delete role

Q AssumeRole-Chhavi

Showing 1 result

Role name ▼	Trusted entities	Last activity ▼
<input checked="" type="checkbox"/> AssumeRole-Chhavi	AWS service: ec2	None

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

Create policy

12

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](#)

▼ STS (1 action) ⚠ 1 warning [Clone](#) [Remove](#)

▶ Service STS

▶ Actions Write
AssumeRole

▼ Resources ☒ Specific
[close](#) ☐ All resources

role ? Specify **role** resource ARN for the **AssumeRole** action. ☐ Any

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

Step 3: Add previous policy's ARN

Services ▼ Res

▶ S

▶ A

▼ Res

▶ Request con

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/Chhavi-S3-FullAccess

Account * 187632318301 ☐ Any

Role name with path * Chhavi-S3-FullAccess ☐ Any

[Cancel](#) [Add](#)

➕ Add additional permissions

character count: 39 of 6,144. [Cancel](#) [Review policy](#)

Actions Write

AssumeRole

Resources ☒ Specific ☐ All resources

close

role ? EDIT x ☐ Any

Add ARN to restrict access

Request conditions Specify request conditions (optional)

+ Add additional permissions

Character count: 170 of 6,144.

Cancel Review policy

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

Step 4: Attach new policy to new role created.

**and Access
ment (IAM)**

Create policy **Policy actions** ↺ ⚙ ?

Filter policies ▼

	Policy name <small>▼</small>	Type	Used as	Description
<input checked="" type="radio"/>	AssumeRole-Chhavi	Customer managed	None	S3 Assume Role
<input type="radio"/>	DataAdmin-Policy-Chhavi	Customer managed	None	Get,Put,List

ard
management
providers
settings
reports

Attach policy

Attach the policy to users, groups, or roles in your account

Filter: [Filter](#) Showing 1 result

<input checked="" type="checkbox"/>	Name	Type
<input checked="" type="checkbox"/>	AssumeRole-Chhavi	Role

[Cancel](#)

[Attach policy](#)

[Feedback](#) [English \(US\)](#)

© 2008 - 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

Step 5: Check New role's summary

Identity and Access Management (IAM)

Dashboard

Access management

- Groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
 - Archive rules
 - Analyzer details
- Credential report
- Organization activity

Summary

Delete role

Role ARN

arn:aws:iam::187632318301:role/AssumeRole-Chhavi

Role description

Allows EC2 instances to call AWS services on your behalf. | [Edit](#)

Instance Profile ARNs

arn:aws:iam::187632318301:instance-profile/AssumeRole-Chhavi

Path

/

Creation time

2020-02-27 17:22 UTC+0530

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

Permissions policies (1 policy applied)

Attach policies

[Add inline policy](#)

Policy name	Policy type
AssumeRole-Chhavi	Managed policy

[Feedback](#) [English \(US\)](#)

© 2008 - 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

You can see the assumed role attached

Copy the ARN of assume role .

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with 'Identity and Access Management (IAM)' selected. The main content area is titled 'Roles > AssumeRole-Chhavi' and 'Summary'. It displays role details: Role ARN, Role description, Instance Profile ARNs, Path, Creation time, Last activity, and Maximum CLI/API session duration. Below this is a tabbed interface with 'Permissions' selected, showing 'Permissions policies (1 policy applied)' and buttons for 'Attach policies' and 'Add inline policy'.

Identity and Access Management (IAM)

Dashboard

Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzer details

Credential report

Organization activity

Roles > AssumeRole-Chhavi

Summary

Delete role

Role ARN: [arn:aws:iam::187632318301:role/AssumeRole-Chhavi](#)

Role description: Allows EC2 instances to call AWS services on your behalf. | [Edit](#)

Instance Profile ARNs: [arn:aws:iam::187632318301:instance-profile/AssumeRole-Chhavi](#)

Path: /

Creation time: 2020-02-27 17:22 UTC+0530

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

Permissions policies (1 policy applied)

[Attach policies](#) [Add inline policy](#)

Policy name	Policy type
-------------	-------------

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

Goto Trust Relationship Tab in the previous policy.

The screenshot shows the AWS IAM console interface for the 'Chhavi-S3-FullAccess' role. The 'Trust relationships' tab is selected, displaying instructions on viewing trusted entities and access conditions. It includes a button to 'Edit trust relationship' and sections for 'Trusted entities' and 'Conditions'.

Roles > Chhavi-S3-FullAccess

Summary

Delete role

Role ARN: [arn:aws:iam::187632318301:role/Chhavi-S3-FullAccess](#)

Role description: Allows EC2 instances to call AWS services on your behalf. | [Edit](#)

Instance Profile ARNs: [arn:aws:iam::187632318301:instance-profile/Chhavi-S3-FullAccess](#)

Path: /

Creation time: 2020-02-26 21:05 UTC+0530

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.

Conditions

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

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

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

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": "arn:aws:iam::187632318301:role/AssumeRole-Chhavi",
8       },
9       "Service": "ec2.amazonaws.com"
10    },
11  ],
12  "Action": "sts:AssumeRole"
13 }

```

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.

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

[Privacy Policy](#)

[Terms of Use](#)

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

Step 3: Configure Instance Details

Network *i* vpc-05380bb7018d7282f | vpcdemo *↕* Create new VPC

Subnet *i* subnet-00b26cdd8f633e3a9 | dev | us-east-1a *↕* Create new subnet
250 IP Addresses available

Auto-assign Public IP *i* Enable *↕*

Placement group *i* ☐ Add instance to placement group

Capacity Reservation *i* Open *↕* Create new Capacity Reservation

IAM role *i* AssumeRole-Chhavi *↕* Create new IAM role

Shutdown behavior *i* Stop *↕*

Enable termination protection *i* ☐ Protect against accidental termination

Monitoring *i* ☐ Enable CloudWatch detailed monitoring

Cancel Previous Review and Launch Next: Add Storage

EC2 Experience
what you think

Dashboard New

Launch Instance Connect Actions

search : chhavi-assume Add filter

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
Chhavi-Assu...	i-0b9aa24eb579434...	t2.micro	us-east-1a	running	Initializing	None

ICES

es

Types

Templates New

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": "ASIASXL6B650QRLQTPDF",
    "SecretAccessKey": "MPUnLCRcx9Na7qIJhxKXbNx2CcNSEKHjKfF7voZn",
    "SessionToken": "IQoJb3JpZ2luX2VjEA0aCXVzLWVhc3QtMSJGMEQCIH7HRcMyIj4KgIBoCrD7bT02wdn75KosptNtoJytorq4AiBnYjhEGtHAQCBXY9NK+bEXu28KeT0D0SAU2ZjRwKdHdSreAQjV//////////8BEAIaDDE4NzYzMjMxODMwMSIMdPgJUWwVz5y7W4jpKrIBPnWSPruSRlWQp/Vyp3/yeF74Qgff+yMY7ZhqC9r9K9/Grydrx1bM5gYwYt4PbZ9vRT7+LcsPwVR3e3+l964AaHBfL7qcq0UxZpwhR9qf/hdFjd4FrccCMFQ9R50Jcb0yNWIB1VGQ4/8iqR8icGUTUUhPPrL6BjrhCEmq5SdN7bzzZb6q1uodWbPLi/1wh3j0RVTun90VElUVXpMyYqH0U8rW+SoqFKtf8lUW6n1o29okgTC9iuTyBTrkASv8SDlp0T8vjRrVAEdwh7iWU+oCBTI05UrDrL7UUbPSibwghNeK6kxh1W1Qdxn8piuULGC9IJFbJ04xHcmANlqSufaXQ+kpG3mGZbM2UEm5jW0mXKV0r/fxFWQxxLRh2ChWKBsPT8kQ+1mPIK8BvxEKgEpM1Sxs1ap270zeVxEDAs90QzKgB98A2+Cc02fNl8r0TvjgCj0v+4NYelqmYZJZnoB2QnzecE/Gc0Ez0u6eLnxBQ5uqdAbzIEvwtrs87Spk4ZzE00+Hz8Q/0JUXJdZ2wxr3ilQRYFwWtd8yJ7TY91niw==",
    "Expiration": "2020-02-28T13:19:09+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AR0ASXL6B6507H67PBCRZ:chhaviststoken",
    "Arn": "arn:aws:sts::187632318301:assumed-role/Chhavi-S3-FullAccess/chhaviststoken"
  }
}
```

Export access key id , secret access key and token.

```
ubuntu@ip-10-0-2-243:~$ export AWS_ACCESS_KEY_ID=ASIASXL6B650QRLQTPDF
ubuntu@ip-10-0-2-243:~$ export AWS_SECRET_ACCESS_KEY=MPUnLCRcx9Na7qIJhxKXbNx2CcNSEKHjKfF7voZn
```

```
ubuntu@ip-10-0-2-243:~$ export AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEA0aCXVzLWVhc3QtMSJGMEQCIH7HRcMyIj4KgIBoCrD7bT02wdn75KosptNtoJytorq4AiBnYjhEGtHAQCBXY9NK+bEXu28KeT0D0SAU2ZjRwKdHdSreAQjV//////////8BEAIaDDE4NzYzMjMxODMwMSIMdPgJUWwVz5y7W4jpKrIBPnWSPruSRlWQp/Vyp3/yeF74Qgff+yMY7ZhqC9r9K9/Grydrx1bM5gYwYt4PbZ9vRT7+LcsPwVR3e3+l964AaHBfL7qcq0UxZpwhR9qf/hdFjd4FrccCMFQ9R50Jcb0yNWIB1VGQ4/8iqR8icGUTUUhPPrL6BjrhCEmq5SdN7bzzZb6q1uodWbPLi/1wh3j0RVTun90VElUVXpMyYqH0U8rW+SoqFKtf8lUW6n1o29okgTC9iuTyBTrkASv8SDlp0T8vjRrVAEdwh7iWU+oCBTI05UrDrL7UUbPSibwghNeK6kxh1W1Qdxn8piuULGC9IJFbJ04xHcmANlqSufaXQ+kpG3mGZbM2UEm5jW0mXKV0r/fxFWQxxLRh2ChWKBsPT8kQ+1mPIK8BvxEKgEpM1Sxs1ap270zeVxEDAs90QzKgB98A2+Cc02fNl8r0TvjgCj0v+4NYelqmYZJZnoB2QnzecE/Gc0Ez0u6eLnxBQ5uqdAbzIEvwtrs87Spk4ZzE00+Hz8Q/0JUXJdZ2wxr3ilQRYFwWtd8yJ7TY91niw==
```

Aws configure.

```
ubuntu@ip-10-0-2-243:~$ aws configure
AWS Access Key ID [None]: ASIASXL6B650QRLQTPDF
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 avcab
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

aws

Services

Resource Groups

chhavi.sharma@tothenew.com @ t... Global Support

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

Set Group Name

Specify a group name. Group names can be edited any time.

Group Name:

DataAdmin-Chhavi

Example: Developers or ProjectAlpha

Maximum 128 characters

Create New Group

Group Actions

Showing 1 results

<input type="checkbox"/>	Group Name	Users	Inline Policy	Creation Time
<input type="checkbox"/>	DataAdmin-Chhavi	0		2020-02-27 16:15 UTC+0530

Step2: Create a user : Alice

Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+ 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.

Console password*

* Required

[Cancel](#) [Next: Permissions](#)

Step 3: Add user to Group

Add user to group

[Create group](#) [Refresh](#)

Showing 1 result

Group	Attached policies
<input checked="" type="checkbox"/> DataAdmin-Chhavi	None

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

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](#)

[Visual editor](#) [JSON](#) [Import managed policy](#)

[Expand all](#) [Collapse all](#)

S3 (75 actions) [Clone](#) [Remove](#)

Service S3

Actions List

HeadBucket

ListAllMyBuckets

ListBucket

Read

DescribeJob

GetAccelerateConfiguration

GetBucketPolicy

GetBucketPolicyStatus

GetBucketPublicAccessBlock

GetBucketReplication

GetObjectTagging

GetObjectTorrent

GetPublicAccessBlock

Create policy

12

Review policy

Name*DataAdmin-Policy-Chhavi

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

DescriptionGet,Put,List

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

Summary

Filter

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

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

✔ DataAdmin-Policy-Chhavi has been created.

Create policy

Policy actions

Filter policies

DataAdmin-Policy

	Policy name	Type	Used as	Description
<input checked="" type="radio"/>	DataAdmin-Policy-Chhavi	Customer managed	None	Get,Put,List

s)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

Step 5: Attach policy to group.

Attach policy

Attach the policy to users, groups, or roles in your account

Filter: Filter ▼		Showing 1 result
DataAdmin-Chhavi		
✓ Name ▼	Type ▼	
✓ DataAdmin-Chhavi	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

aws

Services

Resource Groups

chhavi.sharma@tothenew.com @ t...GlobalSupport

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

Set Group Name

Specify a group name. Group names can be edited any time.

Group Name:

DeveloperGroup-Chhavi

Example: Developers or ProjectAlpha

Maximum 128 characters

chhaviShowing 2 results

<input type="checkbox"/>	Group Name	Users	Inline Policy	Creation Time
<input type="checkbox"/>	DataAdmin-Chhavi	1		2020-02-27 16:15 UTC+0530
<input checked="" type="checkbox"/>	DeveloperGroup-Chhavi	0		2020-02-28 15:13 UTC+0530

Step 2: Now add a User.

Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+ 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

[Cancel](#) [Next: Permissions](#)

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

Add user to group

[Create group](#) [Refresh](#)

Showing 1 result

Group	Attached policies
<input checked="" type="checkbox"/> DeveloperGroup-Chhavi	None

[Cancel](#) [Previous](#) [Next: Tags](#)

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

AutoScaling a....pdf Show all

Identity and Access Management (IAM)

[Add user](#) [Delete user](#)

User name	Groups	Access key age	Password age	Last activity
<input type="checkbox"/> Alice-Chhavi	DataAdmin-Chhavi	None	Today	None
<input checked="" type="checkbox"/> Chhavi_DG	DeveloperGroup-Chhavi	None	Today	None
<input type="checkbox"/> chhavi.shar...	BootCamp2019	7 days	8 days	Today

Dashboard

- Access management
 - Groups
 - Users**
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules

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

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

▼ **EC2** (119 actions) ⚠ 6 warnings [Clone](#) [Remove](#)

► **Service** EC2

▼ **Actions** Specify the actions allowed in EC2 ? [Switch to deny permissions](#) ⓘ

close

Q Filter actions

Manual actions (add actions)

☐ All EC2 actions (ec2:*)

☒ ec2:*Volume (Edit | Remove)

☒ ec2:*Instances (Edit | Remove)

☒ ec2:*CreateTags (Edit | Remove)

☒ ec2:Describe* (Edit | Remove)

Access level [Expand all](#) [Collapse all](#)

► ☐ List (94 selected)

► ☐ Read (7 selected)

► ☐ Tagging (1 selected)

► ☐ Write (17 selected)

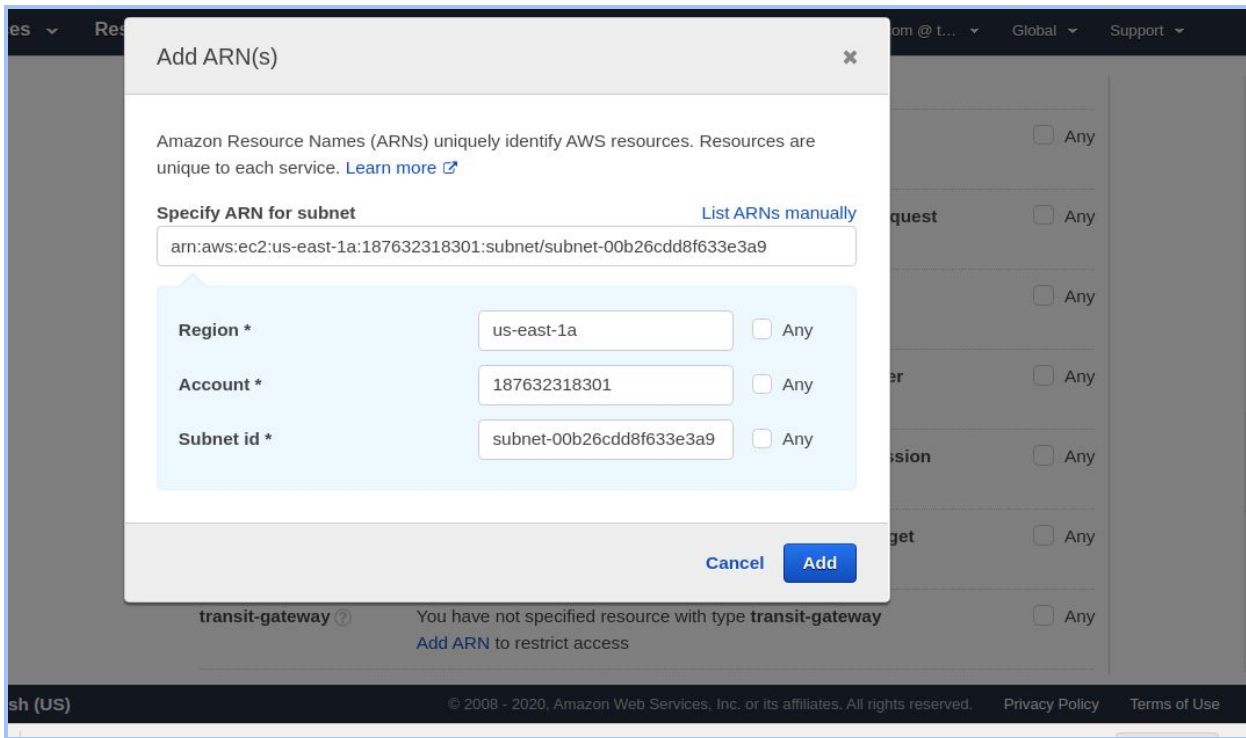
► ☐ Permissions management

► **Resources** Specify **image** resource ARN for the **RunInstances** action.
Specify **instance** resource ARN for the **AttachVolume** and 6 more actions.

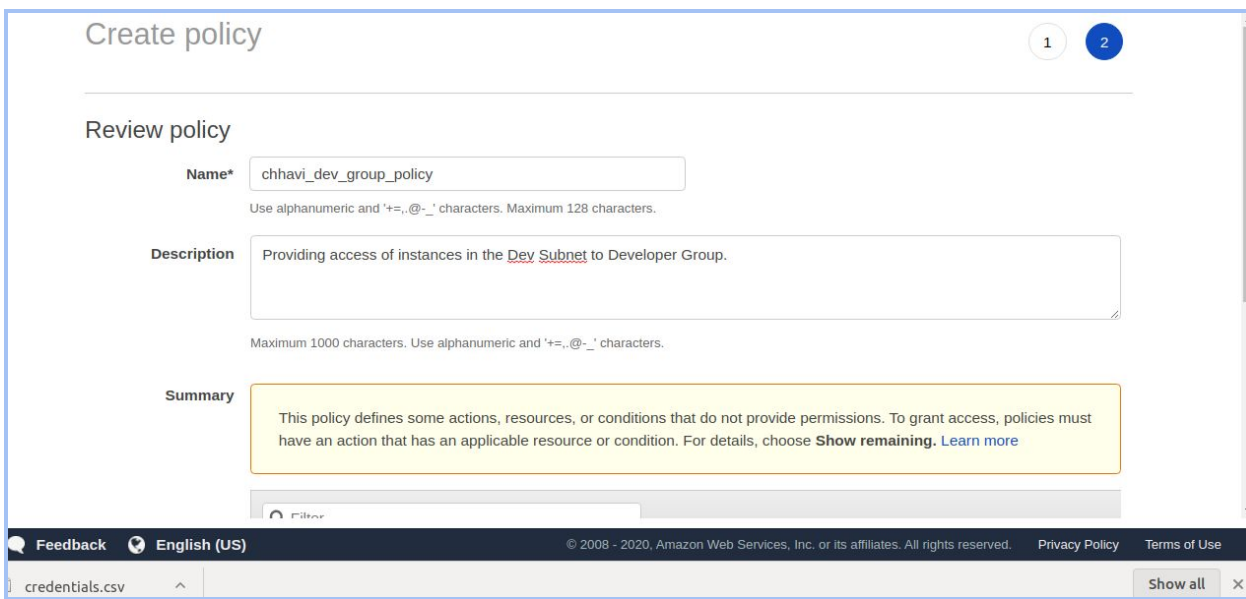
ack English (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

ials.csv ^ [Show all](#) ×

Add the ARN of the Subnet(dev subnet)



Review Policy



Step 5: Attach Policy to group (Developer Group)

✓ **chhavi_dev_group_policy** has been created.

Create policy Policy actions

Filter policies

Attach
Detach
Delete

	Policy	Type	Used as	Description
<input type="radio"/>	AssumeRole-Chhavi	Customer managed	Permissions policy (1)	S3 Assume Role
<input checked="" type="radio"/>	chhavi_dev_group_policy	Customer managed	None	Providing access of inst
<input type="radio"/>	DataAdmin-Policy-Chhavi	Customer managed	None	Get,Put,List

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

Show all X

Attach policy

Attach the policy to users, groups, or roles in your account

Filter: Filter Q developergroup Showing 3 results

<input type="checkbox"/>	Name	Type
<input checked="" type="checkbox"/>	DeveloperGroup-Chhavi	Group
<input type="checkbox"/>	DeveloperGroup_diksha	Group
<input type="checkbox"/>	DeveloperGroup_gargi	Group

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

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with 'Identity and Access Management (IAM)' selected. Under 'Access management', 'Groups' is highlighted. The main content area shows the 'Summary' tab for a group. The group details are: Group ARN: arn:aws:iam::187632318301:group/DeveloperGroup- Chhavi, Users (in this group): 1, Path: /, and Creation Time: 2020-02-28 15:13 UTC+0530. Below this, there are tabs for 'Users', 'Permissions', and 'Access Advisor'. The 'Users' tab is active, showing a message: 'This view shows all users in this group: 1 User'. There are buttons for 'Remove Users from Group' and 'Add Users to Group'. A table lists the users in the group:

User	Actions
Chhavi_DG	Remove User from Group

The screenshot shows the same AWS IAM console interface, but with the 'Permissions' tab selected. The group details remain the same. The 'Managed Policies' section is expanded, showing a message: 'The following managed policies are attached to this group. You can attach up to 10 managed policies.' There is an 'Attach Policy' button. A table lists the attached policies:

Policy Name	Actions
chhavi_dev_group_policy	Show Policy Detach Policy Simulate Policy

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": "AIDASXL6B650Q4RMZ427Z",
      "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": "AIDASXL6B650YD7UUCZUJ",
      "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": "AIDASXL6B650SGPOGZHFO",
      "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"
"Graina"
"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

The screenshot shows the AWS Management Console interface. At the top, there are buttons for 'Launch Instance', 'Connect', and 'Actions'. Below these is a search bar with the text 'search : chhavi-s3' and an 'Add filter' button. A table lists the EC2 instances. The first instance is 'Chhavi-S3Access' with ID 'i-01654bb3da5c83911', type 't2.micro', and state 'running'. Below the table, the instance details are shown: 'Instance: i-01654bb3da5c83911 (Chhavi-S3Access)' and 'Public DNS: ec2-3-88-43-25.compute-1.amazonaws.com'.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
Chhavi-S3Access	i-01654bb3da5c83911	t2.micro	us-east-1c	running	Initializing	None

Instance: i-01654bb3da5c83911 (Chhavi-S3Access) Public DNS: ec2-3-88-43-25.compute-1.amazonaws.com

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 ▾		Q s3full	Showing 1 result
	Policy name ▾	Used as	
<input checked="" type="checkbox"/>	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

Identity and Access Management (IAM)

Dashboard

Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzer details

Credential report

Organization activity

Feedback English (US)

The role EC2-S3-FullAccess-Role has been created.

Create role Delete role

ec2-s3 Showing 3 results

	Role name	Trusted entities	Last activity
<input type="checkbox"/>	ec2-s3-ayush	AWS service: ec2	None
<input checked="" type="checkbox"/>	EC2-S3-FullAccess-Role	AWS service: ec2	None
<input type="checkbox"/>	ec2-s3-trust	Account: 187632318301	Today

© 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

New EC2 Experience

Launch Instance Connect Actions

search : chhavi-s3 Add filter

Name Instance ID

Chhavi-S3Ac... i-01654bb3da5c83911

Instance State running

2/2 checks ... None

Instance Settings

Instance State

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-01654bb3da5c83911 (Chhavi-S3Access) Public DNS: ...

Description Status Checks Monitoring Tags

Instance ID i-01654bb3da5c83911

Instance state running

Instance type t2.micro

Finding You may not have permission

IPv4 Public IP 3.88.43.25

IPv6 IPs -

Elastic IPs

Instances > Attach/Replace IAM Role

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-01654bb3da5c83911 (Chhavi-S3Access) ⓘ

IAM role* ⓘ [Create new IAM role](#) ⓘ

* Required

[Cancel](#) [Apply](#)

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

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/YF5TTbLrVGvaoMRzUW3HRXQLeGN0o0.
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.

```

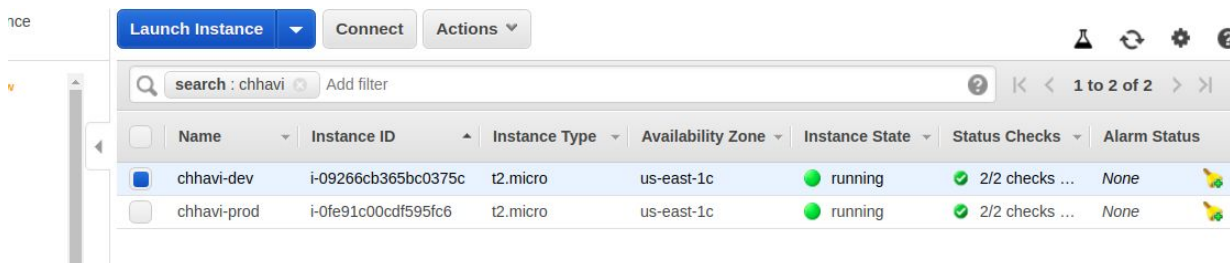
ubuntu@ip-172-31-51-9:~$ aws s3 ls
2019-06-26 12:11:08 0testuser11
2018-04-20 16:59:22 187632318301-awsmacietrail-dataevent
2019-04-02 10:11:33 7testdemo
2019-03-11 04:51:59 abhinanyucftemplate
2020-02-28 10:55:02 abhishek-bootcamp
2019-03-04 06:55:23 abneesh1
2019-03-11 11:00:41 adityamun007
2020-02-26 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 avcab
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-codestartest2-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



	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
<input checked="" type="checkbox"/>	chhavi-dev	i-09266cb365bc0375c	t2.micro	us-east-1c	running	2/2 checks ...	None
<input type="checkbox"/>	chhavi-prod	i-0fe91c00cdf595fc6	t2.micro	us-east-1c	running	2/2 checks ...	None

Create two users

Production - chhaviproduct

Development - chhaviddev

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](#)

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": [
8         "ec2:StartInstances",
9         "ec2:StopInstances"
10      ],
11      "Resource": "arn:aws:ec2:*:*:instance/*",
12      "Condition": {
13        "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

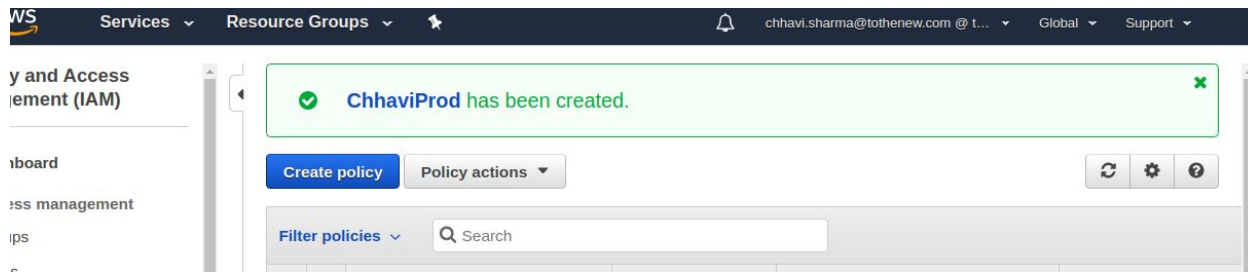
chhavi-assin nem

Show all x

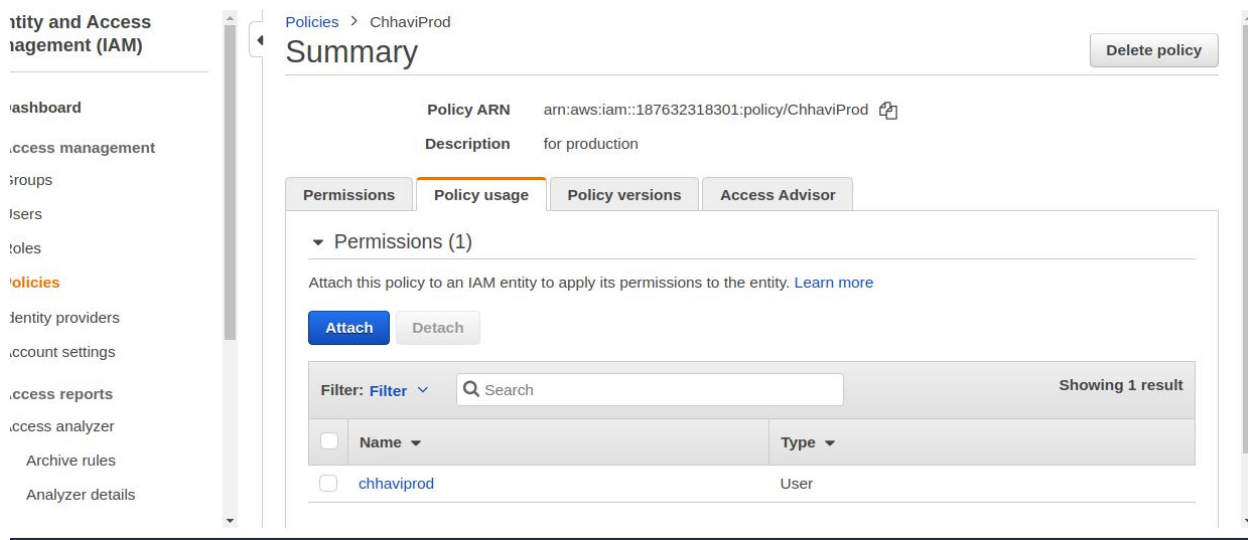
A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor JSON Import managed policy

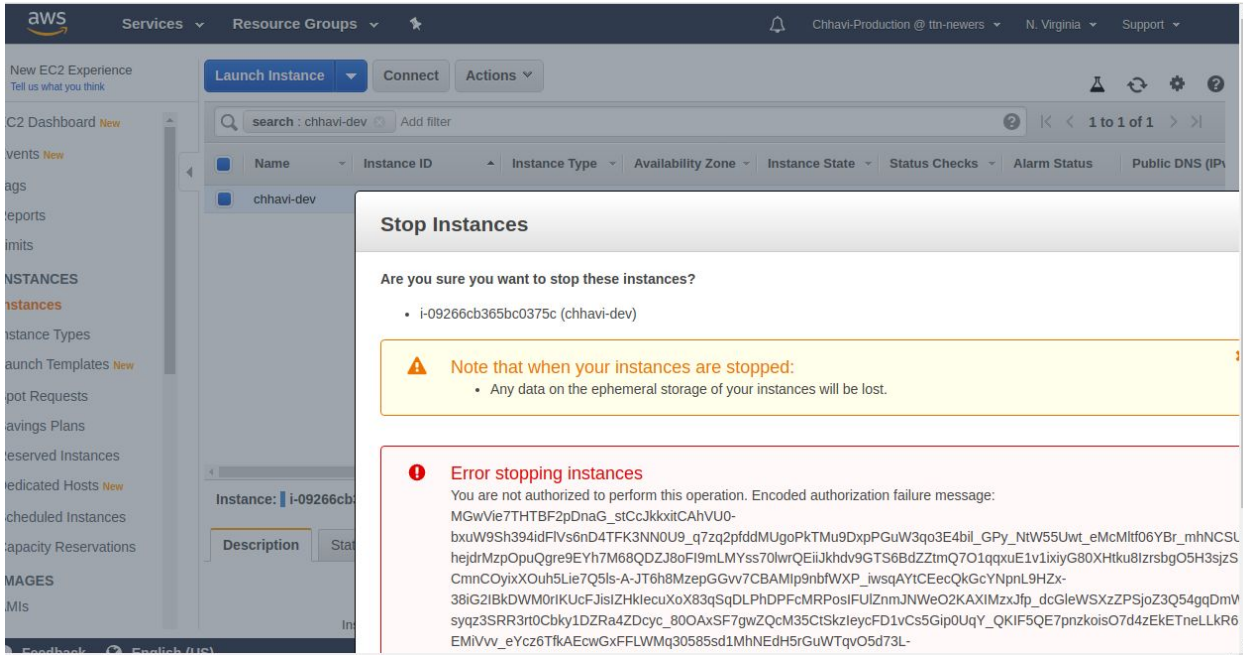
```
11 {
12   "Resource": "arn:aws:ec2:*:*:instance/*",
13   "Condition": {
14     "StringEquals": {
15       "ec2:ResourceTag/Name": "chhavi-prod"
16     }
17   },
18 },
19 {
20   "Sid": "VisualEditor1",
21   "Effect": "Allow",
22   "Action": "ec2:DescribeInstances",
23   "Resource": "*"
24 }
```



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.

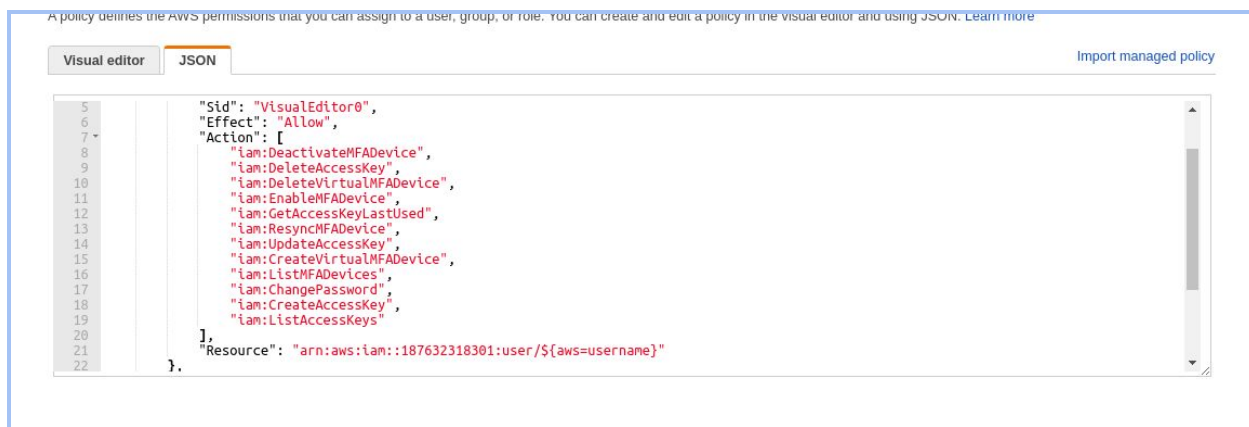


Incase of Development, just change the resource Resource tags.

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 }
```