

IAM:

Q1. Create a Role with full access to S3

Creating a role under the IAM service

Create role

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](#)

* Required

Cancel **Next: Permissions**

Allowing S3 full access:

Filter policies Showing 15 results

	Policy name	Used as
<input type="checkbox"/>	alice-s3-maithely	Permissions policy (2)
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	None
<input checked="" type="checkbox"/>	AmazonS3FullAccess	Permissions policy (32)
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	Permissions policy (1)
<input type="checkbox"/>	AWSLambdaS3ExecutionRole-1a3ddce4-a989-4828-88a4-7f5e701af3ef	Permissions policy (1)
<input type="checkbox"/>	AWSLambdaS3ExecutionRole-34f3178e-e3ee-4238-8c64-0e27432978a2	Permissions policy (1)
<input type="checkbox"/>	AWSLambdaS3ExecutionRole-9954a81d-a49b-408c-aa07-78234306319f	Permissions policy (1)
<input type="checkbox"/>	AWSLambdaS3ExecutionRole-c8b9c2ec-9d50-4969-8163-87e2da653db6	Permissions policy (1)

Set permissions boundary

* Required

Cancel Previous **Next: Tags**

aws

Services ▾ Resource Groups ▾ ☆

vedant.sharma@tothenew.com @ t... Global ▾ Support ▾

Create role

1 2 3 4

Review

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

Role name*

Vedant-S3-access

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

Role description


Allows S3 to call AWS services on your behalf.

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

Trusted entities

AWS service: s3.amazonaws.com

Policies

 AmazonS3FullAccess [↗](#)

Permissions boundary

Permissions boundary is not set

* Required

Cancel

Previous

Create role

aws

Services ▾ Resource Groups ▾ ☆

vedant.sharma@tothenew.com @ t... Global ▾ Support ▾

Dashboard

Access management

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

Access reports

- Access analyzer
 - Archive rules
 - Analyzer details
- Credential report
- Organization activity
- Service control policies (SCPs)

Roles > Vedant-S3-access

Summary

Delete role

Role ARN

arn:aws:iam::187632318301:role/Vedant-S3-access [↗](#)

Role description

Allows S3 to call AWS services on your behalf. [| Edit](#)

Instance Profile ARNs

[↗](#)

Path

/

Creation time

2020-02-28 11:22 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

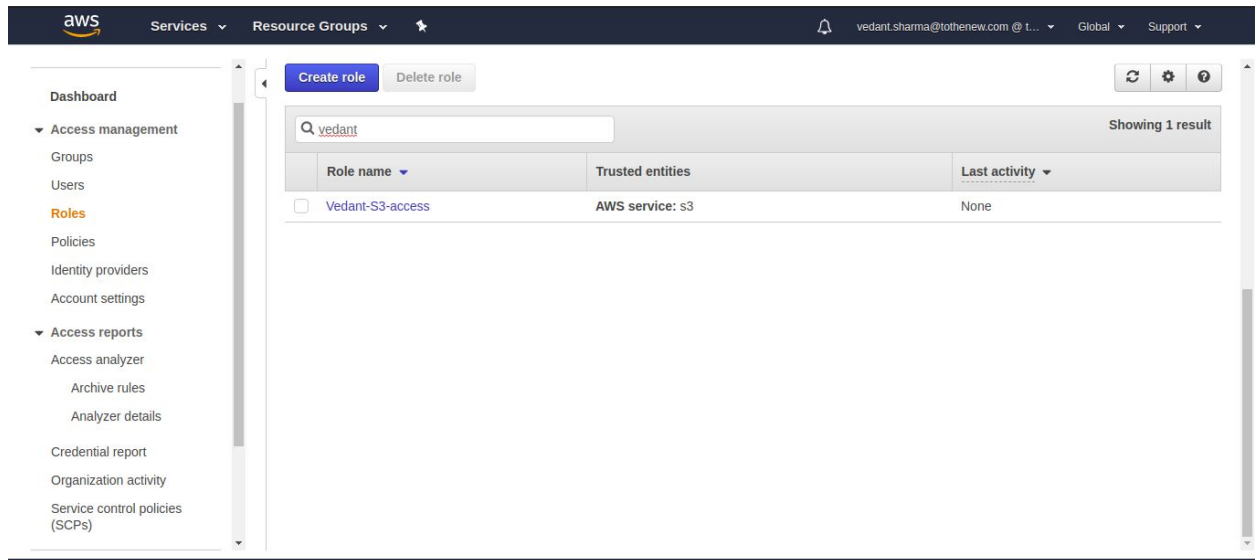
Revoke sessions

Permissions policies (1 policy applied)

Attach policies

Add inline policy

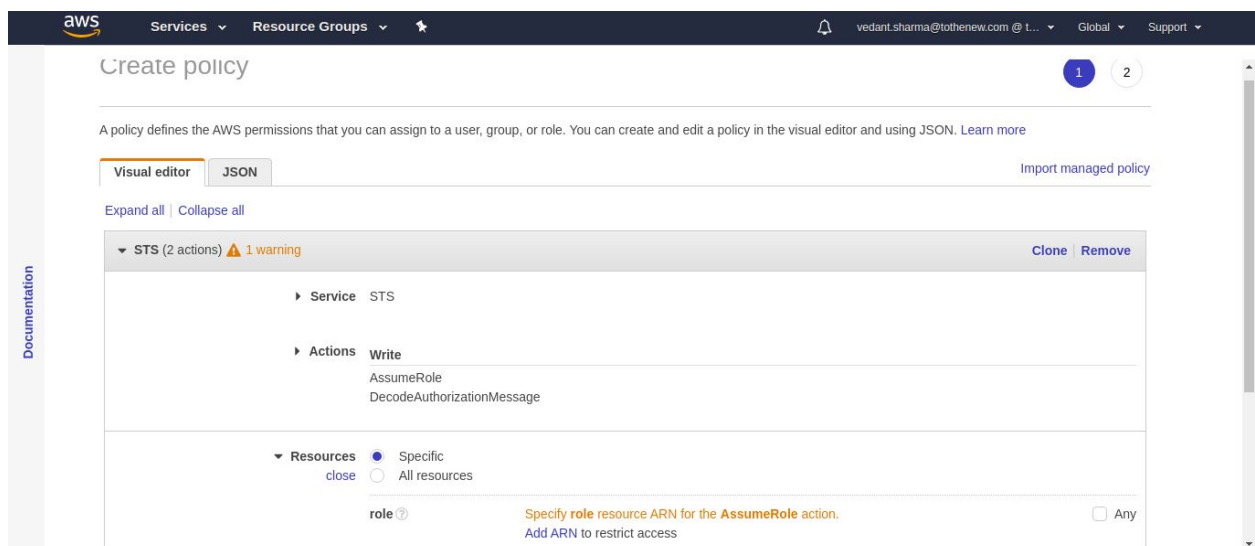
Policy name ▾	Policy type ▾	
▶  AmazonS3FullAccess	AWS managed policy	✕



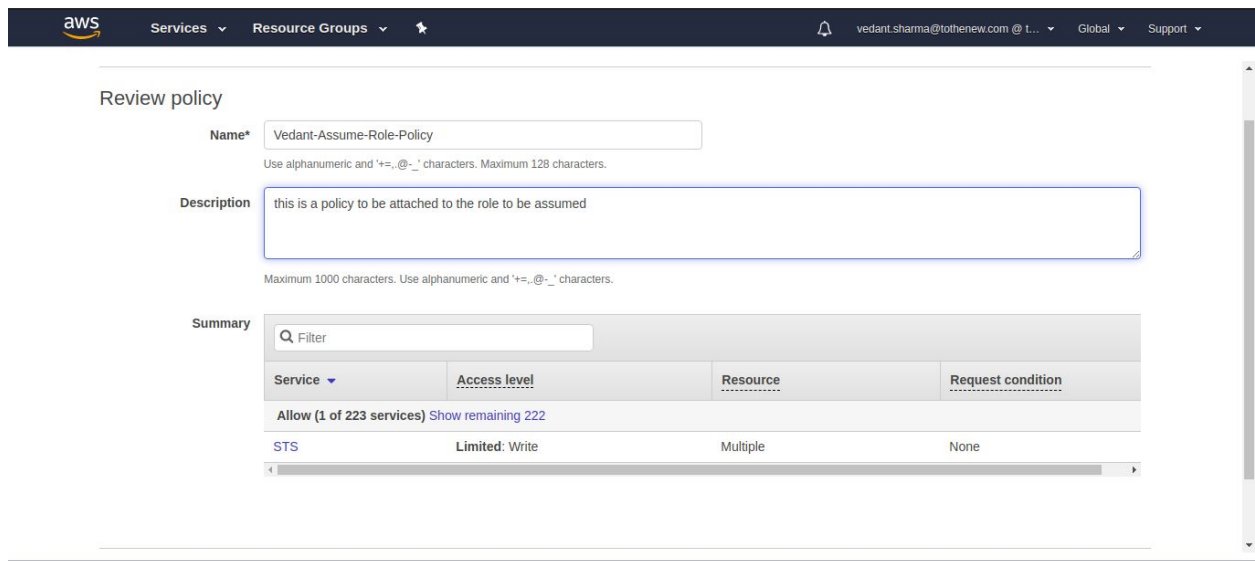
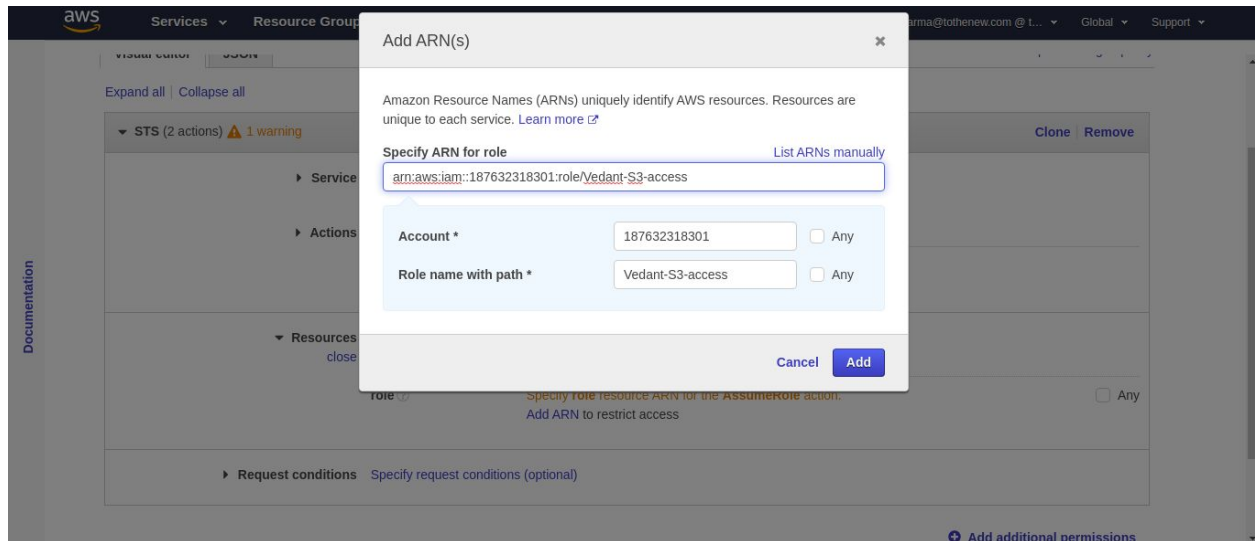
Q2. Create another which has the policy to assume the previous Role

After creating a new role we create a new policy and then we select a assume role action

Selection of STS service:



Adding ARN of the previously created account



Attaching policy to newly created role

aws

Services

Resource Groups

vedant.sharma@tothenew.com @ t...GlobalSupport

Dashboard

Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzer details

Credential report

Organization activity

Service control policies (SCPs)

Summary

Delete role

Role ARN

arn:aws:iam::187632318301:role/assume-role-vedant

Role description

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

Instance Profile ARNs

arn:aws:iam::187632318301:instance-profile/assume-role-vedant

Path

/

Creation time

2020-02-28 12:24 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

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

aws

Services

Resource Groups

vedant.sharma@tothenew.com @ t...GlobalSupport

Add permissions to assume-role-vedant

Attach Permissions

Create policy

Filter policies

Q vedant

Showing 1 result

	Policy name	Type	Used as
<input checked="" type="checkbox"/>	Vedant-Assume-Role-Policy	Customer managed	None

Cancel

Attach policy

Assume policy attached

Role ARN `arn:aws:iam::187632318301:role/assume-role-vedant`

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

Instance Profile ARNs `arn:aws:iam::187632318301:instance-profile/assume-role-vedant`

Path /

Creation time 2020-02-28 12:24 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
Vedant-Assume-Role-Policy	Managed policy

► Permissions boundary (not set)

Adding ARN of assumed role to the trusted relationship of the policy for full access:

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/assume-role-vedant"
8       },
9       "Service": "ec2.amazonaws.com"
10    },
11    "Action": "sts:AssumeRole"
12  ]
13 }
  
```

[Cancel](#) [Update Trust Policy](#)

Q3. Attach this to an instance and get an sts token.

Attaching an IAM role to the instance:

aws

Services

Resource Groups

vedant.sharma@tothenew.com @ t...N. VirginiaSupport

New EC2 Experience
Tell us what you think

Launch InstanceConnectActions

EC2 Dashboard
Events
Tags
Reports
Limits

INSTANCES

Instances

Instance Types

Launch Templates
Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts
Scheduled Instances

Capacity Reservations

IMAGES

search : vedantAdd filter

Name	Instance ID	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
vedant-insta...	i-000dae29bc70	us-east-1b	running	2/2 checks ...	None	
Vedant-Test-...	i-03934b9b638f8a40a			checks ...	None	
Vedant-Test-...	i-0cdaa6f6276a3			checks ...	None	

Instance: i-03934b9b638f8a40a (Vedant-Test-ALB)Public IP: 100.25.117.111

Description

Status Checks

Monitoring

Tags

Instance ID

i-03934b9b638f8a40a

Instance state

running

Instance type

t2.micro

Public DNS (IPv4)

-

IPv4 Public IP

100.25.117.111

IPv6 IPs

-

Connect

Get Windows Password

Create Template From Instance

Launch More Like This

Instance State

Instance Settings

Image

Networking

CloudWatch Monitoring

Add/Edit Tags

Attach to Auto Scaling Group

Attach/Replace IAM Role

Change Instance Type

Change Termination Protection

View/Change User Data

Change Shutdown Behavior

Change T2/T3 Unlimited

Get System Log

Get Instance Screenshot

Modify Instance Placement

Modify Capacity Reservation Settings

aws Services Resource Groups

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-03934b9b638f8a40a (Vedant-Test-ALB)

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

* Required

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

Accessing aws s3 bucket using instance and aws cli:

```
ubuntu@ip-10-0-3-131:~$  
ubuntu@ip-10-0-3-131:~$ aws s3 ls | grep vedant  
2020-02-27 19:13:36 vedant-static  
ubuntu@ip-10-0-3-131:~$
```

Getting STS details after going to the IAM service console and then selecting account settings:

aws Services Resource Groups

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

Allow users to change their own password

[Change password policy](#) [Delete password policy](#)

Security Token Service (STS)

Session Tokens from the STS endpoints

AWS recommends using regional STS endpoints to reduce latency. Session tokens from regional STS endpoints are valid in all AWS Regions. If you use regional STS endpoints, no action is required.

Session tokens from the global STS endpoint (<https://sts.amazonaws.com>) are valid only in AWS Regions that are enabled by default. If you intend to enable a new Region for your account, you can use session tokens from regional STS endpoints or activate the global STS endpoint to issue session tokens that are valid in all AWS Regions. [Learn more](#)

Endpoints	Region compatibility of session tokens	Actions
Global endpoint	Valid only in AWS Regions enabled by default	Edit
Regional endpoints	Valid in all AWS Regions	

Endpoints

You can enable additional endpoints from which you can request temporary credentials. Activate only endpoints you intend to use. [Learn more](#)

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

No permission to perform STS token fetching:

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

Session tokens from the global STS endpoint (<https://sts.amazonaws.com>) are valid only in AWS Regions that are enabled by default. If you intend to enable a new Region for your account, you can use session tokens from regional STS endpoints or activate the global STS endpoint to issue session tokens that are valid in all AWS Regions. [Learn more](#)

Endpoints	Region compatibility of session tokens	Actions
Global endpoint	Valid only in AWS Regions enabled by default	Edit
Regional endpoints	Valid in all AWS Regions	

Endpoints

You can enable additional endpoints from which you can request temporary credentials. Activate only endpoints you intend to use. [Learn more](#)

You need permissions

You do not have the permission required to perform this operation. Ask your administrator to add permissions. [Learn more](#)

User: `arn:aws:iam::187632318301:user/vedant.sharma@tothenew.com` is not authorized to perform: `iam:*` on resource: `*`

Region name	Endpoint	STS status	Actions
-------------	----------	------------	---------

Q4. 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)

Services
Resource Groups

vedant.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:

Example: Developers or ProjectAlpha
Maximum 128 characters

Cancel
Next Step

Creating a Policy for mentioned actions:

The screenshot shows the 'Create policy' page in the AWS IAM console, specifically the 'Visual editor' tab. The page title is 'Create policy' with step indicators '1' and '2'. A description states: '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](#)'. There are tabs for 'Visual editor' (selected) and 'JSON', and a link for 'Import managed policy'. Below the tabs are links for 'Expand all' and 'Collapse all'. The main content area shows a policy for the 'S3' service, with a search bar 'Filter actions' and a list of actions. The 'Access level' section shows 'List (3 selected)', 'Read (41 selected)', and 'Tagging' (unchecked). There are 'Clone' and 'Remove' buttons at the top right of the policy list.

Documentation

aws Services Resource Groups

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) 3 warnings Clone Remove

Service S3

Actions Specify the actions allowed in S3 Switch to deny permissions

Filter actions

Manual actions (add actions)

All S3 actions (s3:*)

Access level

List (3 selected)

Read (41 selected)

Tagging

Expand all Collapse all

The screenshot shows the 'Create policy' page in the AWS IAM console, specifically the 'JSON' tab. The page title is 'Create policy' with step indicators '1' and '2'. The 'Visual editor' tab is selected. The main content area shows a policy for the 'S3' service, with a search bar 'Filter actions' and a list of actions. The 'Access level' section shows 'List (3 selected)', 'Read (41 selected)', 'Tagging' (unchecked), 'Write (31 selected)', and 'Permissions management' (unchecked). There are 'Expand all' and 'Collapse all' buttons at the top right of the policy list. The 'Resources' section shows a list of resource ARNs: 'Specify accesspoint resource ARN for the GetAccessPointPolicy and 3 more actions.', 'Specify job resource ARN for the DescribeJob and 2 more actions.', and 'Specify object resource ARN for the PutObjectRetention and 20 more actions.'. The 'Request conditions' section shows 'Specify request conditions (optional)'. There is an 'Add additional permissions' button at the bottom right.

Documentation

aws Services Resource Groups

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) 3 warnings Clone Remove

Service S3

Actions Specify the actions allowed in S3 Switch to deny permissions

Filter actions

Manual actions (add actions)

All S3 actions (s3:*)

Access level

List (3 selected)

Read (41 selected)

Tagging

Write (31 selected)

Permissions management

Expand all Collapse all

Resources Specify accesspoint resource ARN for the GetAccessPointPolicy and 3 more actions. Specify job resource ARN for the DescribeJob and 2 more actions. Specify object resource ARN for the PutObjectRetention and 20 more actions. arn:aws:s3::*

Request conditions Specify request conditions (optional)

Add additional permissions

Selecting ARN as a resource

PutAnalyticsConfiguration PutMetricsConfiguration

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

accesspoint ?	Specify accesspoint resource ARN for the GetAccessPointPolicy and 3 more actions. ⓘ Add ARN to restrict access	<input type="checkbox"/> Any
bucket ?	Any resource of type = bucket	<input checked="" type="checkbox"/> Any
job ?	Specify job resource ARN for the DescribeJob and 2 more actions. ⓘ Add ARN to restrict access	<input type="checkbox"/> Any
object ?	Specify object resource ARN for the PutObjectRetention and 20 more actions. ⓘ Add ARN to restrict access	<input type="checkbox"/> Any

► Request conditions [Specify request conditions \(optional\)](#)

[Add additional permissions](#)

Character count: 2,059 of 6,144.

[Cancel](#) [Review policy](#)

Review policy

Name*
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

[Cancel](#) [Review](#) [Create policy](#)

Now creating a group and attaching the previously created policy to the group

aws

Services

Resource Groups

vedant.sharma@tothenew.com @ t...GlobalSupport

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

Attach Policy

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

Filter: Policy Typevedant

Showing 2 results

	Policy Name	Attached Entities	Creation Time
<input type="checkbox"/>	Vedant-Assume-Role-Policy	1	2020-02-28 12:33 UTC+...
<input checked="" type="checkbox"/>	Alice-vedant-Policy	0	2020-02-28 13:17 UTC+...

Cancel

Previous

Next Step

Adding alice as a user to the group created previously:

aws

Services

Resource Groups

vedant.sharma@tothenew.com @ t...GlobalSupport

Add user

12345

Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

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

Add user to group

Create groupRefresh

Q vedant

Showing 1 result

Group	Attached policies
<input checked="" type="checkbox"/> Vedant-Data-administration	Alice-vedant-Policy

Cancel

Previous

Next: Tags

aws Services Resource Groups

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

Add user

1 2 3 4 5

Success

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

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

Download .csv

User	Password	Email login instructions
Vedant-alice	***** Show	Send email

Close

aws Services Resource Groups

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

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

IAM > Groups > Vedant-Data-administration

Summary

Group ARN: arn:aws:iam::187632318301:group/Vedant-Data-administration

Users (in this group): 1

Path: /

Creation Time: 2020-02-28 13:23 UTC+0530

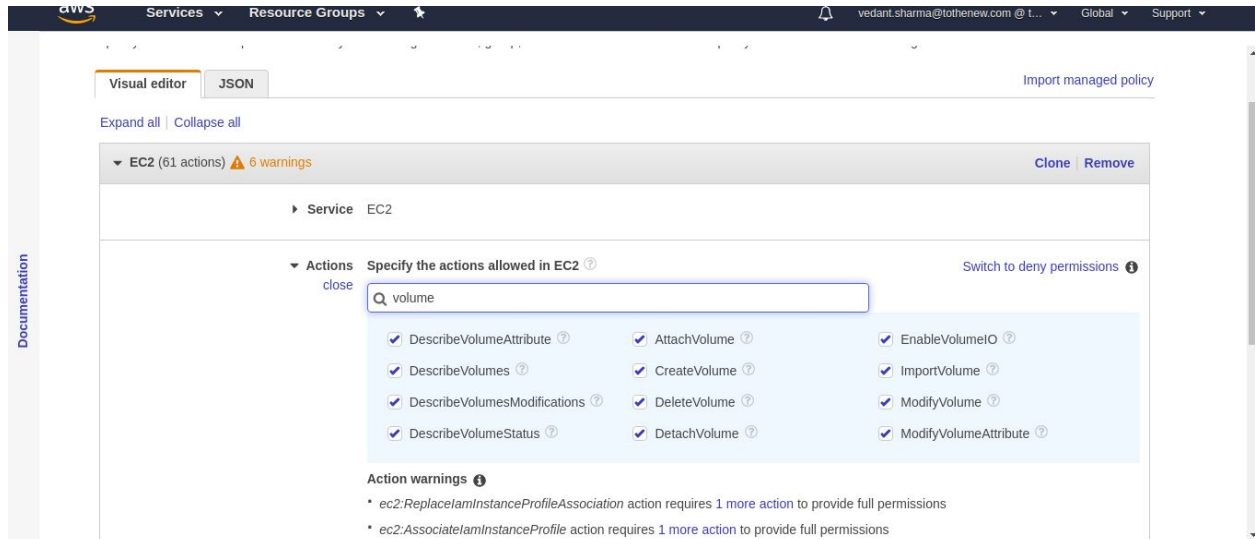
Users Permissions Access Advisor

This view shows all users in this group: 1 User

Remove Users from Group Add Users to Group

User	Actions
Vedant-alice	Remove User from Group

Q5. 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



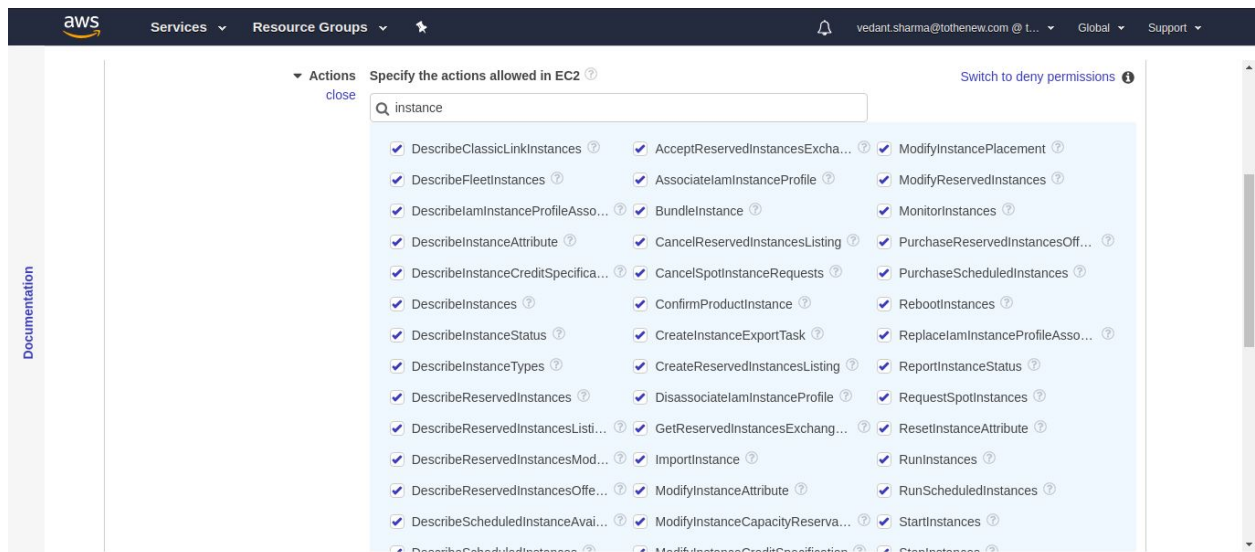
instances. Provide the following access to this group:

Service: Amazon EC2

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

Condition: Dev Subnets only

Creating a new policy with instance actions



Volume*

EC2 (142 actions) 6 warnings

Clone Remove

Service EC2

Actions

close

Specify the actions allowed in EC2 ?

Switch to deny permissions ?

☒ DescribeVolumeAttribute ?

☒ DescribeVolumes ?

☒ DescribeVolumesModifications ?

☒ DescribeVolumeStatus ?

☒ AttachVolume ?

☒ CreateVolume ?

☒ DeleteVolume ?

☒ DetachVolume ?

☒ EnableVolumeIO ?

☒ ImportVolume ?

☒ ModifyVolume ?

☒ ModifyVolumeAttribute ?

Action warnings ?

* ec2:ReplaceIamInstanceProfileAssociation action requires 1 more action to provide full permissions

* ec2:AssociateIamInstanceProfile action requires 1 more action to provide full permissions

Describe*

aws

Services Resource Groups

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

Expand all Collapse all

EC2 (142 actions) 6 warnings

Clone Remove

Service EC2

Actions

close

Specify the actions allowed in EC2 ?

Switch to deny permissions ?

☒ DescribeAccountAttributes ?

☒ DescribeAddresses ?

☒ DescribeAggregateIdFormat ?

☒ DescribeAvailabilityZones ?

☒ DescribeBundleTasks ?

☒ DescribeByoipCidrs ?

☒ DescribeCapacityReservations ?

☒ DescribeClassicLinkInstances ?

☒ DescribeClientVpnAuthorization... ?

☒ DescribeImportSnapshotTasks ?

☒ DescribeInstanceAttribute ?

☒ DescribeInstanceCreditSpecifica... ?

☒ DescribeInstances ?

☒ DescribeInstanceStatus ?

☒ DescribeInstanceTypes ?

☒ DescribeInternetGateways ?

☒ DescribeKeyPairs ?

☒ DescribeLaunchTemplates ?

☒ DescribeElasticGpus ?

☒ DescribeFastSnapshotRestores ?

☒ DescribeScheduledInstanceAvai... ?

☒ DescribeScheduledInstances ?

☒ DescribeSpotInstanceRequests ?

☒ DescribeSpotPriceHistory ?

☒ DescribeStaleSecurityGroups ?

☒ DescribeSubnets ?

☒ DescribeTags ?

Tags (read and write)

The screenshot shows the AWS IAM console interface for configuring permissions for the EC2 service. The left sidebar contains a 'Documentation' link. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and a star icon. The user's email 'vedant.sharma@tothenew.com' and 'Global' region are displayed. The main content area is titled 'Service EC2'. Under the 'Actions' section, there is a search bar labeled 'Filter actions'. Below it, the 'Manual actions (add actions)' section shows a checkbox for 'All EC2 actions (ec2:*)' which is unchecked. The 'Access level' section is expanded, showing three categories: 'List (94 selected)' (unchecked), 'Read (8 selected)' (unchecked), and 'Tagging (2 selected)' (checked). The 'Tagging' category is further expanded, showing 'CreateTags' and 'DeleteTags' both checked. There are also checkboxes for 'Write (39 selected)' and 'Permissions management', both of which are unchecked. A 'Switch to deny permissions' link is visible in the top right of the actions section. At the bottom, there is an 'Action warnings' section.

Specifying resources:

The screenshot shows the AWS IAM console interface for specifying resources for permissions. The left sidebar contains a 'Documentation' link. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and a star icon. The user's email 'vedant.sharma@tothenew.com' and 'Global' region are displayed. The main content area is titled 'Resources'. Under the 'Resources' section, there are two radio buttons: 'Specific' (selected) and 'All resources' (unchecked). Below this, there is a list of resource types with their corresponding permissions. The list includes: 'capacity-reservati...' (You have not specified resource with type capacity-reservation, Add ARN to restrict access, Any), 'client-vpn-endpoint' (You have not specified resource with type client-vpn-endpoint, Add ARN to restrict access, Any), 'dhcp-options' (You have not specified resource with type dhcp-options, Add ARN to restrict access, Any), 'fpga-image' (You have not specified resource with type fpga-image, Add ARN to restrict access, Any), 'image' (Specify image resource ARN for the RunInstances action, Add ARN to restrict access, Any), 'instance' (Any resource of type = instance, Any, checked), 'internet-gateway' (You have not specified resource with type internet-gateway, Add ARN to restrict access, Any), and 'key-pair' (Any resource of type = key-pair, Any, checked).

aws

Services

Resource Groups

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

Review policy

Name*

bob-vedant-ec2-access

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

Description

specific access to bob for EC2

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

Summary

Filter

Service	Access level	Resource	Request condition
Allow (1 of 223 services) Show remaining 222			
EC2	Full: Tagging Limited: List, Read, Write	Multiple	None

Creating a developer group and attached a previous policy to the group:

aws

Services

Resource Groups

vedant.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:

Vedant-Developer-group

Example: Developers or ProjectAlpha

Maximum 128 characters

Cancel

Next Step

aws

Services

Resource Groups

vedant.sharma@tothenew.com @ t...GlobalSupport

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

Attach Policy

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

Filter: Policy Typevedant

Showing 3 results

	Policy Name	Attached Entities	Creation Time
<input type="checkbox"/>	Alice-vedant-Policy	1	2020-02-28 13:17 UTC+...
<input type="checkbox"/>	Vedant-Assume-Role-Policy	1	2020-02-28 12:33 UTC+...
<input checked="" type="checkbox"/>	bob-vedant-ec2-access	0	2020-02-28 15:35 UTC+...

CancelPreviousNext Step

Adding bob to the created group:

aws

Services

Resource Groups

vedant.sharma@tothenew.com @ t...GlobalSupport

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

Connection settings

IAM > Groups > Vedant-Developer-group

Summary

Group ARN:arn:aws:iam::187632318301:group/Vedant-Developer-group

Users (in this group):0

Path:/

Creation Time:2020-02-28 15:38 UTC+0530

Users

Permissions

Access Advisor

This group does not contain any users.

Add Users to Group

Creating bob user

aws

Services

Resource Groups

★

vedant.sharma@tothenew.com @ t...

Global

Support

Set user details

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

User name*

Bob-Vedant

[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*

☒ Autogenerated password

☐ Custom password

* Required

Cancel

Next: Permissions

Feedback

English (US)

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

Adding bob to the previous group:

aws

Services

Resource Groups

★

vedant.sharma@tothenew.com @ t...

Global

Support

Add user to group

Create group

Refresh

Q vedant

Showing 2 results

Group	Attached policies
<input type="checkbox"/> Vedant-Data-administration	Alice-vedant-Policy
<input checked="" type="checkbox"/> Vedant-Developer-group	bob-vedant-ec2-access

Cancel

Previous

Next: Tags

aws

ServicesResource Groups

vedant.sharma@tothenew.com @ L...GlobalSupport

12345

Review

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

User details

User name	Bob-Vedant
AWS access type	Programmatic access and AWS Management Console access
Console password type	Autogenerated
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

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

Type	Name
Group	Vedant-Developer-group

[Cancel](#)[Previous](#)[Create user](#)

Added to the group with a specified policy:

aws

ServicesResource Groups

vedant.sharma@tothenew.com @ L...GlobalSupport

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

IAM > Groups > Vedant-Developer-group

Summary

Group ARN:arn:aws:iam::187632318301:group/Vedant-Developer-group

Users (in this group):1

Path:/

Creation Time:2020-02-28 15:38 UTC+0530

UsersPermissionsAccess Advisor

This view shows all users in this group: 1 User

User

Bob-Vedant

Actions

Remove User from Group

Q6. Identify the unused IAM users/credentials using AWS CLI.

To identify the unused IAM user/credentials we use “aws iam list-users” this displays list of users with their details. Each with a `PasswordLastUsed` value. If the value is missing, then the user either has no password or the password has not been used since IAM began tracking password

```
ubuntu@ip-10-0-3-131:~$ aws iam get-user
{
  "User": {
    "UserName": "vedant.sharma@tothenew.com",
    "PasswordLastUsed": "2020-02-28T05:35:35Z",
    "CreateDate": "2020-02-19T11:04:05Z",
    "UserId": "AIDASXL6B650Y2RMI3I40",
    "Path": "/",
    "Arn": "arn:aws:iam::187632318301:user/vedant.sharma@tothenew.com"
  }
}
ubuntu@ip-10-0-3-131:~$ aws iam get-user --user-name Bob-Vedant
{
  "User": {
    "UserName": "Bob-Vedant",
    "Tags": [
      {
        "Value": "vedant-bob-user",
        "Key": "Name"
      }
    ],
    "CreateDate": "2020-02-28T10:14:37Z",
    "UserId": "AIDASXL6B65030WW60WHX",
    "Path": "/",
    "Arn": "arn:aws:iam::187632318301:user/Bob-Vedant"
  }
}
ubuntu@ip-10-0-3-131:~$ aws iam list-users | less
```

```

    "Arn": "arn:aws:iam::187632318301:user/aditya.upadhyay@tothenew.com"
  },
  {
    "UserName": "akshay.shrivastava@tothenew.com",
    "PasswordLastUsed": "2020-02-28T04:20:30Z",
    "CreateDate": "2020-02-19T11:03:26Z",
    "UserId": "AIDASXL6B650SGPOGZHFO",
    "Path": "/",
    "Arn": "arn:aws:iam::187632318301:user/akshay.shrivastava@tothenew.com"
  },
  {
    "UserName": "Alice",
    "Path": "/",
    "CreateDate": "2020-02-27T12:11:40Z",
    "UserId": "AIDASXL6B6506DXIQS5RS",
    "Arn": "arn:aws:iam::187632318301:user/Alice"
  },
  {
    "UserName": "Alice-Chhavi",
    "Path": "/",
    "CreateDate": "2020-02-27T10:46:11Z",
    "UserId": "AIDASXL6B650VCZQE5BOM",
    "Arn": "arn:aws:iam::187632318301:user/Alice-Chhavi"
  },
  {
    "UserName": "alice-maithely",
    "Path": "/",
    "CreateDate": "2020-02-27T10:45:57Z",
    "UserId": "AIDASXL6B65042J5DDSPA",
    "Arn": "arn:aws:iam::187632318301:user/alice-maithely"
  }
]

```

The details missing PasswordLastUsed are the unused user/credentials

```
vedant@vedant:~$ aws iam list-users | jq '.Users[ ] | select(.PasswordLastUsed==null) | .UserName'
"Alice"
"Alice-baban"
"Alice-Chhavi"
"alice-maithely"
"alice-sampurna"
"Alice1"
"alice_aman"
"asusumeuser"
"Bob"
"Bob-Chirag"
"Bob-maithely"
"Bob-Srima"
"Bob-Vedant"
"bob1"
"bobpooja"
"bob_developer_baban"
"bob_sampurna"
"chhavidev"
"chhaviprod"
"Chhavi_DG"
"Chirag-Alice"
"CloudCheckr"
"Dev-diksha"
"Dev-vaibhav"
"Dev1-Arun"
"Dev1-Gargi"
"developer_baban"
"dev3-sampurna"
```

Q7. Identify all the instances having the tag key-value "backup=true" using AWS CLI.

Accessing the instances mentioned in the ec2 account tagged in a particular manner taking vedant-instance as an example.

We can use `aws ec2 describe-instance` and using the filter utility to get the instance details based on the tags.


```

ubuntu@ip-10-0-3-131:~$ sudo aws ec2 describe-instances --filter Name=tag:
Name,Values=vedant-instance | jq
{
  "Reservations": [
    {
      "Groups": [],
      "Instances": [
        {
          "AmiLaunchIndex": 0,
          "ImageId": "ami-06273419dccc0dc8d",
          "InstanceId": "i-000dae29bc7d0ef85",
          "InstanceType": "t2.micro",
          "KeyName": "Vedant-Bootcamp",
          "LaunchTime": "2020-02-27T11:56:53.000Z",
          "Monitoring": {
            "State": "disabled"
          },
          "Placement": {
            "AvailabilityZone": "us-east-1b",
            "GroupName": "",
            "Tenancy": "default"
          },
          "PrivateDnsName": "ip-10-0-1-65.ec2.internal",
          "PrivateIpAddress": "10.0.1.65",
          "ProductCodes": [],
          "PublicDnsName": "",
          "PublicIpAddress": "3.226.248.169",
          "State": {
            "Code": 16,
            "Name": "running"
          },
          "StateTransitionReason": "",
          "SubnetId": "subnet-01d770a77bb69a1f8",
          "VpcId": "vpc-00470a42fc196d84e",
          "Architecture": "x86_64",
          "BlockDeviceMappings": [
            {
              "DeviceName": "/dev/sda1"
            }
          ]
        }
      ]
    }
  ]
}

```

Q8. 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.

Creating a new role for EC2 instance

aws

Services

Resource Groups


vedant.sharma@tothenew.com @ t...

Gl


Create role

1


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
Your

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

Robo

Cancel

Next: Permissions

Create role

1




▼ Attach permissions policies

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

Create policy

Filter policies ▼

Q s3

	Policy name ▼	Used as
<input type="checkbox"/>	▶ alice-s3-maithely	Permissions policy
<input type="checkbox"/>	▶  AmazonDMSRedshiftS3Role	None
<input checked="" type="checkbox"/>	▶  AmazonS3FullAccess	Permissions policy
<input type="checkbox"/>	▶  AmazonS3ReadOnlyAccess	Permissions policy
<input type="checkbox"/>	▶ AWSLambdaS3ExecutionRole-1a3ddce4-a989-4828-88a4-7f5e701af3ef	Permissions policy
<input type="checkbox"/>	▶ AWSLambdaS3ExecutionRole-34f3178e-e3ee-4238-8c64-0e27432978a2	Permissions policy
<input type="checkbox"/>	▶ AWSLambdaS3ExecutionRole-0054e01d-40b400-4407-70004000010f	Permissions policy

Cancel

Previous

Next

Create role

1

Add tags (optional)

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

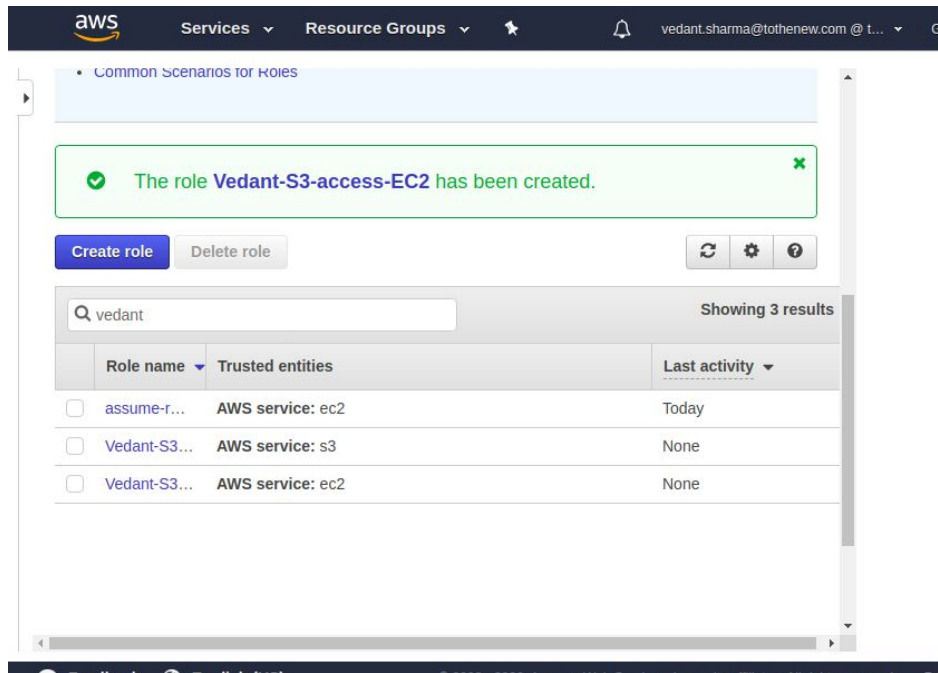
Key	Value (optional)
<input type="text" value="Name"/>	<input type="text" value="S3full-access-EC2-Vedant"/>
<input type="text" value="Add new key"/>	<input type="text"/>

You can add 49 more tags.

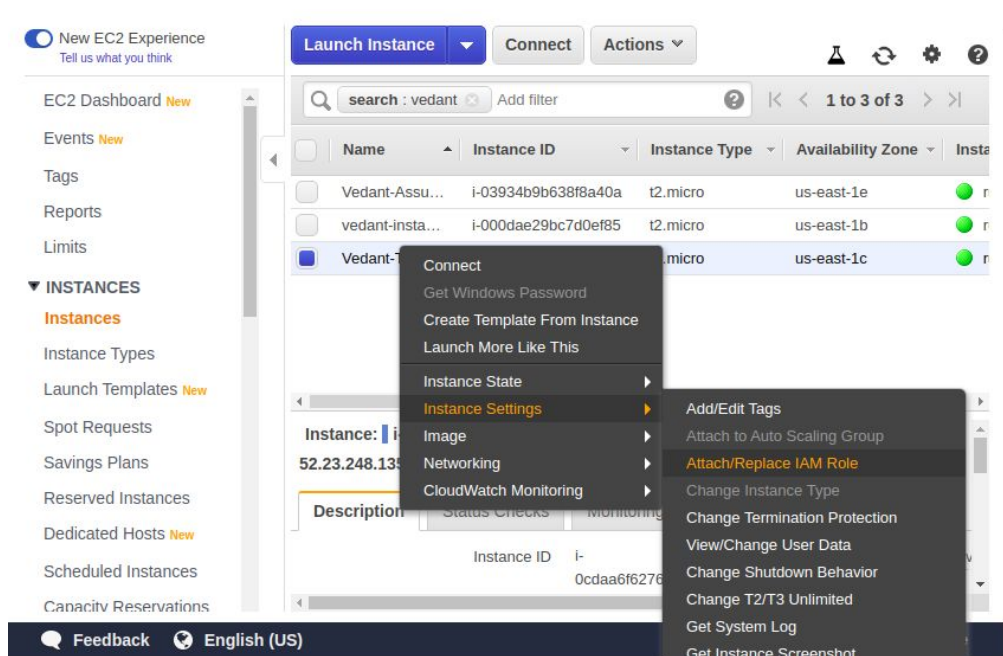
Cancel

Previous

Next



Attaching role to EC2



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-0cdaa6f6276a383ce (Vedant-Test-ALB) ⓘ

IAM role* ⓘ

[Create new IAM role](#) ⓘ

* Required

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

Accessing buckets from the given instance:

```
ubuntu@ip-10-0-2-227:~$ aws s3 ls | grep vedant
2020-02-27 19:13:36 vedant-static
ubuntu@ip-10-0-2-227:~$
```

Q9. 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.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
```

```

    "ec2 *",
  ],
  "Resource": "*",
  "Condition": {"StringEquals":
    {"Condition": {"StringLike": {"iam:ResourceTag/Name": "Vedant-Prod"}}}
  }
}
}
}
}

```

Creating a Policy and adding the policy

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

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "ec2 *"
8       ],
9       "Resource": "*",
10      "Condition": {
11        "StringEquals": {
12          "Condition": {
13            "StringLike": {"iam:ResourceTag/Name": "Vedant-Prod"}
14          }
15        }
16      }
17    }
18  ]
19 }

```

Character count: 186 of 6,144.

Cancel Review policy

Create policy

1 2

Review policy

Name* Vedant-Prod-Policy

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

Description to restrict production instance users to their defined resources

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

Summary

Filter

service	Access level	Resource	Request condition
Allow (1 of 223 services) Show remaining 222			

Creating policy for developers:

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](#)

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "EC2Access",
6       "Effect": "Allow",
7       "Action": [
8         "ec2:*"
9       ],
10      "Resource": "*",
11      "Condition": {
12        "StringEquals": {
13          "ec2:ResourceTag/Name": "Vedant-Dev"
14        }
15      }
16    ]
17  }
18 }
```

aws

Services ▾ Resource Groups ▾ ★

vedant.sharma@tothenew.com @ L... Global ▾ Support ▾

Name*

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			
EC2	Full access	All resources	ec2:ResourceTag/Name = Vedant Dev

* Required

Cancel

Previous

Create policy

Attaching the created policies to the respective groups:

aws

Services

Resource Groups

vedant.sharma@tothenew.com @ t...GlobalSupport

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

Service control policies

IAM > Groups > Vedant-production-Group

Summary

Group ARN:am:aws:iam::187632318301:group/Vedant-production-Group

Users (in this group):1

Path:/

Creation Time:2020-02-28 13:23 UTC+0530

UsersPermissionsAccess Advisor

Managed Policies

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

Attach Policy

Policy Name	Actions
Alice-vedant-Policy	Show Policy Detach Policy Simulate Policy

Inline Policies

aws

Services

Resource Groups

vedant.sharma@tothenew.com @ t...GlobalSupport

Attach Policy

Attach Policy

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

Filter: Policy TypevedantShowing 4 results

	Policy Name	Attached Entities	Creation Time
<input type="checkbox"/>	bob-vedant-ec2-access	1	2020-02-28 15:35 UTC+...
<input type="checkbox"/>	Vedant-Assume-Role-Policy	1	2020-02-28 12:33 UTC+...
<input type="checkbox"/>	Vedant-Dev-Policy	0	2020-03-02 17:06 UTC+...
<input checked="" type="checkbox"/>	Vedant-Prod-Policy	0	2020-03-02 17:00 UTC+...

CancelAttach Policy

Attaching policy to the developer group:

Attach Policy

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

Filter: Policy Type vedant Showing 4 results

	Policy Name	Attached Entities	Creation Time
<input type="checkbox"/>	Alice-vedant-Policy	1	2020-02-28 13:17 UTC+...
<input type="checkbox"/>	Vedant-Assume-Role-Policy	1	2020-02-28 12:33 UTC+...
<input type="checkbox"/>	Vedant-Prod-Policy	1	2020-03-02 17:00 UTC+...
<input checked="" type="checkbox"/>	Vedant-Dev-Policy	0	2020-03-02 17:06 UTC+...

Cancel Attach Policy

Q10. 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.

Creating a policy and associating with user

▼ IAM (9 actions) Clone Remove

► Service IAM

► Actions List

- ListAccessKeys
- ListMFADevices

Read

- GetAccessKeyLastUsed

Write

- ChangePassword
- CreateVirtualMFADevice
- DeleteVirtualMFADevice
- CreateAccessKey
- DeleteAccessKey
- EnableMFADevice

▼ Resources ☐ Specific ☒ All resources close

► Request conditions Specify request conditions (optional)

+ Add additional permissions

