

Task 7: IAM USER

IAM user access

Scenario: Assume Amar is working for 2 government projects, Telangana and Andhra, both of which are in the same account on the Hyd Telangana website and the Mumbai Andhra website. From Telangana govt one admin is there i want to provide OS to EC2 level assume he is amar. If i give ec2full access. By default he can access both Mumbai and hyd region but he doesnt need mumbai region as he is working in telangana govt website. So he need only hyd region level access. We can create the policy in this case

How to add the condition the amar should get only hyd region access. In Json file. Under policies?

Asia Pacific (Hyderabad)	ap-south-2
--------------------------	------------

Asia Pacific (Mumbai)	ap-south-1
-----------------------	------------

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "ap-south-2"
        }
      }
    }
  ]
}
```

Permissions options

☐ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

☒ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1318)

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

[Create policy](#)

Filter by Type				1 match	
<input type="text" value="ec2full"/>		<input type="text" value="All types"/>		1	
<input type="checkbox"/>	Policy name	Type	Attached entities		
<input type="checkbox"/>	AmazonEC2FullAccess	AWS managed	0		

► Set permissions boundary - optional

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

[IAM](#) > [Policies](#) > Create policy

- Step 1 **Specify permissions**
- Step 2 Review and create

Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

VisualJSONActions

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "ec2:*",
7       "Resource": "*",
8       "Condition": {
9         "StringEquals": {
10          "aws:RequestedRegion": "ap-south-2"
11        }
12      }
13    }
14  ]
15 }
```

Edit statement [Remove](#)

Add actions

Choose a service

Included

EC2

Available

AmazonEC2FullAccess

Specify

Add permission

Policy

1 {

2

3

4

5

6

7

8

9

10

11

12

13

14

15 }

Import policy

Policies (1/1316)

Q ec2f

X

5 matches < 1 >

Policy name	Used as	Description
<input checked="" type="radio"/> AmazonEC2FullAccess	None	Provides full access to Amazon EC2 via the AWS Management Console.
<input type="radio"/> AWSEC2FleetServiceRolePolicy	None	Allows EC2 Fleet to launch and manage instances.
<input type="radio"/> EC2FastLaunchFullAccess	None	This policy grants full access to EC2 Fast Launch actions
<input type="radio"/> EC2FastLaunchServiceRolePolicy	None	Policy grants ec2fastlaunch to prepare and manage preprovisioned snapshots in customer's account & publish related metrics.
<input type="radio"/> EC2FleetTimeShiftableServiceRolePolicy	None	Policy granting permissions to EC2 Fleet to launch instances in the future.

Cancel

Import policy

IAM > Policies > Create policy

1 2

- Step 1
- ☒ Specify permissions
- Step 2
- ☐ Review and create

Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

Visual JSON Actions

1 {

2 "Version": "2012-10-17",

3 "Statement": [

4 {

5 "Effect": "Allow",

6 "Action": "ec2:*",

7 "Resource": "*",

8 "Condition": {

9 "StringEquals": {

10 "aws:RequestedRegion": "ap-south-2"

11 }

12 }

13 },

14 {

15 "Action": "ec2:*",

16 "Effect": "Allow",

17 "Resource": "*",

18 }

19 }

Edit statement

Remove

Add actions

Choose a service

Q Filter services

Amplify UI Builder

Apache Kafka APIs for MSK

App Mesh

App Mesh Preview

App Runner

App Studio

App2Container

IAM > Policies > Create policy

1

- Step 1
- ☐ Specify permissions
- Step 2
- ☒ Review and create

Review and create [Info](#)

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

Hyd-EC2-Access1

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

Description - optional

Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+,=, @, _' characters.

Add tags - optional [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#)

[Previous](#)

[Create policy](#)

Click on create policy

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management New

▼ Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Hyd-EC2-Access1 Info

Edit

Delete

Policy details

Type

Customer managed

Creation time

December 28, 2024, 02:12 (UTC-07:00)

Edited time

December 28, 2024, 02:12 (UTC-07:00)

ARN

arn:aws:iam::698822100692:policy/Hyd-EC2-Access1

Permissions

Entities attached

Tags

Policy versions (1)

Last Accessed

Permissions defined in this policy Info

Copy

Edit

Summary

JSON

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

```
1 [{"Version": "2012-10-17",
2   "Statement": [
3     {
4       "Effect": "Allow",
5       "Action": "ec2:*",
6       "Resource": "*",
7       "Condition": {
8         "StringEquals": {
9           "aws:RequestedRegion": "ap-south-2"
10        }
11      }
12    }
13  ]
14 ]
```

aws

Search [Alt+S]

Global

Venkata Balabhadra

IAM

Policies

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management New

▼ Access reports

Access Analyzer

External access

Unused access

Policies (1/1318) Info

Actions

Delete

Create policy

A policy is an object in AWS that defines permissions.

Filter by Type

All types

1 match

Search

north

Policy name

Type

Used as

Description

ec2policy-northeast

Customer managed

None

-

IAM

Policies

ec2policy-northeast

Attach policy

Attach as a permissions policy

To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

IAM Entities (3)

Entities are IAM users, user groups and roles.

Search

Filter by Entity type

All types

Entity name

Entity type

parijatha

IAM Users

SES_user

IAM Users

ses-smtp-user.20150325-120301

IAM Users

Cancel

Attach policy

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management New

Access reports

Access Analyzer

External access

Unicon access

- Step 1
Specify user details
- Step 2
Set permissions
- Step 3
Review and create
- Step 4
Retrieve password

Summary

ARN
[arn:aws:iam::698822100692:user/parijatha](#)

Created
December 28, 2024, 02:18 (UTC-07:00)

Console access
Enabled without MFA

Last console sign-in
Today

Access key 1
[Create access key](#)

[Permissions](#) [Groups](#) [Tags](#) [Security credentials](#) [Last Accessed](#)


Permissions policies (2)






Permissions are defined by policies attached to the user directly or through groups.

Filter by Type

Q Search

All types

< 1 > 

<input type="checkbox"/>	Policy name 	Type	Attached via 
<input type="checkbox"/>	 ec2policy-northeast	Customer managed	Directly
<input type="checkbox"/>	  IAMUserChangePassword	AWS managed	Directly

Review and create

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

User details

User name
parijatha

Console password type
Autogenerated

Require password reset
Yes

Permissions summary

Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

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

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

[Email sign-in instructions](#)

Console sign-in URL

[https://698822100692.signin.aws.amazon.com/console](#)

User name

[parijatha](#)

Console password

[Show](#)



You must change your password to continue

AWS account 698822100692

IAM user name parijatha

Old password

New password

Retype new password

Confirm password change

The screenshot shows the AWS Management Console interface. On the left is a navigation sidebar with links to Dashboard, EC2 Global View, Events, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, and Elastic Block Store. The main content area displays the 'Resources' section for the Asia Pacific (Mumbai) Region, showing various EC2 resources like Instances (running), Auto Scaling Groups, Capacity Reservations, Dedicated Hosts, Elastic IPs, Instances, Key pairs, Load balancers, Placement groups, Security groups, Snapshots, and Volumes. Below this is a 'Launch instance' section with a 'Launch instance' button and a 'Migrate a server' button. To the right, a 'Service health' section shows an error message: 'An error occurred. An error occurred retrieving service health information'. A region dropdown menu is open on the right side of the console, showing a list of regions grouped by continent: United States (N. Virginia, Ohio, N. California, Oregon), Asia Pacific (Mumbai, Osaka, Seoul, Singapore, Sydney, Tokyo), Canada (Central), and Europe (Frankfurt, Ireland, London). The dropdown menu also shows the current region as 'Mumbai' and the user as 'parijatha @ 6988-2210-0692'.

Steps to Implement:

1. Go to the **IAM Console** in AWS.
2. Navigate to **Policies** and click on **Create Policy**.
3. Select the **JSON** tab and paste the above policy JSON.
4. Review and save the policy with an appropriate name, e.g., **Hyd-EC2-Access**.
5. Attach this policy to Amar's IAM user or role.