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 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

ec2full | All types | 1 match | 1

Policy name	Type	Attached entities
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

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 }
```

Edit statement | Remove

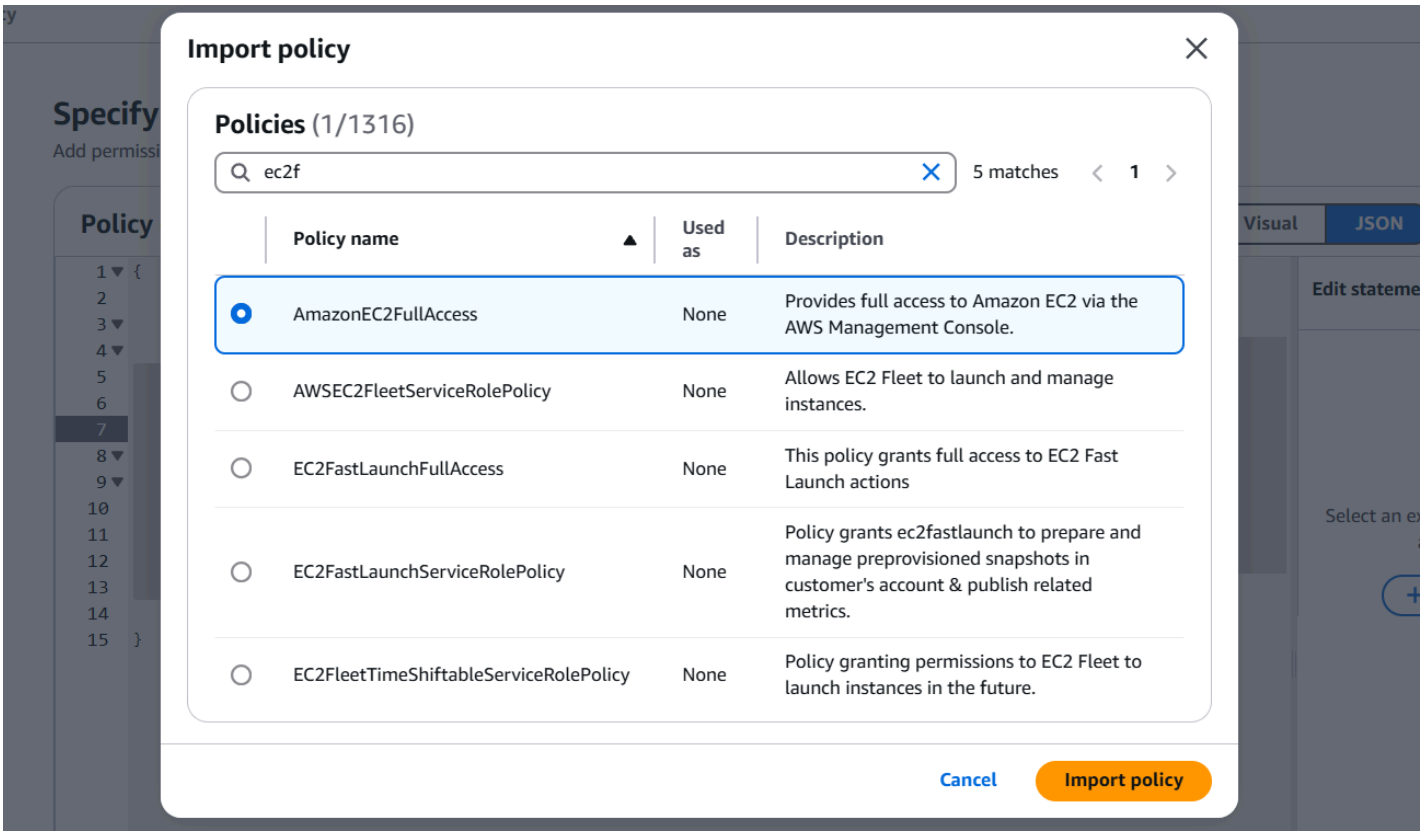
Add actions

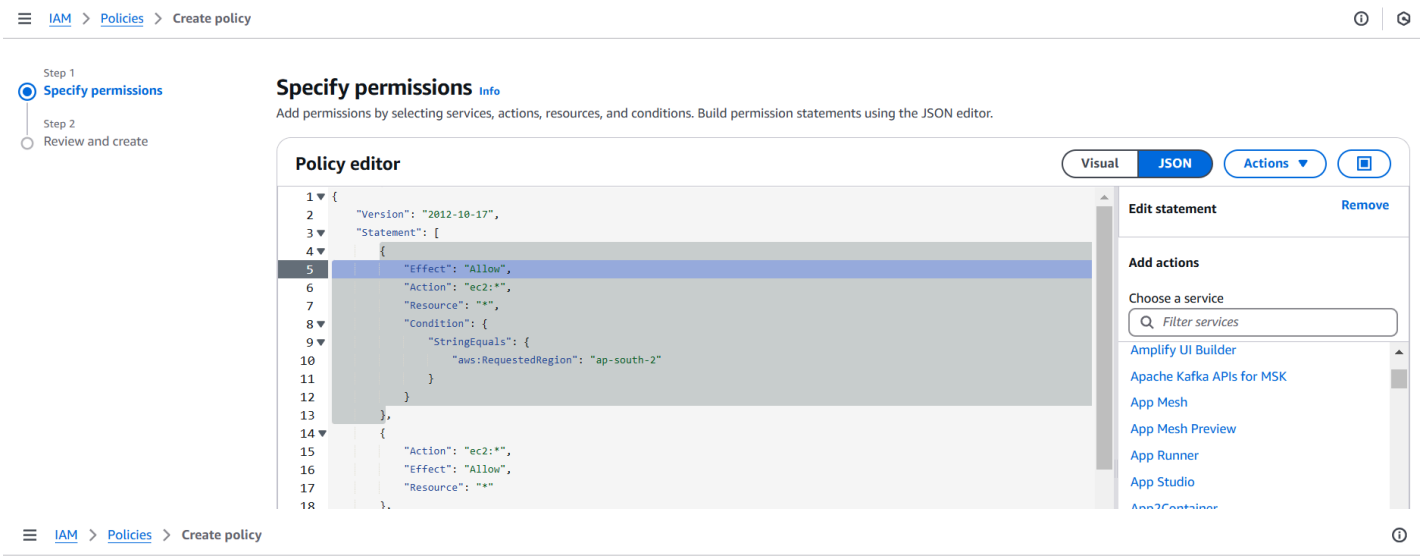
Choose a service

Filter services

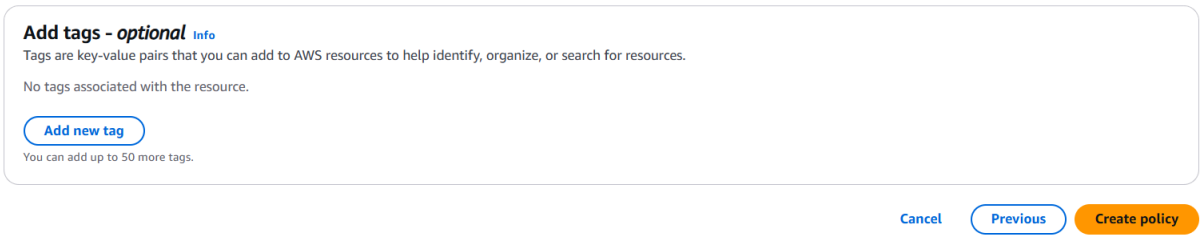
Included
EC2

Available

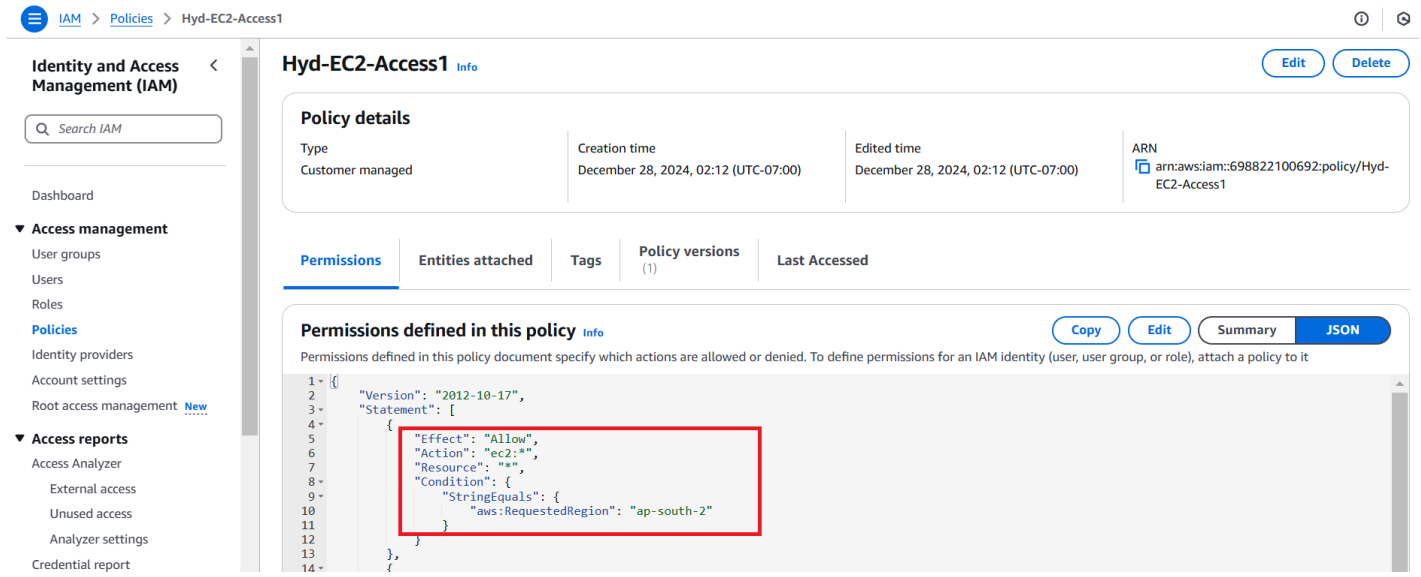

Import policy
Policies (1/1316)
ec2f
5 matches
1
Policy name
Used as
Description
AmazonEC2FullAccess
None
Provides full access to Amazon EC2 via the AWS Management Console.
AWSEC2FleetServiceRolePolicy
None
Allows EC2 Fleet to launch and manage instances.
EC2FastLaunchFullAccess
None
This policy grants full access to EC2 Fast Launch actions
EC2FastLaunchServiceRolePolicy
None
Policy grants ec2fastlaunch to prepare and manage preprovisioned snapshots in customer's account & publish related metrics.
EC2FleetTimeShiftableServiceRolePolicy
None
Policy granting permissions to EC2 Fleet to launch instances in the future.
Cancel
Import policy

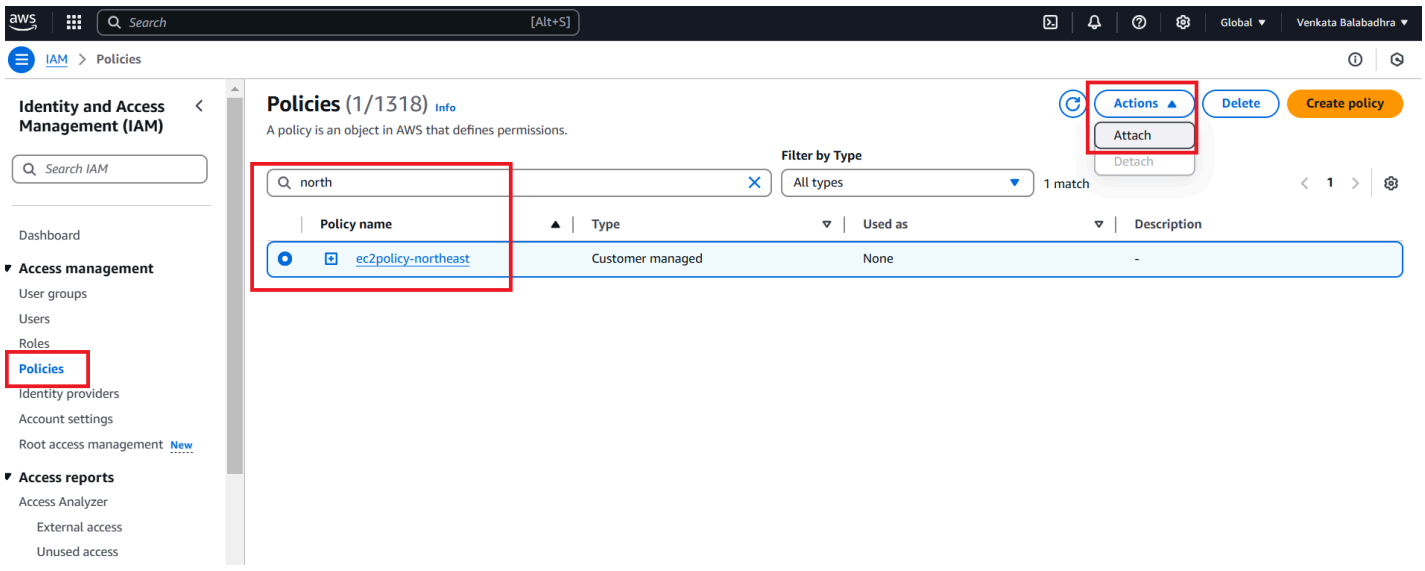

IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
Edit statement
Remove
Add actions
Choose a service
Filter services
Amplify UI Builder
Apache Kafka APIs for MSK
App Mesh
App Mesh Preview
App Runner
App Studio

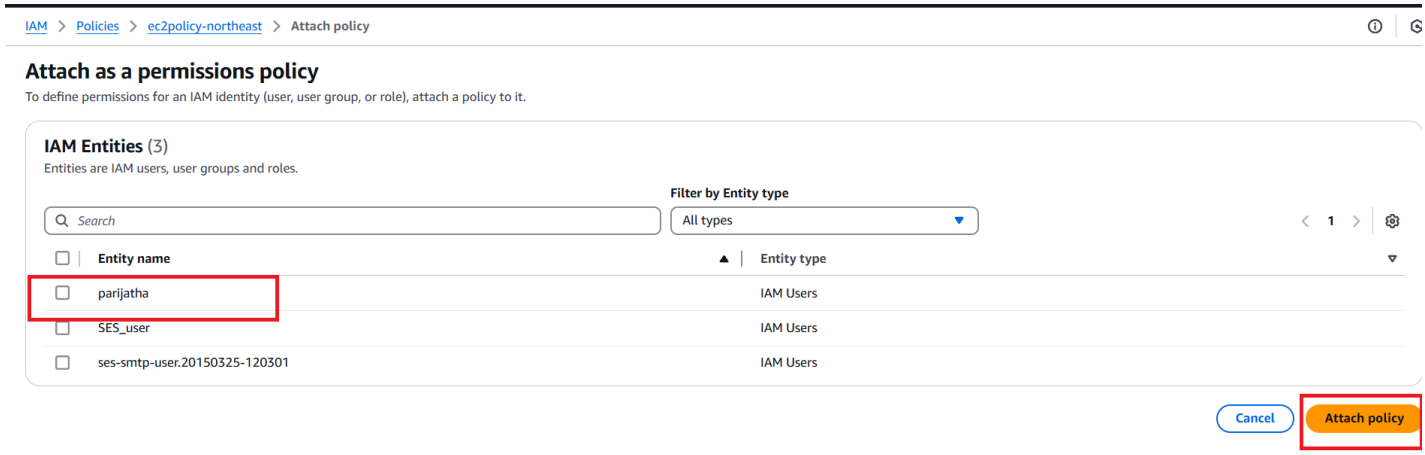

IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
Hyd-EC2-Access1
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

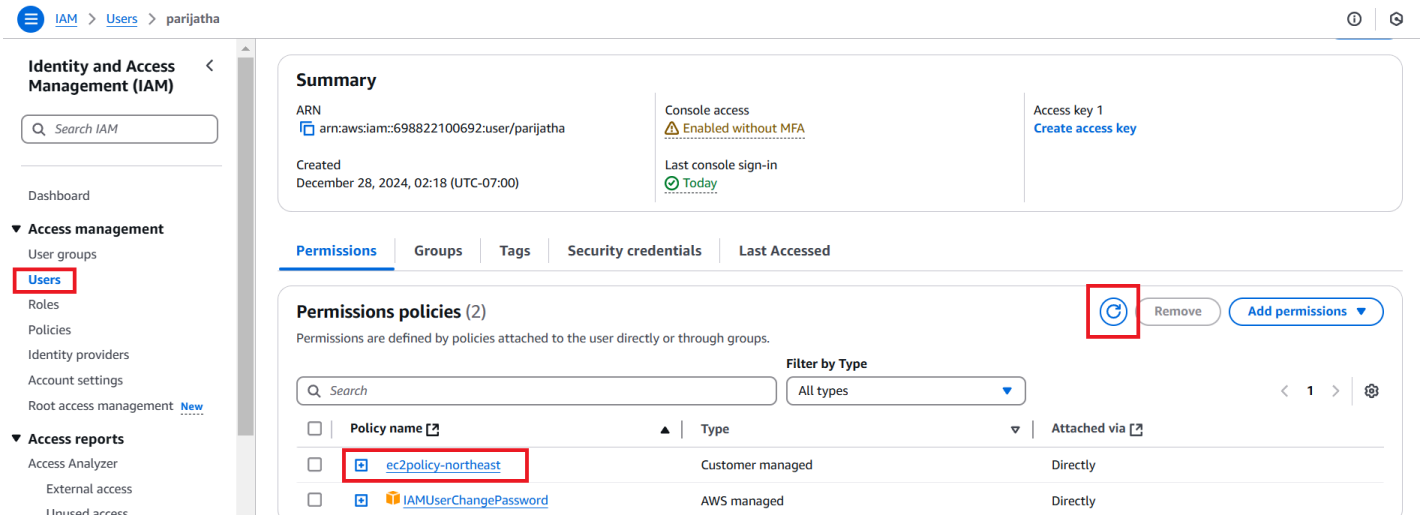


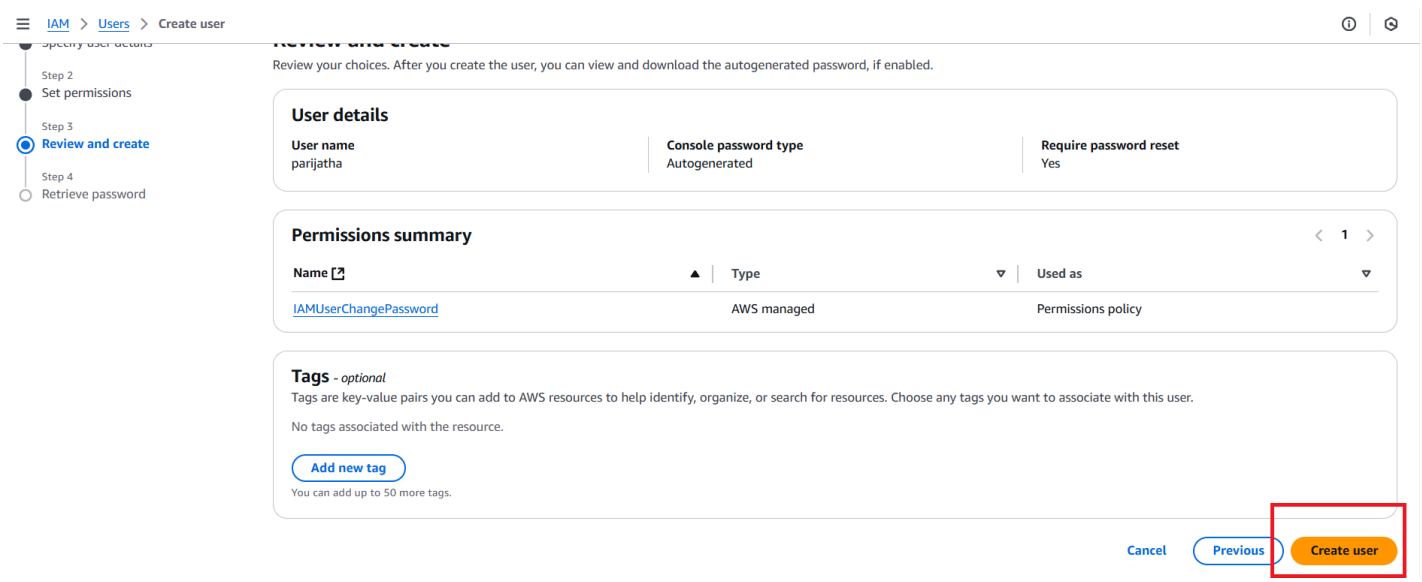
Click on create policy

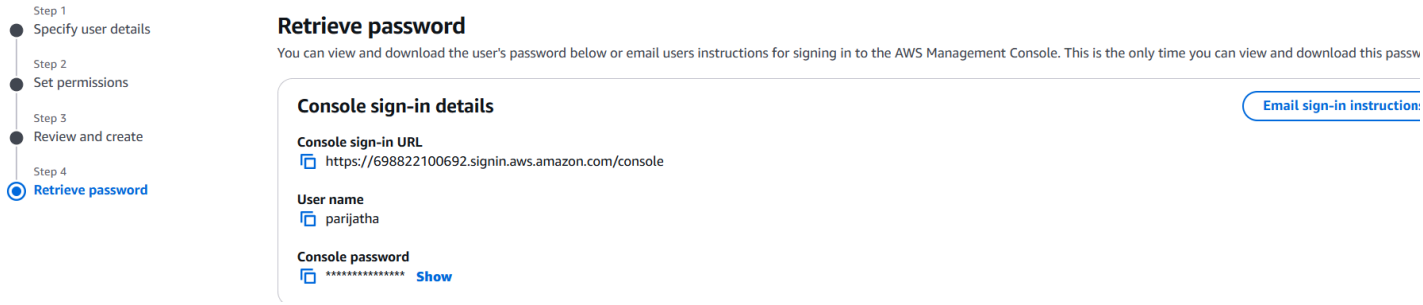


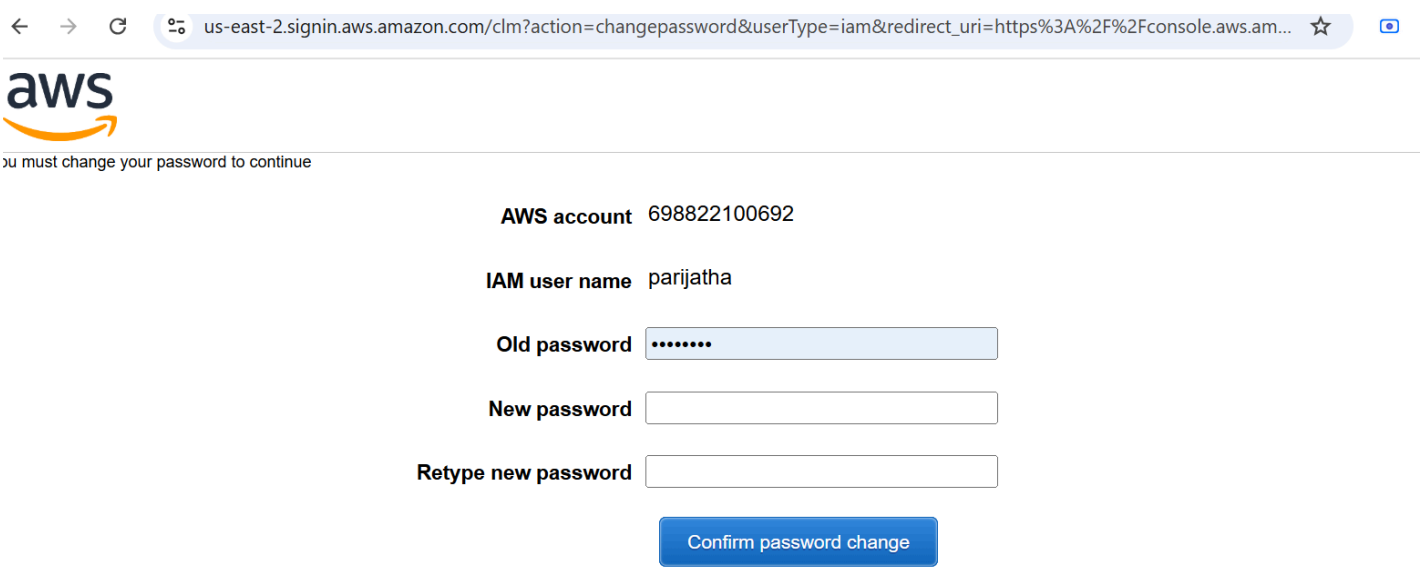


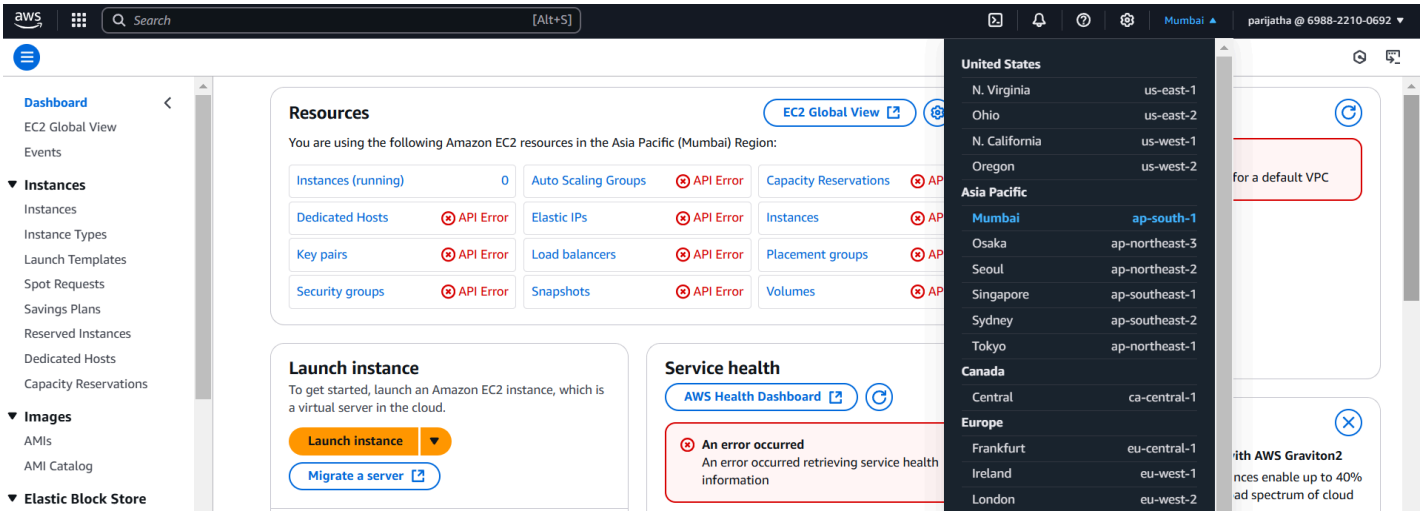



IAM > Users > parijatha
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Summary
ARN
arn:aws:iam::698822100692:user/parijatha
Console access
Enabled without MFA
Access key 1
Create access key
Created
December 28, 2024, 02:18 (UTC-07:00)
Last console sign-in
Today
Permissions
Groups
Tags
Security credentials
Last Accessed
Permissions policies (2)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Search
Filter by Type
All types
Policy name
Type
Attached via
ec2policy-northeast
Customer managed
Directly
IAMUserChangePassword
AWS managed
Directly


IAM > Users > Create user
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
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


Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
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 passw
Console sign-in details
Email sign-in instruction
Console sign-in URL
https://698822100692.signin.aws.amazon.com/console
User name
parijatha
Console password
********** Show





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.