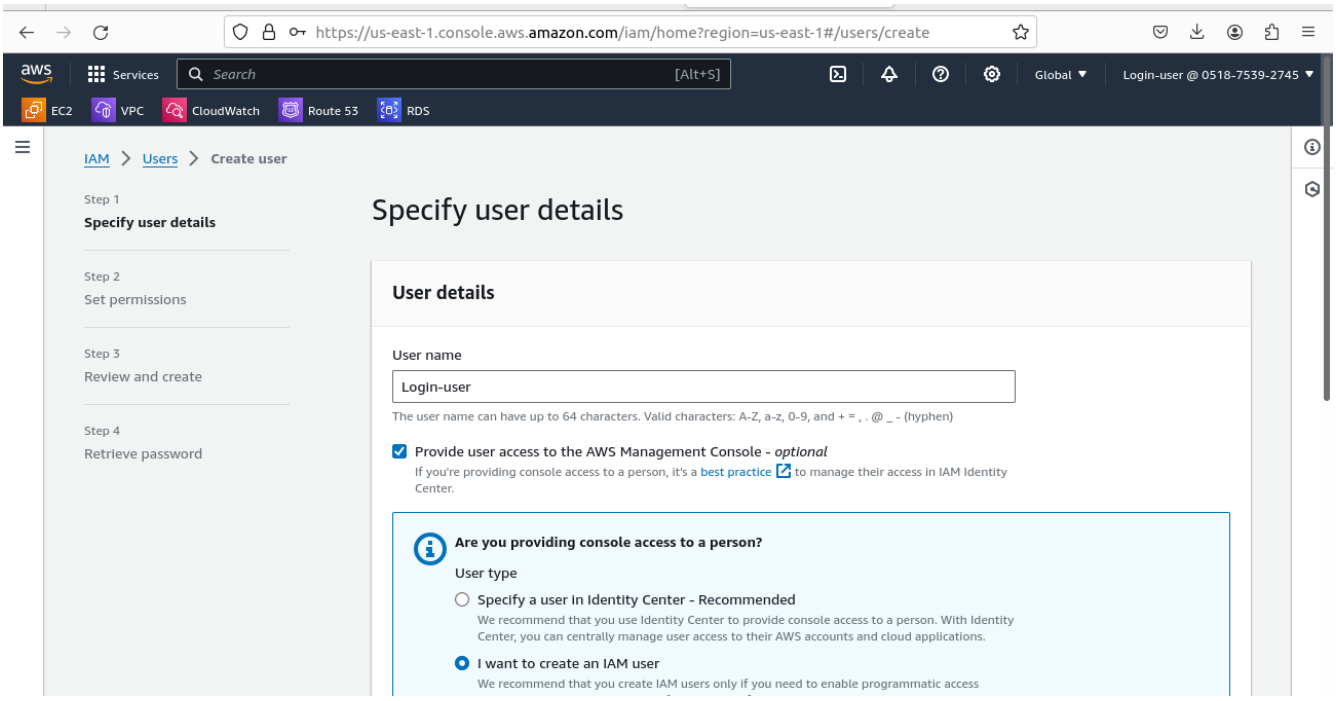
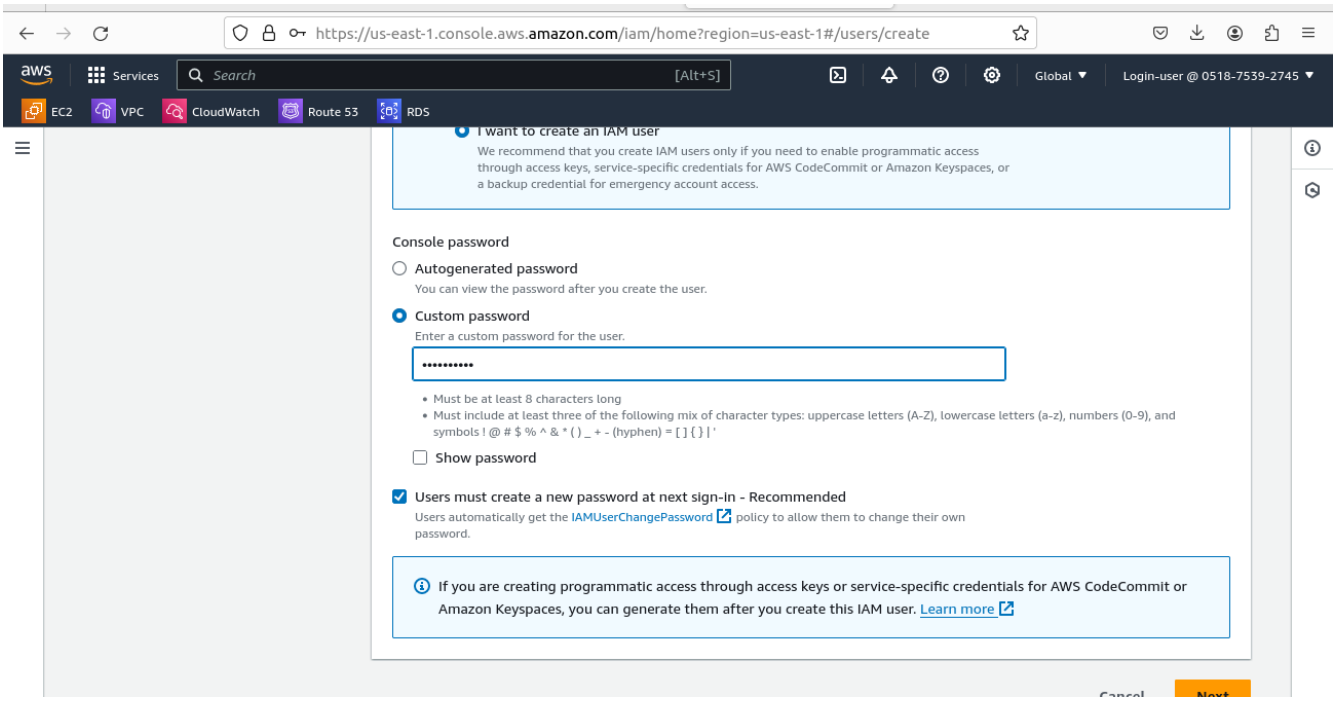
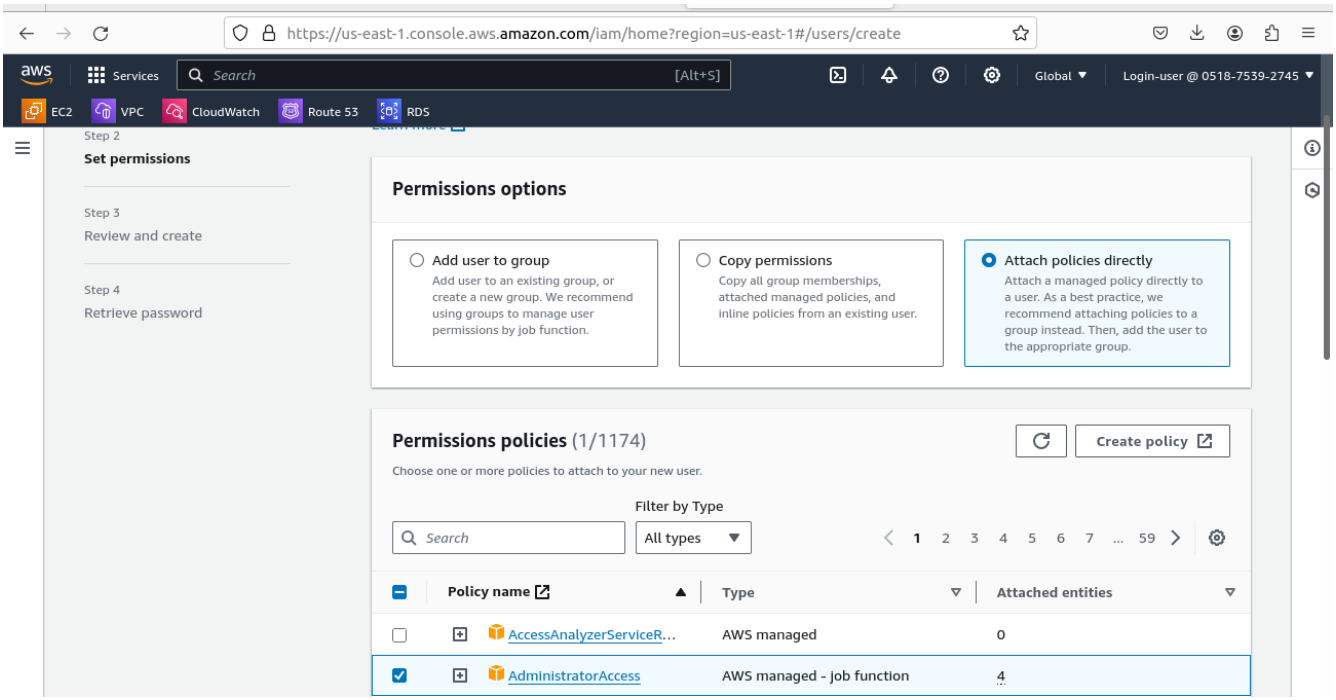
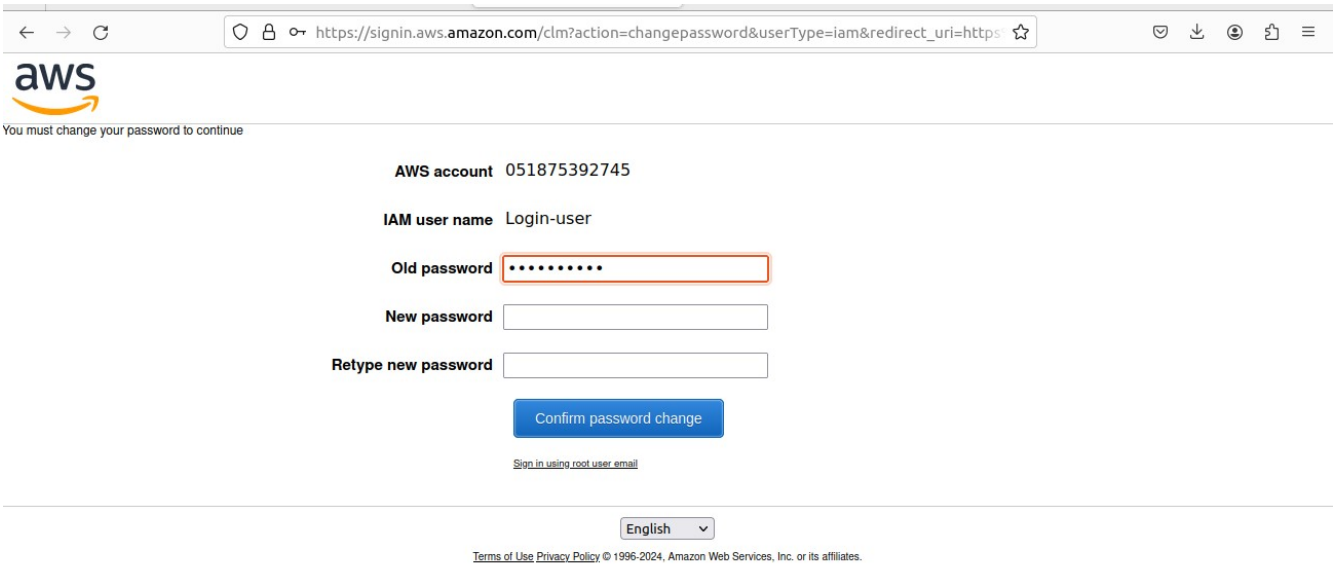
1.
a. Create a user account that can login to the console
b. Create a group and make sure that the group can only launch and stop EC2 instances using that previously created account.





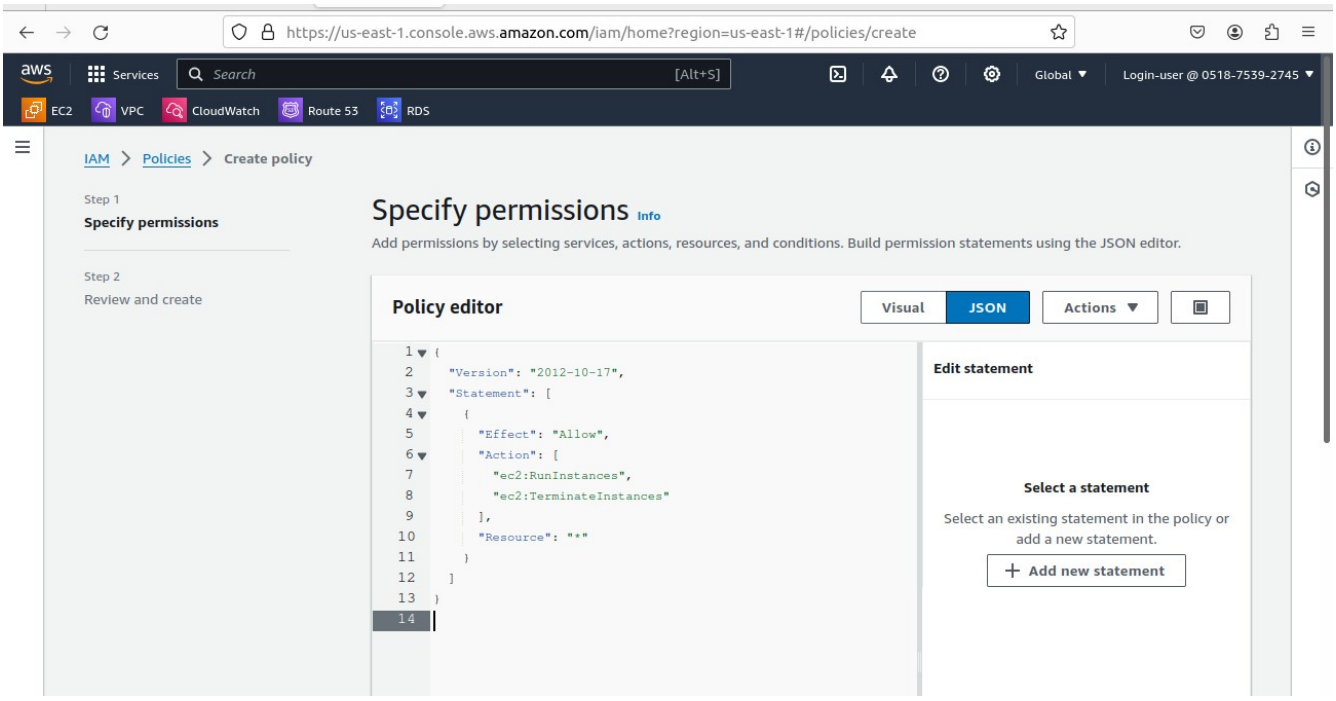


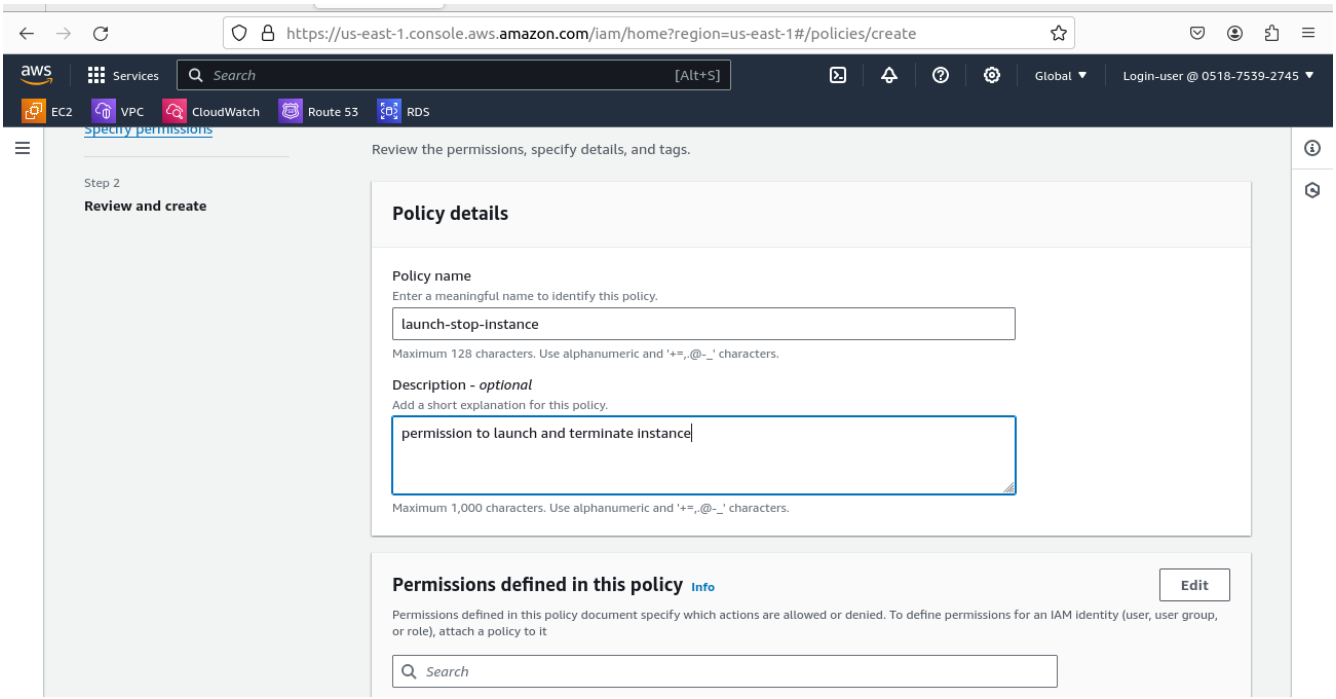
Login url /details download

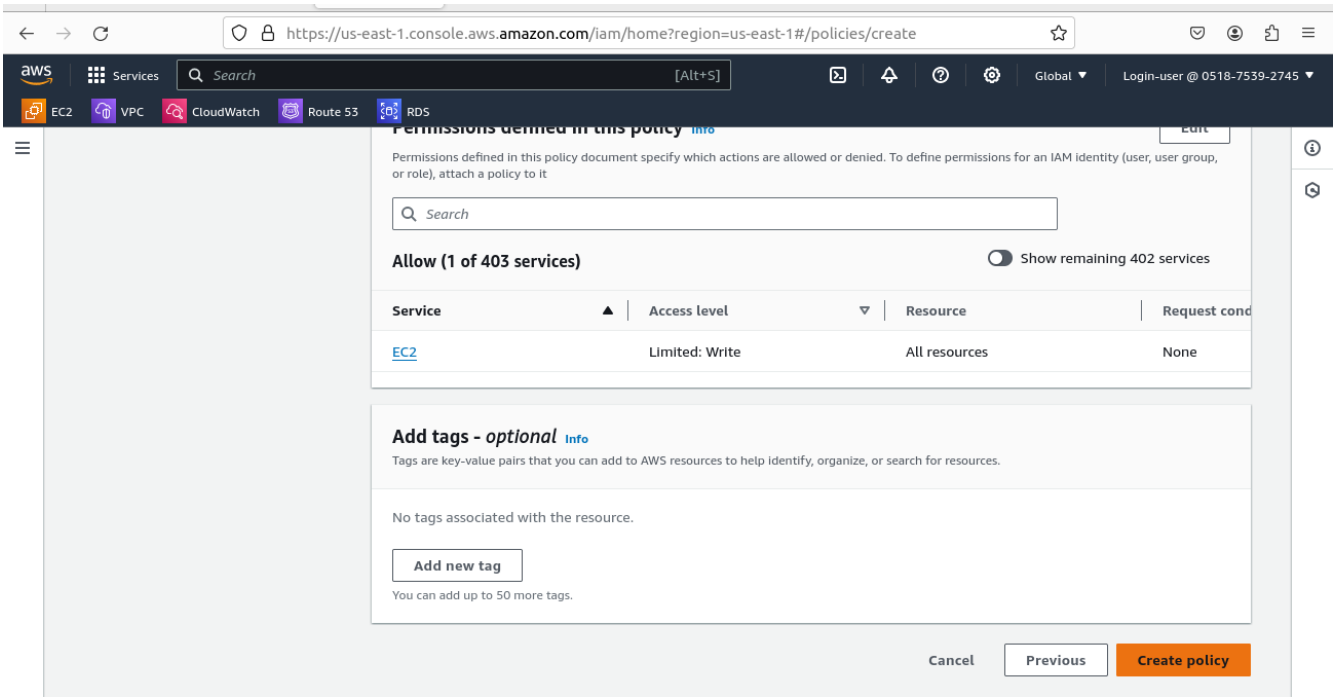


b. Create a group and make sure that the group can only launch and stop EC2 instances using that previously created account.

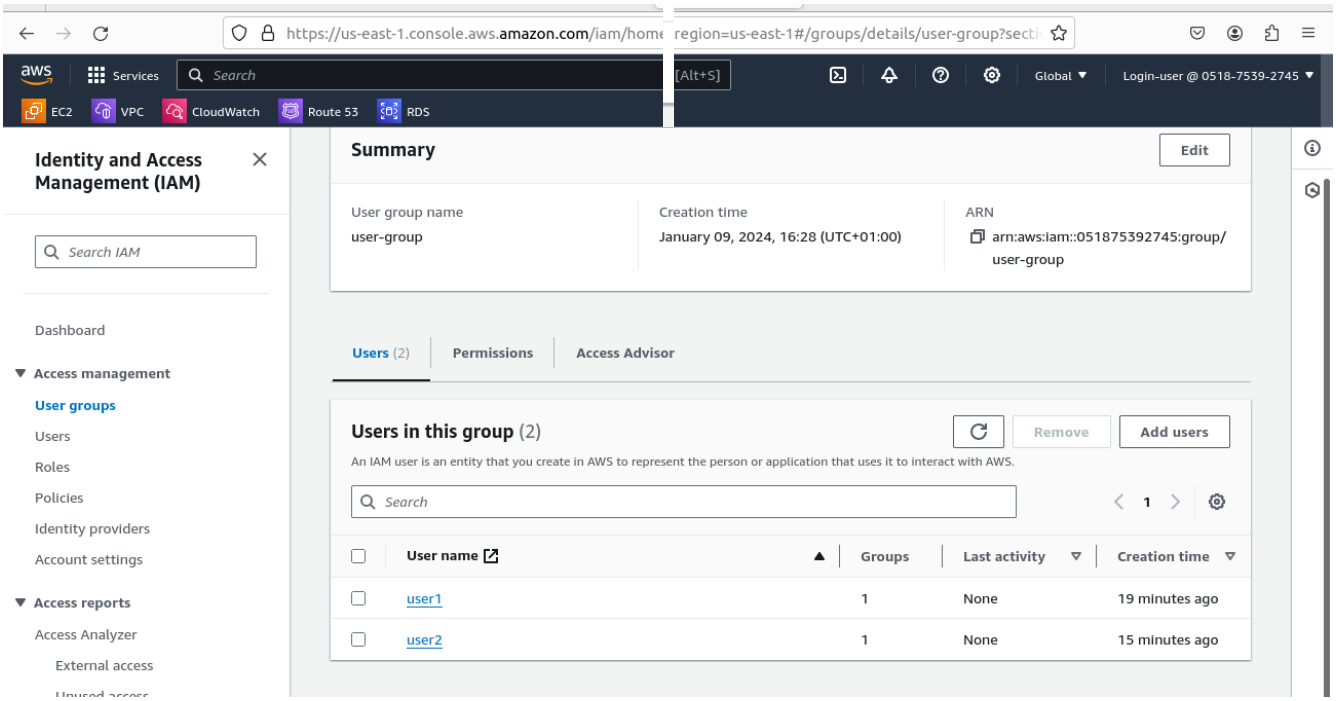
CREATE POLICY







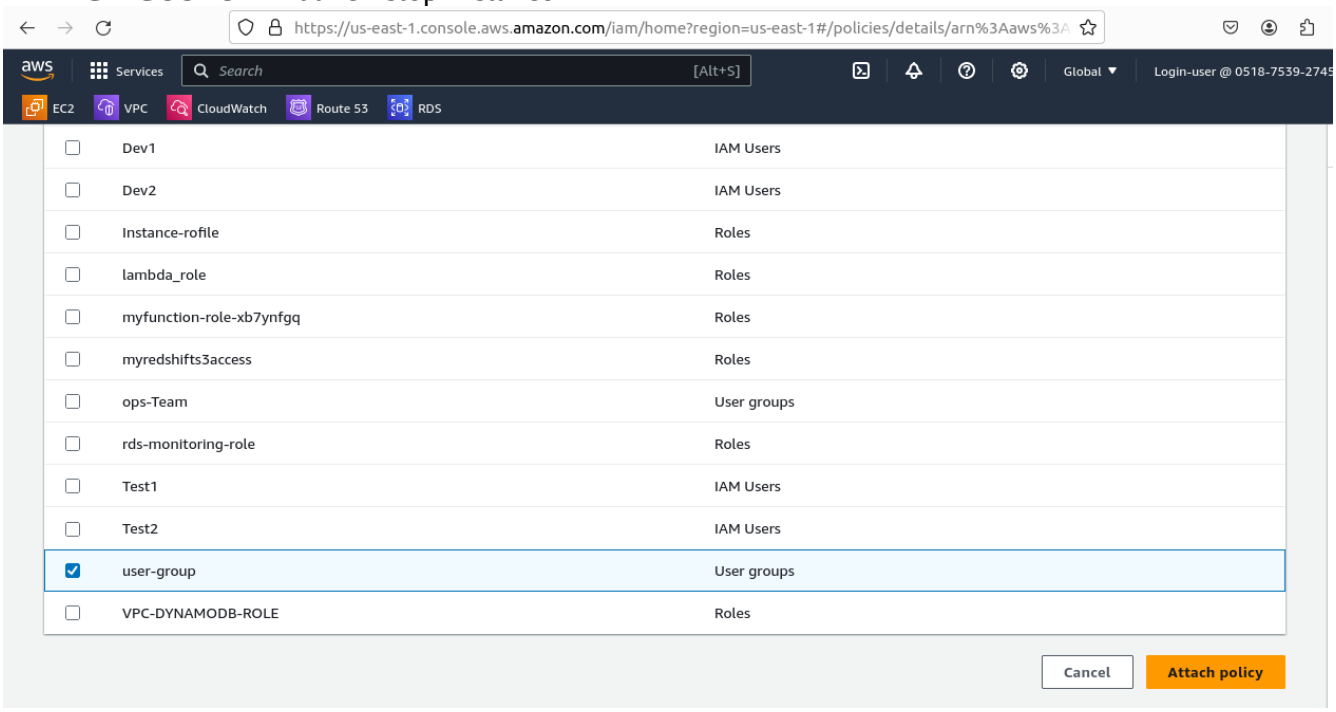
USER GROUP: HAS 2 USERS: USER1 AND USER2



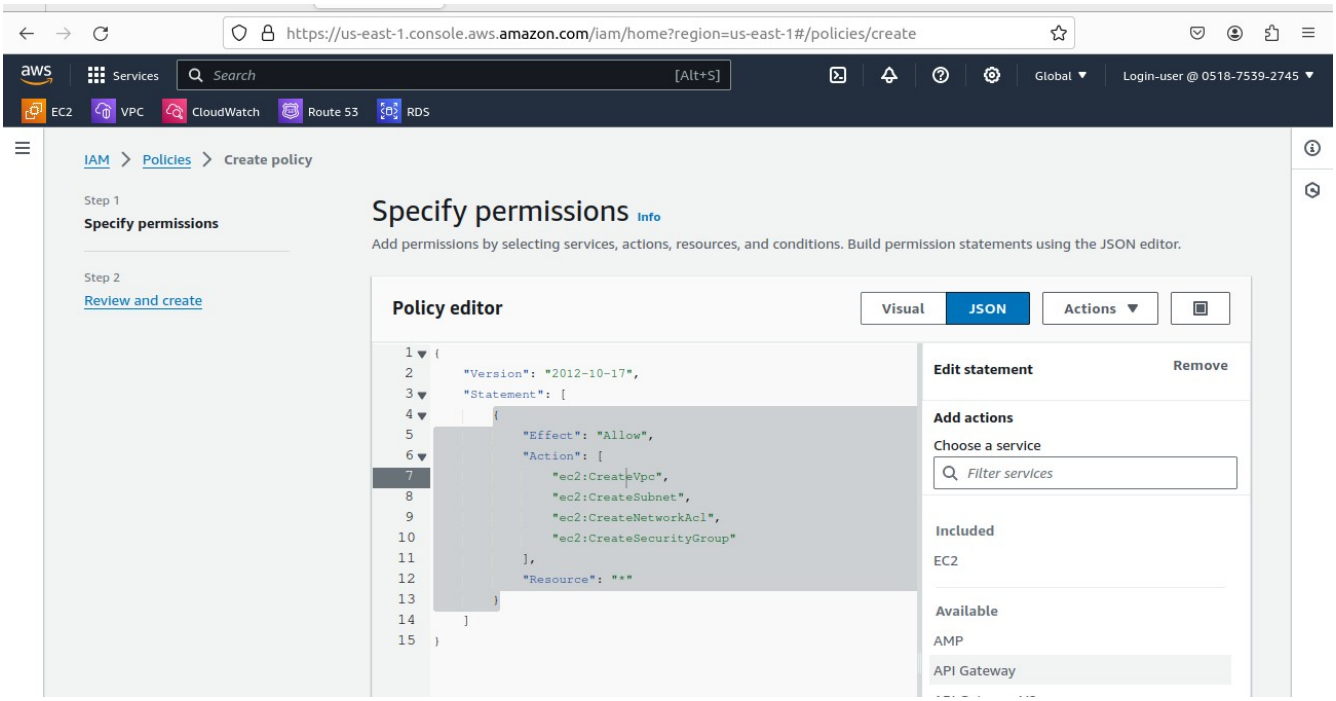
COPY OF POLICY ATTACHED:

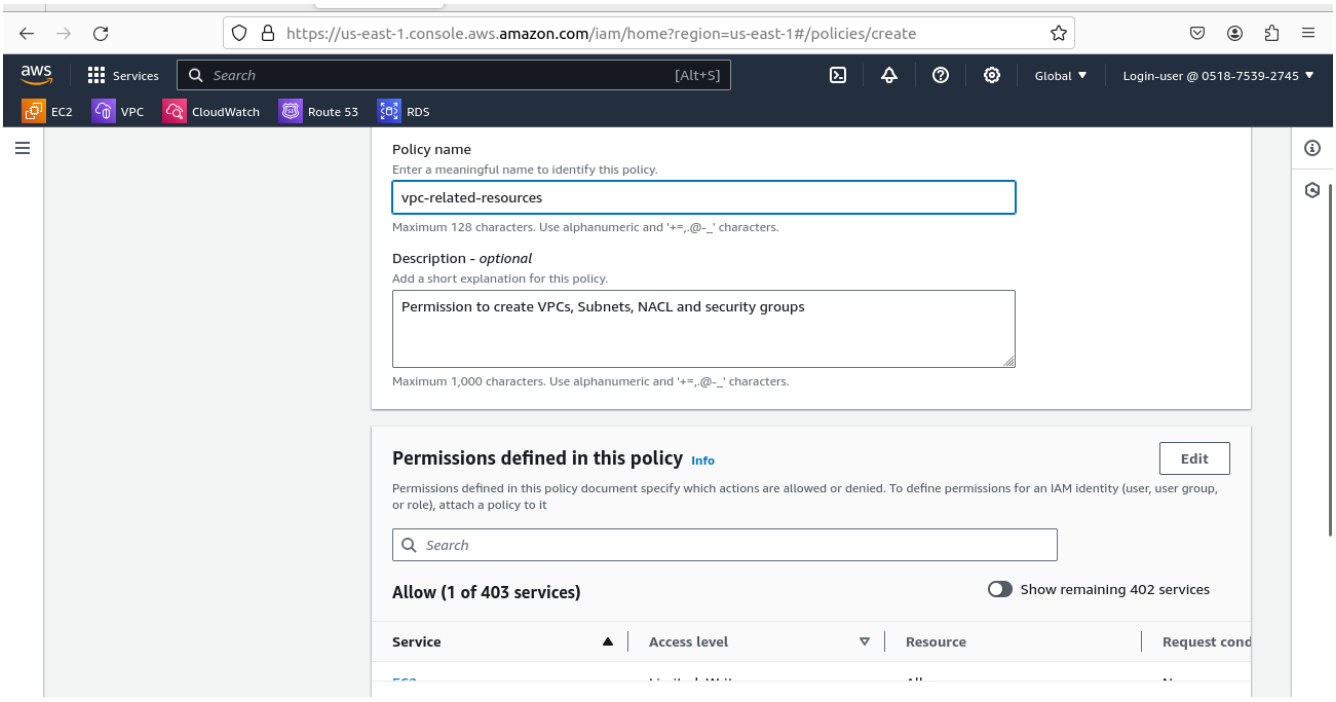
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*"
    }
  ]
}
```

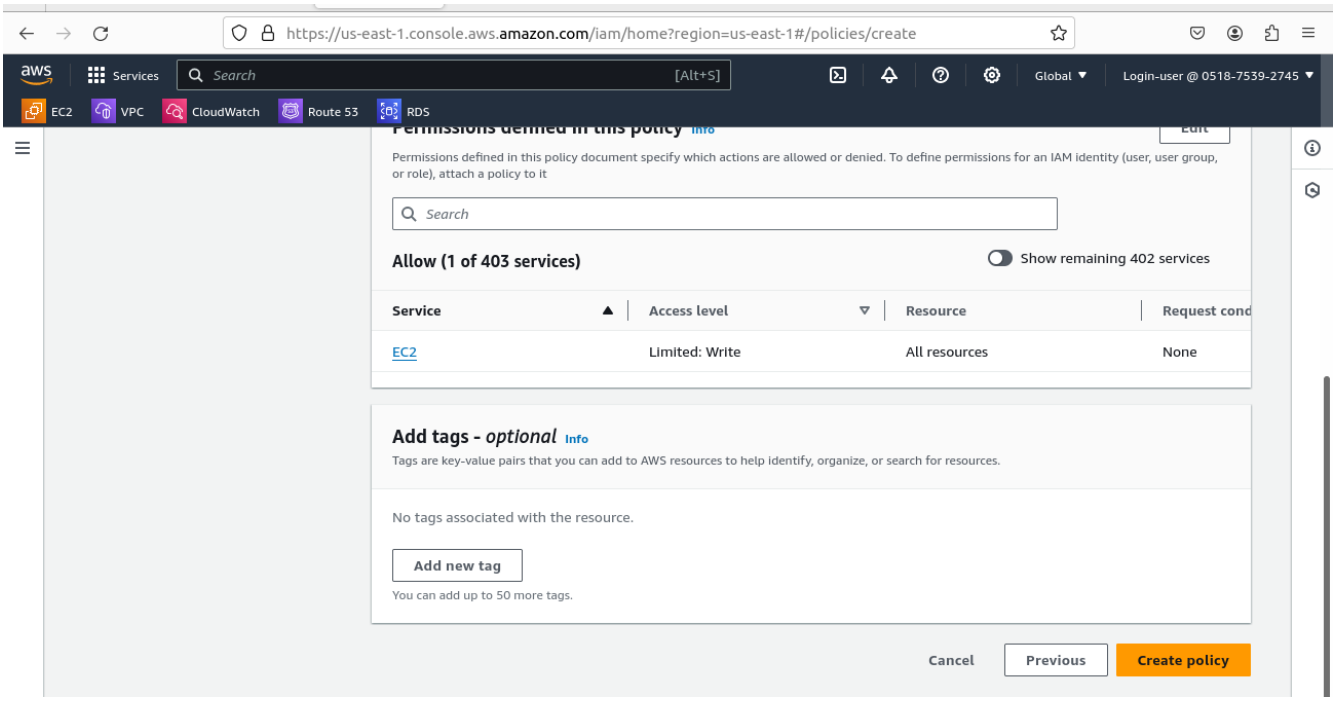
ATTACH CUSTOM “launch-stop-instance”



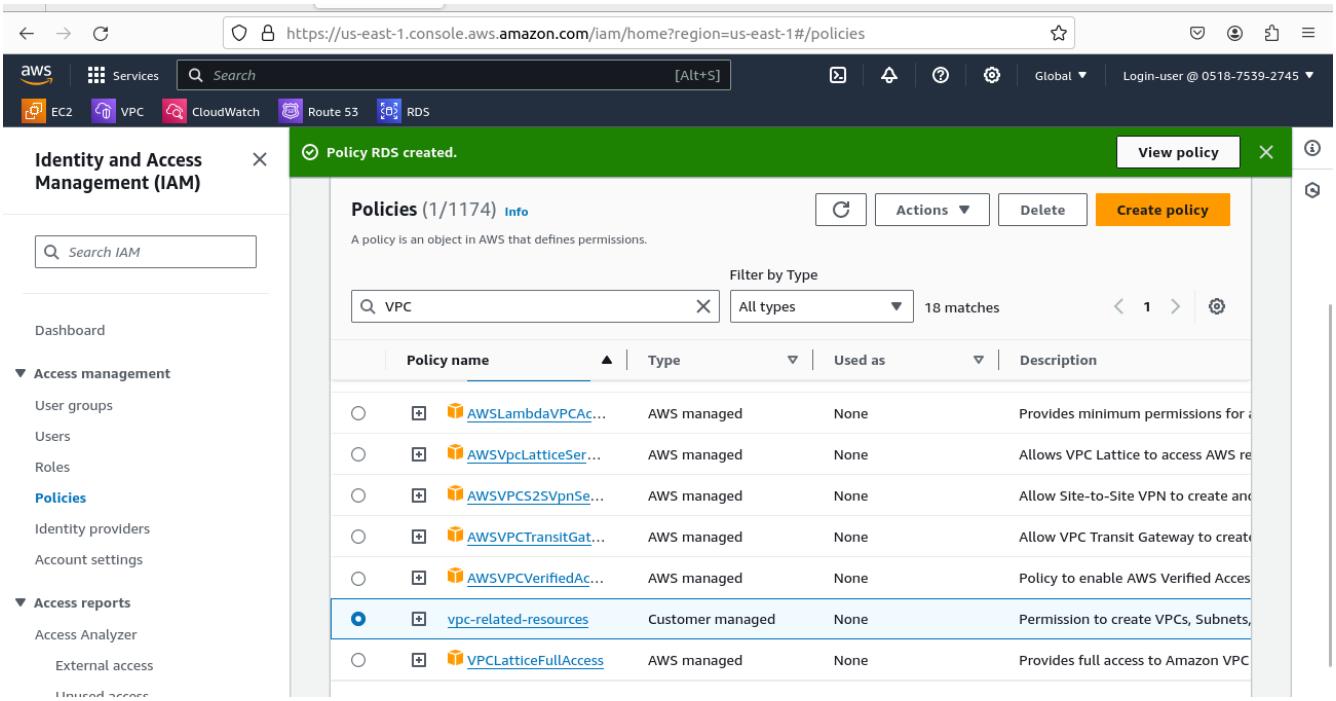
2a. Provide permission to let the user of a previously created account to create VPCs, Subnets, NACL and security groups
(create custom IAM policies for these actions and attach them to the user/GROUP)

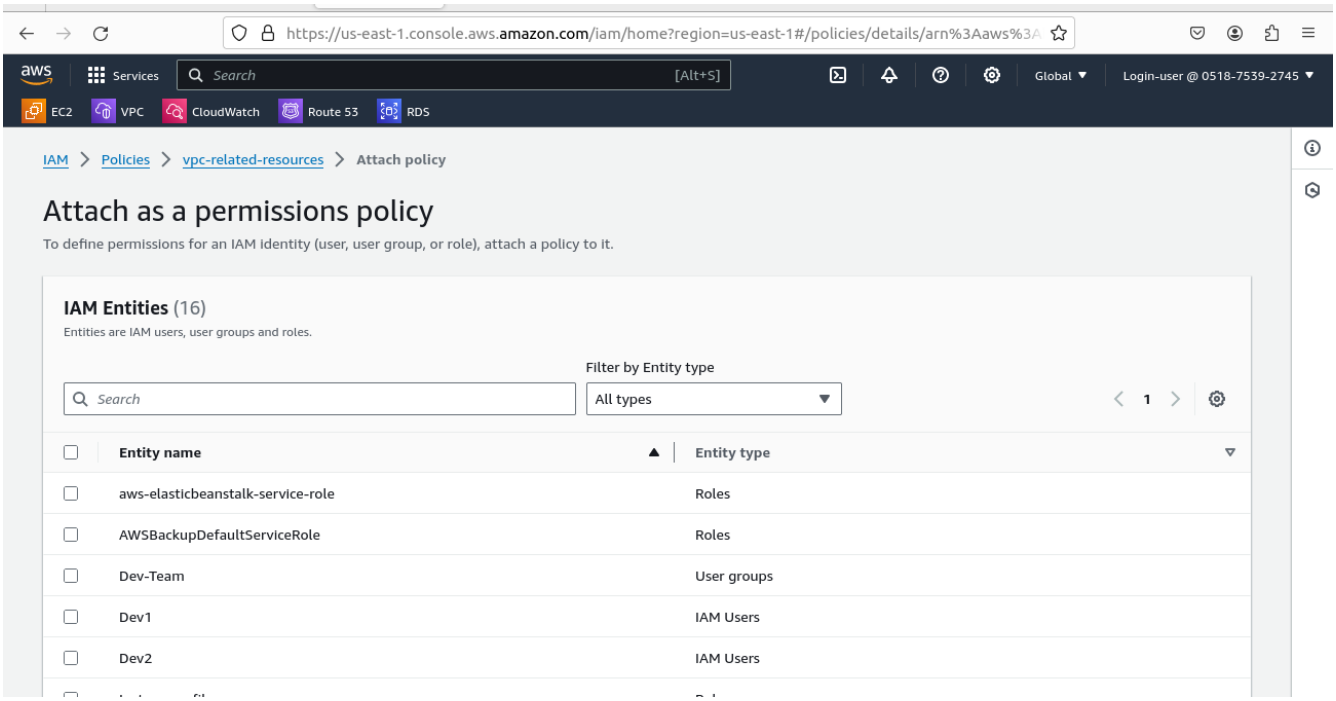

https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create
Services
Search
[Alt+S]
Global
Login-user @ 0518-7539-2745
EC2
VPC
CloudWatch
Route 53
RDS
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"ec2:CreateVpc",
"ec2:CreateSubnet",
"ec2:CreateNetworkAcl",
"ec2:CreateSecurityGroup"
],
"Resource": "*"
}
]
}
Edit statement
Remove
Add actions
Choose a service
Filter services
Included
EC2
Available
AMP
API Gateway

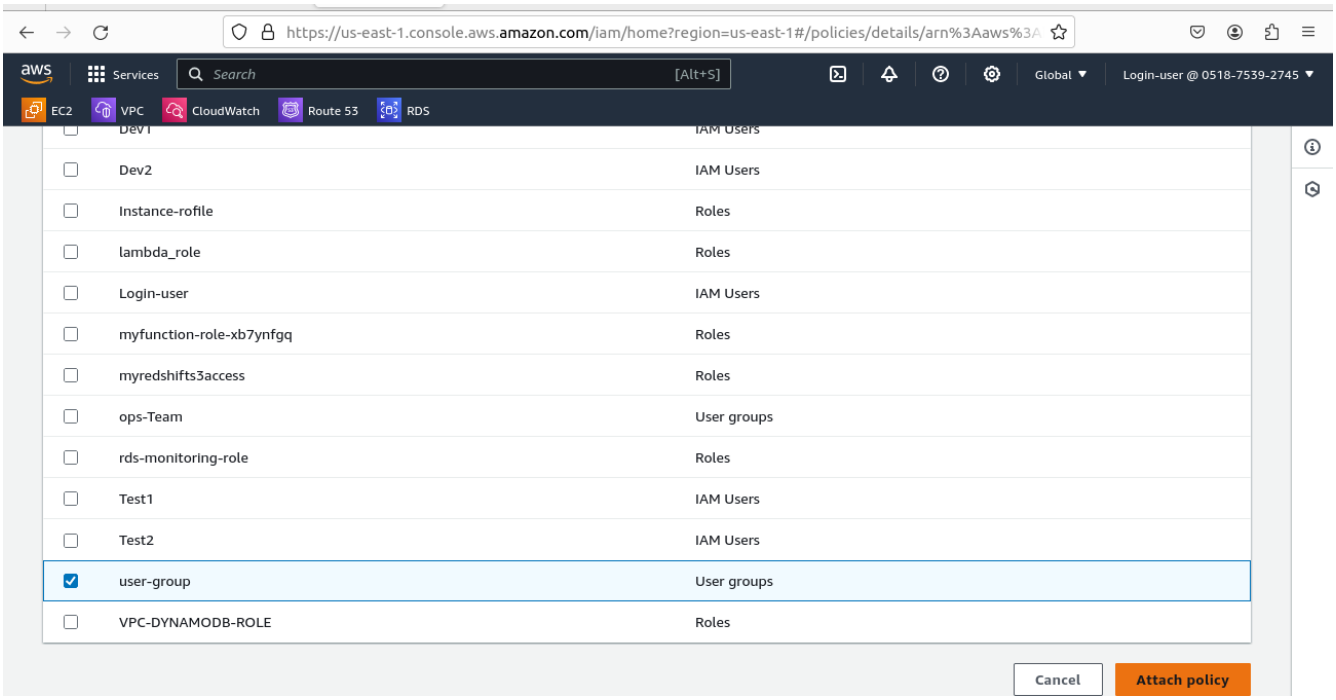

https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create
Services
Search
[Alt+S]
Global
Login-user @ 0518-7539-2745
EC2
VPC
CloudWatch
Route 53
RDS
Policy name
Enter a meaningful name to identify this policy.
vpc-related-resources
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
Permission to create VPCs, Subnets, NACL and security groups
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions defined in this policy Info
Edit
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
Search
Allow (1 of 403 services)
Show remaining 402 services
Service
Access level
Resource
Request cond



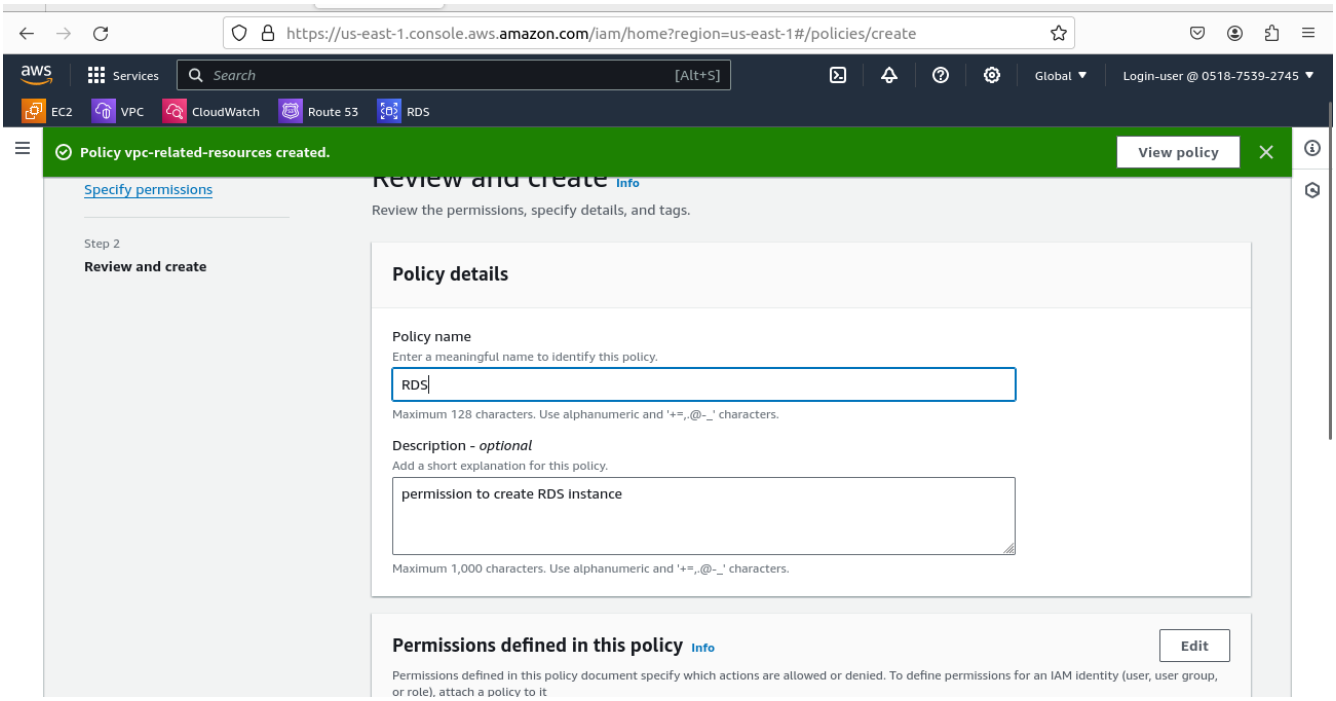
ATTACH THE CUSTOM ‘vpc-related-policy’ TO THE GROUP CREATED IN EXERCISE 2 ABOVE

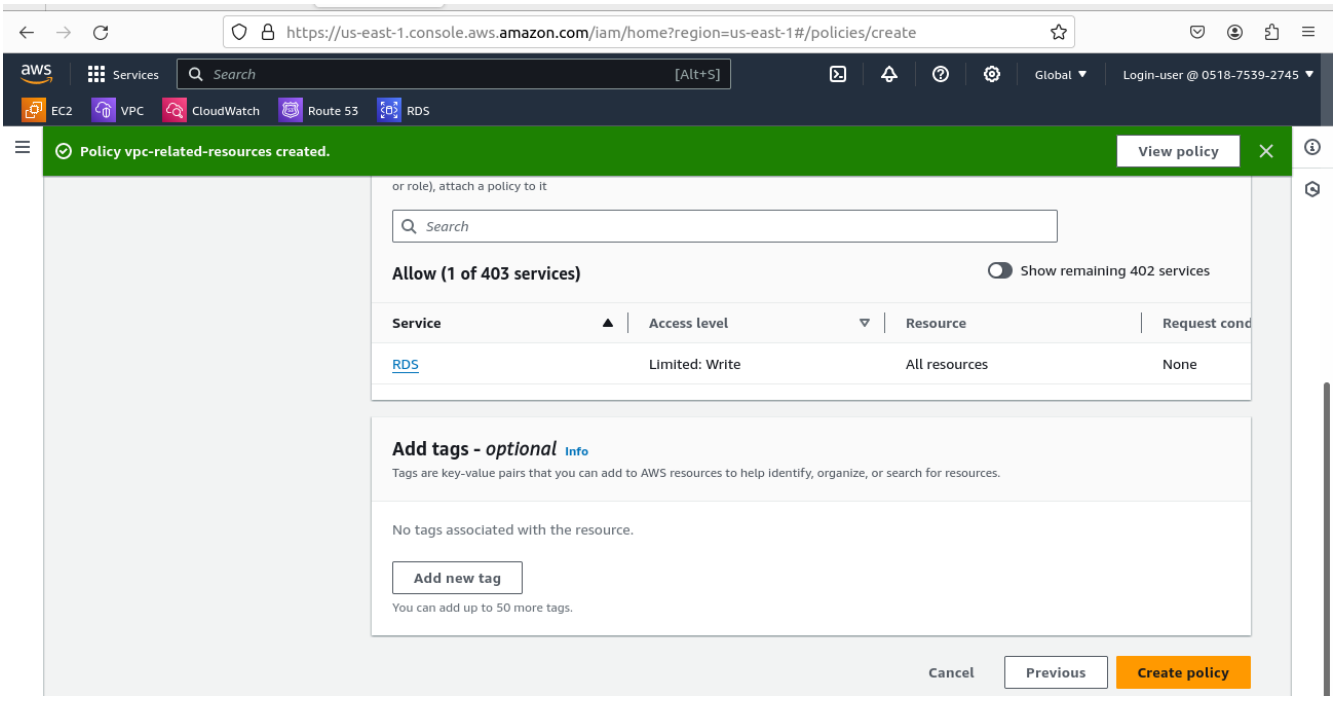




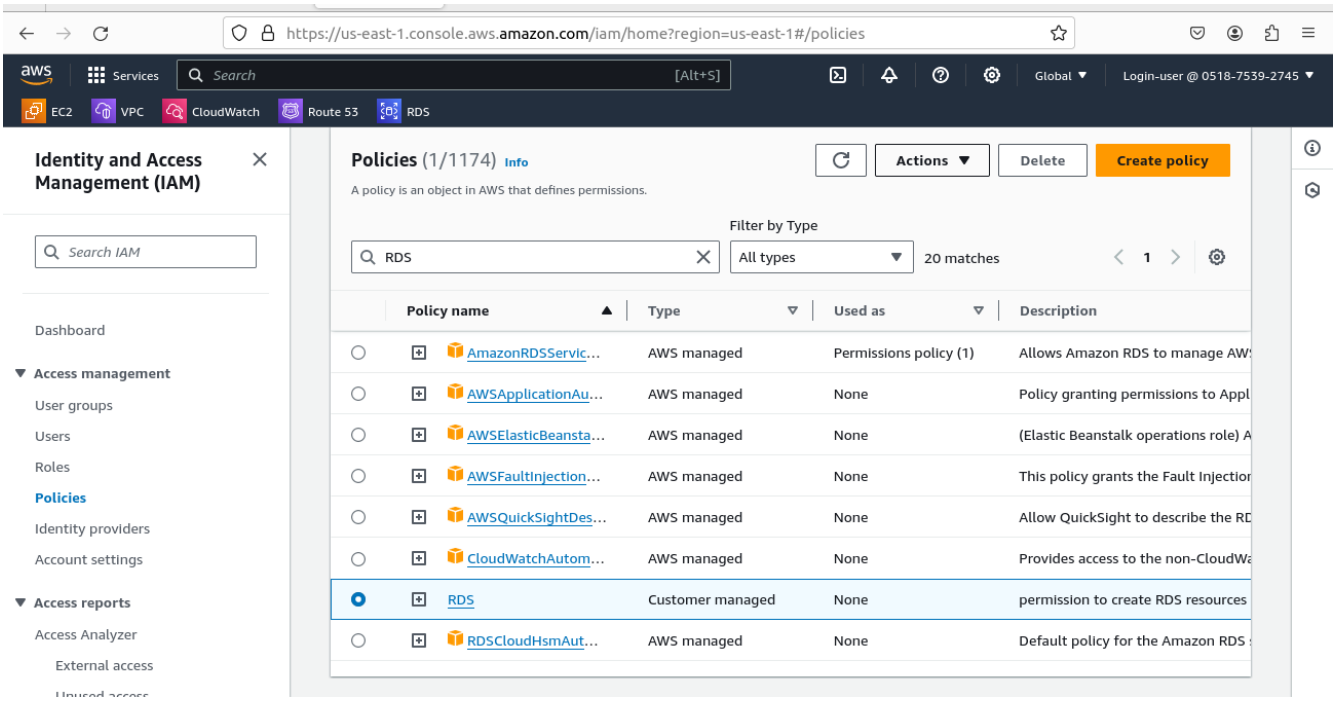


b. Further add the permission so that the user can create RDS instance

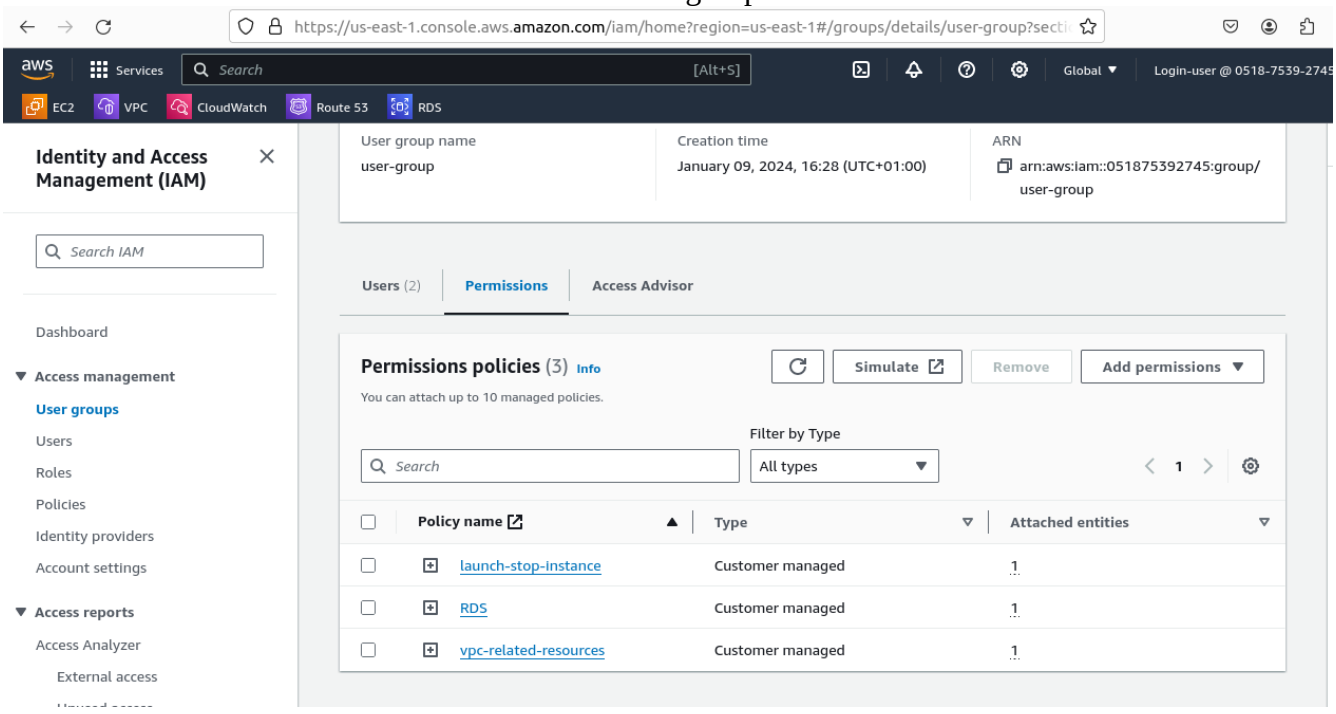

https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create
Services
Search
[Alt+S]
Global
Login-user @ 0518-7539-2745
EC2
VPC
CloudWatch
Route 53
RDS
Policy vpc-related-resources created.
View policy
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
RDS
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
permission to create RDS instance
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions defined in this policy Info
Edit
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


https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create
Services
Search
[Alt+S]
Global
Login-user @ 0518-7539-2745
EC2
VPC
CloudWatch
Route 53
RDS
Policy vpc-related-resources created.
View policy
or role), attach a policy to it
Search
Allow (1 of 403 services)
Show remaining 402 services
Service
Access level
Resource
Request cond
RDS
Limited: Write
All resources
None
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

ATTACH CUSTOM RDS POLICY



3 CUSTOM POLICIES ATTACHED TO THE “user-group”



Explore security options to protect the AWS resources and secure the permissions provided to the group.

This will involve setting up measures such as IAM policies, security groups, network ACLs, and other security i.e data encryption, monitoring logging, regular audit and compliance checks, backup and recover to protect the infrastructure in AWS.