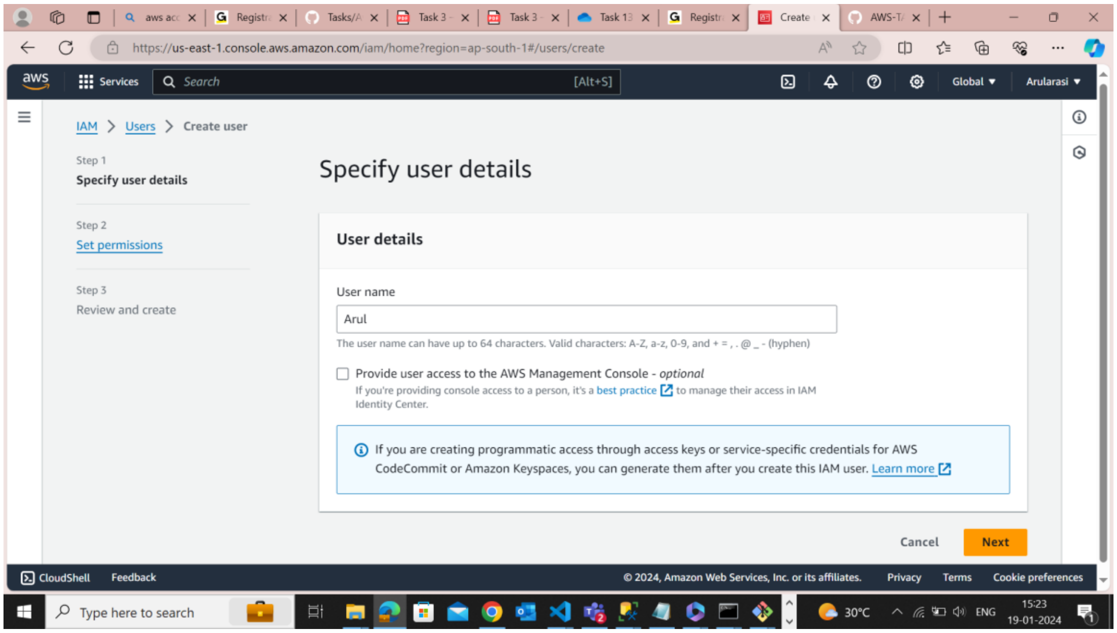
Task 4 – IAM in AWS


https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
aws
Services
Search
[Alt+S]
Global ▾
Arularasi ▾
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
30°C
ENG
15:23
19-01-2024

IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Specify user details

User details

User name

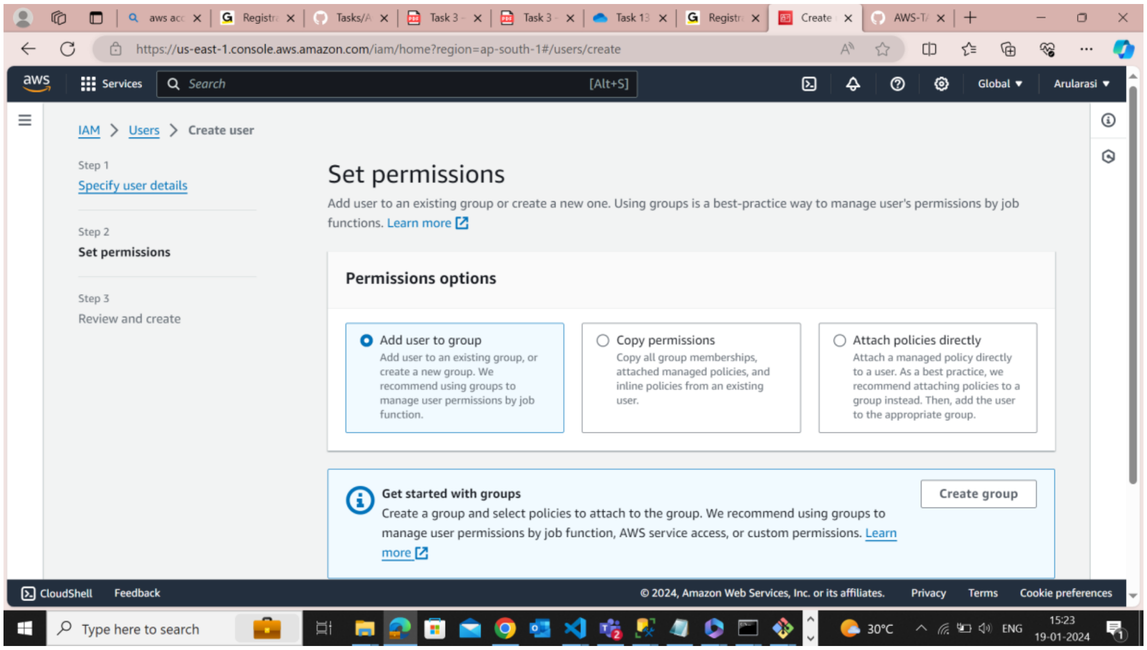
Arul

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

□ Provide user access to the AWS Management Console - *optional*
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

ⓘ If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more

Cancel Next


https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
aws
Services
Search
[Alt+S]
Global ▾
Arularasi ▾
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
30°C
ENG
15:23
19-01-2024

IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Set permissions

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

Permissions options

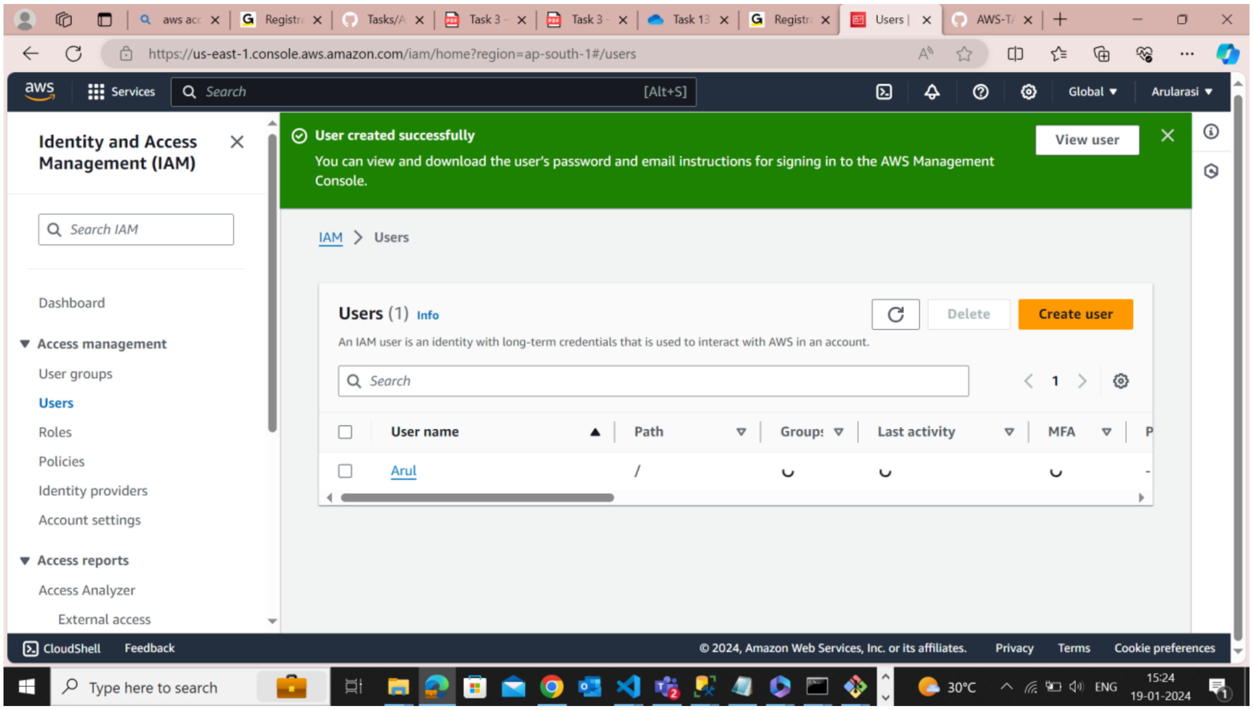
● Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ 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.

ⓘ **Get started with groups**
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more

Create group



https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

View user

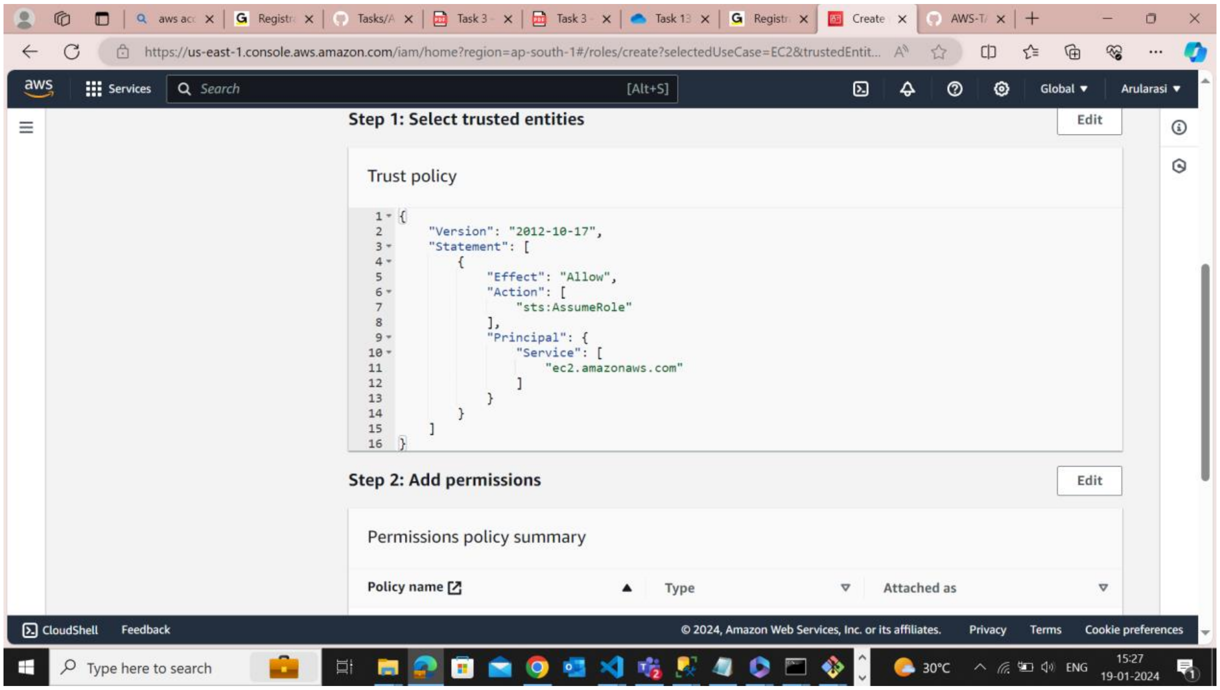
Identity and Access Management (IAM)

IAM > Users

Users (1) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Groups	Last activity	MFA	P
Arul	/				-



https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create?selectedUseCase=EC2&trustedEntit...

Step 1: Select trusted entities

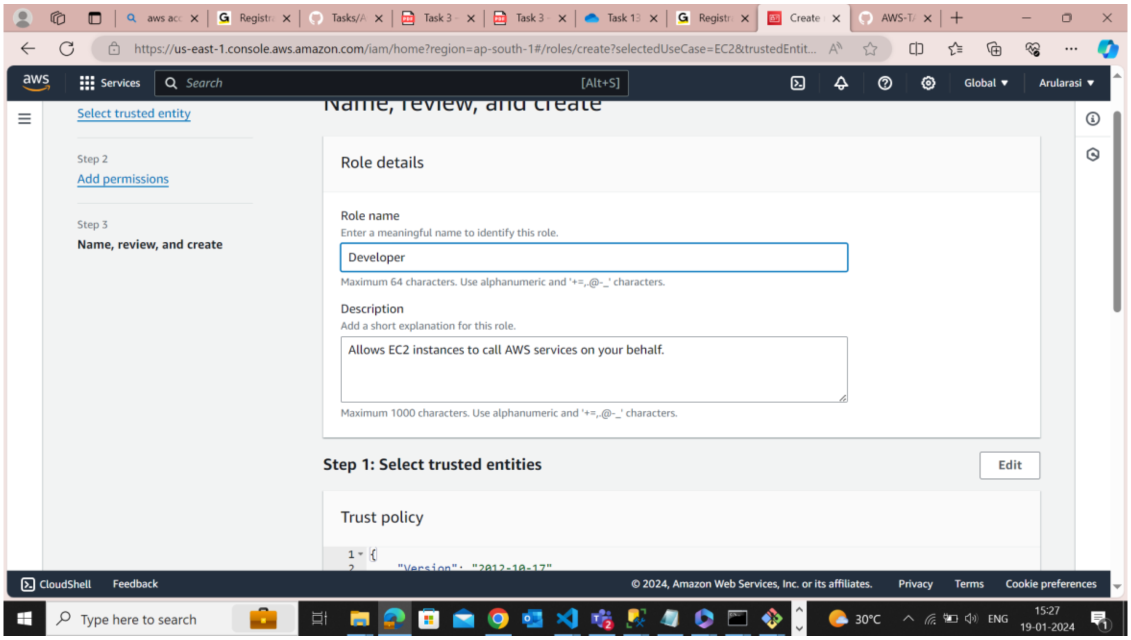
Trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Principal": {
                "Service": [
                    "ec2.amazonaws.com"
                ]
            }
        }
    ]
}
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as



Name, review, and create

Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
Developer
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

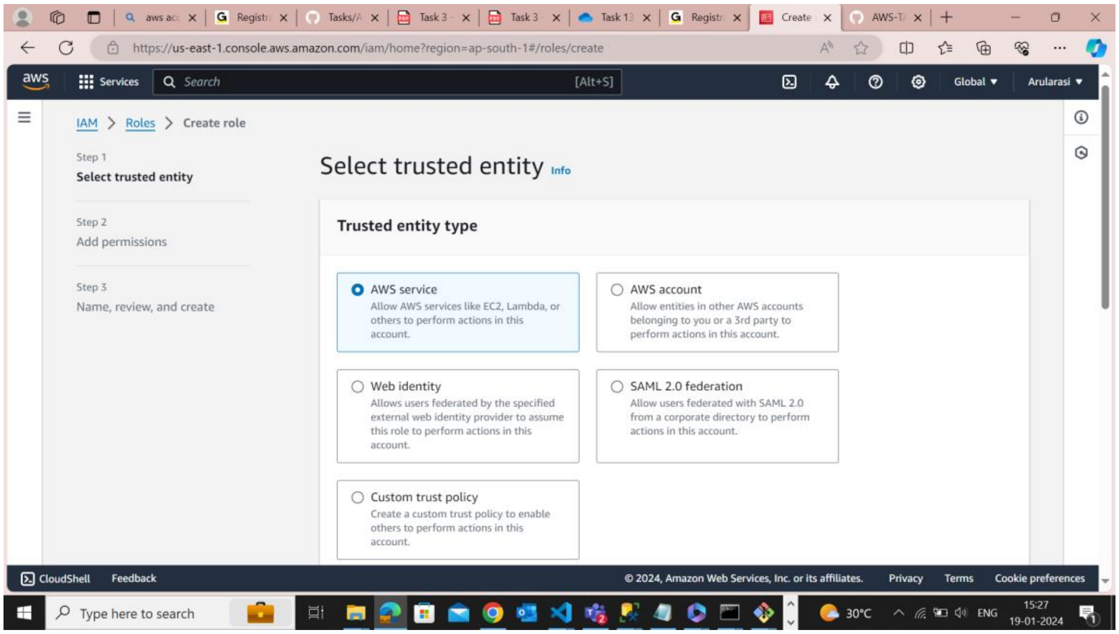
Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Step 1: Select trusted entities

Edit

Trust policy

```
{
    "Version": "2012-10-17"
```



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

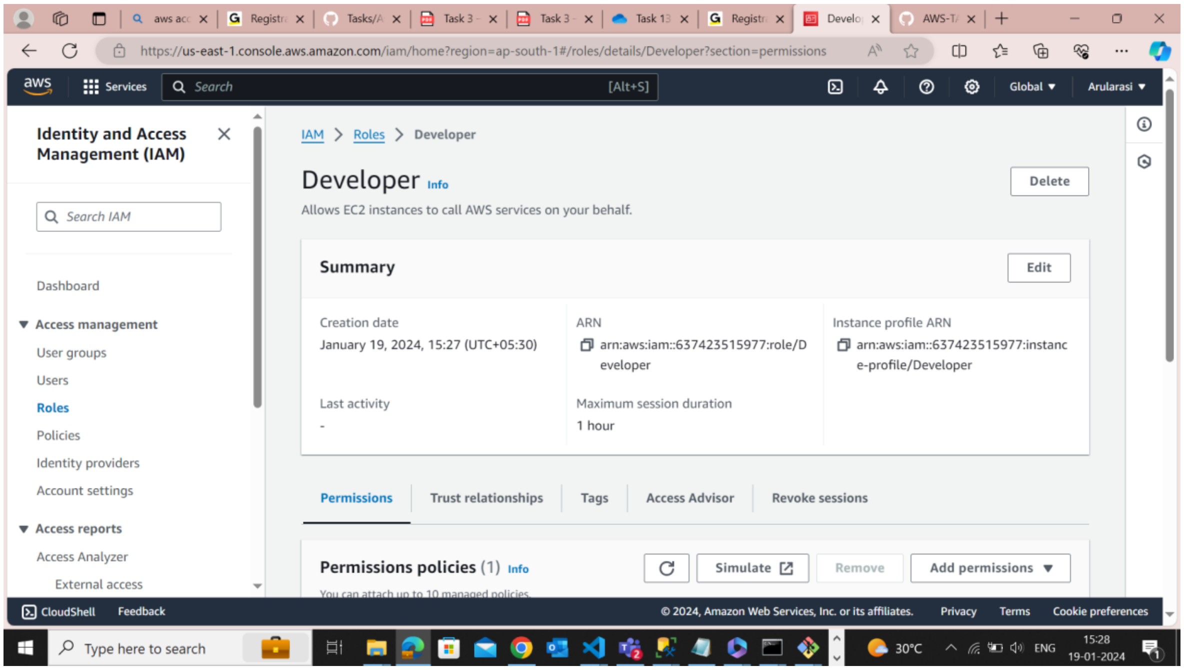
● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.



Developer Info

Allows EC2 instances to call AWS services on your behalf.

Summary

Creation date
January 19, 2024, 15:27 (UTC+05:30)

ARN
arn:aws:iam::637423515977:role/Developer

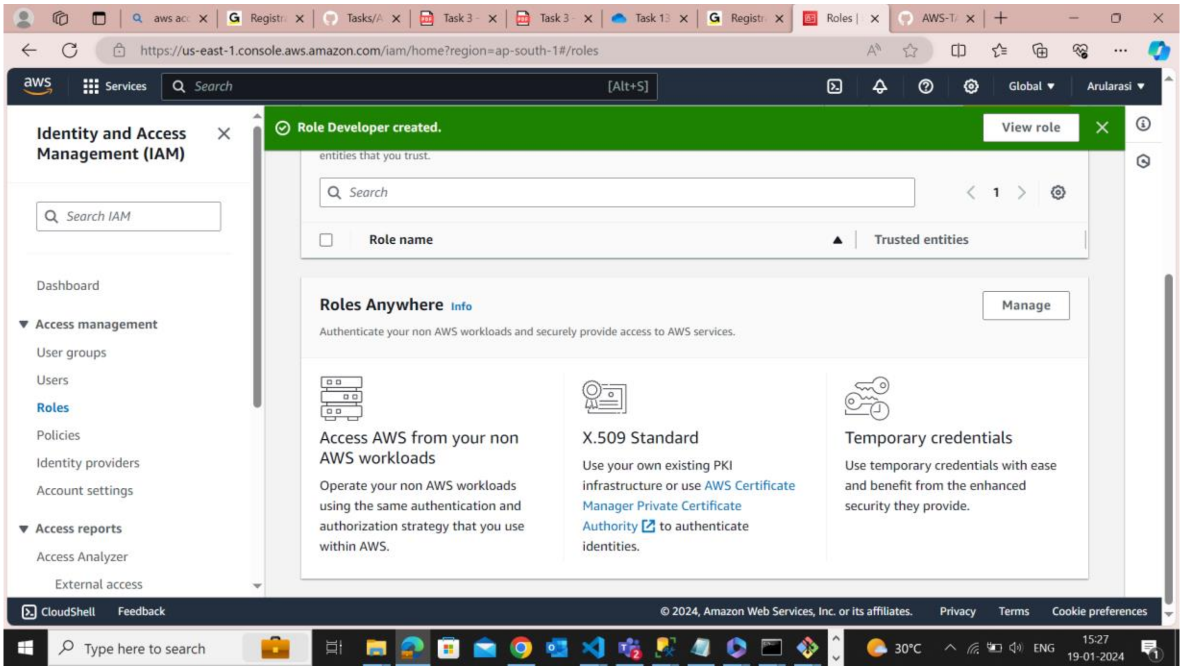
Instance profile ARN
arn:aws:iam::637423515977:instance-profile/Developer

Last activity
-

Maximum session duration
1 hour

Permissions policies (1) Info

You can attach up to 10 managed policies.



Role Developer created.

entities that you trust.

□	Role name ▲	Trusted entities

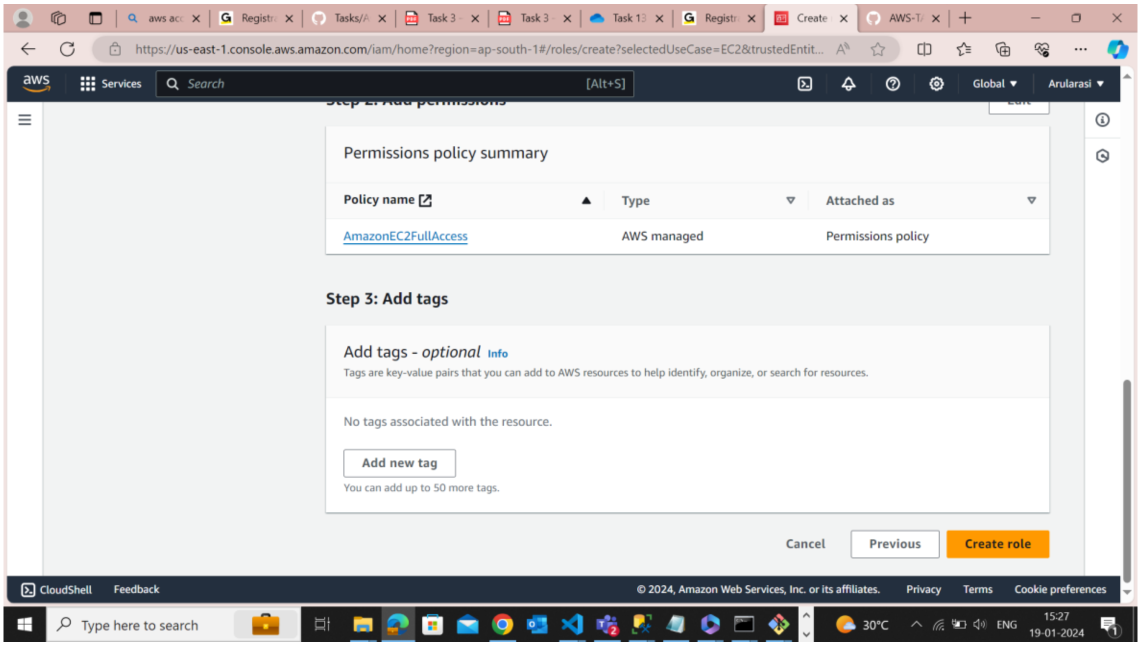
Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads
Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard
Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials
Use temporary credentials with ease and benefit from the enhanced security they provide.



aws acc
Registr
Tasks/A
Task 3
Task 3
Task 13
Registr
Create
AWS-T/
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create?selectedUseCase=EC2&trustedEntit...
aws
Services
Search
[Alt+S]
Global
Arularasi
Edit

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonEC2FullAccess	AWS managed	Permissions policy

Step 3: Add tags

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.