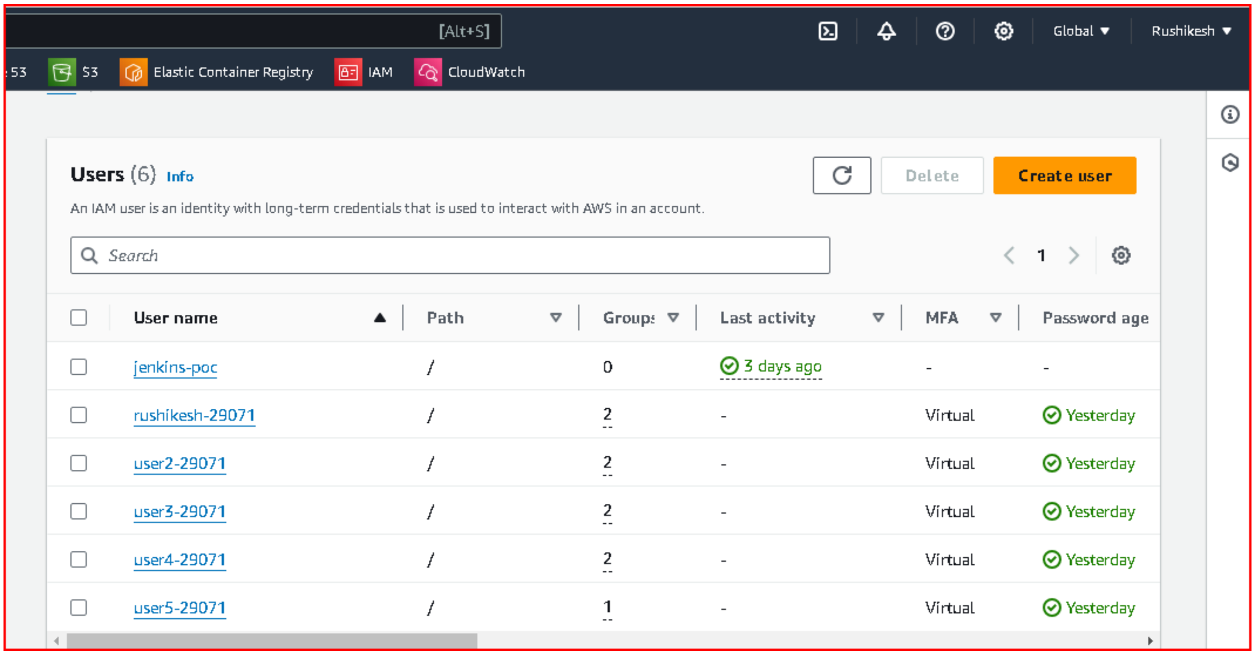
Tasks on IAM

a. Create 5 IAM users:

User 1: Rushikesh-29071

User2-29071, User3-29071, User4-29071, User5-29071



Users (6) 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	Password age
□	jenkins-poc	/	0	✓ 3 days ago	-	-
□	rushikesh-29071	/	2	-	Virtual	✓ Yesterday
□	user2-29071	/	2	-	Virtual	✓ Yesterday
□	user3-29071	/	2	-	Virtual	✓ Yesterday
□	user4-29071	/	2	-	Virtual	✓ Yesterday
□	user5-29071	/	1	-	Virtual	✓ Yesterday

b. For all users, enable MFA using a virtual MFA device.

Go to the IAM Management Console.

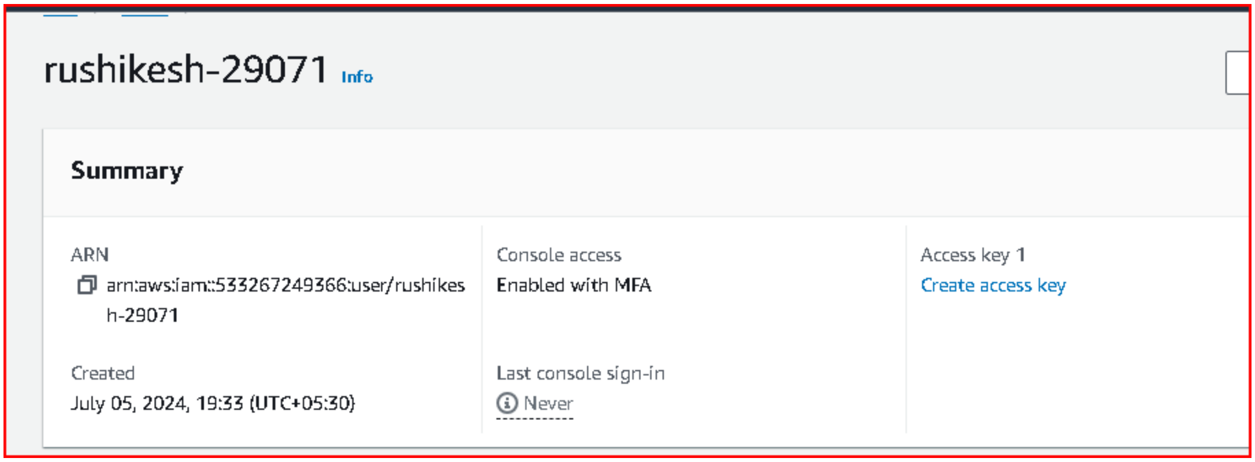
Click on Users in the left navigation pane.

Click on the username of the first user (e.g., name1-your_empid).

Scroll down to the Security credentials tab.

Click Manage next to Assigned MFA device.

Choose Virtual MFA device and click Continue.



rushikesh-29071 Info

Summary

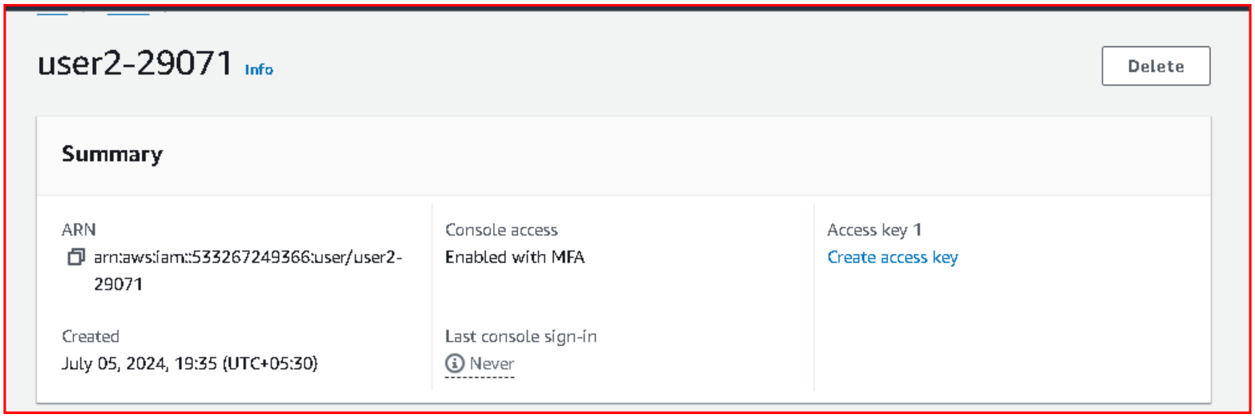
ARN
arn:aws:iam::533267249366:user/rushikesh-29071

Created
July 05, 2024, 19:33 (UTC+05:30)

Console access
Enabled with MFA

Last console sign-in
Never

Access key 1
Create access key



user2-29071 Info

Summary

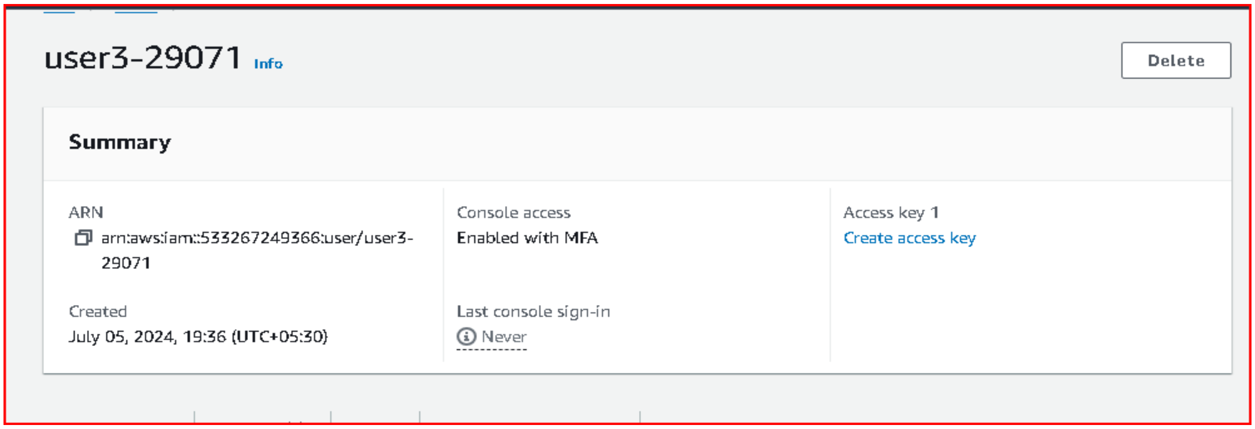
ARN
arn:aws:iam::533267249366:user/user2-29071

Created
July 05, 2024, 19:35 (UTC+05:30)

Console access
Enabled with MFA

Last console sign-in
Never

Access key 1
Create access key



user3-29071 Info

Summary

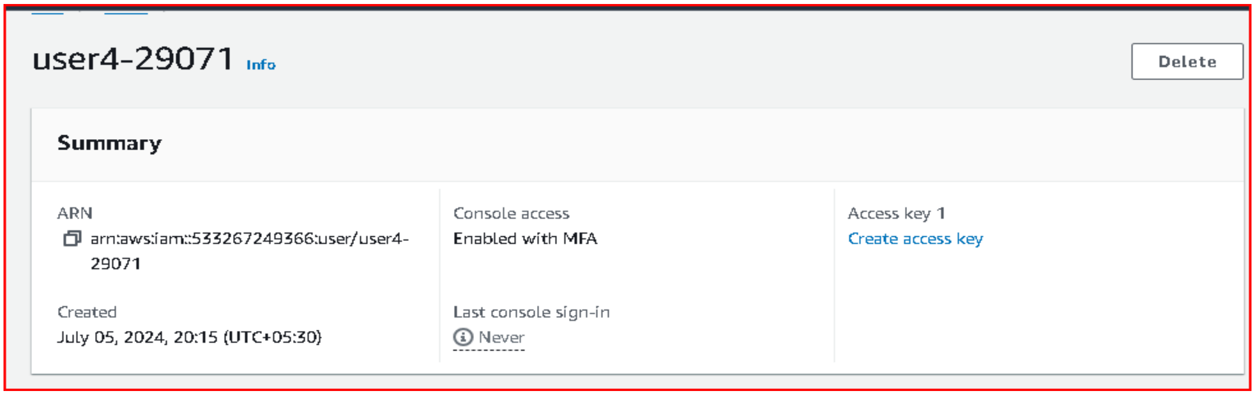
ARN
arn:aws:iam::533267249366:user/user3-29071

Created
July 05, 2024, 19:36 (UTC+05:30)

Console access
Enabled with MFA

Last console sign-in
Never

Access key 1
Create access key



user4-29071 Info

Delete

Summary

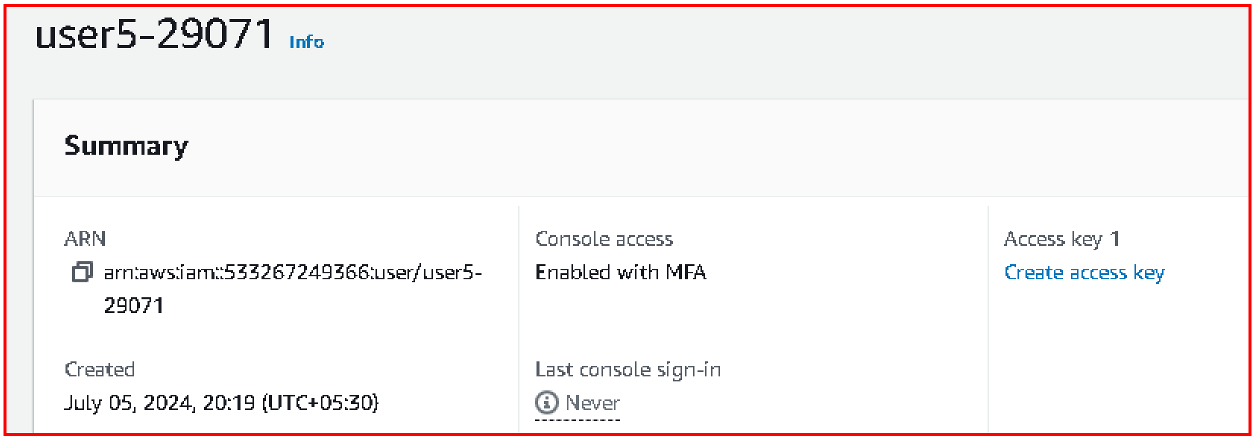
ARN
arn:aws:iam::533267249366:user/user4-29071

Created
July 05, 2024, 20:15 (UTC+05:30)

Console access
Enabled with MFA

Last console sign-in
Never

Access key 1
Create access key



user5-29071 Info

Summary

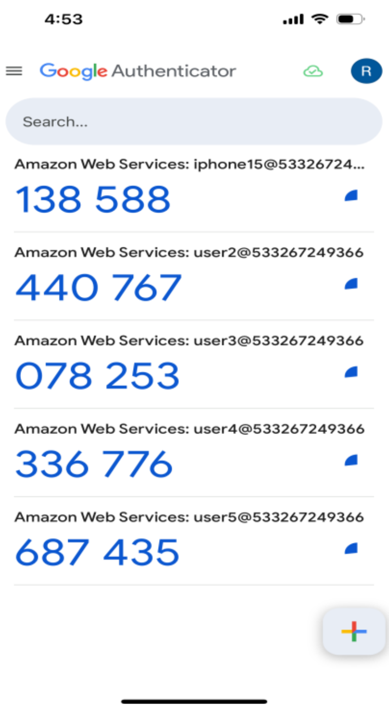
ARN
arn:aws:iam::533267249366:user/user5-29071

Created
July 05, 2024, 20:19 (UTC+05:30)

Console access
Enabled with MFA

Last console sign-in
Never

Access key 1
Create access key



4:53

Google Authenticator

R

Search...

Amazon Web Services: iphone15@53326724...
138 588

Amazon Web Services: user2@533267249366
440 767

Amazon Web Services: user3@533267249366
078 253

Amazon Web Services: user4@533267249366
336 776

Amazon Web Services: user5@533267249366
687 435

+

c. Create an IAM group named "EC2Management", “VPCManagement”.

Go to the IAM Management Console.

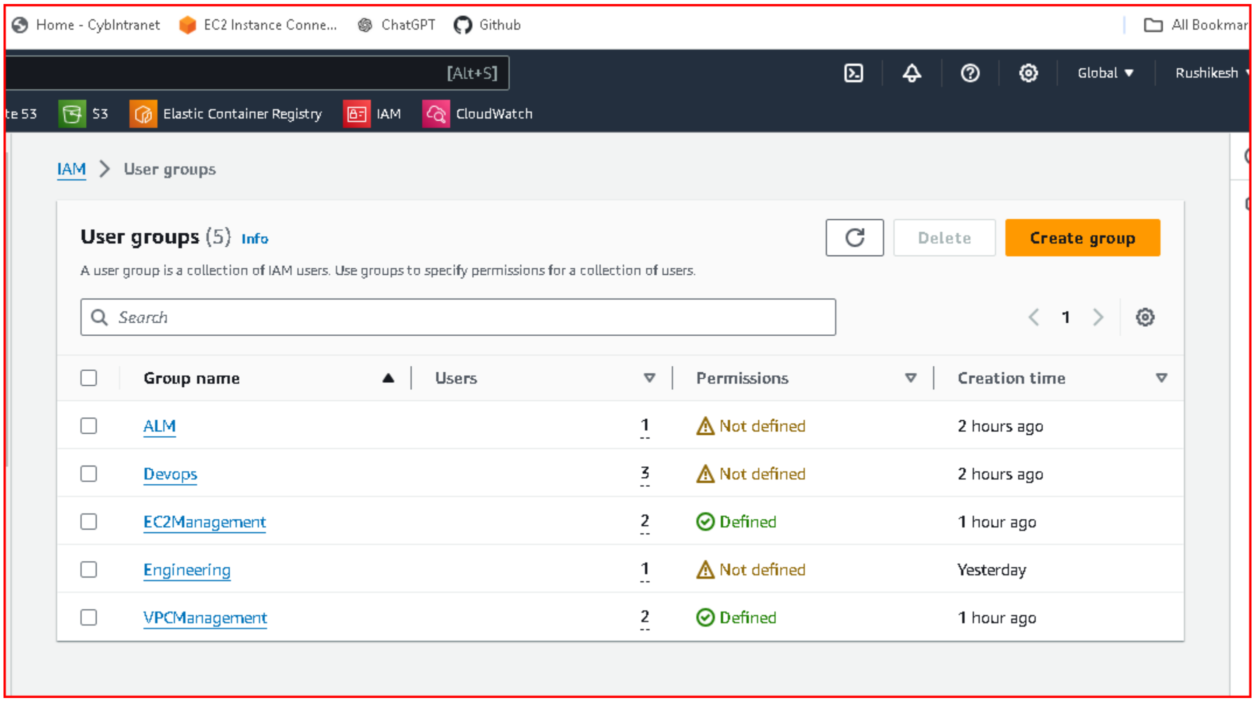
Click on Groups in the left navigation pane.

Click Create group.

Enter EC2Management as the Group name.

Click Next Step.

Review and click Create group



User groups (5) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

□	Group name ▲	Users	Permissions	Creation time
□	ALM	1	⚠ Not defined	2 hours ago
□	Devops	3	⚠ Not defined	2 hours ago
□	EC2Management	2	✓ Defined	1 hour ago
□	Engineering	1	⚠ Not defined	Yesterday
□	VPCManagement	2	✓ Defined	1 hour ago

d. After creating "EC2Management" group, add User 1 & User 2 to this group.

Go to the IAM Management Console.

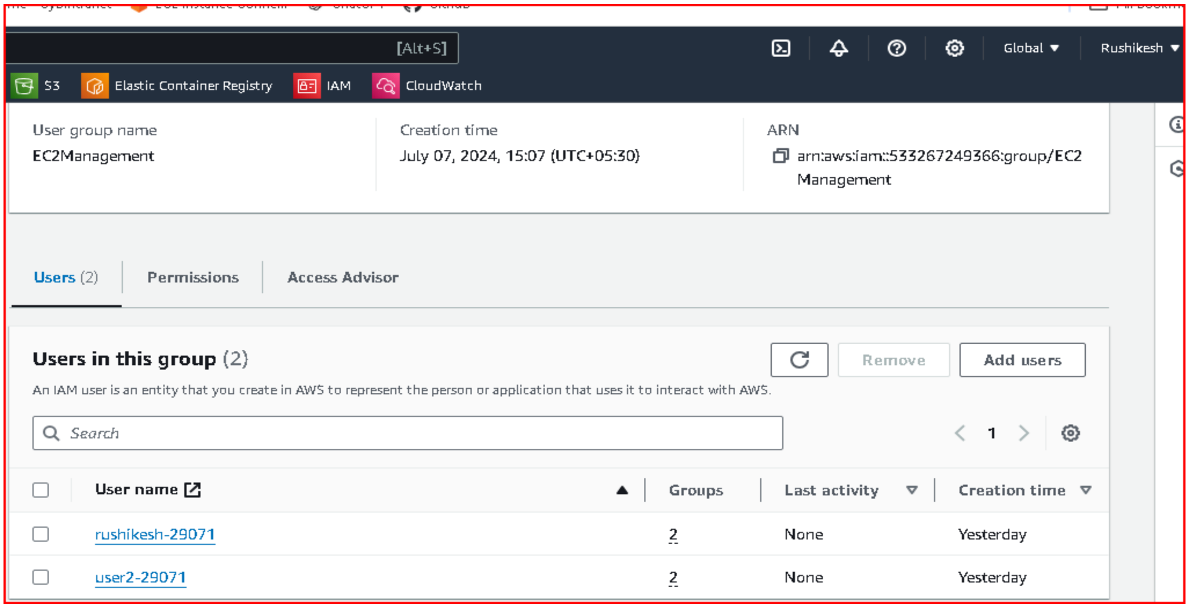
Click on Groups in the left navigation pane.

Click on the EC2Management group.

Click on the Add users to group button.

Check the boxes next to rushikesh_29071 and user2-29071

Click Add users.



User group name
EC2Management

Creation time
July 07, 2024, 15:07 (UTC+05:30)

ARN
arn:aws:iam::533267249366:group/EC2Management

Users in this group (2)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

□	User name	Groups	Last activity	Creation time
□	rushikesh-29071	2	None	Yesterday
□	user2-29071	2	None	Yesterday

e. User 3 and User 4 in “VPCManagement” group.

Go to the IAM Management Console.

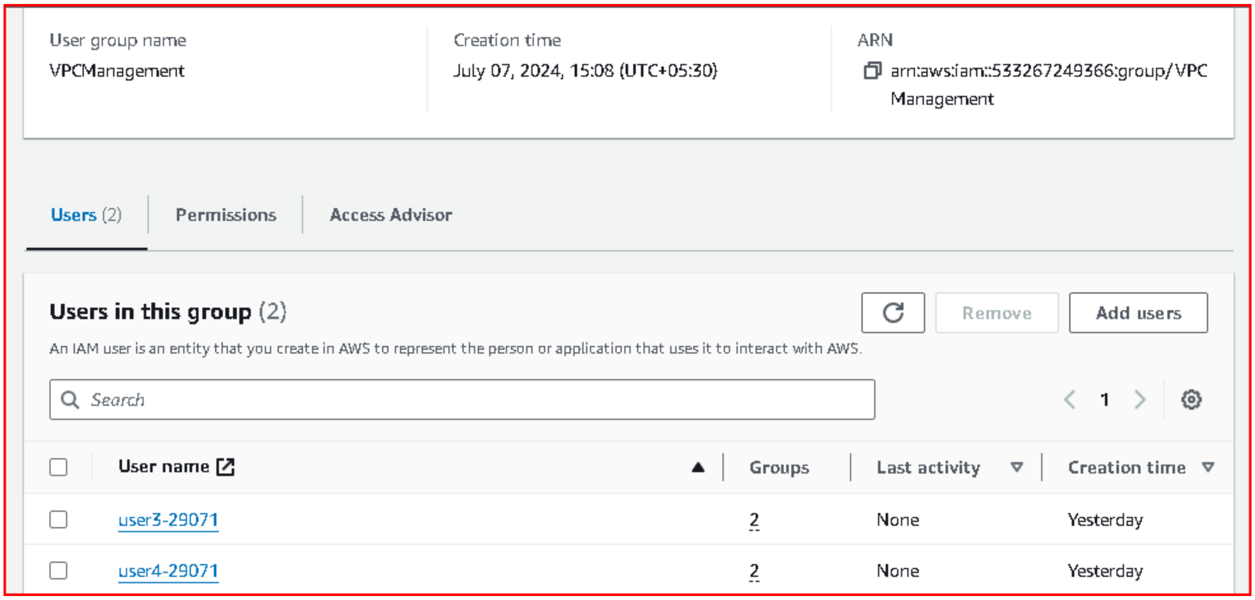
Click on Groups in the left navigation pane.

Click on the EC2Management group.

Click on the Add users to group button.

Check the boxes next to user3-29071 and user4-29071

Click Add users.



User group name
VPCManagement

Creation time
July 07, 2024, 15:08 (UTC+05:30)

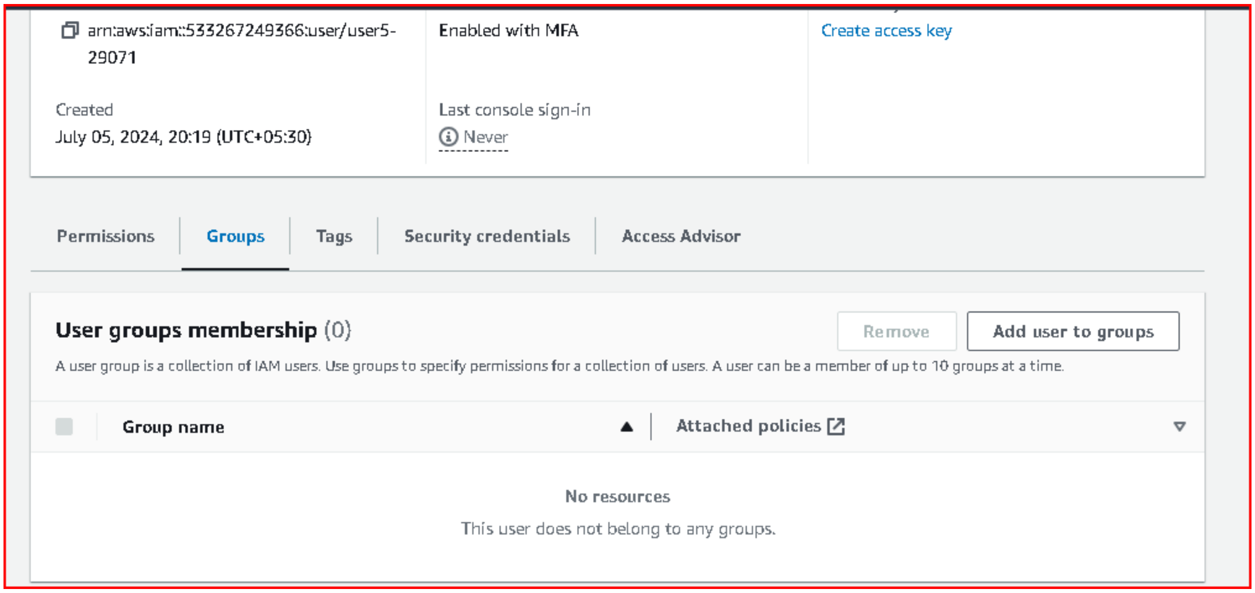
ARN
arn:aws:iam::533267249366:group/VPCManagement

Users in this group (2)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

□	User name	Groups	Last activity	Creation time
□	user3-29071	2	None	Yesterday
□	user4-29071	2	None	Yesterday

f. User 5 will not be part of any group.



arn:aws:iam::533267249366:user/user5-29071

Enabled with MFA

Created
July 05, 2024, 20:19 (UTC+05:30)

Last console sign-in
Never

User groups membership (0)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.

Group name	Attached policies

No resources
This user does not belong to any groups.

g. Create a policy for "EC2Management" group for creating & terminating EC2 instances

Go to the IAM Management Console: IAM Console.

Click on Policies in the left navigation pane.

Click Create policy.

Choose the visual editor tab.

Click Review policy.

Provide a name for the policy, e.g., EC2ManagementPolicy.

Optionally, add a description.

Click Create policy.

Attaching the Policy to the "EC2Management" Group

Go to the IAM Management Console.

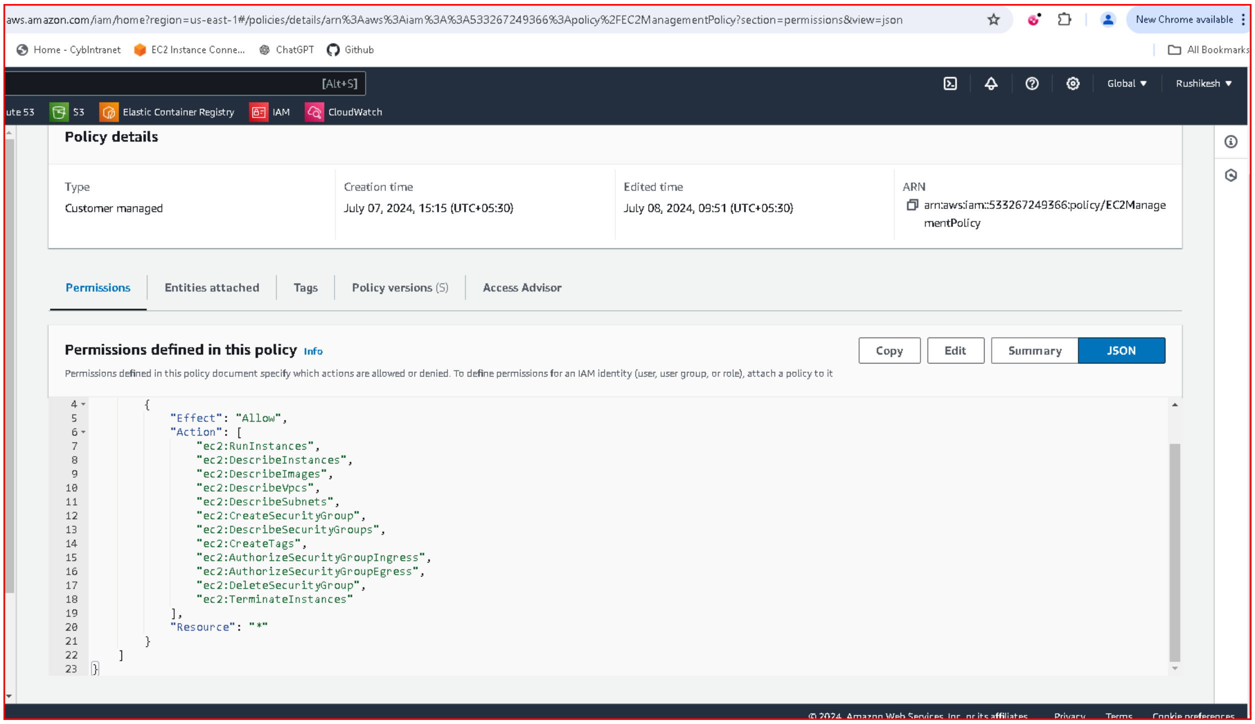
Click on Groups in the left navigation pane.

Click on the EC2Management group.

In the Permissions tab, click Attach policies.

Search for the policy you created (EC2ManagementPolicy).

Click Attach policy.


aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3A533267249366%3Apolicy%2FEC2ManagementPolicy?section=permissions&view=json
New Chrome available
Home - CybIntranet
EC2 Instance Conne...
ChatGPT
Github
All Bookmarks
[Alt+S]
Global ▼
Rushikesh ▼
ute 53
S3
Elastic Container Registry
IAM
CloudWatch

Policy details

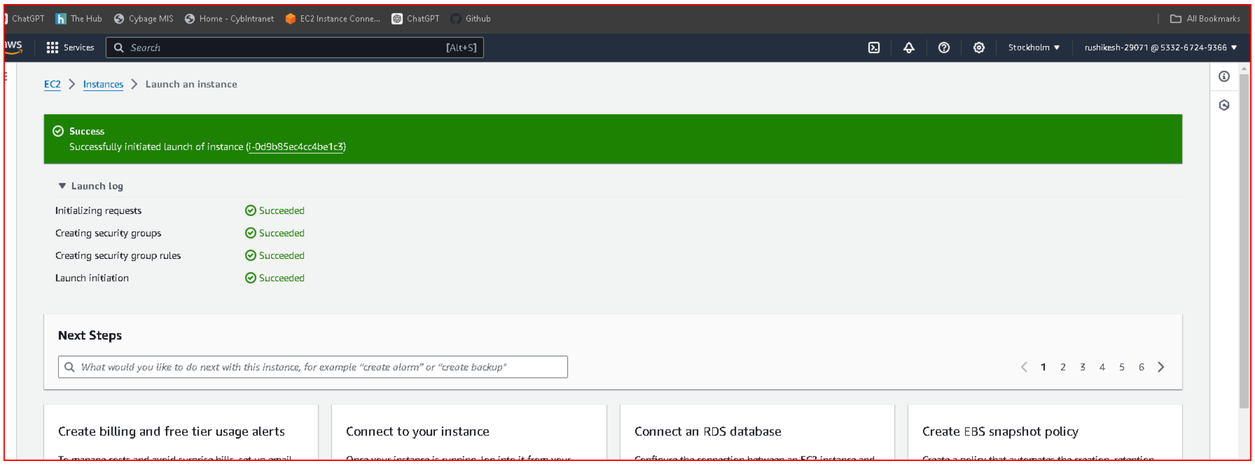
Type	Creation time	Edited time	ARN
Customer managed	July 07, 2024, 15:15 (UTC+05:30)	July 08, 2024, 09:51 (UTC+05:30)	arn:aws:iam::533267249366:policy/EC2ManagementPolicy

Permissions defined in this policy Info

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

```
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateTags",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


ChatGPT
The Hub
Cybage MIS
Home - CybIntranet
EC2 Instance Conne...
ChatGPT
Github
All Bookmarks
Services
Search
[Alt+S]
Stockholm ▼
rushikesh-29071 @ 5332-6724-9366 ▼
EC2 > Instances > Launch an instance

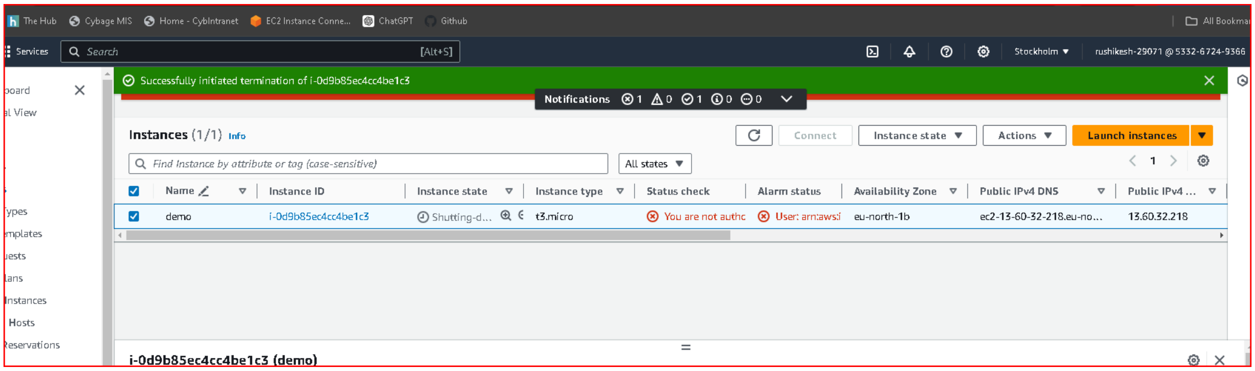
Success
Successfully initiated launch of instance (i-0d9b85ec4cc4be1c3)

▼ Launch log

Initializing requests	Succeeded
Creating security groups	Succeeded
Creating security group rules	Succeeded
Launch initiation	Succeeded

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"
1 2 3 4 5 6
Create billing and free tier usage alerts
Connect to your instance
Connect an RDS database
Create EBS snapshot policy

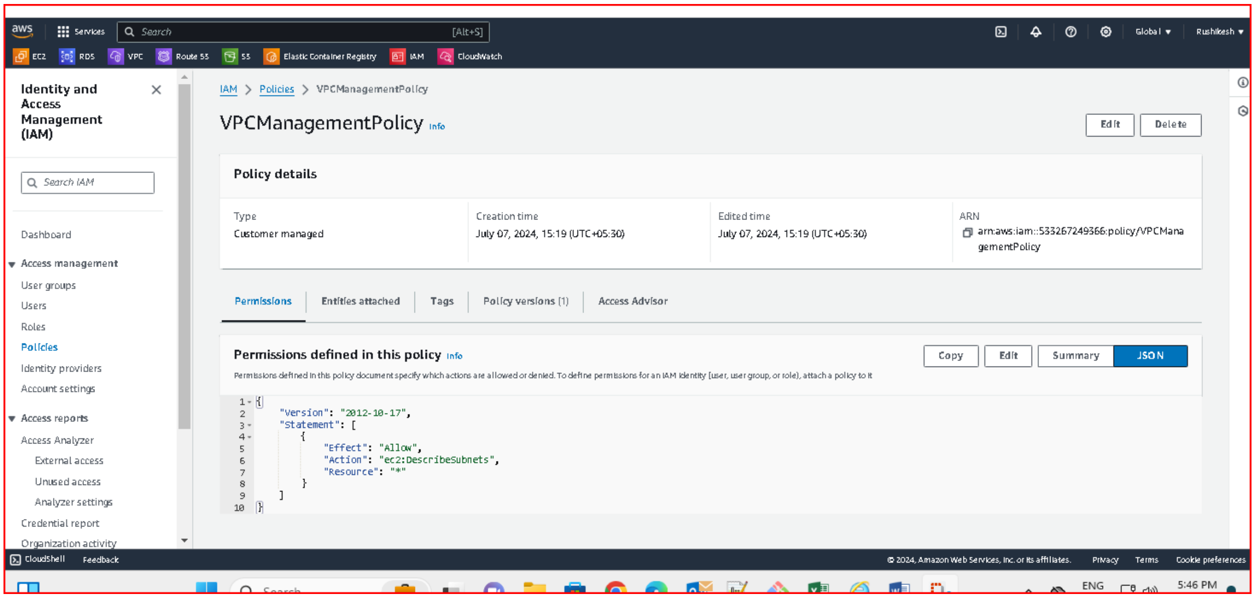


Successfully initiated termination of i-0d9b85ec4cc4be1c3

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
☑	demo	i-0d9b85ec4cc4be1c3	Shutting-d...	t3.micro	You are not authc	User: arn:aws:i	eu-north-1b	ec2-13-60-32-218.eu-no...	13.60.32.218

i-0d9b85ec4cc4be1c3 (demo)

h. Create a policy for " VPCManagement” group for only listing the Subnets in your account



VPCManagementPolicy Info

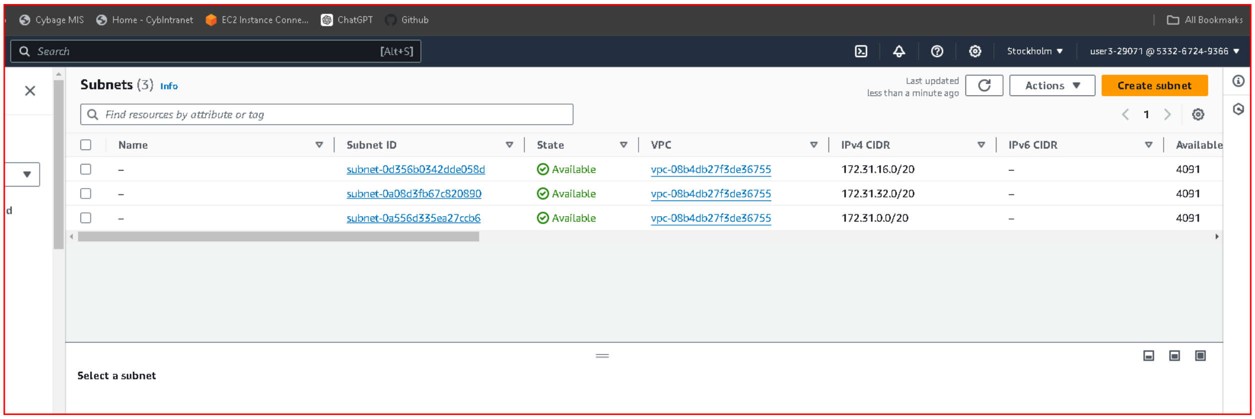
Policy details

Type	Creation time	Edited time	ARN
Customer managed	July 07, 2024, 15:19 (UTC+05:30)	July 07, 2024, 15:19 (UTC+05:30)	arn:aws:iam::533267249366:policy/VPCManagementPolicy

Permissions defined in this policy Info

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

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



Subnets (3) Info

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available
–	subnet-0d356b0342dde058d	Available	vpc-08b4db27f3de36755	172.31.16.0/20	–	4091
–	subnet-0a08d3fb67c820890	Available	vpc-08b4db27f3de36755	172.31.32.0/20	–	4091
–	subnet-0a556d335ea27ccb6	Available	vpc-08b4db27f3de36755	172.31.0.0/20	–	4091

Select a subnet

i. Create 1 Role for EC2 instance for accessing data from ECR(read-only)

A.

1. Navigate to the IAM Console:

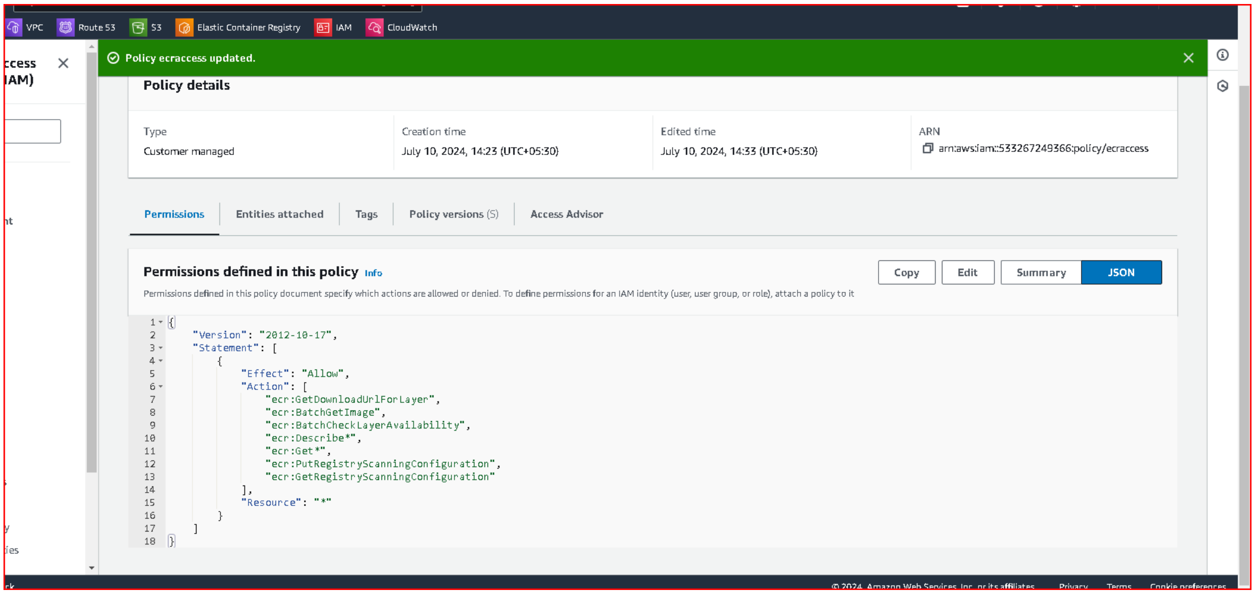
2. Create Policy:

Click on "Policies" in the left sidebar.

Click on "Create policy", then select the "JSON" tab.

3. Policy JSON:

Use the following JSON as a template for your policy



Policy ecraccess updated.

Policy details

Type: Customer managed

Creation time: July 10, 2024, 14:23 (UTC+05:30)

Edited time: July 10, 2024, 14:33 (UTC+05:30)

ARN: arn:aws:iam::533267249366:policy/ecraccess

Permissions defined in this policy Info

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecr:GetDownloadUrlForLayer",
                "ecr:BatchGetImage",
                "ecr:BatchCheckLayerAvailability",
                "ecr:Describe*",
                "ecr:Get*",
                "ecr:PutRegistryScanningConfiguration",
                "ecr:GetRegistryScanningConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

© 2024, Amazon Web Services, Inc. or its affiliates Privacy Terms Cookie preferences

Click Next: Review.

Click "Create policy".

B. Create an IAM Role for EC2 Instance

Now, create an IAM role that the EC2 instance will assume, with the policy you just created attached.

1. Navigate to Roles:

In the IAM Console, click on "Roles" in the left sidebar.

Click on Create role

2. Choose the service that will use this role:

Select "EC2" as the service that will use this role.

Click "Next: Permissions"

3. Attach Policies:

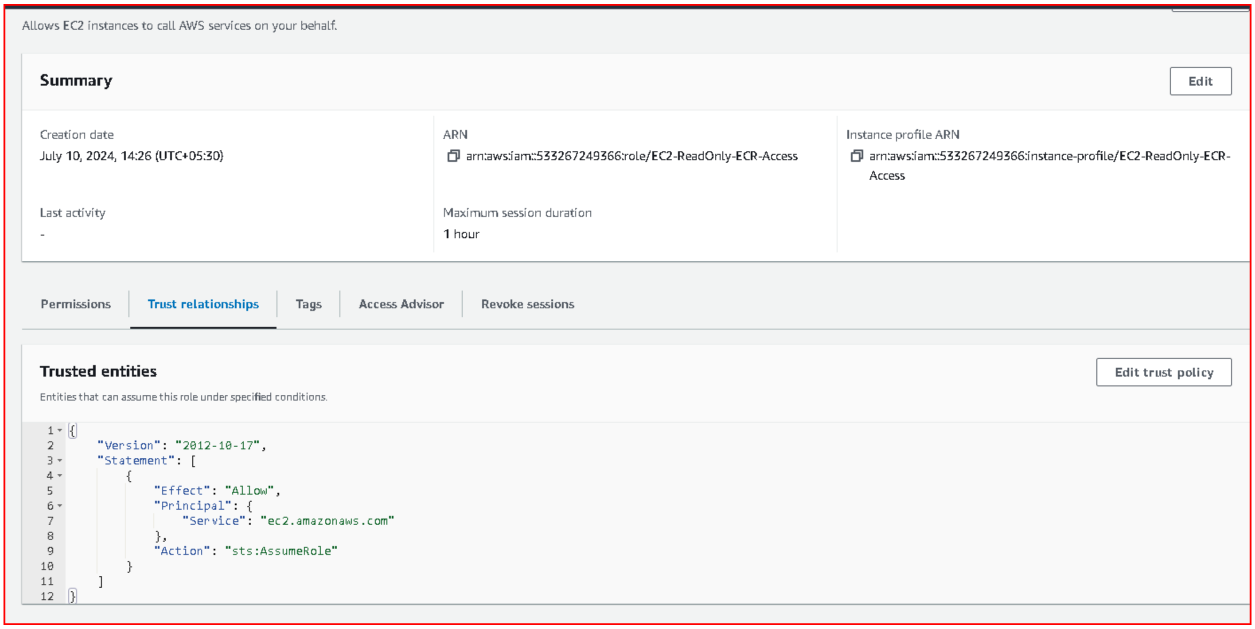
Search for and select the policy you created earlier

Click "Next: Tags" if you need to add tags. Otherwise, click "Next: Review".

4. Review and Create Role:

Provide a name and description for your role (e.g., `EC2-ReadOnly-ECR-Access`).

Click "Create role".



Allows EC2 instances to call AWS services on your behalf.

Summary

Creation date
July 10, 2024, 14:26 (UTC+05:30)

ARN
arn:aws:iam::533267249366:role/EC2-ReadOnly-ECR-Access

Instance profile ARN
arn:aws:iam::533267249366:instance-profile/EC2-ReadOnly-ECR-Access

Last activity
-

Maximum session duration
1 hour

Trusted entities

Entities that can assume this role under specified conditions.

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

C. Attach Role to EC2 Instance

Finally, attach the IAM role you created to your EC2 instance.

1. Navigate to EC2 Instances:

Go to the [EC2 Console](https://console.aws.amazon.com/ec2/).

2. Select Instance:

Select the instance to which you want to attach the role.

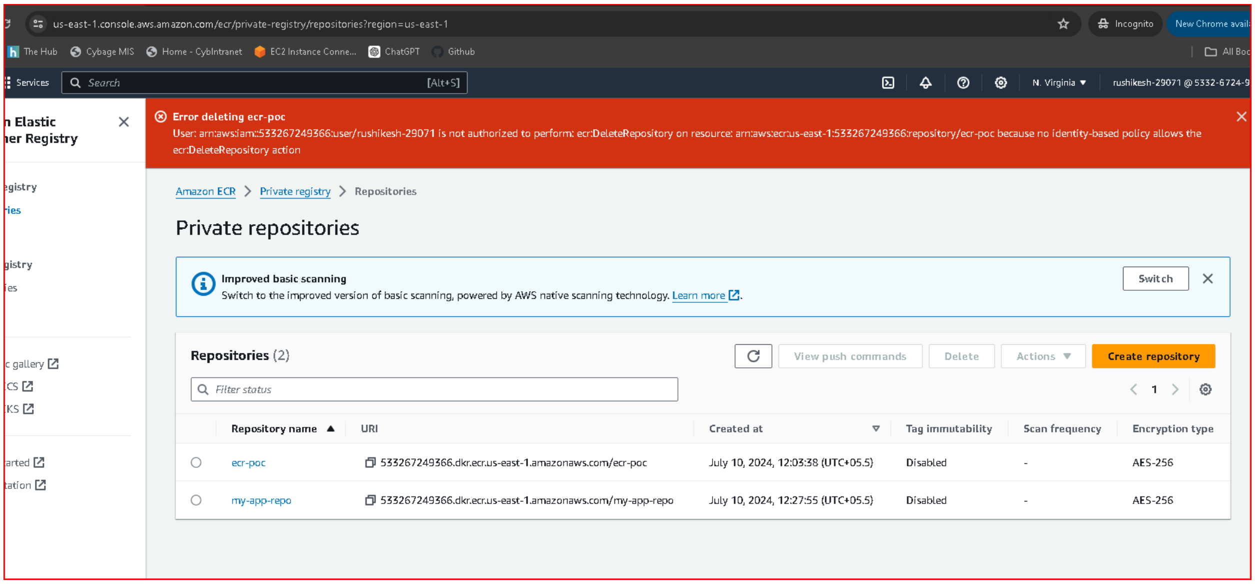
3. Attach IAM Role:

In the instance details pane, click on "Actions" -> "Security" -> "Modify IAM role".

Choose the IAM role you created (e.g., `EC2-ReadOnly-ECR-Access`).

Click "Apply".

We have read only access I cannot delete or edit the ecr repo created in root account.



us-east-1.console.aws.amazon.com/ecr/private-registry/repositories?region=us-east-1

Error deleting ecr-poc

User: arn:aws:iam::533267249366:user/rushikesh-29071 is not authorized to perform: ecr:DeleteRepository on resource: arn:aws:ecr:us-east-1:533267249366:repository/ecr-poc because no identity-based policy allows the ecr:DeleteRepository action

Amazon ECR > Private registry > Repositories

Private repositories

Improved basic scanning

Switch to the improved version of basic scanning, powered by AWS native scanning technology. Learn more.

Repositories (2)

	Repository name ▲	URI	Created at	Tag immutability	Scan frequency	Encryption type
○	ecr-poc	533267249366.dkr.ecr.us-east-1.amazonaws.com/ecr-poc	July 10, 2024, 12:03:38 (UTC+05.5)	Disabled	-	AES-256
○	my-app-repo	533267249366.dkr.ecr.us-east-1.amazonaws.com/my-app-repo	July 10, 2024, 12:27:55 (UTC+05.5)	Disabled	-	AES-256

j. Assume role for test-user and give read-only access to S3

Create an IAM Policy for Read-Only Access to S3

Navigate to IAM Policies:

Go to the AWS Management Console.

Search for and click on "IAM" under "Security, Identity, & Compliance".

Create Policy:

Click on "Policies" in the left-hand menu.

Click on "Create policy".

Policy Configuration:

Choose the "JSON" tab.

Review Policy:

Click on "Review policy".

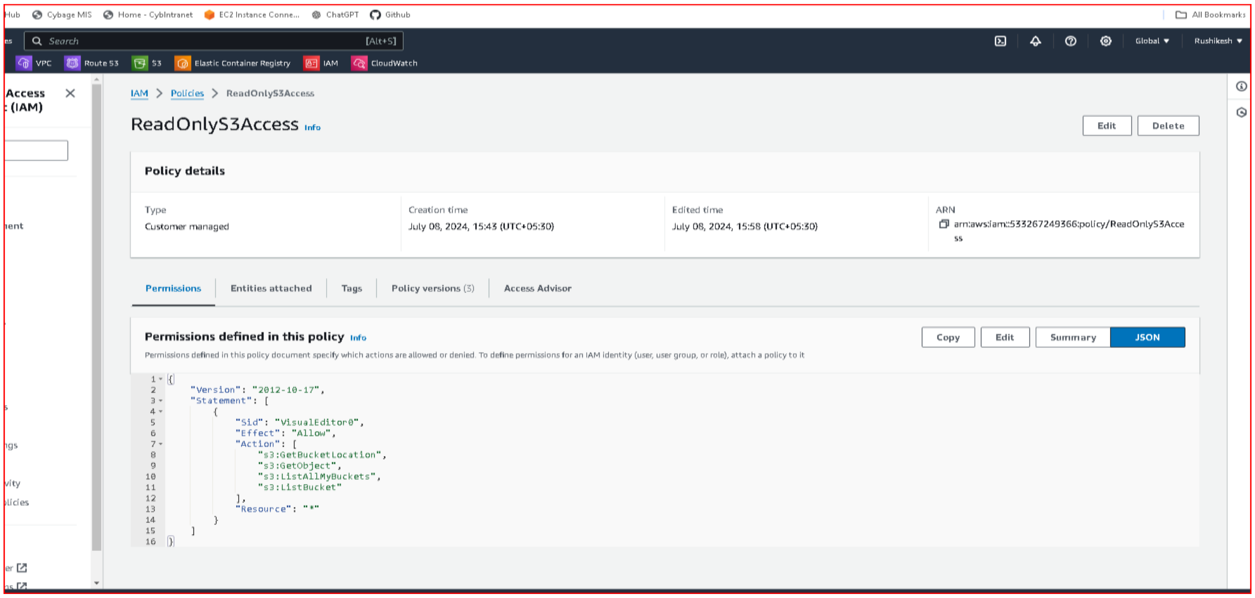
Name your policy (e.g., ReadOnlyS3AccessPolicy).

Optionally, provide a description.

Click on "Create policy".

Attach this policy to user5

login using user5 and check the list of buckets



ReadOnlyS3Access

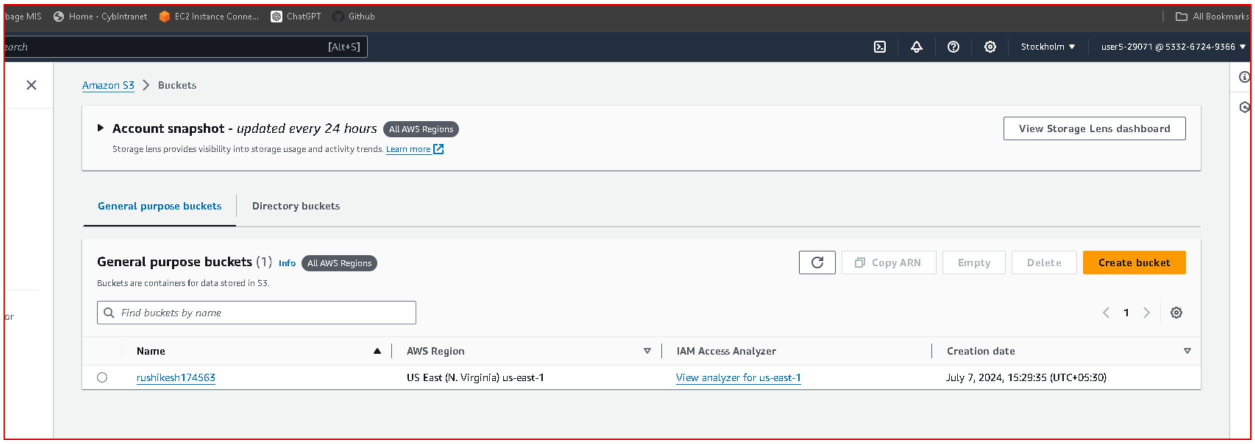
Policy details

Type	Creation time	Edited time	ARN
Customer managed	July 08, 2024, 15:43 (UTC+05:30)	July 08, 2024, 15:58 (UTC+05:30)	arn:aws:iam::533267249366:policy/ReadOnlyS3Access

Permissions defined in this policy

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetObject",
                "s3:ListAllMyBuckets",
                "s3:ListBucket"
            ],
            "Resource": "*"
        }
    ]
}
```



Account snapshot - *updated every 24 hours*

Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (1)

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	rushikesh174563	US East (N. Virginia) us-east-1	View analyzer for us-east-1	July 7, 2024, 15:29:35 (UTC+05:30)

Session has been expired after 1 hour

1. Write a policy to restrict EC2 instance creation to t2.micro and t2.medium instances

Go to the AWS Management Console and navigate to the IAM service.

In the left sidebar, click on "Policies" and then click on the "Create policy" button.

Select the "visual editor" tab to switch to the visual editor mode.

Action: ec2:RunInstances is denied.

Resource: All EC2 instance resources (arn:aws:ec2:*:*:instance/*).

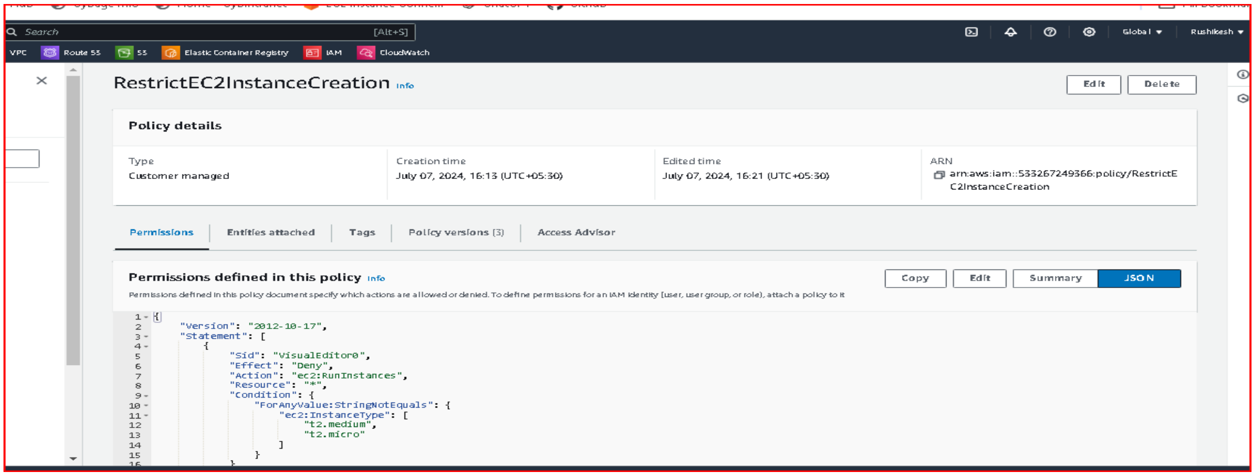
Condition: Allows only t2.micro and t2.medium instance types.

Click on the "Review policy" button.

Provide a name for the policy (e.g., RestrictEC2InstanceCreationToT2MicroAndT2Medium).

Optionally, you can provide a description for the policy.

Click on the "Create policy" button to save the policy.



RestrictEC2InstanceCreation Info

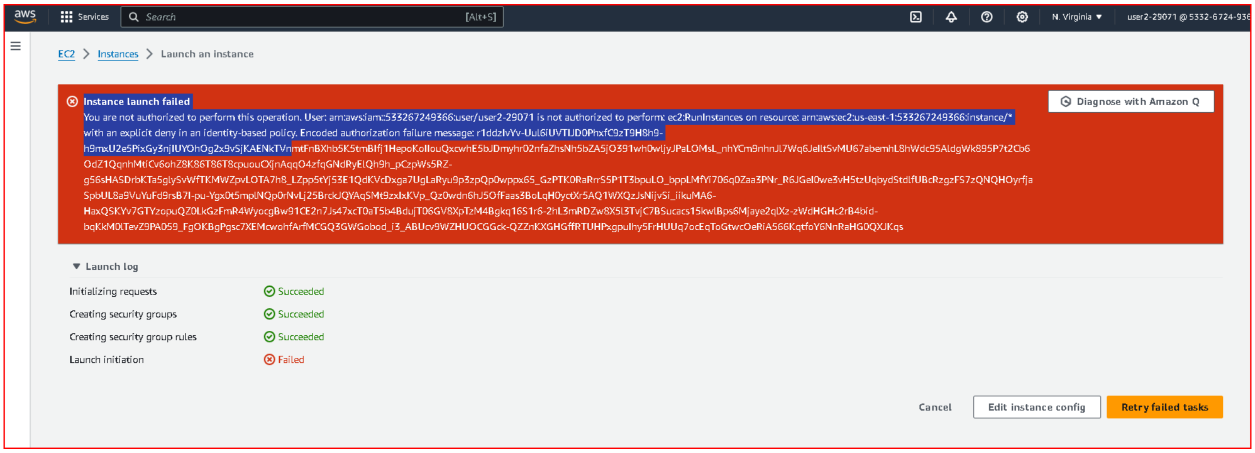
Policy details

Type	Creation time	Edited time	ARN
Customer managed	July 07, 2024, 16:13 (UTC+05:30)	July 07, 2024, 16:21 (UTC+05:30)	arn:aws:iam::533267249366:policy/RestrictEC2InstanceCreation

Permissions defined in this policy Info

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "ec2:InstanceType": [
                        "t2.medium",
                        "t2.micro"
                    ]
                }
            }
```



aws
Services
Search [Alt+S]
N. Virginia ▾
user2-29071 @ 5332-6724-936
EC2 > Instances > Launch an instance
Diagnose with Amazon Q

Instance launch failed

You are not authorized to perform this operation. User: arn:aws:iam::533267249366:user/user2-29071 is not authorized to perform: ec2:RunInstances on resource: arn:aws:ec2:us-east-1:533267249366:instance/* with an explicit deny in an identity-based policy. Encoded authorization failure message: r1ddzIvYv-UuL6iUVTIJD0PhxfC9zT9H8h9-
h9mxU2e5PixGy3njIUYOhOg2x9vSjKAENkTVnmtFnBXhb5K5tmBIfj1HepoKoIIouQxcwhE5bJDmyhr02nfaZhsNh5bZA5jO391wh0wljyJPaLOMsL_nhYCm9nhnJl7Wq6JeIltSvMU67abemhL8hWdc95AldgWk895P7t2Cb6
OdZ1QqnhMtiCv6ohZ8K86T86T8cpuouCXjnAqqO4zfqGNdRyElQh9h_pCzpWs5RZ-
g56sHASDrbKTa5glySvWfTKMWZpvLOTA7h8_LZpp5tYj53E1QdKVcDxga7UgLaRyu9p3zpQp0wppx65_GzPTK0RaRrrS5P1T3bpuLO_bppLMfYi706q0Zaa3PNr_R6JGeI0we3vH5tzUqbydStdlfUBcRzgzFS7zQNQHOyrfja
SpbUL8a9VuYuFd9rsB7I-pu-Ygx0t5mplNQp0rNvLj25BrckJQYAqSMt9zxIxKVp_Qz0wdn6hJ5OfFaas3BoLqH0yctXr5AQ1WXQzJsNijvSi_iikuMA6-
HaxQSKYv7GTYzopuQZ0LkGzFmR4WyocgBw91CE2n7Js47xcT0aT5b4BdujT06GV8XpTzM4Bgkq16S1r6-2hL3mRDZw8X5l3TvjC7BSucacs15kwlBps6Mjaye2qlXz-zWdHGHc2rB4bid-
bqKkM0lTevZ9PA059_FgOKBgPgsc7XEMcwohfArfMCGQ3GWGobod_i3_ABUcv9WZHUOCGGck-QZZnKXGHGffRTUHPxgpulhy5FrHUUq7ocEqToGtwcOeRiA566KqtfoY6NnRaHG0QXJKqs

▼ Launch log

Initializing requests	✓ Succeeded
Creating security groups	✓ Succeeded
Creating security group rules	✓ Succeeded
Launch initiation	⊗ Failed

2. Write an IAM Policy to Restrict EKS Node Creation to t3.medium Instances

Go to the AWS Management Console and navigate to the IAM service.

In the left sidebar, click on "Policies" and then click on the "Create policy" button.

Select the "visual editor" tab to switch to the visual editor mode.

Action: eks:CreateNodegroup is denied.

Resource: All EKS Nodegroup resources (*).

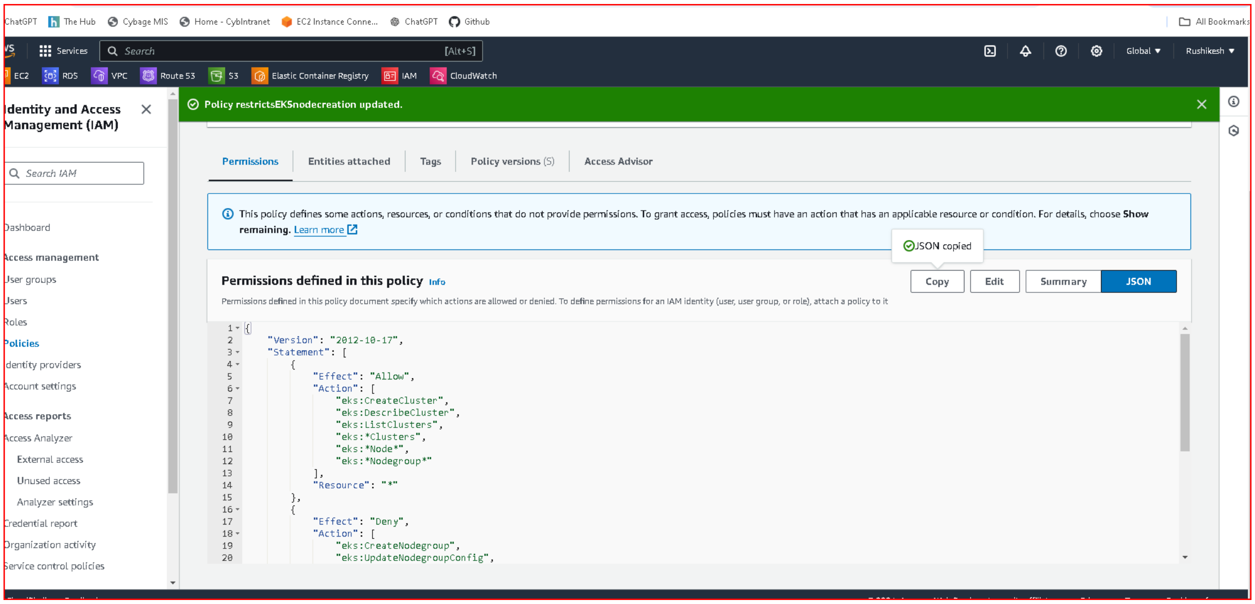
Condition: Allows only t3.medium instance types.

Click on the "Review policy" button.

Provide a name for the policy (e.g., RestrictEKSNodeCreationToT3Medium).

Optionally, you can provide a description for the policy.

Click on the "Create policy" button to save the policy.



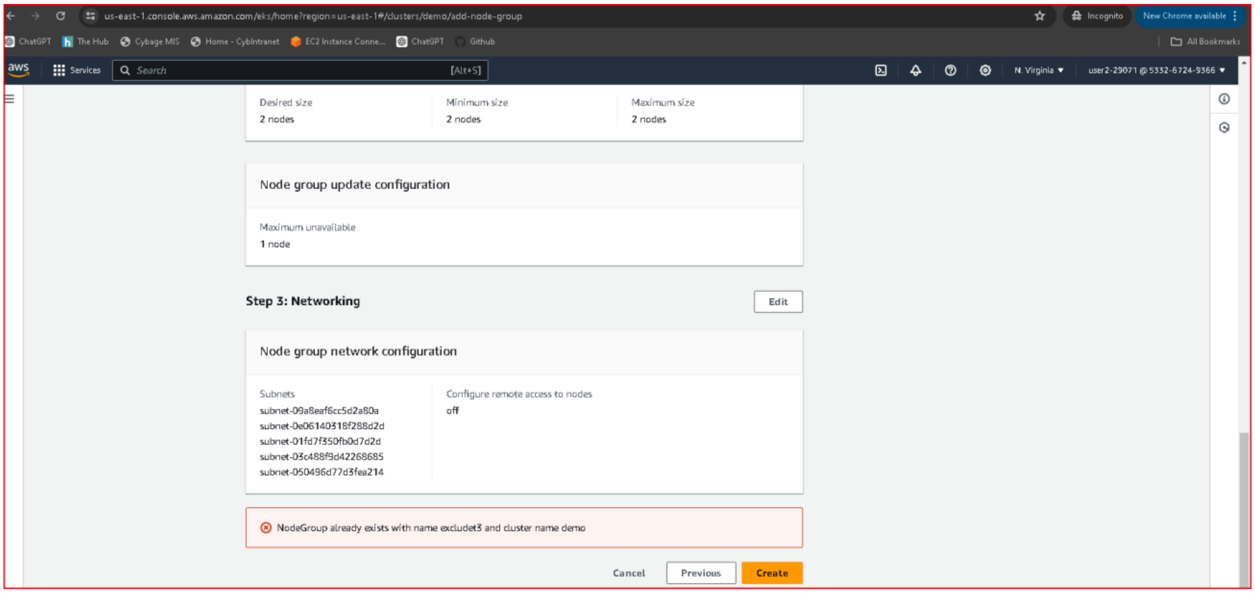
Policy restrictsEKSnodecreation updated.

This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose **Show remaining.** Learn more

Permissions defined in this policy

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "eks:CreateCluster",
                "eks:DescribeCluster",
                "eks:ListClusters",
                "eks:*Clusters",
                "eks:*Node*",
                "eks:*Nodegroup*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "eks:CreateNodegroup",
                "eks:UpdateNodegroupConfig",
```



Desired size	Minimum size	Maximum size
2 nodes	2 nodes	2 nodes

Node group update configuration

Maximum unavailable
1 node

Step 3: Networking

Node group network configuration

Subnets	Configure remote access to nodes
subnet-09a8eaf6cc5d2a80a subnet-0e06140318f288d2d subnet-01fd7f350fb0d7d2d subnet-03c488f9d42268685 subnet-050496d77d3fea214	off

NodeGroup already exists with name excludet3 and cluster name demo

3. Write an IAM Policy to Limit RDS Database Creation to db.t3.micro Instances

Go to the AWS Management Console and navigate to the IAM service.

In the left sidebar, click on "Policies" and then click on the "Create policy" button.

Select the "visual editor" tab to switch to the visual editor mode.

Action: rds:CreateDBInstance is denied.

Resource: All RDS DB instance resources (*).

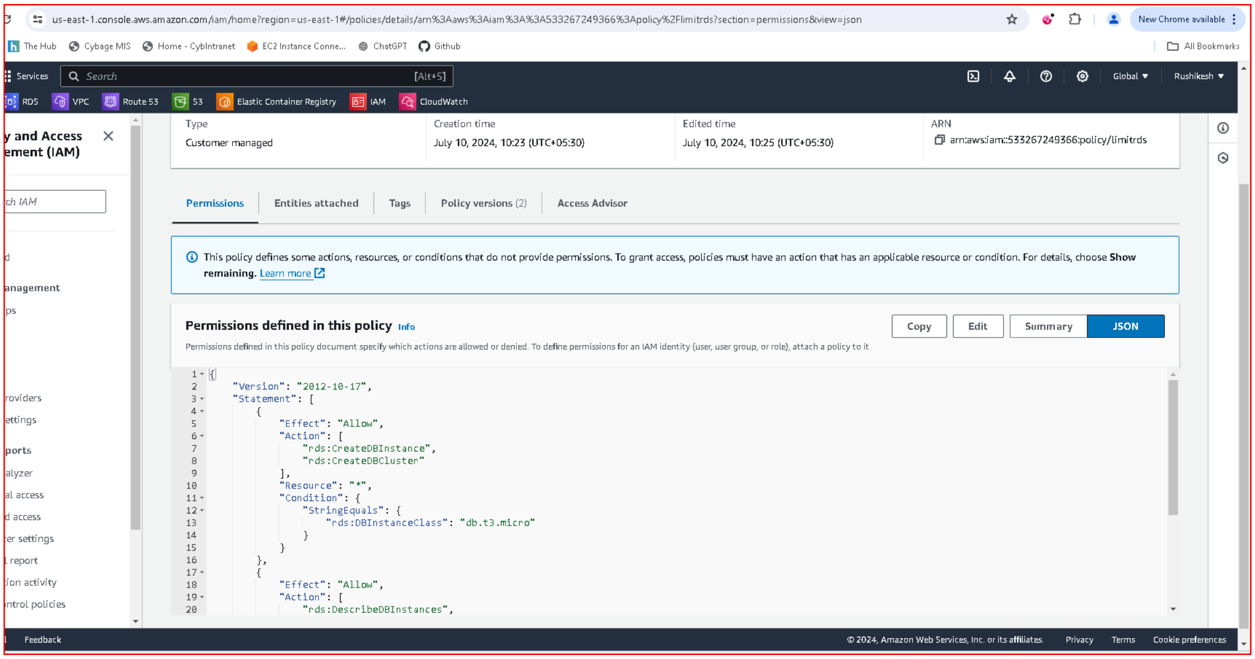
Condition: Allows only db.t3.micro database classes.

Click on the "Review policy" button.

Provide a name for the policy (e.g., LimitRDSDatabaseCreationToDbT3Micro).

Optionally, you can provide a description for the policy.

Click on the "Create policy" button to save the policy.



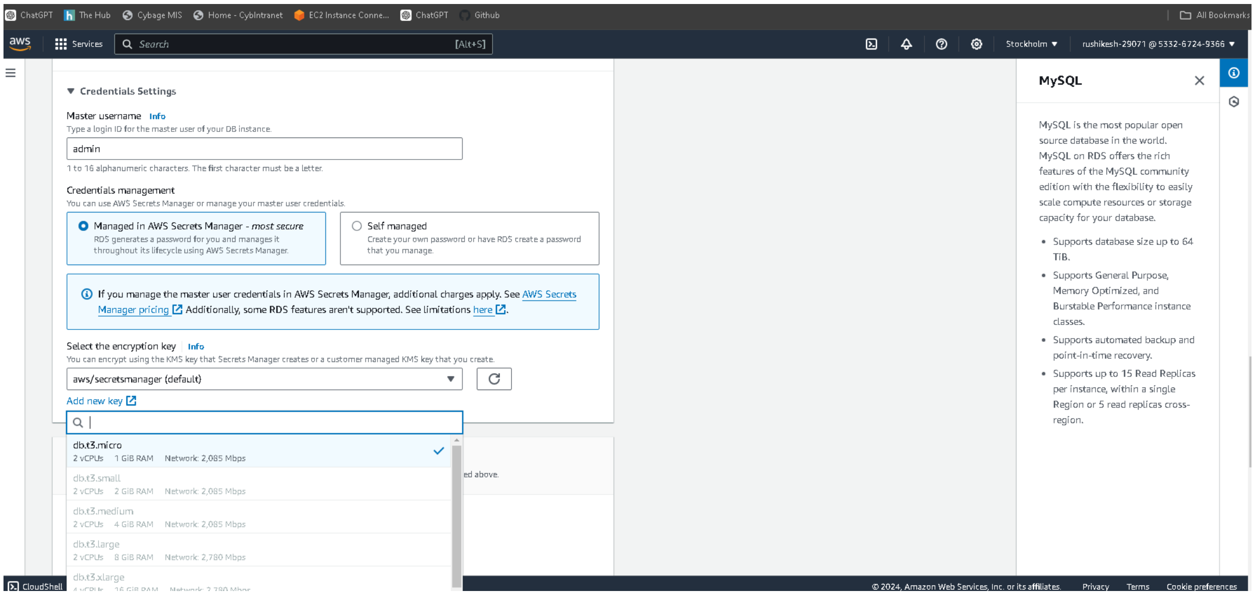
Type	Creation time	Edited time	ARN
Customer managed	July 10, 2024, 10:23 (UTC+05:30)	July 10, 2024, 10:25 (UTC+05:30)	arn:aws:iam::533267249366:policy/limitrds

This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose **Show remaining.** Learn more

Permissions defined in this policy Info

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "rds:CreateDBInstance",
                "rds:CreateDBCluster"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "rds:DBInstanceClass": "db.t3.micro"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances",
```



▼ **Credentials Settings**

Master username Info

Type a login ID for the master user of your DB instance.

admin

1 to 16 alphanumeric characters. The first character must be a letter.

Credentials management

You can use AWS Secrets Manager or manage your master user credentials.

● Managed in AWS Secrets Manager - *most secure*
RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.

○ Self managed
Create your own password or have RDS create a password that you manage.

If you manage the master user credentials in AWS Secrets Manager, additional charges apply. See AWS Secrets Manager pricing Additionally, some RDS features aren't supported. See limitations here.

Select the encryption key Info

You can encrypt using the KMS key that Secrets Manager creates or a customer managed KMS key that you create.

aws/secretsmanager (default) ▼

Add new key

db.t3.micro ✓
2 vCPUs 1 GiB RAM Network: 2,085 Mbps

db.t3.small
2 vCPUs 2 GiB RAM Network: 2,085 Mbps

db.t3.medium
2 vCPUs 4 GiB RAM Network: 2,085 Mbps

db.t3.large
2 vCPUs 8 GiB RAM Network: 2,780 Mbps

db.t3.xlarge
4 vCPUs 16 GiB RAM Network: 2,780 Mbps

ed above.

MySQL

MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.

- Supports database size up to 64 TiB.
- Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
- Supports automated backup and point-in-time recovery.
- Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.

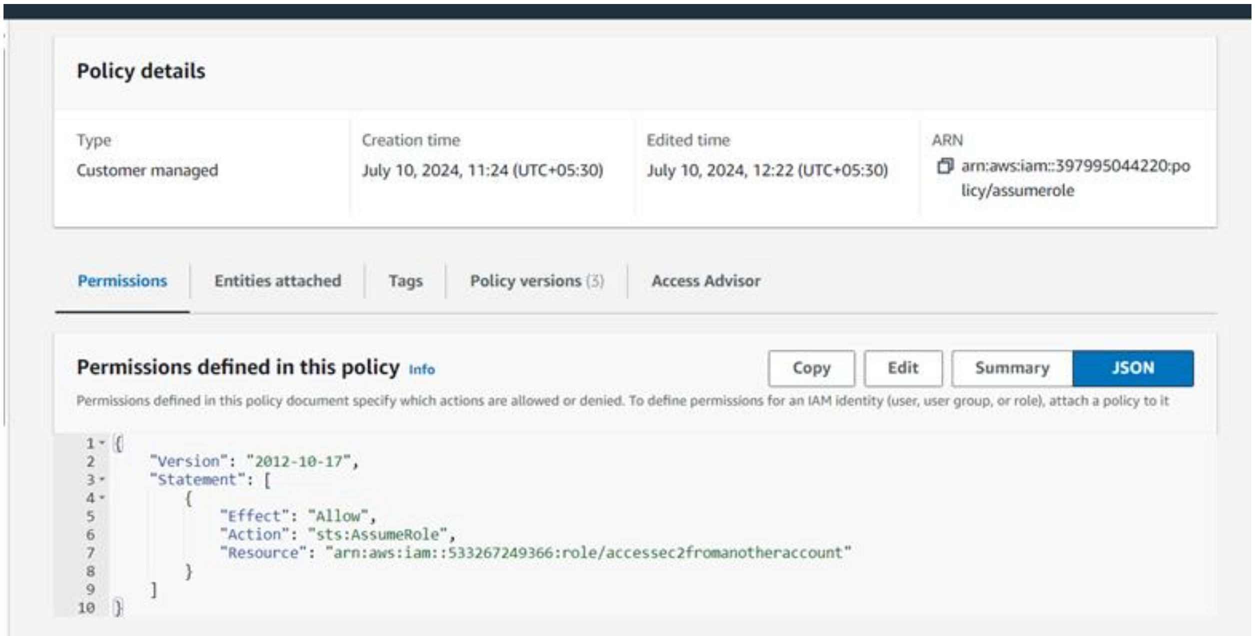
4. Write IAM Policies for accessing EC2 instance from another account.(AssumeRole - cross account)

Create an IAM Policy:

Click on Policies in the left navigation pane.

Click Create policy.

Choose the visual editor and enter a policy that allows assuming the role (accessEc2FromAnotherAccount) in your AWS account:



Policy details

Type	Creation time	Edited time	ARN
Customer managed	July 10, 2024, 11:24 (UTC+05:30)	July 10, 2024, 12:22 (UTC+05:30)	arn:aws:iam::397995044220:policy/assumerole

Permissions defined in this policy Info

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::533267249366:role/accessec2fromanotheraccount"
        }
    ]
}
```

Attach the IAM Policy to the karan1_29221 IAM User:

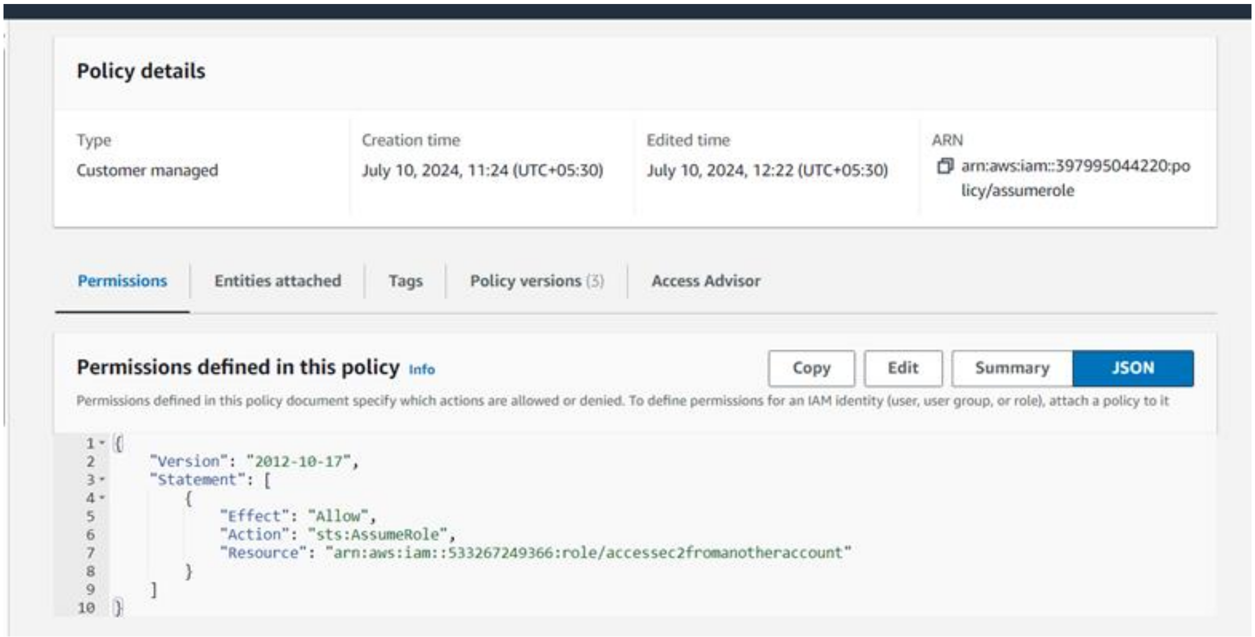
Navigate to Users in the IAM console.

Click on the karan1_29221 user to view its details.

Click on the Add permissions button or Attach policies.

Search for and select the IAM policy you just created.

Click Attach policy to attach the policy to the karan1_29221 IAM user.



Policy details

Type	Creation time	Edited time	ARN
Customer managed	July 10, 2024, 11:24 (UTC+05:30)	July 10, 2024, 12:22 (UTC+05:30)	arn:aws:iam::397995044220:policy/assumerole

Permissions defined in this policy

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::533267249366:role/accessec2fromanotheraccount"
        }
    ]
}
```

Sign in as karan1_29221:

Sign in to the AWS Management Console using the credentials of the karan1_29221 IAM user.

Switch Roles:

Navigate to the IAM console: https://console.aws.amazon.com/iam/

Click on Roles in the left navigation pane.

Search for and click on the accessEc2FromAnotherAccount role.

Click Switch Role.

Enter your AWS account ID and the ARN of the role (accessEc2FromAnotherAccount) in your AWS account.

Click Switch Role.