Module - 3

1. IAM Users Assignment

Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

Tasks to be Performed:

1. Create 4 IAM users named “Dev1”, “Dev2”, “Test1”, and “Test2”.

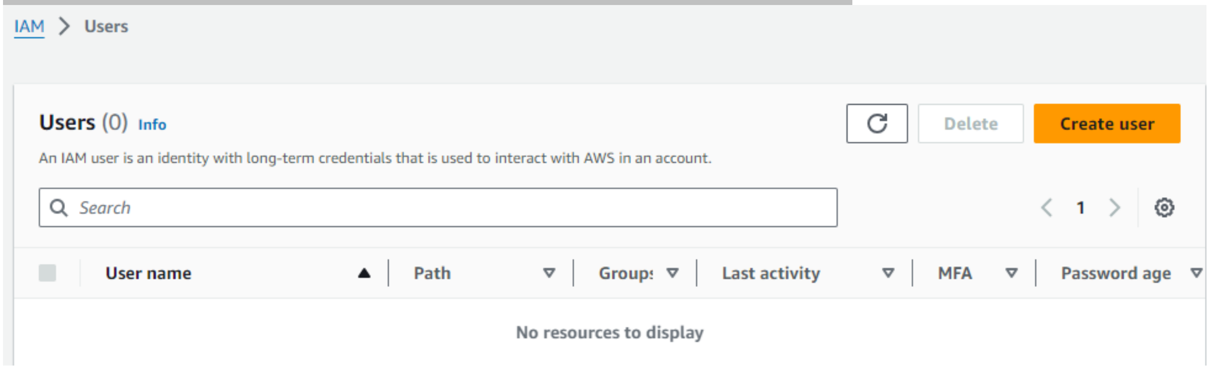
2. Create 2 groups named “Dev Team” and “Ops Team”.

3. Add Dev1 and Dev2 to the Dev Team.

4. Add Dev1, Test1 and Test2 to the Ops Team.

Solution:

Creating 4 IAM user, IAM console > Users > Create Users



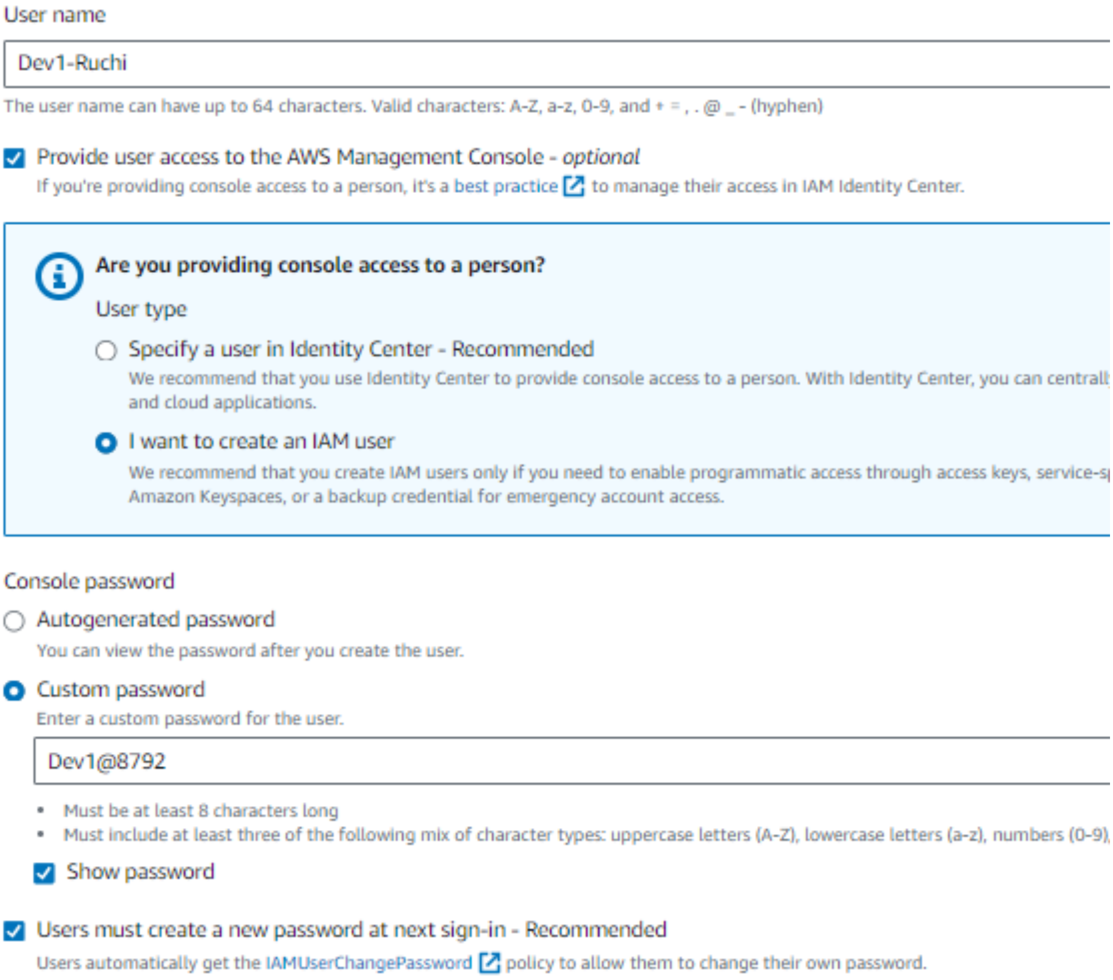
Users (0) Info

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

No resources to display

Provide the details according to the Assignment and provide user access



User name

Dev1-Ruchi

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.

Are you providing console access to a person?

User type

○ Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrall and cloud applications.

● I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-s Amazon Keyspaces, or a backup credential for emergency account access.

Console password

○ Autogenerated password

You can view the password after you create the user.

● Custom password

Enter a custom password for the user.

Dev1@8792

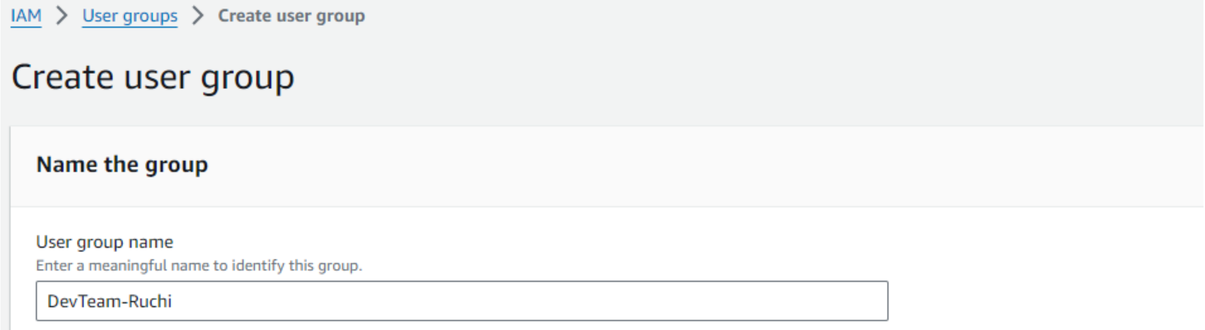
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9),

☑ Show password

☑ Users must create a new password at next sign-in - Recommended

Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

Create 2 Groups for Dev and Ops Team and add the User to the Group.



IAM > User groups > Create user group

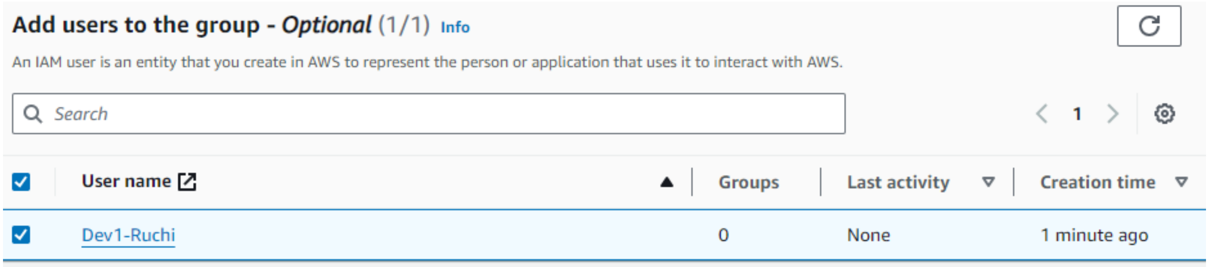
Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

DevTeam-Ruchi

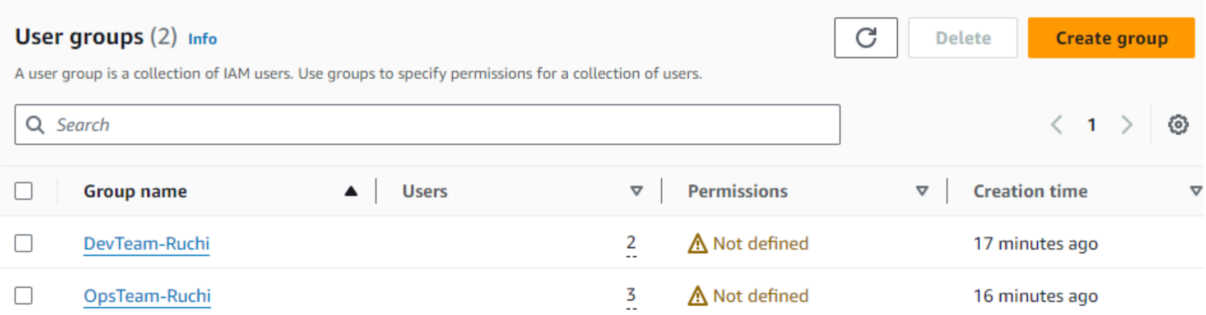


Add users to the group - ***Optional*** (1/1) Info

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
☑	Dev1-Ruchi	0	None	1 minute ago

Created 2 groups named “Dev Team” and “Ops Team”

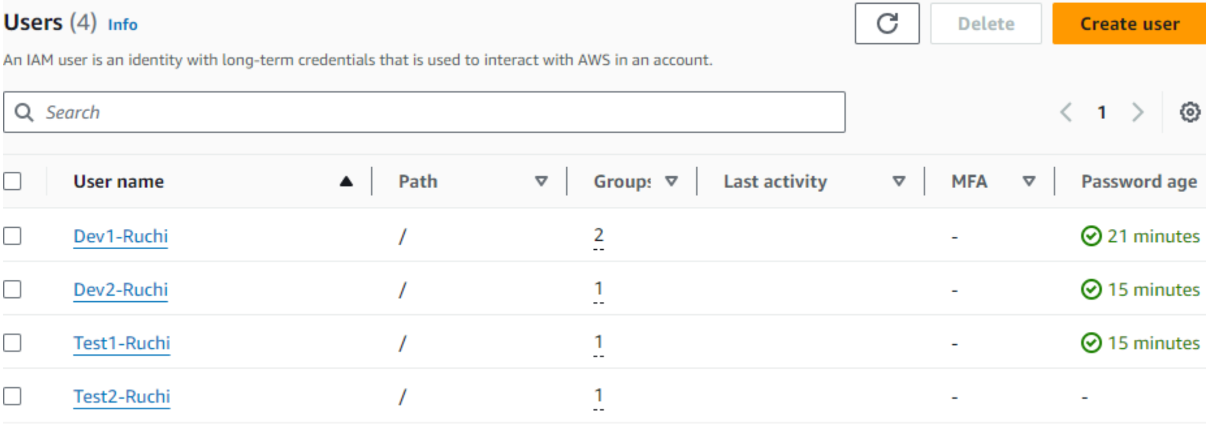


User groups (2) Info

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
□	DevTeam-Ruchi	2	⚠ Not defined	17 minutes ago
□	OpsTeam-Ruchi	3	⚠ Not defined	16 minutes ago

Similarly, Created all 4 IAM users named “Dev1”, “Dev2”, “Test1”, and “Test2” and Attached them to the mentioned Groups.



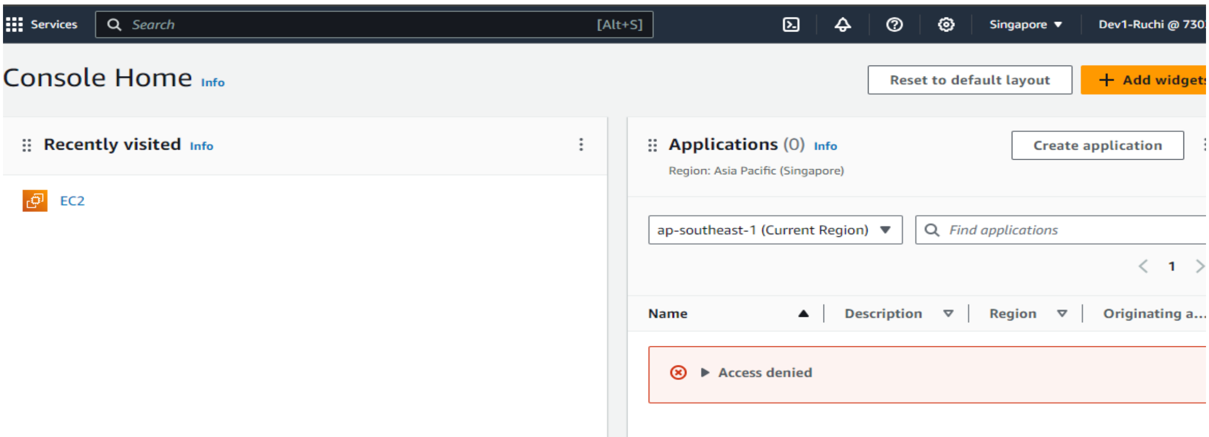
Users (4) Info

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

□	User name	Path	Group:	Last activity	MFA	Password age
□	Dev1-Ruchi	/	2		-	✓ 21 minutes
□	Dev2-Ruchi	/	1		-	✓ 15 minutes
□	Test1-Ruchi	/	1		-	✓ 15 minutes
□	Test2-Ruchi	/	1		-	-

Now sign in to a IAM user account, Dev1-Ruchi with a credentials

But the access is denied as there are no permission policies



Access denied

2. IAM Policies Assignment

Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

Tasks to be Performed:

1. Create policy number 1 which lets the users to:
   a. Access S3 completely
   b. Only create EC2 instances
   c. Full access to RDS

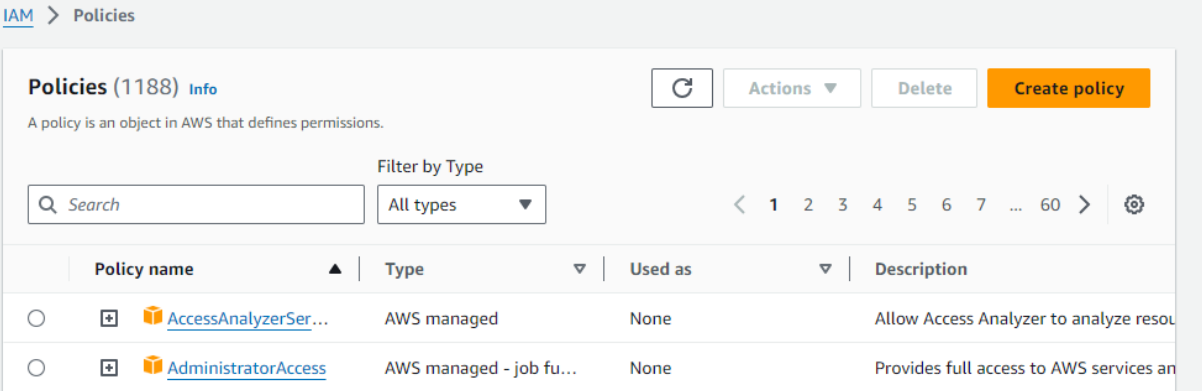
2. Create a policy number 2 which allows the users to:
   a. Access Cloudwatch and billing completely
   b. Can only list EC2 and S3 resources

3. Attach policy number 1 to the Dev Team from task 1

4. Attach policy number 2 to ops team from task 1

Solution:

Create Policies Go to IAM Dashboard > Polices > Create Policy

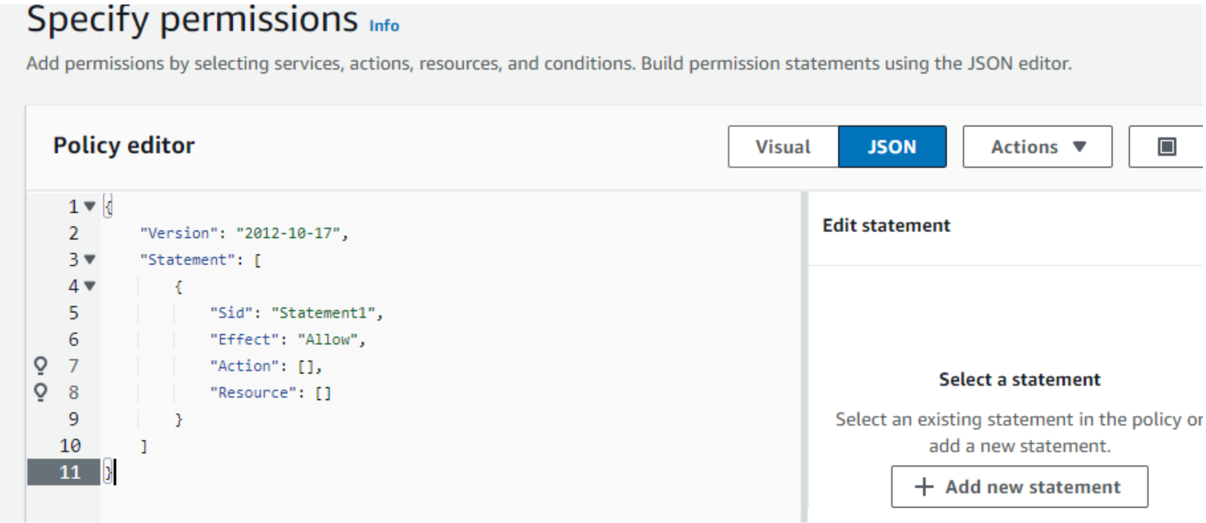


Policies (1188) Info

A policy is an object in AWS that defines permissions.

		Policy name ▲	Type	Used as	Description
○	⊞	AccessAnalyzerSer...	AWS managed	None	Allow Access Analyzer to analyze resou
○	⊞	AdministratorAccess	AWS managed - job fu...	None	Provides full access to AWS services an

Add permissions using Visual or Json, and am using Json.



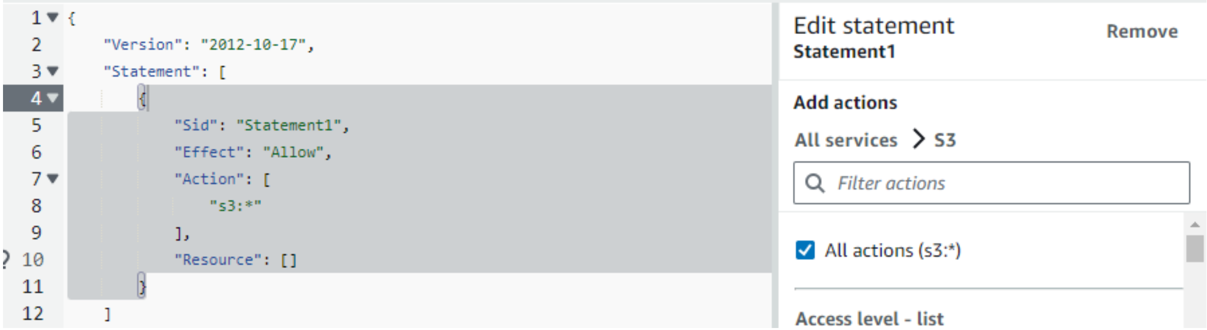
Specify permissions Info

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [],
            "Resource": []
        }
    ]
}
```

Select an existing statement in the policy or add a new statement.

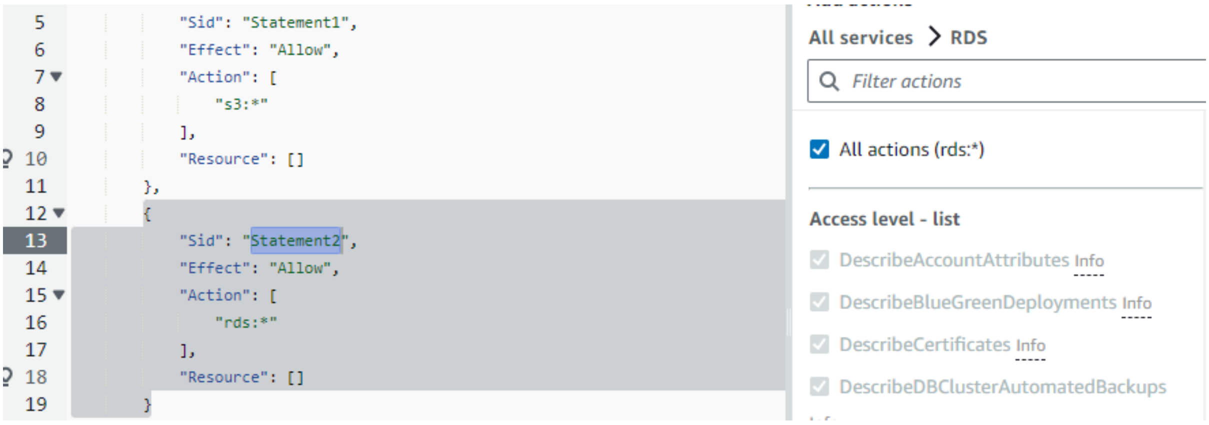
As per question provided S3 full access.



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "s3:*"
            ],
            "Resource": []
        }
    ]
```

☑ All actions (s3:*)

Select new Statement > RDS > All actions



```
        "Sid": "Statement1",
        "Effect": "Allow",
        "Action": [
            "s3:*"
        ],
        "Resource": []
    },
    {
        "Sid": "Statement2",
        "Effect": "Allow",
        "Action": [
            "rds:*"
        ],
        "Resource": []
    }
```

☑ All actions (rds:*)

Access level - list

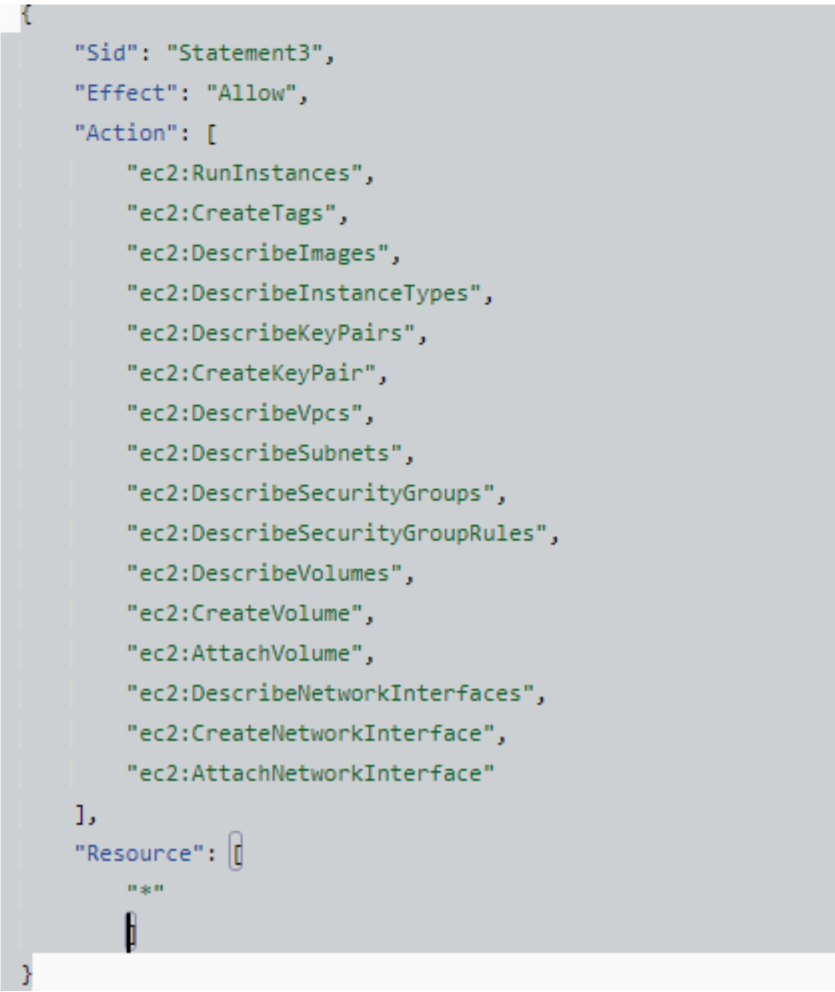
☑ DescribeAccountAttributes Info

☑ DescribeBlueGreenDeployments Info

☑ DescribeCertificates Info

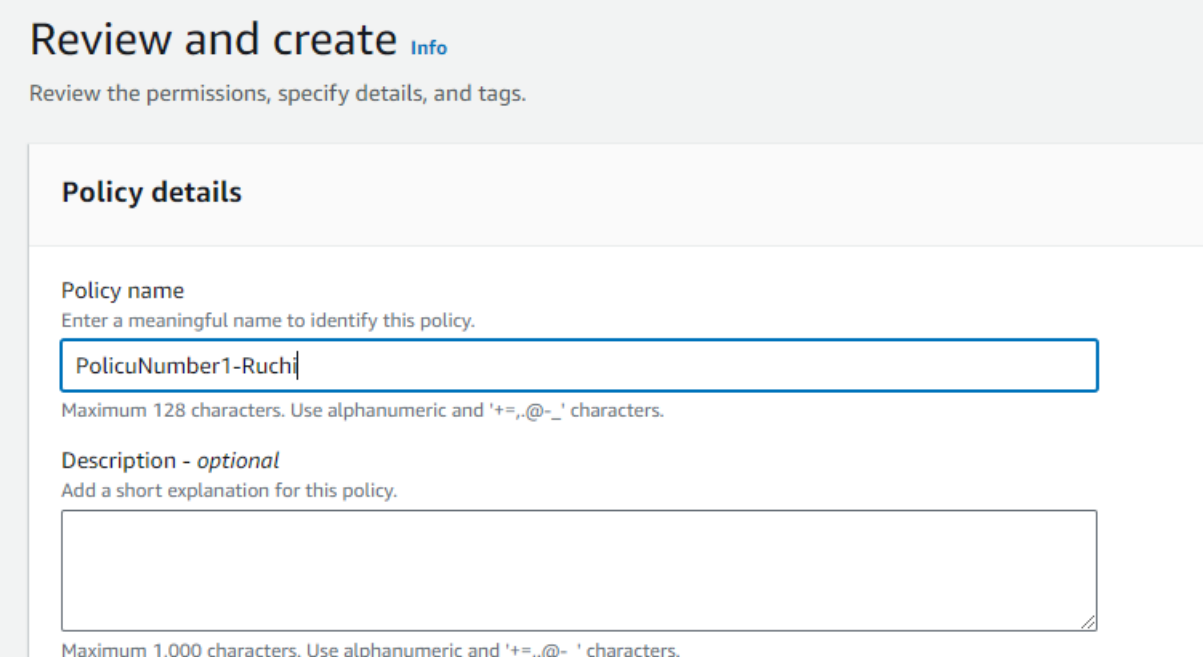
☑ DescribeDBClusterAutomatedBackups

Add Statement 3 for EC2 and add all the below Services which allows for EC2 creations



```
{
    "Sid": "Statement3",
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeKeyPairs",
        "ec2:CreateKeyPair",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeVolumes",
        "ec2:CreateVolume",
        "ec2:AttachVolume",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterface",
        "ec2:AttachNetworkInterface"
    ],
    "Resource": [
        "*"
    ]
}
```

Give the Policy name and create the policy.



Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

PolicuNumber1-Ruchi

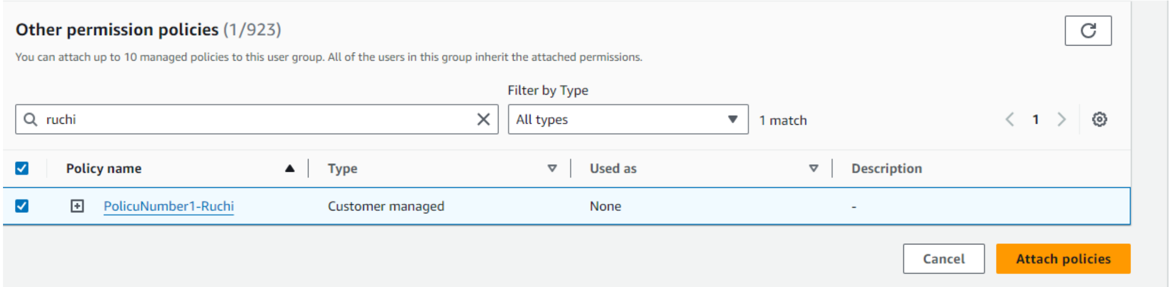
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*

Add a short explanation for this policy.

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

Add the permission policy 1 to the Group Dev team as per the task



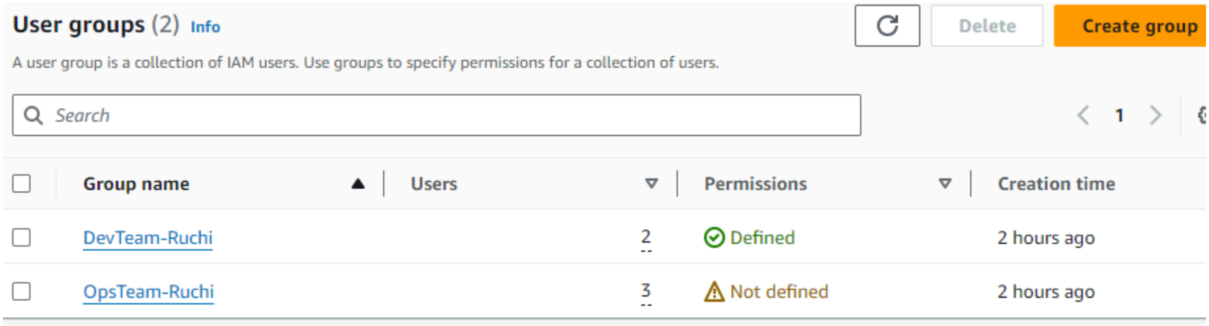
Other permission policies (1/923)

You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

Filter by Type: All types

Search: ruchi — 1 match

☑	Policy name	Type	Used as	Description
☑	PolicuNumber1-Ruchi	Customer managed	None	-

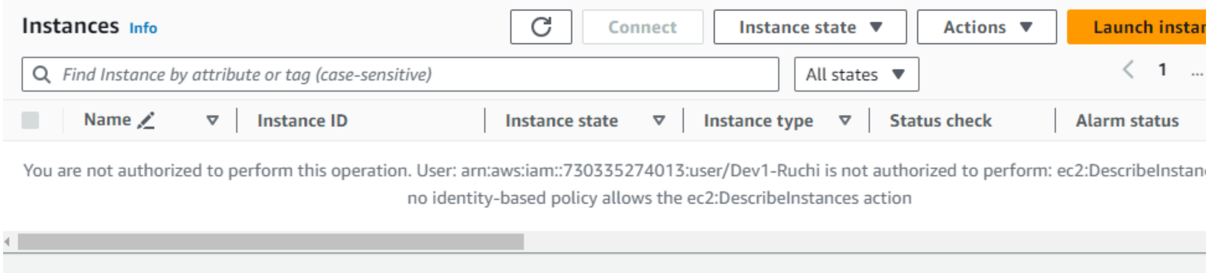


User groups (2) Info

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
□	DevTeam-Ruchi	2	✓ Defined	2 hours ago
□	OpsTeam-Ruchi	3	⚠ Not defined	2 hours ago

Now Able to create a new instance inside IAM user after adding Policy 1 But unable to authorized.

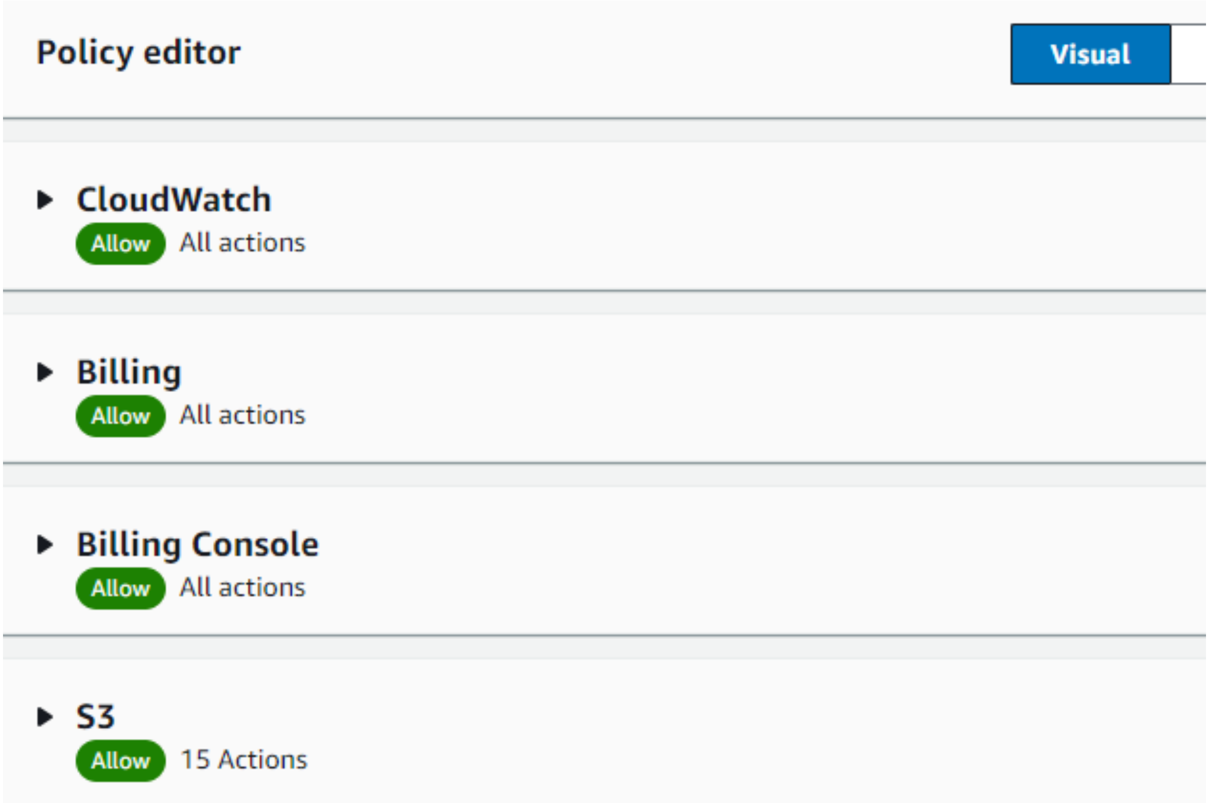


Instances Info

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status

You are not authorized to perform this operation. User: arn:aws:iam::730335274013:user/Dev1-Ruchi is not authorized to perform: ec2:DescribeInstan
no identity-based policy allows the ec2:DescribeInstances action

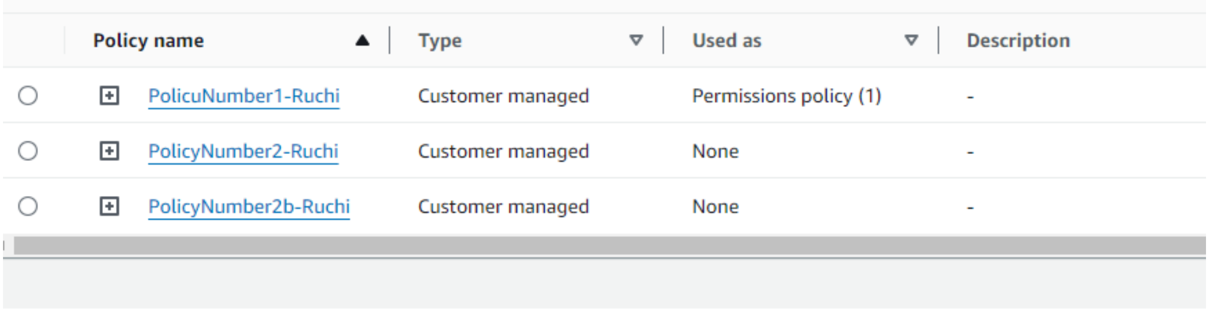
Add Policy number 2 for Cloud watch and billing all access and Ec2, S3 for list access.



Policy editor

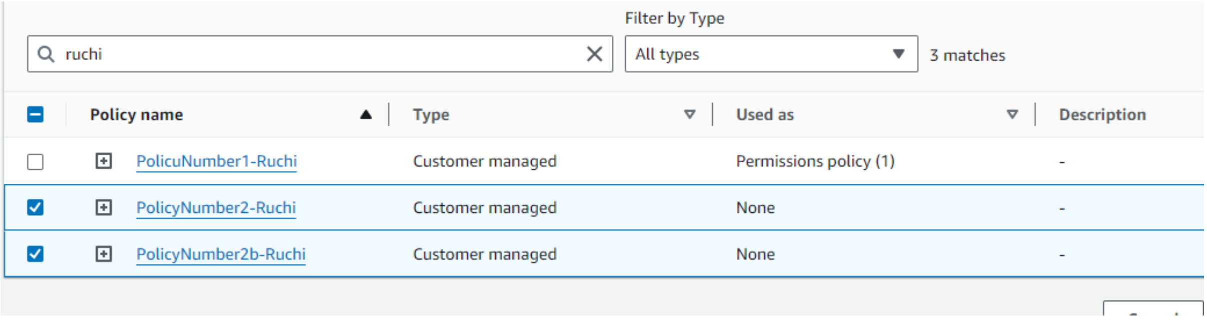
- CloudWatch — Allow All actions
- Billing — Allow All actions
- Billing Console — Allow All actions
- S3 — Allow 15 Actions

Ec2 crossed the limit hence divided the policy into two part inside PolicyNumber 2.



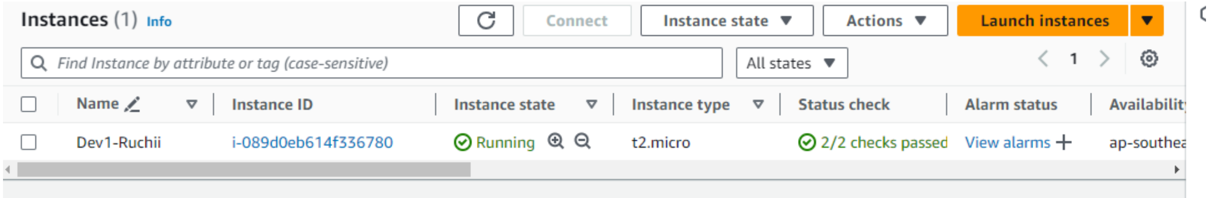
	Policy name	Type	Used as	Description
○	PolicuNumber1-Ruchi	Customer managed	Permissions policy (1)	-
○	PolicyNumber2-Ruchi	Customer managed	None	-
○	PolicyNumber2b-Ruchi	Customer managed	None	-

Add Policy Number 2 for the group ops team.



☑	Policy name	Type	Used as	Description
□	PolicuNumber1-Ruchi	Customer managed	Permissions policy (1)	-
☑	PolicyNumber2-Ruchi	Customer managed	None	-
☑	PolicyNumber2b-Ruchi	Customer managed	None	-

After adding Policy 2, we can see the instances running as we also specified for the particular region.



□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availabilit
□	Dev1-Ruchii	i-089d0eb614f336780	Running	t2.micro	2/2 checks passed	View alarms +	ap-southea

3. IAM Roles Assignment

Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

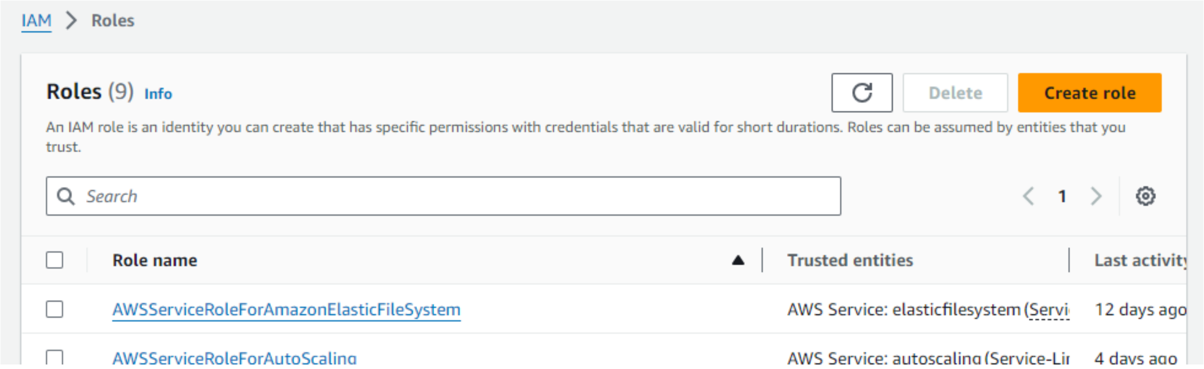
Tasks to be Performed:

1. Create a role which only lets user1 and user2 from task 1 to have complete access to VPCs and Dynamo DB.

2. Login into user1 and shift to the role to test out the feature.

Solutions:

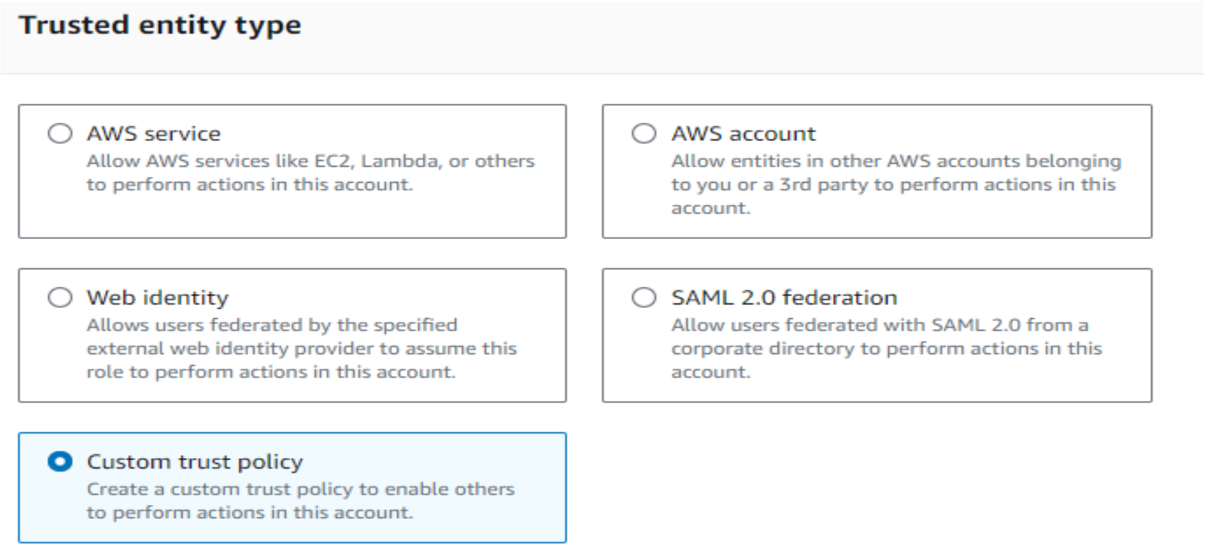
Go to IAM > Roles > Create role



An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

□	Role name	Trusted entities	Last activity
□	AWSServiceRoleForAmazonElasticFileSystem	AWS Service: elasticfilesystem (Servi	12 days ago
□	AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Li	4 days ago

Select Custom trust policy.



Trusted entity type

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

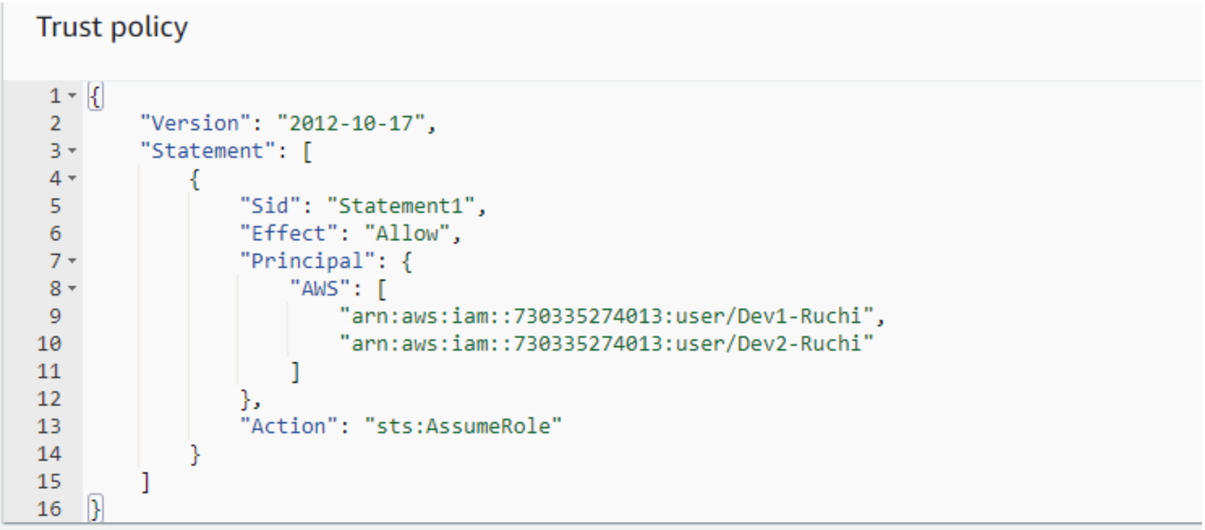
○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ 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.

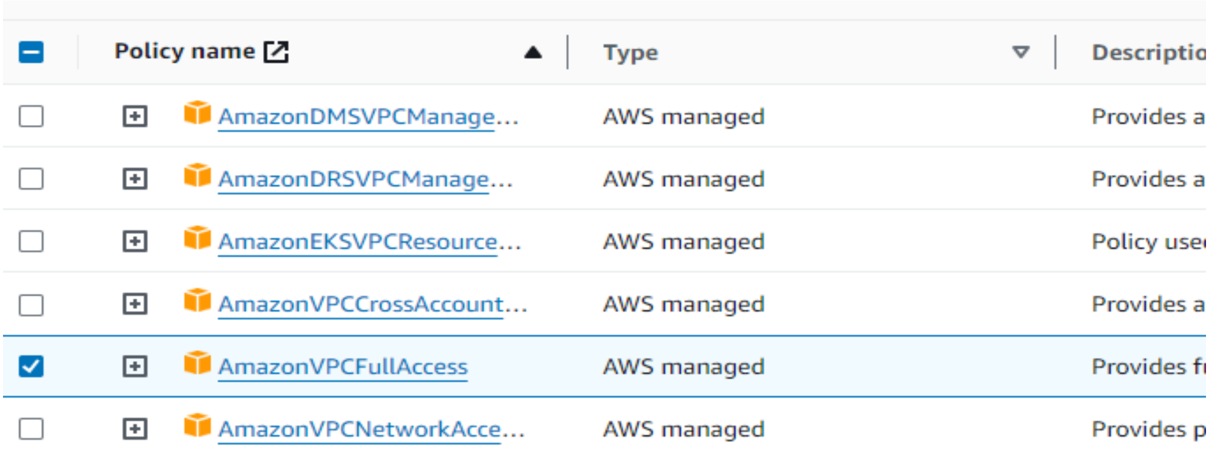
Create the policy, copy arn from 1st and 2nd user.



Trust policy

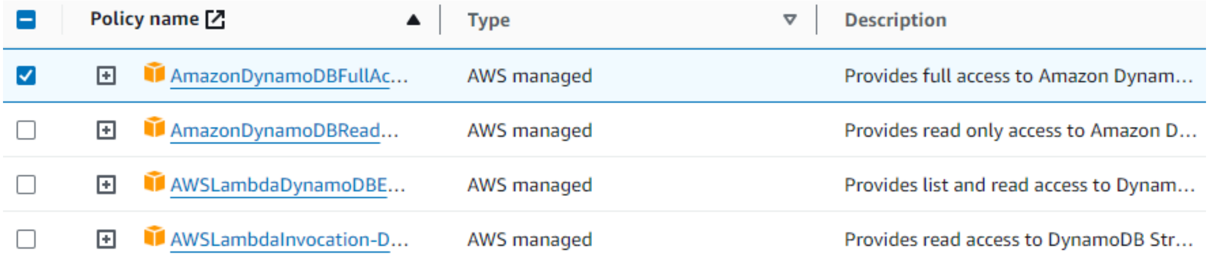
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::730335274013:user/Dev1-Ruchi",
                    "arn:aws:iam::730335274013:user/Dev2-Ruchi"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Provide the complete access for VPC.



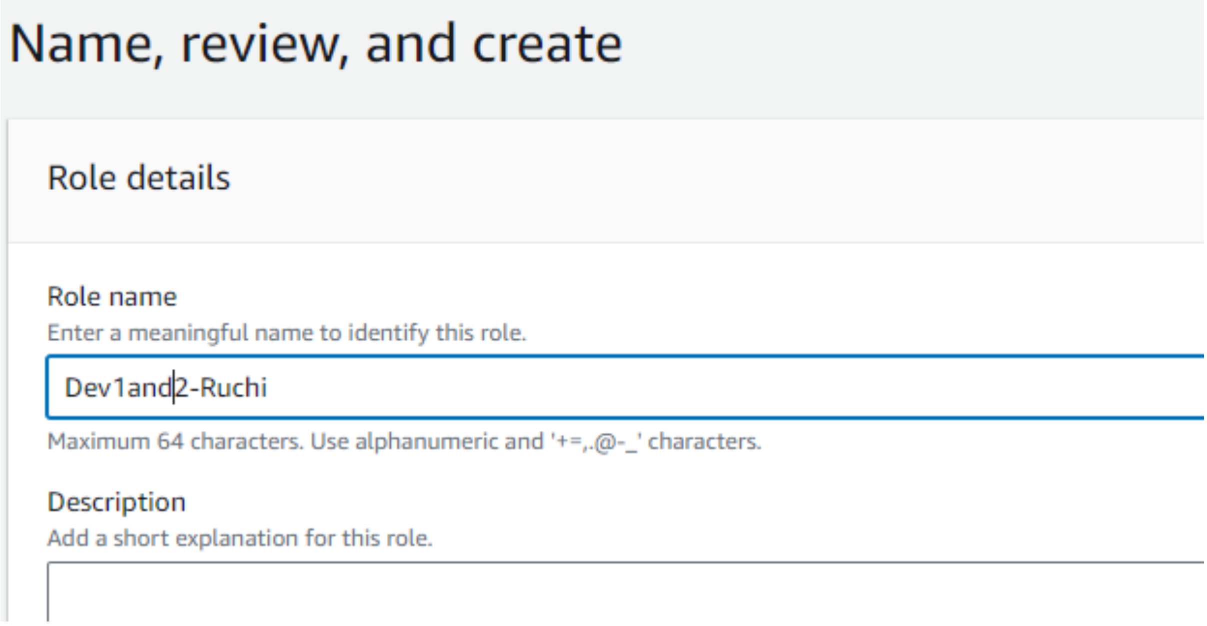
▬		Policy name ↗ ▲	Type ▽	Descriptio
☐	⊞	AmazonDMSVPCManage...	AWS managed	Provides a
☐	⊞	AmazonDRSVPCManage...	AWS managed	Provides a
☐	⊞	AmazonEKSVPCResource...	AWS managed	Policy use
☐	⊞	AmazonVPCCrossAccount...	AWS managed	Provides a
☑	⊞	AmazonVPCFullAccess	AWS managed	Provides f
☐	⊞	AmazonVPCNetworkAcce...	AWS managed	Provides p

Provide the full access for DynamoDB.



▬		Policy name ↗ ▲	Type ▽	Description
☑	⊞	AmazonDynamoDBFullAc...	AWS managed	Provides full access to Amazon Dynam...
☐	⊞	AmazonDynamoDBRead...	AWS managed	Provides read only access to Amazon D...
☐	⊞	AWSLambdaDynamoDBE...	AWS managed	Provides list and read access to Dynam...
☐	⊞	AWSLambdaInvocation-D...	AWS managed	Provides read access to DynamoDB Str...

Select the name, review and create the roles.



Name, review, and create

Role details

Role name

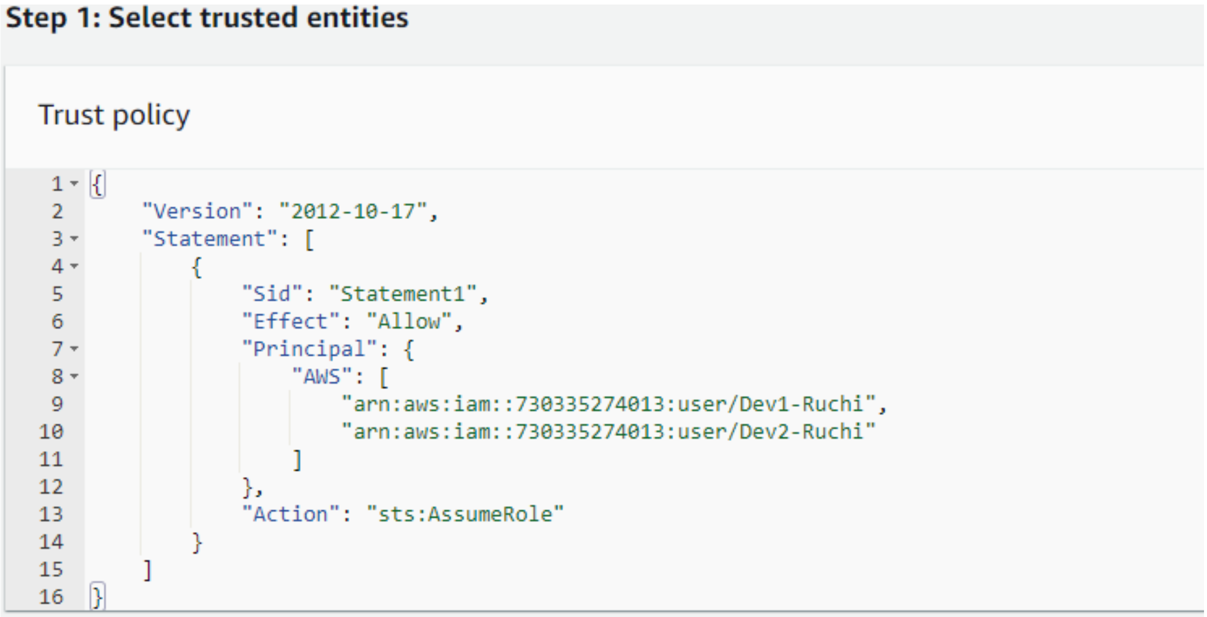
Enter a meaningful name to identify this role.

Dev1and2-Ruchi

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description

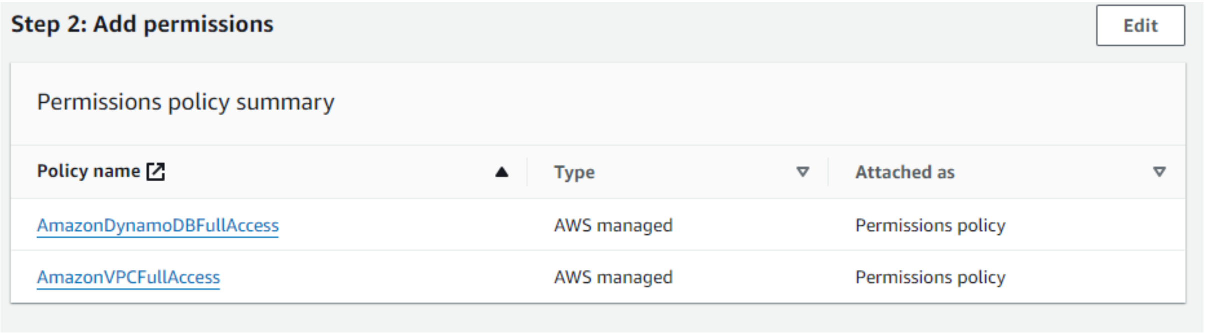
Add a short explanation for this role.



Step 1: Select trusted entities

Trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::730335274013:user/Dev1-Ruchi",
                    "arn:aws:iam::730335274013:user/Dev2-Ruchi"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

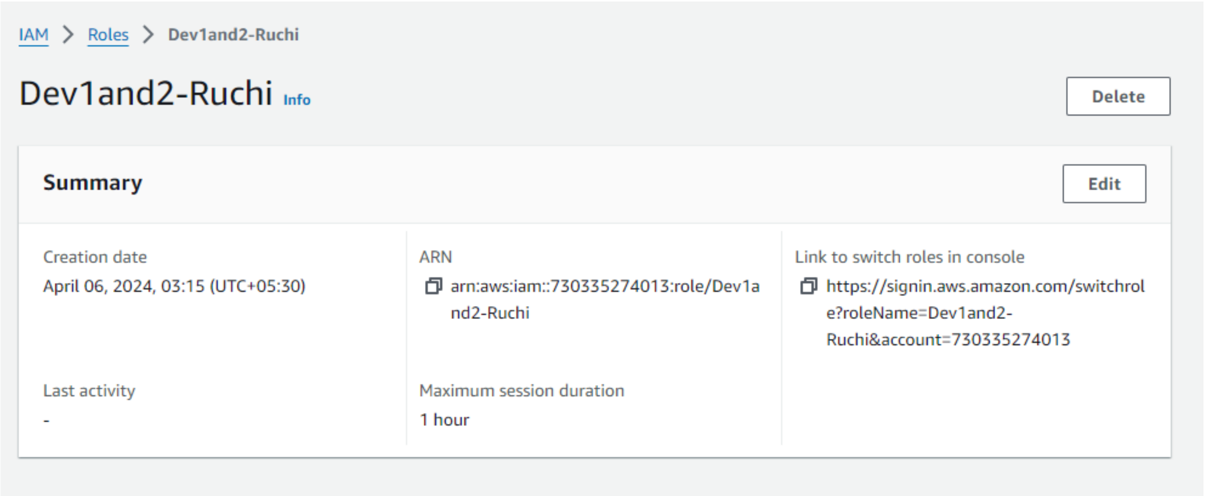


Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonDynamoDBFullAccess	AWS managed	Permissions policy
AmazonVPCFullAccess	AWS managed	Permissions policy

The role is created



Dev1and2-Ruchi

Summary

Creation date
April 06, 2024, 03:15 (UTC+05:30)

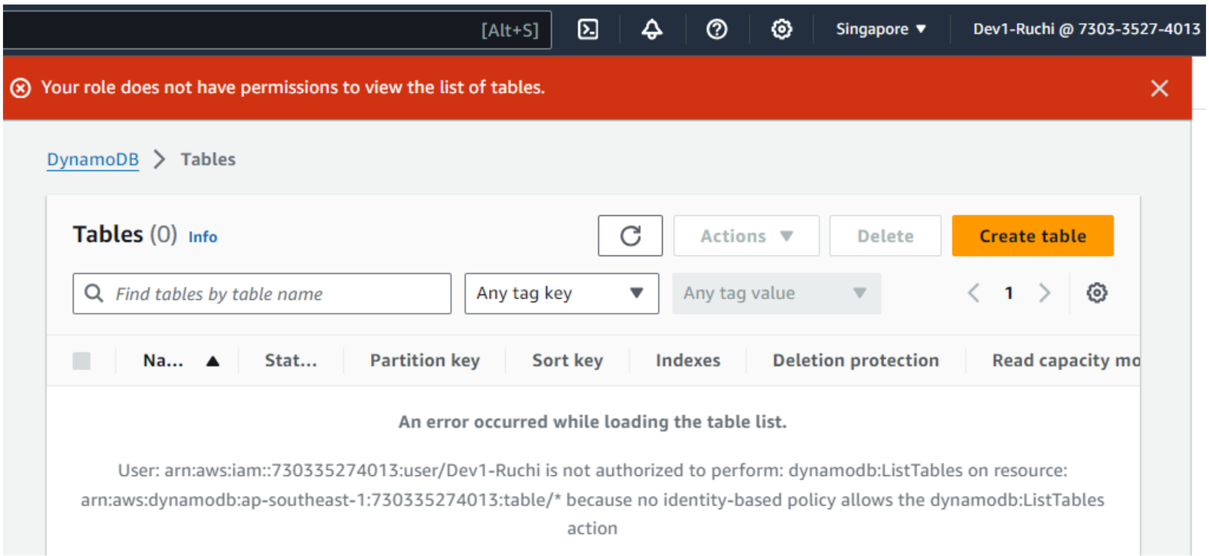
ARN
arn:aws:iam::730335274013:role/Dev1and2-Ruchi

Link to switch roles in console
https://signin.aws.amazon.com/switchrole?roleName=Dev1and2-Ruchi&account=730335274013

Last activity
-

Maximum session duration
1 hour

If you select the Dynamo DB in Dev1 User, it gives error.
So switch the User to the created Role and check

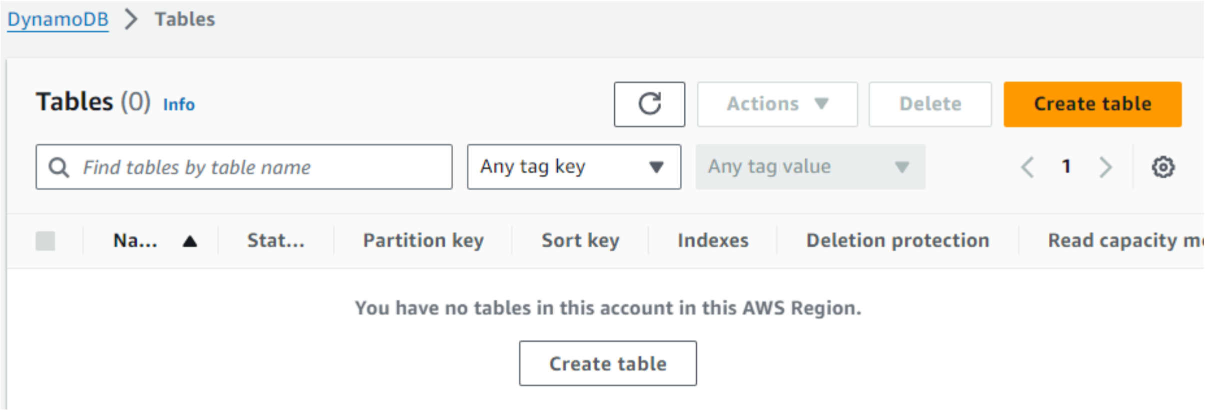


Your role does not have permissions to view the list of tables.

An error occurred while loading the table list.

User: arn:aws:iam::730335274013:user/Dev1-Ruchi is not authorized to perform: dynamodb:ListTables on resource: arn:aws:dynamodb:ap-southeast-1:730335274013:table/* because no identity-based policy allows the dynamodb:ListTables action

Dynamo DB is opening in the role, It can accessed once the roles are changed



You have no tables in this account in this AWS Region.

==