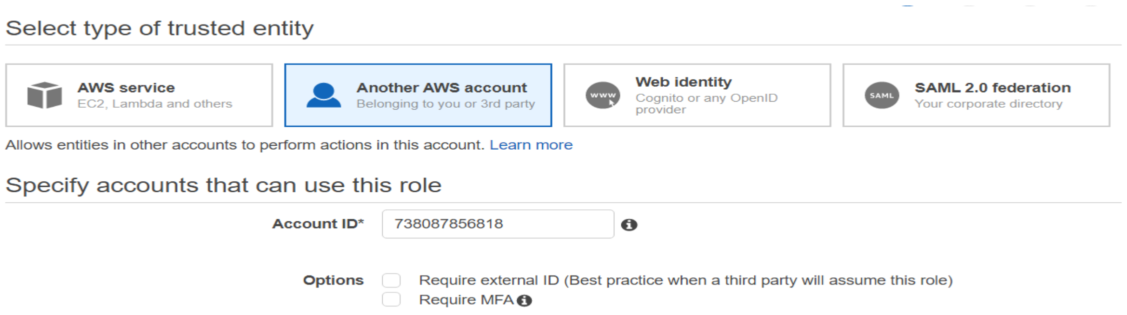
3. Create a new IAM role called power users and attach a policy who should have read only privileges to EC2,S3,Clouwatch,EBS,Codebuild,Autoscalling,resource group using AWS console and terraform

AWS Console:



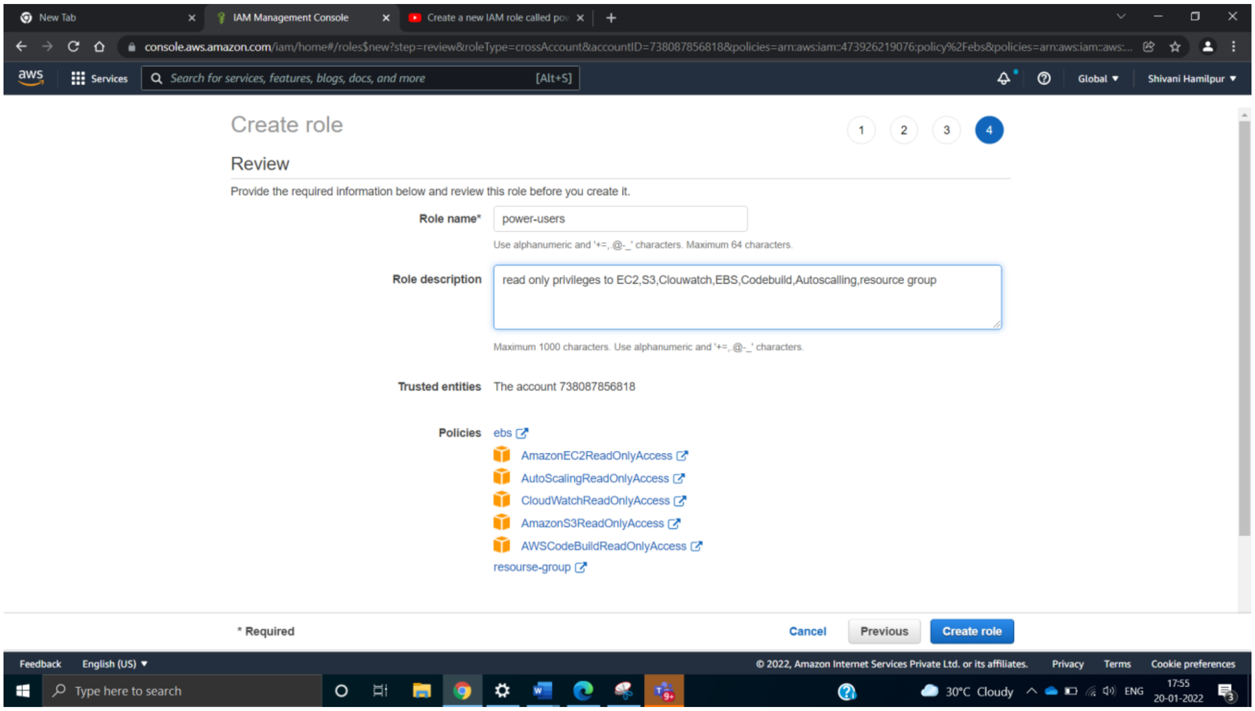
Select type of trusted entity

Allows entities in other accounts to perform actions in this account. Learn more

Specify accounts that can use this role

Account ID* 738087856818

Options
□ Require external ID (Best practice when a third party will assume this role)
□ Require MFA



New Tab
IAM Management Console
Create a new IAM role called pow
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Shivani Hamilpur
1
2
3
4

console.aws.amazon.com/iam/home#/roles$new?step=review&roleType=crossAccount&accountID=738087856818&policies=arn:aws:iam::473926219076:policy%2Febs&policies=arn:aws:iam::aws:...

Create role

Review

Provide the required information below and review this role before you create it.

Role name* power-users

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

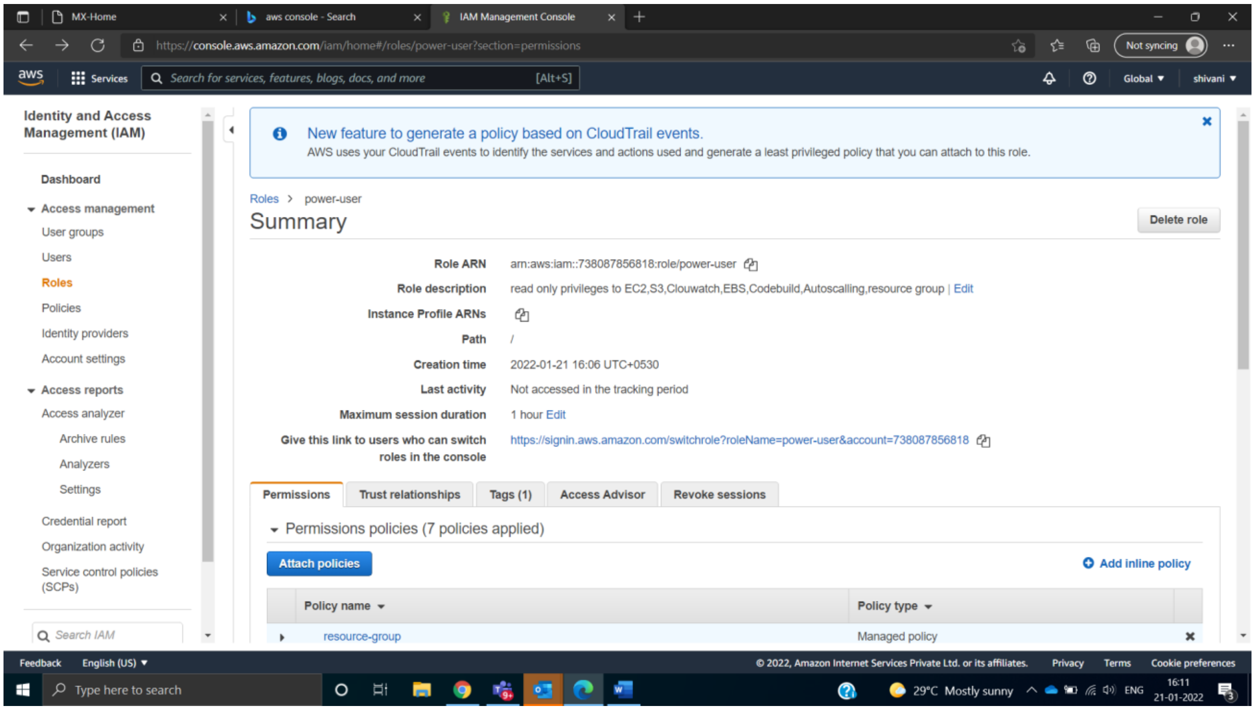
Role description read only privileges to EC2,S3,Clouwatch,EBS,Codebuild,Autoscalling,resource group

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities The account 738087856818

Policies
ebs
AmazonEC2ReadOnlyAccess
AutoScalingReadOnlyAccess
CloudWatchReadOnlyAccess
AmazonS3ReadOnlyAccess
AWSCodeBuildReadOnlyAccess
resourse-group

* Required



https://console.aws.amazon.com/iam/home#/roles/power-user?section=permissions

Identity and Access Management (IAM)

New feature to generate a policy based on CloudTrail events.
AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this role.

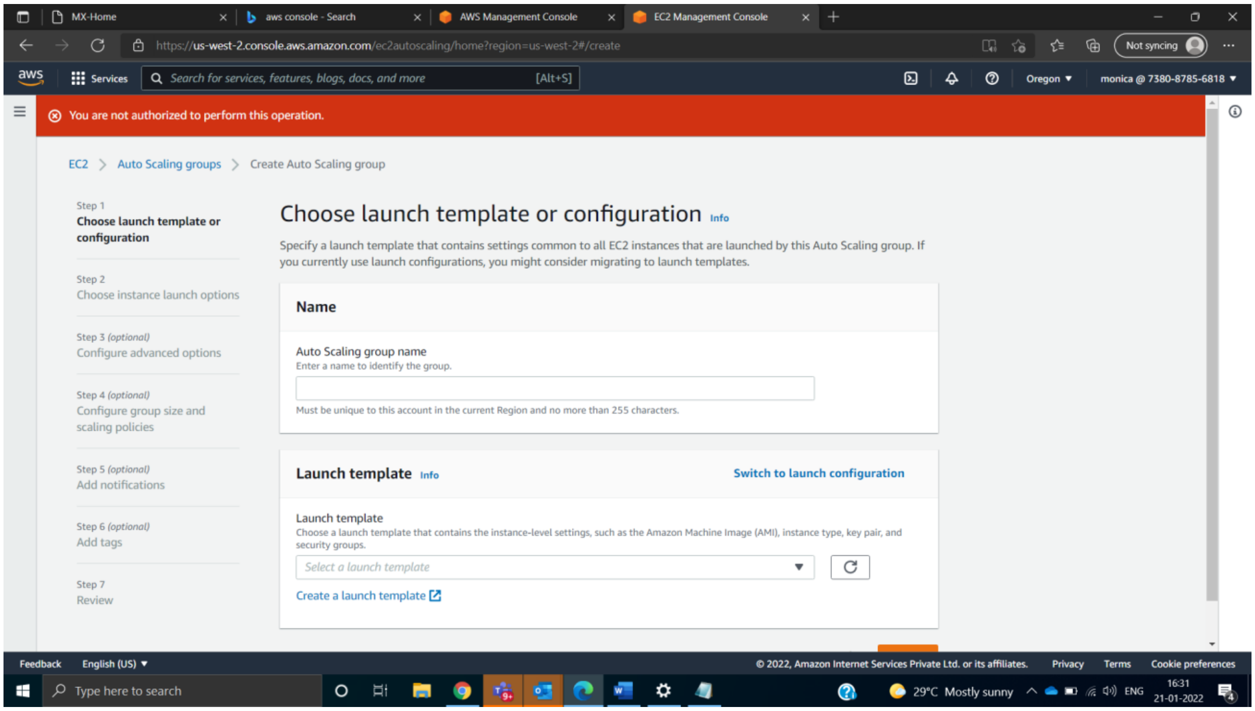
Roles > power-user

Summary

Role ARN	arn:aws:iam::738087856818:role/power-user
Role description	read only privileges to EC2,S3,Clouwatch,EBS,Codebuild,Autoscalling,resource group | Edit
Instance Profile ARNs	
Path	/
Creation time	2022-01-21 16:06 UTC+0530
Last activity	Not accessed in the tracking period
Maximum session duration	1 hour Edit
Give this link to users who can switch roles in the console	https://signin.aws.amazon.com/switchrole?roleName=power-user&account=738087856818

Permissions policies (7 policies applied)

Policy name	Policy type
resource-group	Managed policy



https://us-west-2.console.aws.amazon.com/ec2autoscaling/home?region=us-west-2#/create

You are not authorized to perform this operation.

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template or configuration

Step 2
Choose instance launch options

Step 3 (optional)
Configure advanced options

Step 4 (optional)
Configure group size and scaling policies

Step 5 (optional)
Add notifications

Step 6 (optional)
Add tags

Step 7
Review

Choose launch template or configuration

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group. If you currently use launch configurations, you might consider migrating to launch templates.

Name

Auto Scaling group name
Enter a name to identify the group.

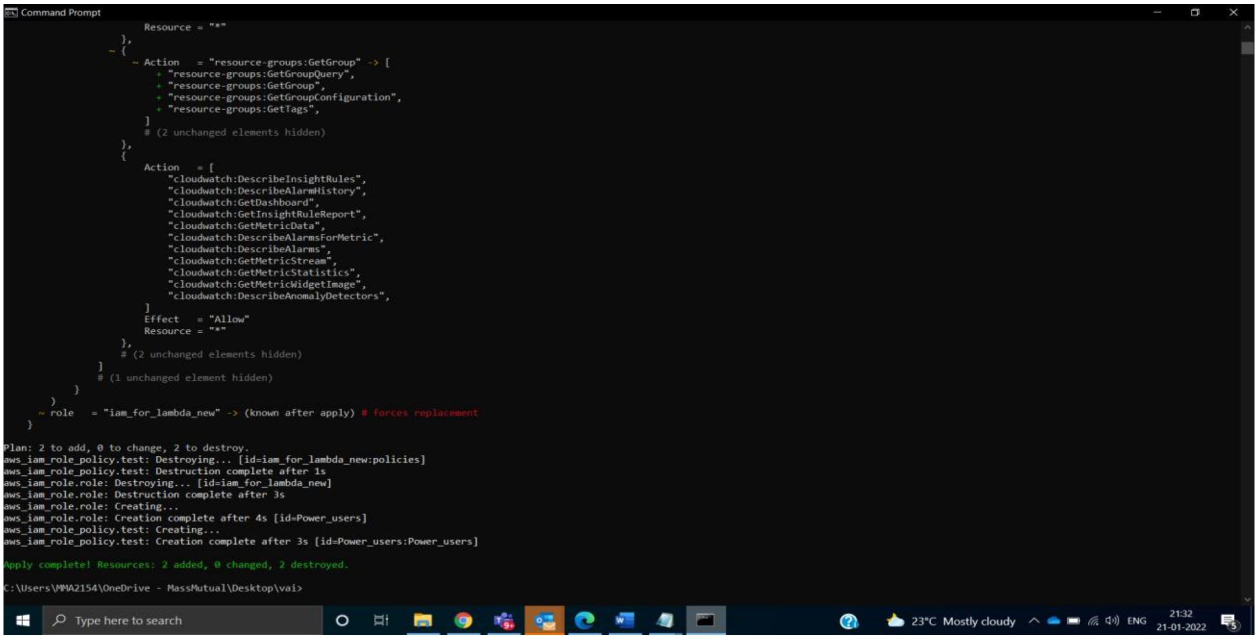
Must be unique to this account in the current Region and no more than 255 characters.

Launch template

Launch template
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

Select a launch template

Using Terraform:

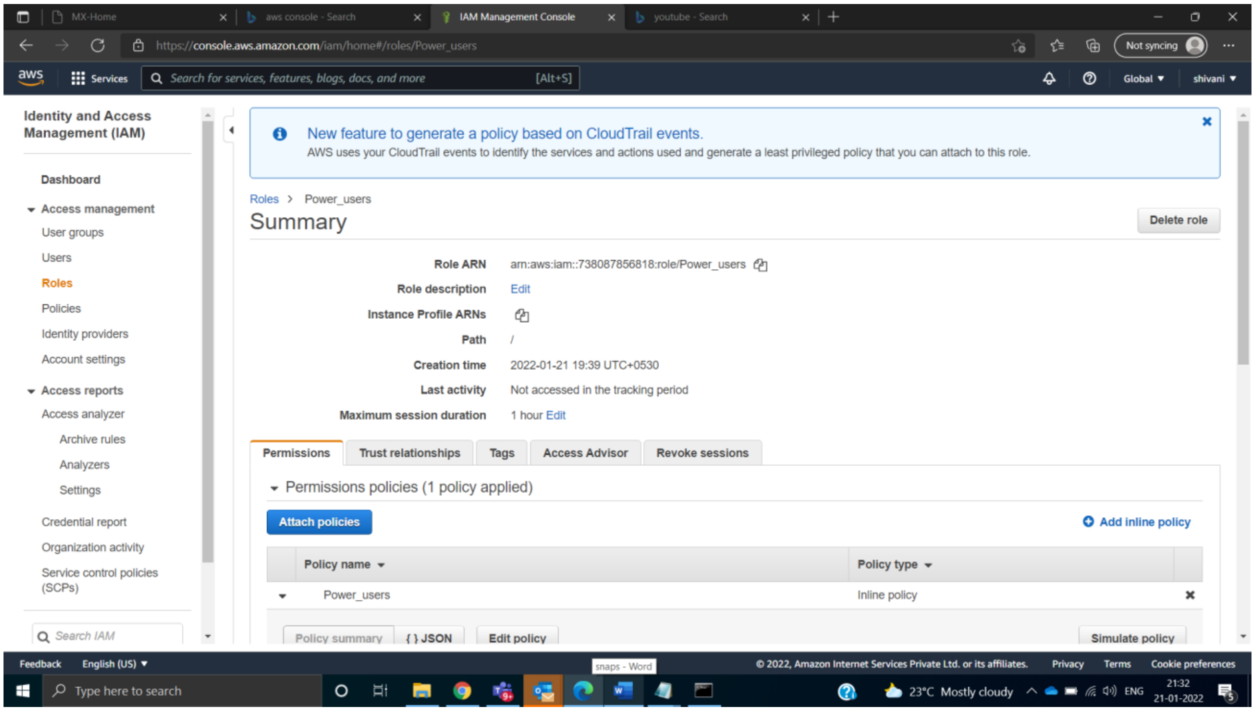


```
                        Resource = "*"
                    },
                  ~ {
                      ~ Action   = "resource-groups:GetGroup" -> [
                          + "resource-groups:GetGroupQuery",
                          + "resource-groups:GetGroup",
                          + "resource-groups:GetGroupConfiguration",
                          + "resource-groups:GetTags",
                        ]
                        # (2 unchanged elements hidden)
                    },
                    {
                        Action   = [
                            "cloudwatch:DescribeInsightRules",
                            "cloudwatch:DescribeAlarmHistory",
                            "cloudwatch:GetDashboard",
                            "cloudwatch:GetInsightRuleReport",
                            "cloudwatch:GetMetricData",
                            "cloudwatch:DescribeAlarmsForMetric",
                            "cloudwatch:DescribeAlarms",
                            "cloudwatch:GetMetricStream",
                            "cloudwatch:GetMetricStatistics",
                            "cloudwatch:GetMetricWidgetImage",
                            "cloudwatch:DescribeAnomalyDetectors",
                        ]
                        Effect   = "Allow"
                        Resource = "*"
                    },
                    # (2 unchanged elements hidden)
                ]
                # (1 unchanged element hidden)
            }
        )
      ~ role   = "iam_for_lambda_new" -> (known after apply) # forces replacement
    }

Plan: 2 to add, 0 to change, 2 to destroy.
aws_iam_role_policy.test: Destroying... [id=iam_for_lambda_new:policies]
aws_iam_role_policy.test: Destruction complete after 1s
aws_iam_role.role: Destroying... [id=iam_for_lambda_new]
aws_iam_role.role: Destruction complete after 3s
aws_iam_role.role: Creating...
aws_iam_role.role: Creation complete after 4s [id=Power_users]
aws_iam_role_policy.test: Creating...
aws_iam_role_policy.test: Creation complete after 3s [id=Power_users:Power_users]

Apply complete! Resources: 2 added, 0 changed, 2 destroyed.

C:\Users\MMA2154\OneDrive - MassMutual\Desktop\vai>
```



New feature to generate a policy based on CloudTrail events.

AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this role.

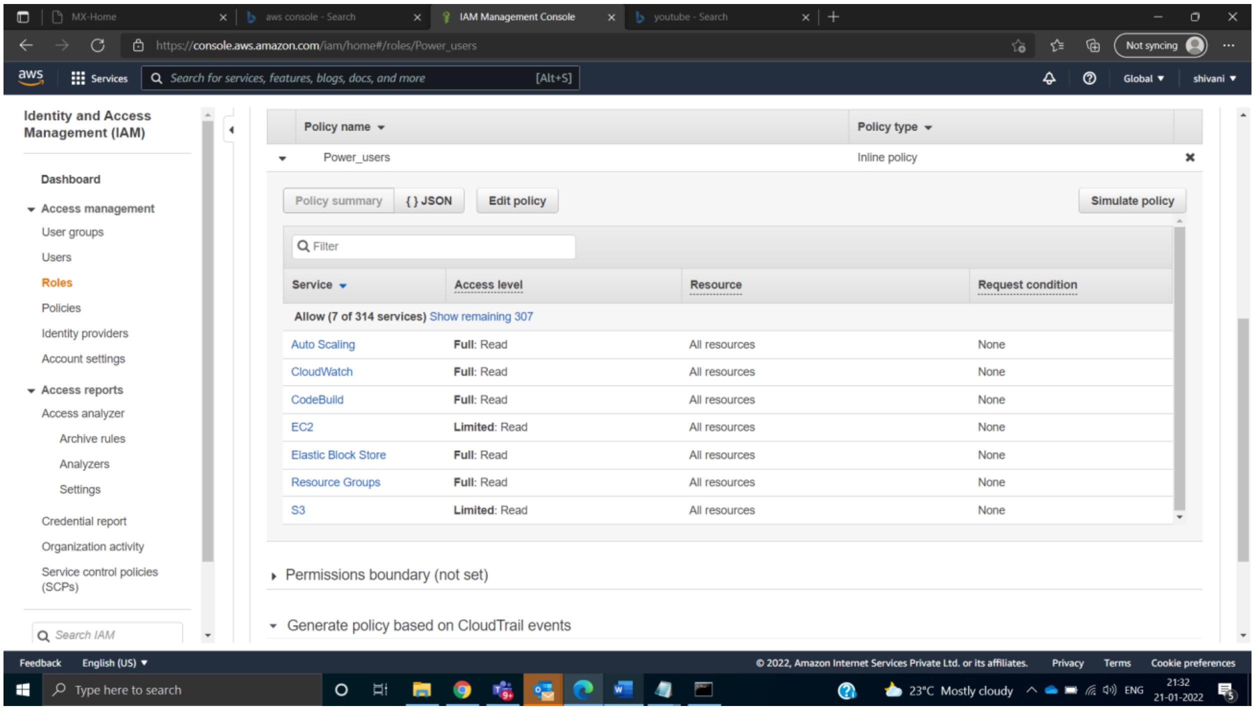
Roles > Power_users

Summary

Role ARN	arn:aws:iam::738087856818:role/Power_users
Role description	Edit
Instance Profile ARNs	
Path	/
Creation time	2022-01-21 19:39 UTC+0530
Last activity	Not accessed in the tracking period
Maximum session duration	1 hour Edit

Permissions policies (1 policy applied)

Policy name	Policy type
Power_users	Inline policy



Policy name	Policy type
Power_users	Inline policy

Service	Access level	Resource	Request condition
Allow (7 of 314 services) Show remaining 307			
Auto Scaling	**Full**: Read	All resources	None
CloudWatch	**Full**: Read	All resources	None
CodeBuild	**Full**: Read	All resources	None
EC2	**Limited**: Read	All resources	None
Elastic Block Store	**Full**: Read	All resources	None
Resource Groups	**Full**: Read	All resources	None
S3	**Limited**: Read	All resources	None