




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

**AWS service**
EC2, Lambda and others

**Another AWS account**
Belonging to you or 3rd party

**Web identity**
Cognito or any OpenID provider

**SAML 2.0 federation**
Your corporate directory

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID*

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

Create role

1 2 3 4

Review






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

Role name*
Use alphanumeric and '+', '@', '_' characters. Maximum 64 characters.

Role description
Maximum 1000 characters. Use alphanumeric and '+', '@', '_' characters.

Trusted entities The account 738087856818

Policies [ebs](#)

-  [AmazonEC2ReadOnlyAccess](#)
-  [AutoScalingReadOnlyAccess](#)
-  [CloudWatchReadOnlyAccess](#)
-  [AmazonS3ReadOnlyAccess](#)
-  [AWSCodeBuildReadOnlyAccess](#)
- [resource-group](#)

* Required

[Cancel](#) [Previous](#) [Create role](#)

Feedback English (US)

© 2022, Amazon Internet Services Private Ltd. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Type here to search

30°C Cloudy 17:55 20-01-2022

MX-Home x aws console - Search x IAM Management Console x +

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

Search for services, features, blogs, docs, and more [Alt+S]

Global shivani

Identity and Access Management (IAM)

- Dashboard
- Access management
 - User groups
 - Users
 - Roles**
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analyzers
 - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Search 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 Delete role

Summary

| | |
|---|---|
| Role ARN | arn:aws:iam::738087856818:role/power-user |
| Role description | read only privileges to EC2,S3,Cloudwatch,EBS,Codebuild,Autoscaling,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 Trust relationships Tags (1) Access Advisor Revoke sessions

Permissions policies (7 policies applied)

[Attach policies](#) [Add inline policy](#)

| Policy name | Policy type |
|----------------|----------------|
| resource-group | Managed policy |

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Type here to search

29°C Mostly sunny 16:11 21-01-2022

MX-Home x aws console - Search x AWS Management Console x EC2 Management Console x +

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

Search for services, features, blogs, docs, and more [Alt+S]

Oregon monica @ 7380-8785-6818

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 [Info](#)

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 [Info](#) [Switch to launch configuration](#)

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.

[Create a launch template](#)

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Type here to search

29°C Mostly sunny 16:31 21-01-2022

Using Terraform:

```
Command Prompt

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:DescribeAlarmForMetric",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricStream",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:GetMetricGetImage",
    "cloudwatch:DescribeAnomalyDetectors",
  ]
  Effect = "Allow"
  Resource = ""
},
# (2 unchanged elements hidden)
}
# (1 unchanged element hidden)
}
- role = "iam_for_lambda_new" -> (known after apply) # forces replacement
}

Plans: 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\VWA2154\OneDrive - MassMutual\Desktop\va>
```

The screenshot displays the AWS IAM console interface. On the left is a navigation sidebar with sections like 'Dashboard', 'Access management', 'Identity providers', and 'Access reports'. The main content area shows the 'Summary' page for the 'Power_users' role. A blue notification banner at the top states: '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.' The role details include: Role ARN (arn:aws:iam:738087856818:role/Power_users), Role description (with an 'Edit' link), Instance Profile ARNs, Path (/), Creation time (2022-01-21 19:39 UTC+0530), Last activity (Not accessed in the tracking period), and Maximum session duration (1 hour, with an 'Edit' link). Below the summary, there are tabs for 'Permissions', 'Trust relationships', 'Tags', 'Access Advisor', and 'Revoke sessions'. The 'Permissions' tab is active, showing 'Permissions policies (1 policy applied)'. A table lists the attached policy: 'Power_users' (Inline policy). There are buttons for 'Attach policies', 'Add inline policy', 'Policy summary', 'JSON', 'Edit policy', and 'Simulate policy'. The bottom of the screen shows a Windows taskbar with various application icons and system information like '23°C Mostly cloudy' and '21:32 21-01-2022'.

MX-Home

aws console - Search

IAM Management Console

youtube - Search

https://console.aws.amazon.com/iam/home#/roles/Power_users

Not syncing

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

shivani

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

Policy name

Policy type

Power_users

Inline policy

Policy summary

{ } JSON

Edit policy

Simulate policy

Filter

| 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 |

Permissions boundary (not set)

Generate policy based on CloudTrail events

Feedback

English (US)

© 2022, Amazon Internet Services Private Ltd. or its affiliates.

Privacy

Terms

Cookie preferences

Type here to search

23°C. Mostly cloudy

21:32

21-01-2022