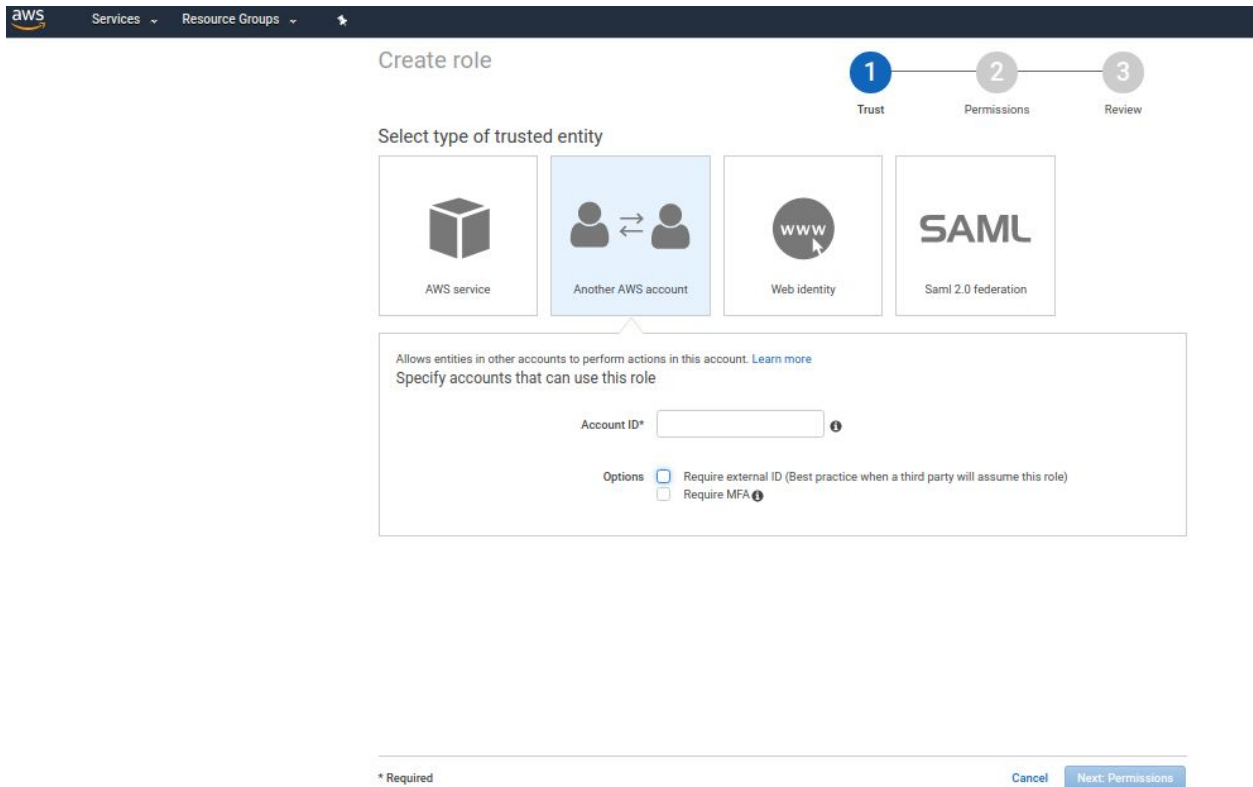


Step 1: open IAM service and select Roles. Click on Create role option.



Step 2: Select 'Select Add another account'

Create role

1 Trust — 2 Permissions — 3 Review

AWS service

Another AWS account

Web identity

SAML
Saml 2.0 federation

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)

You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. [Learn more](#)

External ID

Important: The console does not support using an external ID with the Switch Role feature. If you select this option, entities in the trusted account must use the API, CLI, or a custom federation proxy to make cross-account iam:AssumeRole calls. [Learn more](#)

Require MFA [?](#)

* Required

Cancel **Next: Permissions**

Step 3: The information in above screen needs to be filled from Step 2 on amazon account setup page on app.copperegg.com.

Select **Next: Permissions**.

On Permissions page, do not select any policy, we will add an inline policy later. Select "Next: Review".

aws Services Resource Groups

Create role

1 Trust 2 Permissions 3 Review

Review

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

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

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

Trusted entities The account 193951620307

Policies

* Required Cancel Previous Create role

Step 4: On Review page, Enter a role name and review role details. Select **Create Role**.

aws Services Resource Groups

Roles > [Role Name]

Summary

Delete role

Role ARN

Role description [Edit](#)

Instance Profile ARNs

Path

Creation time

Give this link to users who can switch roles in the console

Permissions Trust relationships Access Advisor Revoke sessions

Get started with permissions
This role doesn't have any permissions yet. Get started by attaching one or more policies to this role. [Learn more](#)

[Attach policy](#)

[Add inline policy](#)

1. When the role is created successfully, select the created role from roles list page.
- 2.
3. From role details page, under Summary section, copy "Role ARN" value.
4. You will be asked to fill this Role ARN in Uptime Cloud Monitor UI in later step.
- 5.
6. Select **Permissions** tab and click on **Add inline policy**

aws Services Resource Groups

Manage Role Permissions

Set Permissions

Select a policy template, generate a policy, or create a custom policy. A policy is a document that formally states one or more permissions. You can edit the policy on the following screen, or at a later time using the user, group, or role detail pages.

Policy Generator

Custom Policy

Use the policy editor to customize your own set of permissions.

Select

Choose Custom Policy

aws Services Resource Groups

Manage Role Permissions

Review Policy

Customize permissions by editing the following policy document. For more information about the access policy language, see [Overview of Policies in the Using IAM guide](#). To test the effects of this policy before applying your changes, use the [IAM Policy Simulator](#).

Policy Name

copperegg_readonly

Policy Document

```
1 { "Version": "2012-10-17", "Statement": [ { "Action": [ "cloudwatch:Describe*", "cloudwatch:Get*", "cloudwatch:List*", "cloudsearch:Describe*", "cloudsearch:Get*", "cloudsearch:List*", "dynamodb:DescribeTable", "dynamodb:ListTables", "ec2:Describe*", "elasticache:Describe*", "elasticache:List*", "iam:List*", "iam:Get*", "redshift:Describe*", "rds:Describe*", "rds:ListTagsForResource", "swf:List*", "swf:Describe*", "autoscaling:Describe*", "autoscaling:List*", "autoscaling:Get*", "elasticloadbalancing:Describe*", "s3:Get*", "s3:List*", "sqs:Get*", "sqs:List*", "route53:Get*", "route53:List*", "opsworks:Describe*", "opsworks:Get*", "elasticbeanstalk:List*", "elasticbeanstalk:Describe*", "cloudfront:List*", "cloudfront:Get*", "kinesis:Describe*", "kinesis:Get*", "kinesis:List*", "machinelearning:Describe*", "machinelearning:Get*", "elasticmapreduce:Describe*", "elasticmapreduce:List*", "sns:Get*", "sns:List*", "storagegateway:Describe*", "storagegateway:List*", "workspaces:Describe*" ], "Effect": "Allow", "Resource": "*" } ] }
```

Use autoforamtting for policy editing

Cancel Validate Policy Apply Policy

Fillup the Policy details.

- **Policy Name:** copperegg_readonly
- **Policy Document:** Fill the details that were provided in Step 2.

Click on **Apply Policy**.