

AWS IAM Roles and STS.

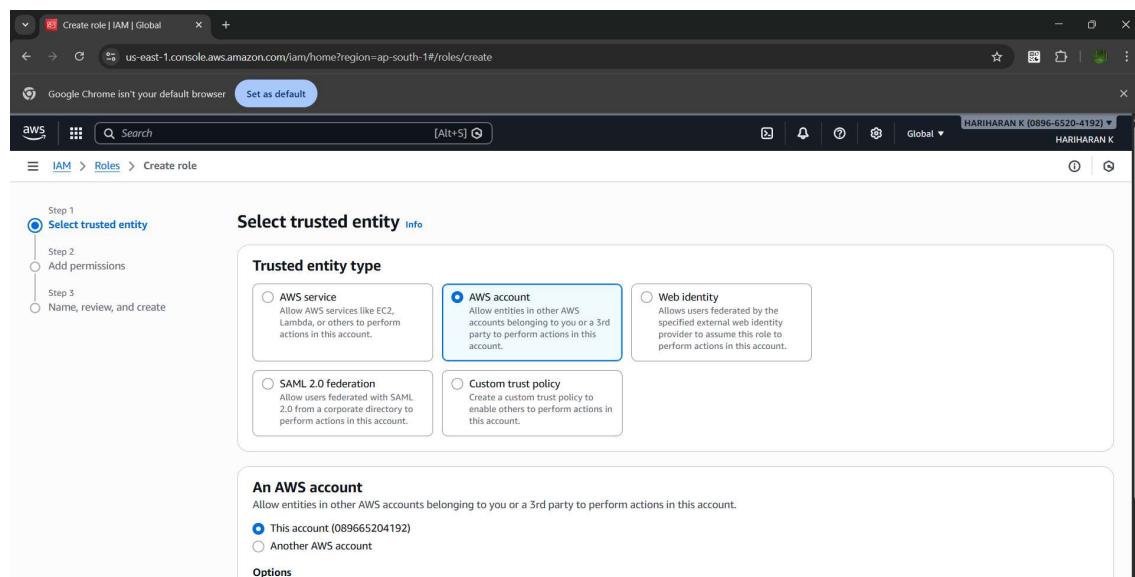
What is an IAM Role?

An IAM Role is a set of permissions that can be assumed temporarily.

Key point:

A role does NOT have permanent credentials.
It gives temporary credentials via STS.

First we created the user role.



Step 1
 Select trusted entity
 Step 2
 Step 3
 Name, review, and create

Select trusted entity Info

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.

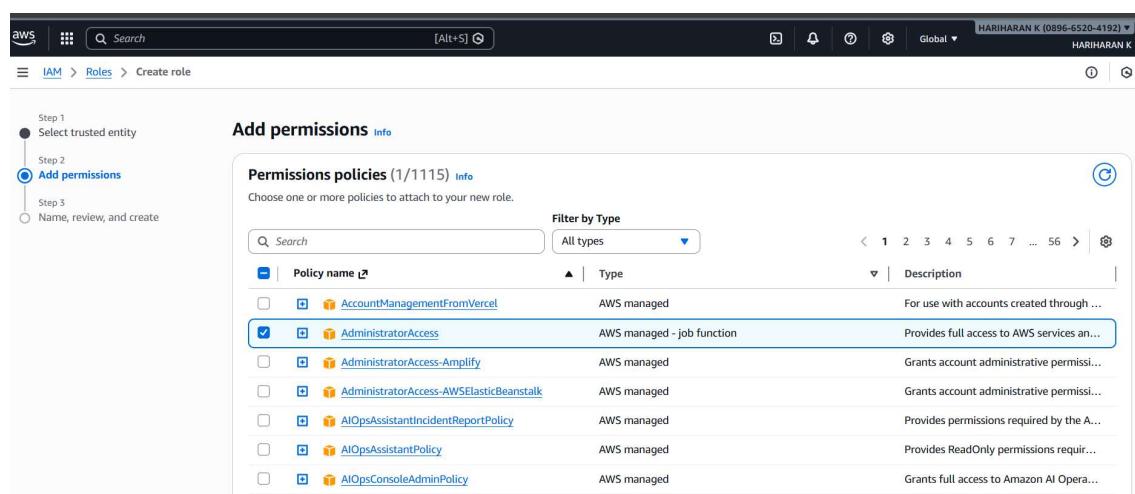
SAML 2.0 federation Allows users federated with SAML 2.0 from a corporate directory to perform actions in this account.

Custom trust policy Create a custom trust policy to enable others to perform actions in this account.

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

This account (089665204192)
 Another AWS account

Options



Step 1
 Select trusted entity
 Add permissions
 Step 3
 Name, review, and create

Add permissions Info

Permissions policies (1/1115) Info

Choose one or more policies to attach to your new role.

Filter by Type

Policy name	Type	Description
<input type="checkbox"/> AccountManagementFromVercel	AWS managed	For use with accounts created through ...
<input checked="" type="checkbox"/> AdministratorAccess	AWS managed - job function	Provides full access to AWS services an...
<input type="checkbox"/> AdministratorAccess-Amplify	AWS managed	Grants account administrative permissi...
<input type="checkbox"/> AdministratorAccess-AWSElasticBeanstalk	AWS managed	Grants account administrative permissi...
<input type="checkbox"/> AIOpsAssistantIncidentReportPolicy	AWS managed	Provides permissions required by the A...
<input type="checkbox"/> AIOpsAssistantPolicy	AWS managed	Provides ReadOnly permissions requir...
<input type="checkbox"/> AIOpsConsoleAdminPolicy	AWS managed	Grants full access to Amazon AI Opera...

Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
temp-user
Maximum 64 characters. Use alphanumeric and '+_-.@-' characters.

Description
Add a short explanation for this role.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: '_+=., @-[\{\}!#\\$%^*-~`-

Step 1: Select trusted entities

Trust policy

```
1 + {  
2   "Version": "2012-10-17",  
3   "Statement": [
```

I have created an user and gave STS policy to that user.

Permissions policies (0)
Permissions are defined by policies attached to the user directly or through groups.

Filter by Type
Q sts X All types 0 matches

Policy name	Type	Attached via
No resources to display		

This is the page of the STS.

STS
Allow All actions

Actions allowed
Specify actions from the service to be allowed.
Q Filter Actions

Effect
Allow Deny

Manual actions | Add actions
 All STS actions (sts:*)

Access level
► Read (Selected 5/5)
► Write (Selected 9/9)
► Tagging (Selected 2/2)

Resources
Specify resource ARNs for these actions.
 All
 Specific

Expand all | Collapse all

You have to give all permission to the user policy.

Manual actions | [Add actions](#)

All STS actions (sts:*)

Access level

- ▶ **Read (Selected 5/5)**
- ▶ **Write (Selected 9/9)**
- ▶ **Tagging (Selected 2/2)**

[Expand all](#) | [Collapse all](#)

▼ Resources

Specify resource ARNs for these actions.

All

Specific

⚠ The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

▶ Request conditions - *optional*

Actions on resources are allowed or denied only when these conditions are met.

Step 1
Modify permissions in temp_policy

Step 2
Review and save

Review and save Info

Review the permissions, specify details, and tags.

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

Search

Allow (1 of 462 services)

Service	Access level	Resource	Request condition
STS	Full access	All resources	None

Show remaining 462 services

[Edit](#) [Cancel](#) [Previous](#) **Save changes**

Then I have created the IAM Role to give the access with the Roles.

And then I have connected using IAM User and Switched to the Role.

Login to the user and click the switch user

The screenshot shows the AWS Account Info page. On the left, there's a sidebar with navigation links for Billing and Cost Management, Home, Getting Started, Dashboards, Billing and Payments, Cost and Usage Analysis, and Customer Carbon Footprint Tool. The main content area has sections for Account settings, Account display settings - new, Contact information, and Alternate contacts. A sidebar on the right displays Account ID (0896-6520-4192), Account name (Access denied), Account color (Access denied), and IAM user (balu). At the bottom, there are links for Turn on multi-session support, Switch role, and Sign out.

Give the account id of the root user and role name.

The screenshot shows the 'Switch Role' configuration dialog. It includes fields for Account ID (089665204192), IAM role name (temp-user), Display name - optional (temp-user @ 089665204192), and Display color - optional (Orange). At the bottom, there are 'Cancel' and 'Switch Role' buttons.

And then we will get this page.

It will give access to all the services.

AWS | Search [Alt+S] Global ▾ HARIHARAN K (0896-6520-4192) ▾ temp-user @ 089665204192

Billing and Cost Management > Account

Account Info ⓘ We are unable to determine the account's name or ID.

Account settings

ⓘ You don't have the account:GetAccountInformation and billing:GetSellerOfRecord permission required to view your account's settings. Learn more

Account display settings - new

Account color: Unset

Contact information ⓘ You don't have the account:GetContactInformation permission required to view your account's contact information.

Alternate contacts ⓘ You don't have the account:GetAlternateContact permission required to view your account's alternate contacts.

Currently active as: temp-user

Account ID: 0896-6520-4192

Account name: HARIHARAN K

Account color: Unset

Account: Organization: Service Quotas: Billing and Cost Management:

Signed in as: balu

Account ID: 0896-6520-4192

Switch back

Role history: temp-user @ 089665204192

Turn on multi-session support

Billings View New

Home Getting Started Dashboards New

Billing and Payments Bills Payments Credits Purchase Orders

Cost and Usage Analysis Cost Explorer Cost Explorer Saved Reports Cost Anomaly Detection Free Tier Data Exports Customer Carbon Footprint Tool