AWS CodePipeline Permission Access - Setup Guide

Overview

AWS CodePipeline does not have a built-in permission management feature. Instead, access control is managed through AWS IAM (Identity and Access Management).

This guide covers how to create IAM users with limited access for developers, allowing them to:

✅ Allowed:

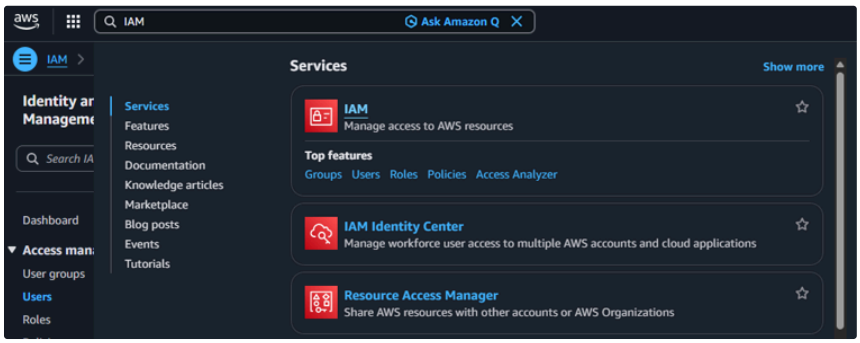
- View pipeline status
- View execution logs
- Re-trigger pipeline (Release change)
- Retry failed stage
- Stop execution

❌ Not Allowed:

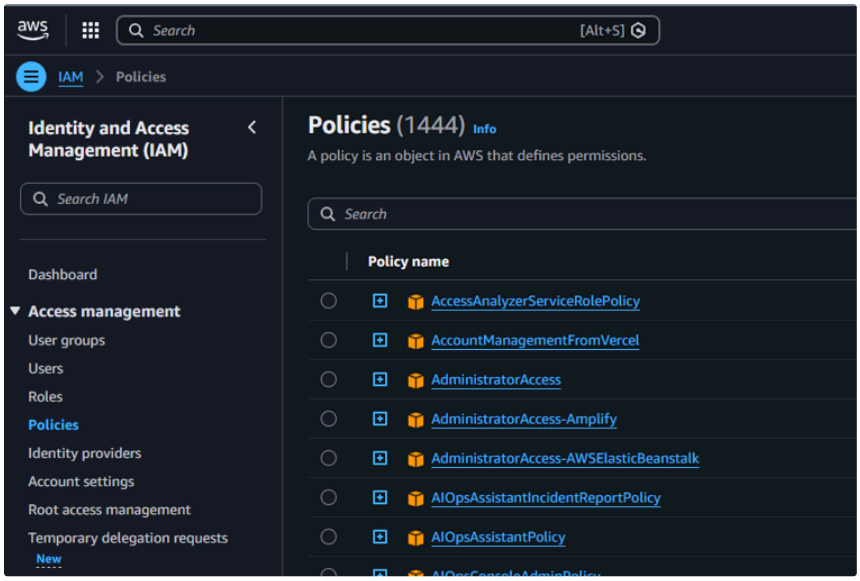
- Create pipeline
- Edit pipeline
- Delete pipeline

Step 1: Create IAM Policy

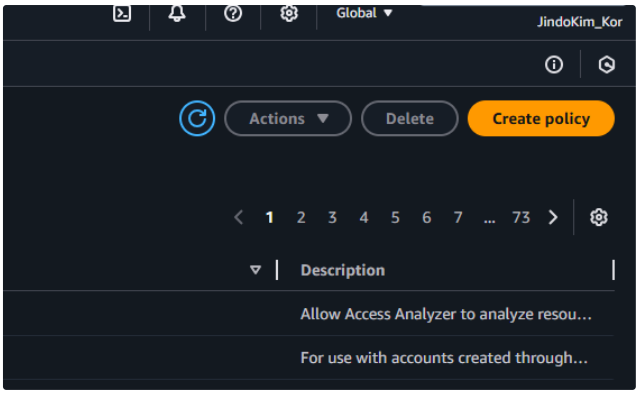
ℹ A policy defines what actions are allowed. In this step, we create a custom policy that grants limited CodePipeline access.



Search/Access 'IAM' service in AWS

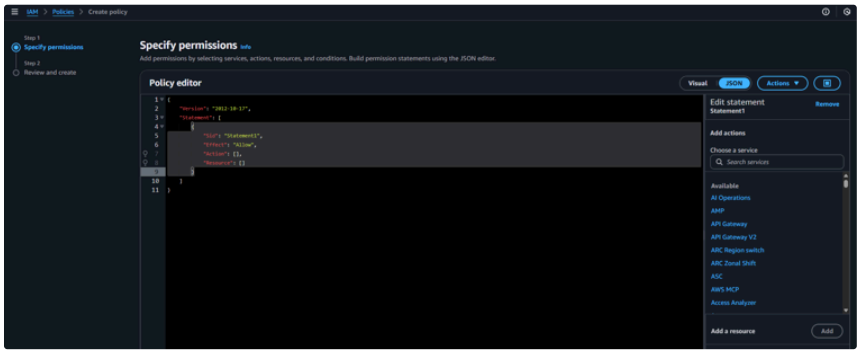


Open ‘Policies’ on the left side of the menu

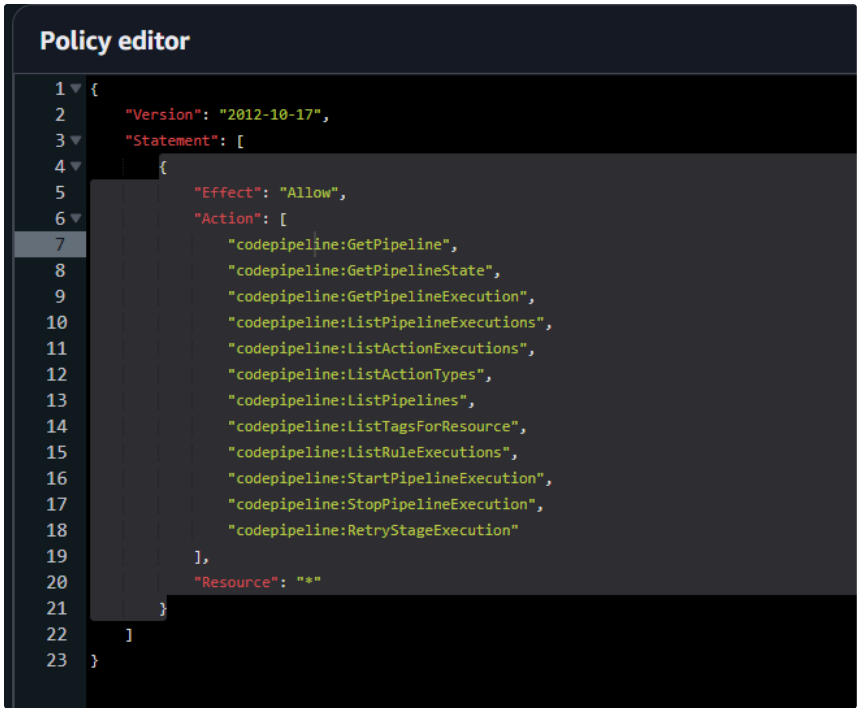


Click ‘Create policy’ button to create a collection of limited access for developers

---



Click ‘JSON’ Button to open JSON Editor



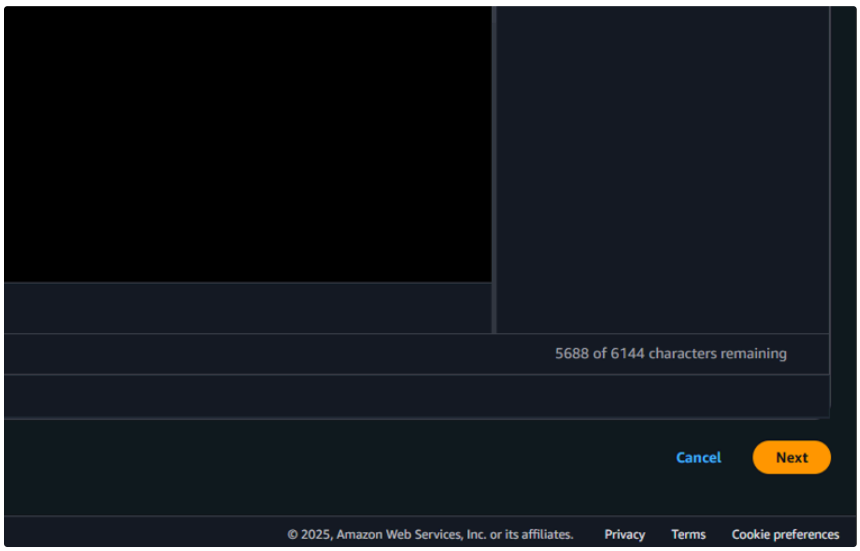
How it should look after applying the JSON file provided below

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "codepipeline:GetPipeline",
                "codepipeline:GetPipelineState",
                "codepipeline:GetPipelineExecution",
                "codepipeline:ListPipelineExecutions",
                "codepipeline:ListActionExecutions",
                "codepipeline:ListActionTypes",
                "codepipeline:ListPipelines",
                "codepipeline:ListTagsForResource",
                "codepipeline:ListRuleExecutions",
                "codepipeline:StartPipelineExecution",
                "codepipeline:StopPipelineExecution",
                "codepipeline:RetryStageExecution"
            ],
            "Resource": "*"
        }
    ]
}
```

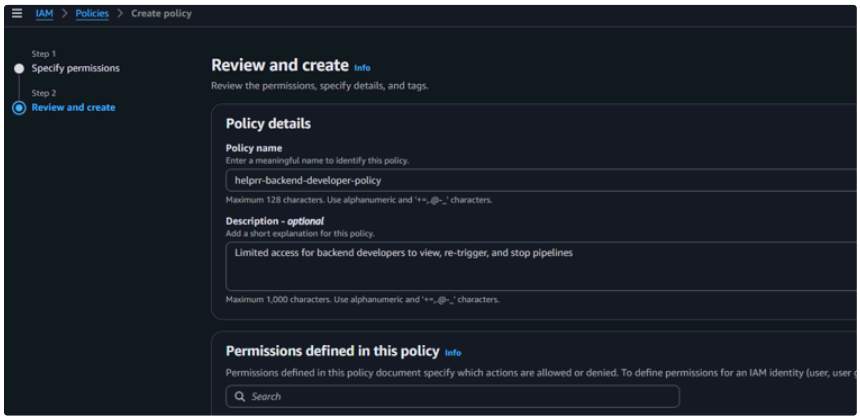
Note: Below is a brief explanation of each permission included in this policy.

Permission	Description
`GetPipeline`	View pipeline configuration
`GetPipelineState`	View current pipeline status
`GetPipelineExecution`	View execution details

`ListPipelineExecutions`	View execution history
`ListActionExecutions`	View action-level execution details
`ListActionTypes`	View available action types
`ListPipelines`	View list of all pipelines
`ListTagsForResource`	View pipeline tags
`ListRuleExecutions`	View rule execution details
`StartPipelineExecution`	Re-trigger pipeline
`StopPipelineExecution`	Stop running pipeline
`RetryStageExecution`	Retry failed stage



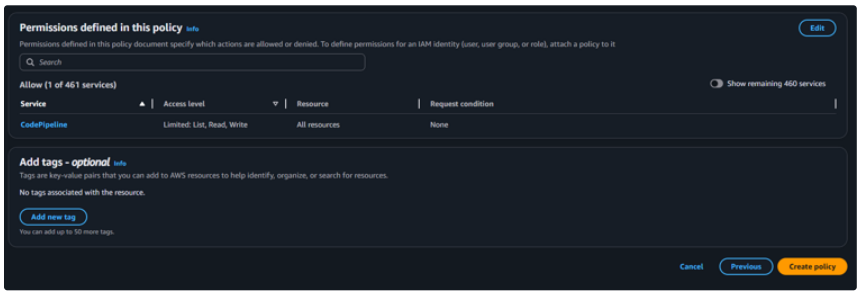
Click 'Next' Button



Fills up the Policy name and description

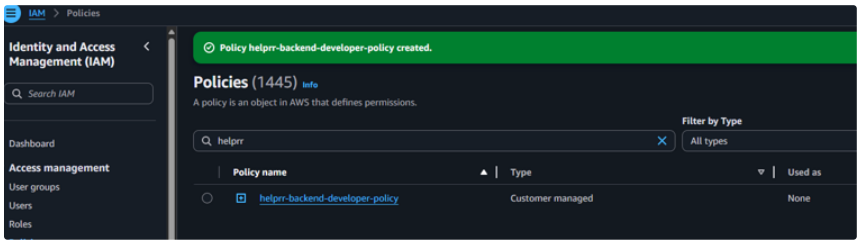
- Example:

- Policy name: `helprr-backend-developer-policy`
- description: `Limited access for backend developers to view, re-trigger, and stop pipelines`



Confirm if 'CodePipeline' Service in the list and Click 'Create policy' button

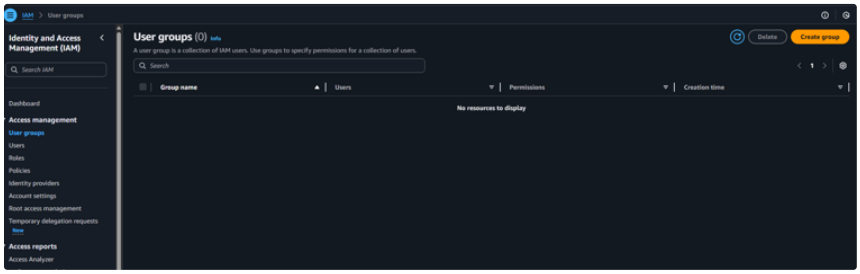
---



The created success toast message showed and search the policy name to see whether it is under policy list

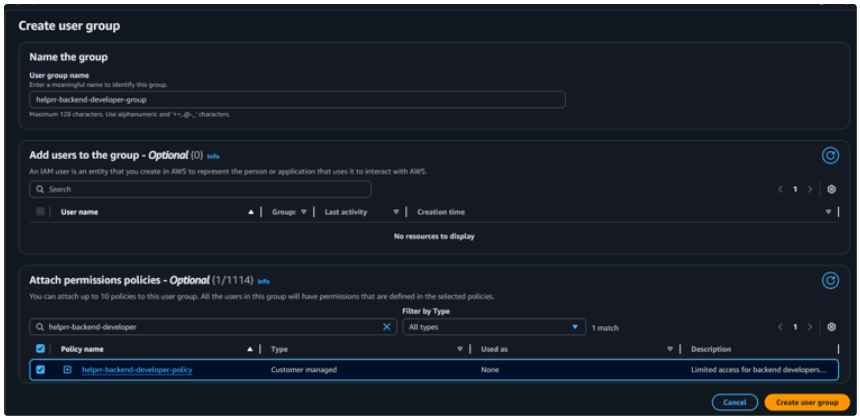
Step 2: Create User Group

A user group allows you to **manage permissions for multiple users at once**. Instead of assigning the policy to each user individually, we attach it to a group. Any user added to this group will automatically have the same permissions.



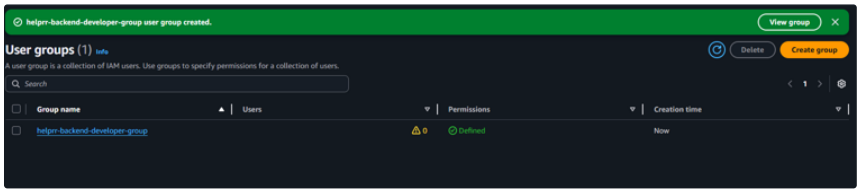
Open 'User groups' on the left side of the menu and Click 'Create group' Button

---



Fills up the ‘User group name’ and Select the custom policy created in previous step, and then Click the ‘Create user group’ button

- Example:
  - group name: `helprr-backend-developer-group`
  - Attach permission policies: `helprr-backend-developer-policy`

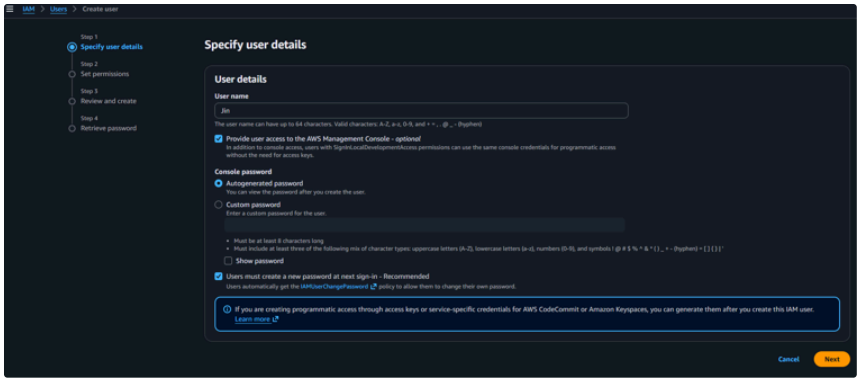


The success message will appear and the group will be shown in the list

Step 3: Create First User

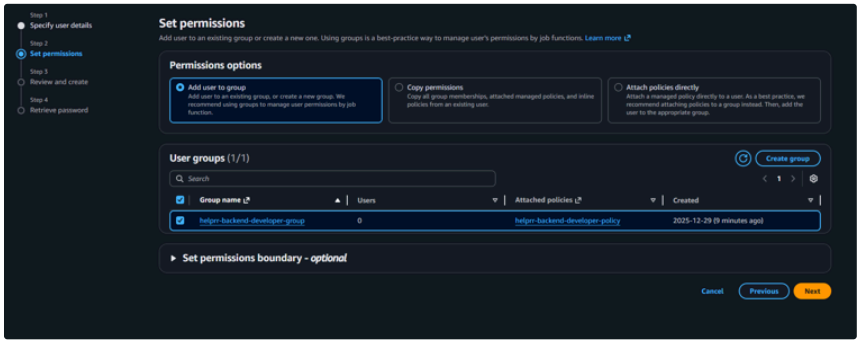
> Now we create an IAM user for the developer. This user will be added to the group we just created, which automatically grants them the limited pipeline access.

Open ‘User’ on the left side of the menu and Click ‘Create user’ Button



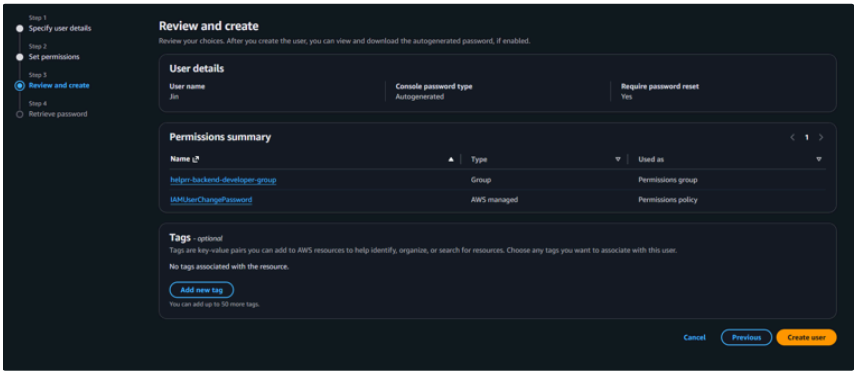
Fills up the ‘User name’ form and check ‘Provide user access to the AWS Management Console - optional’, And then Click ‘Next’ Button

⚠ **Important:** You must check "Provide user access to the AWS Management Console". Without this, the developer cannot log in to AWS Console to view pipelines.

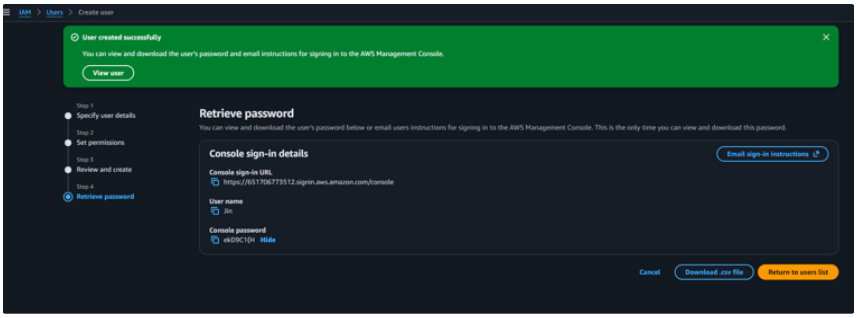


Check the user group created in the previous step, and then Click the ‘Next’ Button

---



Review the settings and Click the ‘Create user’ Button



The success message will appear in green

⚠ **Important:** This is **the only time** you can view the password. Make sure to copy it before closing this page.

Step 4: Share Login Info with Developer

After creating the user, you will see the login credentials. Share the following information with the developer:

- **Console sign-in URL**: The URL to access AWS Console
- **User name**: The username created
- **Console password**: The temporary password