Managing Permissions with AWS IAM

Sristi Acharya

Sristiacharya13

linkedin.com/in/sristiacharya

WHAT IS AWS IAM?

What it does:

It is a web service that helps you securely control access to Aws resources.

Why it’ s useful:

It helps to manage and grant access to resources as a form of providing protection.

How I’ m using it in this project:

To create instances, manage users and groups by assigning permission to be able to access resources by allowing and denying them.

SETTING UP TAGS

- I have set up two EC2 instances to test the effectiveness of the permission settings I will set up in AWS IAM. I have used tags to label them.

- Tags are like labels assigned to Aws resources for an organization to help to identify and manage resources in a more efficient manner. Tags are useful for cost allocation and budgeting, resources organizations and setting security policies.

- The tag have used on my EC2 instances is called Env. The value I have assigned for my instances are Production and development.

i-04efd77d13b057c7a (project-production-sristi)

Details | Status and alarms | Monitoring | Security | Networking | Storage | Tags

Tags

Key	Value
Name	project-production-sristi
Env	production

i-060c654a0afa863e6 (project-development-sristi)

Details | Status and alarms | Monitoring | Security | Networking | Storage | Tags

Tags

Key	Value
Env	development
Name	project-development-sristi

IAM POLICIES

- IAM Policies are set of rules that helps to allow/deny users or resources access or permission to perform a particular actions.

- For this project, I have set up a policy using JSON editor.

- I have created a Policy that will allow permission to EC2 instances that contains a tags **Env** and a value of **development** in the JSON policy file.

When writing JSON Policy statements, we have to specify the
Effect: This will allow/deny for any action. Action: This are things that you can do on a EC2 instances by allowing/deny based on the policy.

Resource: refer to the AWS entities on which actions specified in the policy are allowed or denied.

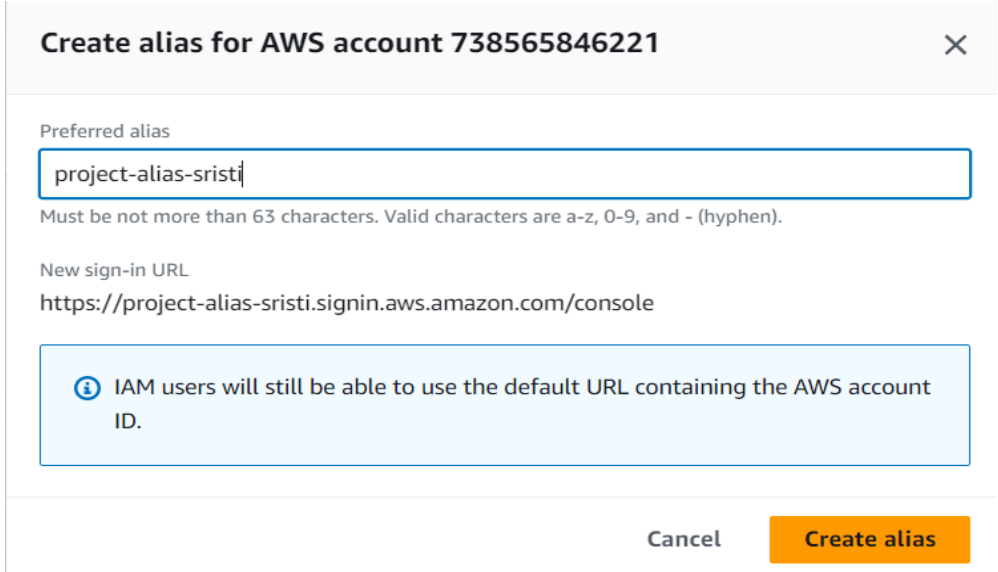
Policy editor

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Action": "ec2:*",
7              "Resource": "*",
8              "Condition": {
9                      "StringEquals": {
10                         "ec2:ResourceTag/Env": "development"
11                     }
12                 }
13             },
14             {
15             "Effect": "Allow",
16             "Action": "ec2:Describe*",
17             "Resource": "*"
18             },
19         {
20             "Effect": "Deny",
21             "Action": [
22                 "ec2:DeleteTags",
23                 "ec2:CreateTags"
24                 ],
25             "Resource": "*"
26         }
27     ]
28 }
```

AWS ACCOUNT ALIAS

- When new users get onboarded onto my AWS account, they get access by signing into a unique URL created for my account' Account ID.

- An account alias is a friendly name for your Aws account you can use to sign into Aws management console instead of your account.



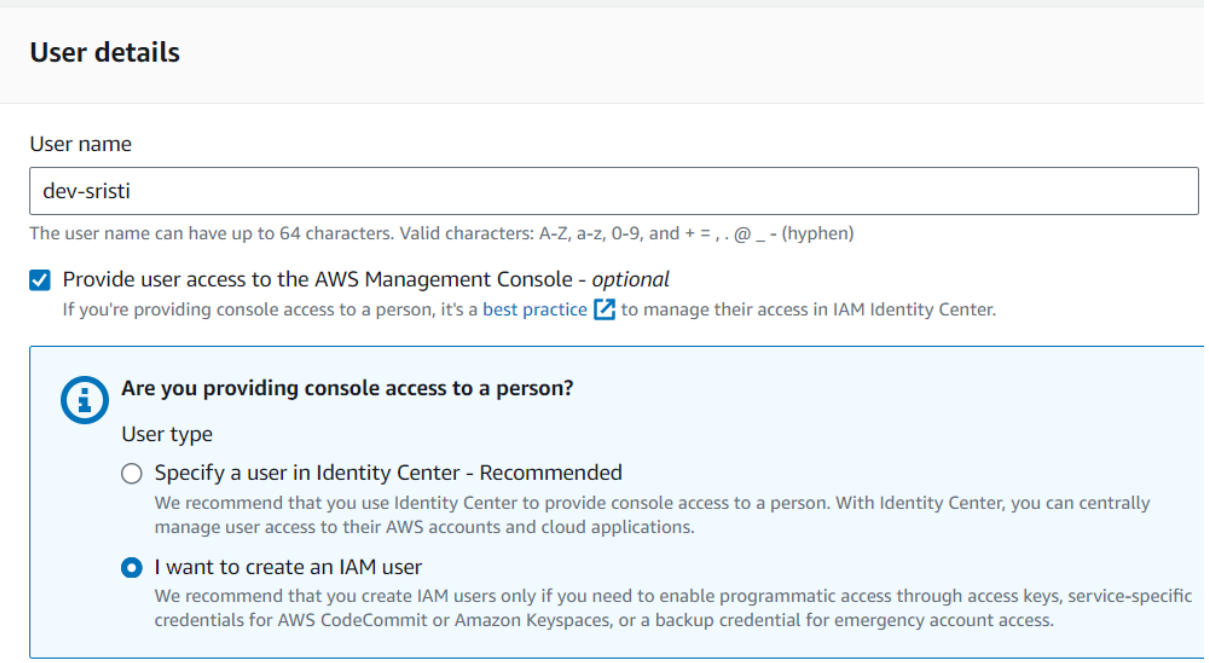
- Now, my new AWS console sign-in URL is https://project-alias-sristi.signin.aws.amazon.com/console

IAM USERS + USER GROUPS

- IAM Users are entities created and granted access to Aws resources and managed by an Administrator of that account/resources.

- I also created a User Group. User Groups are useful for managing and granting access to user a in a particular group.

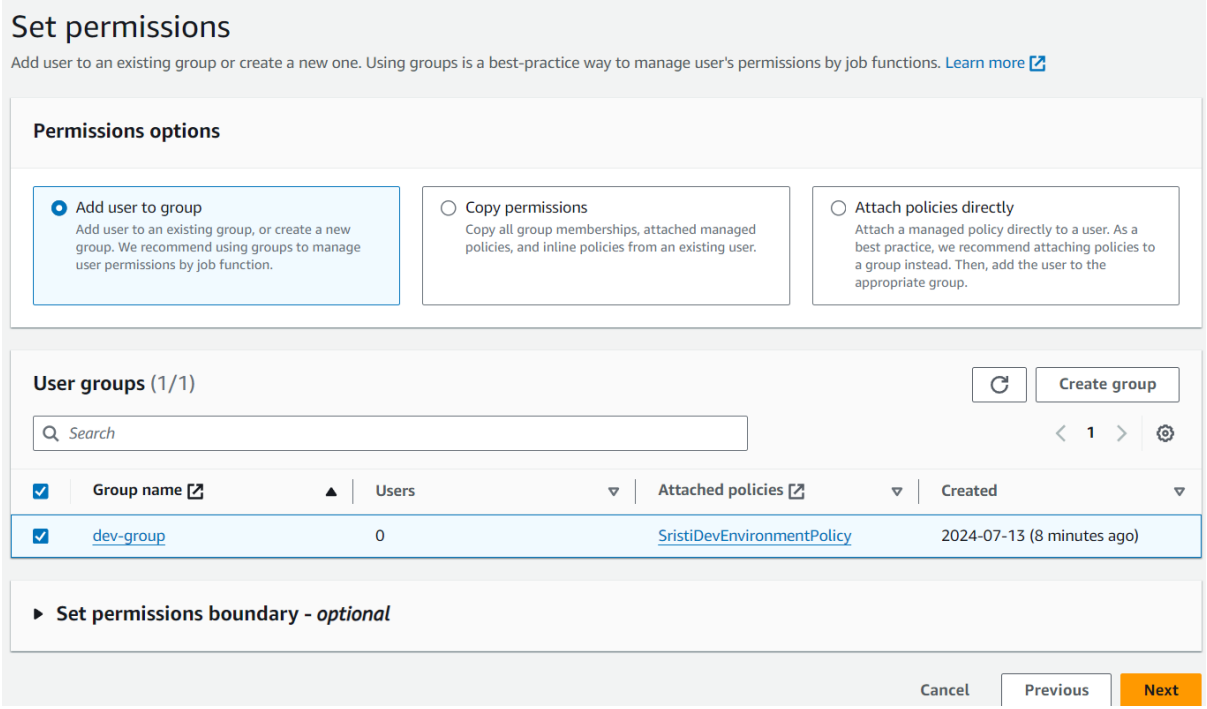
- My User Group is called dev-sristi, I attached the Policy I created to this User Group, which means all users in that group will be granted the access to that resources based on the group permissions set.



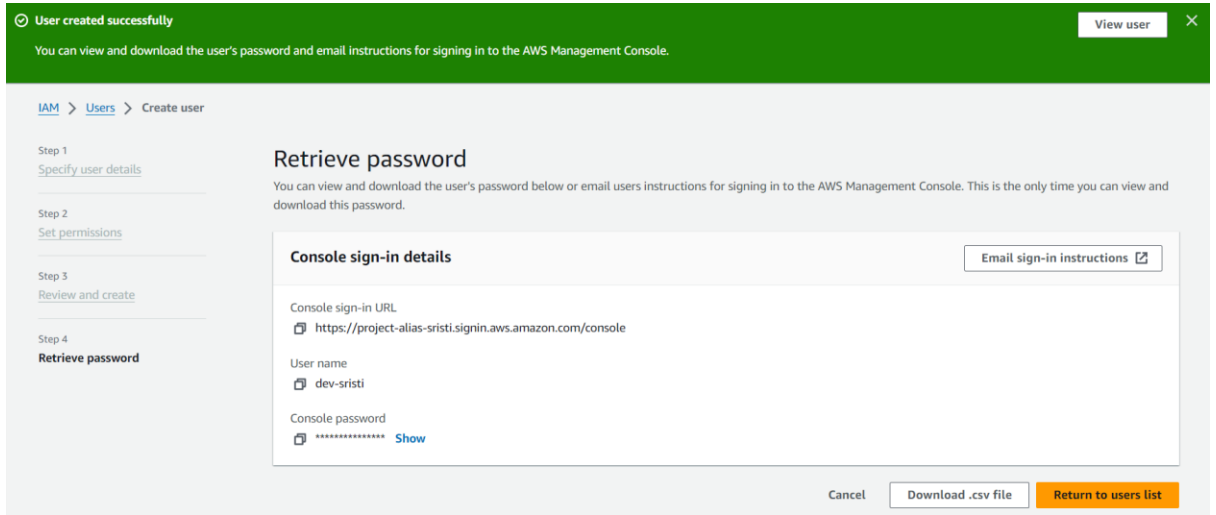
- When I created a new User, I had to tick a checkbox that will grant users to access the Aws management console.

- Once my new user was set up, there were two ways I could share its sign-in details:
  Firstly, by emailing the user with the credentials. Secondly, by downloading the csv.file that contains user credentials.

- My new user had a unique sign-in URL - https://project-alias-sristi.signin.aws.amazon.com/console



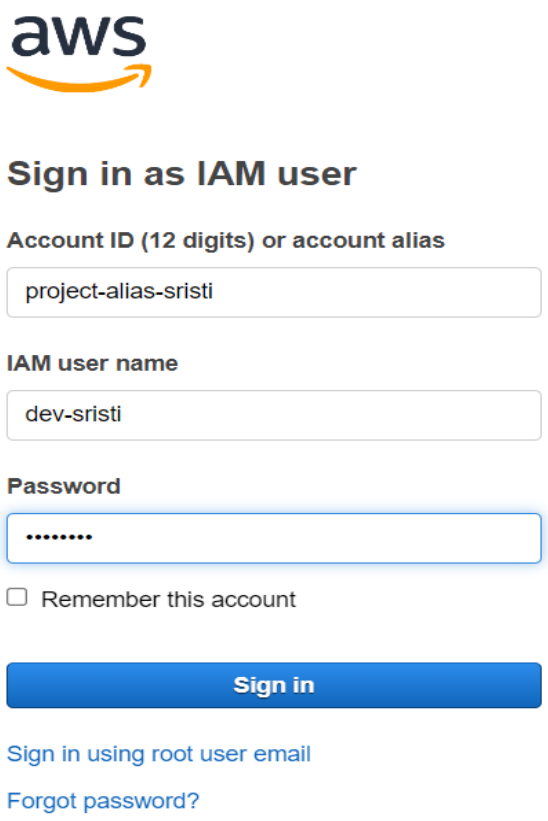
My user's sign-in credentials



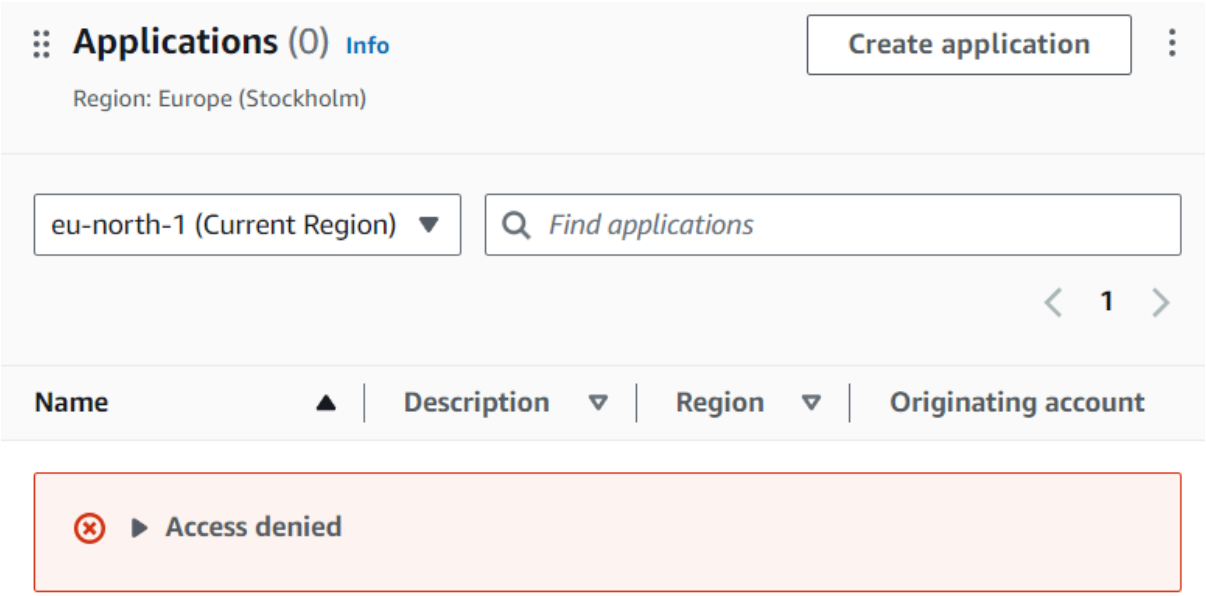
IAM USER IN ACTION

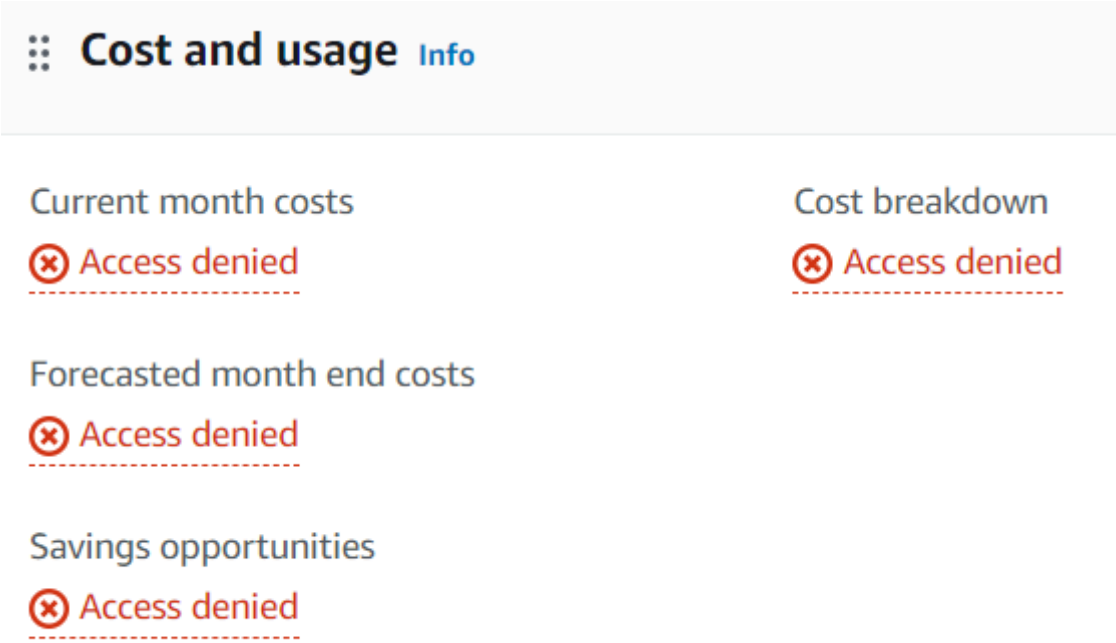
- Now with my IAM Policy, IAM User Group and IAM User all set up, I logged into my AWS account as the new user.

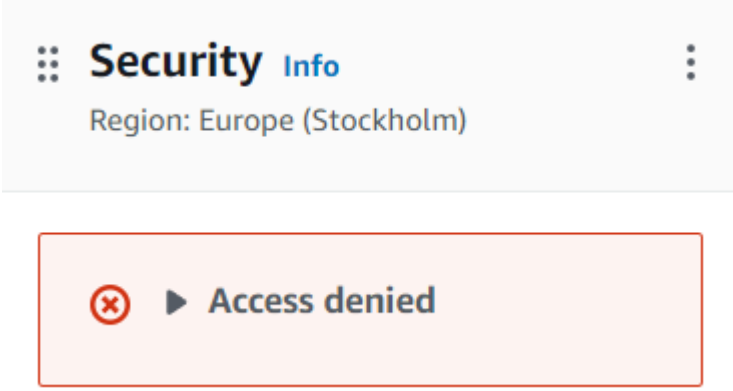
- To log in as my IAM User, I used the URL to login in order to get access to the Aws management console after creating the user.



Once I logged in, I saw so may access denied from different panels on the dashboard. It looks different from then AWS Management Console.







IAM POLICIES IN ACTION

I tested the JSON IAM policy I set up by stopping the development and production instances by triggering an alert. When I tried to stop the production instance, i had a red popup notice/alert. The user did not have the right permission to stop the instance from running.

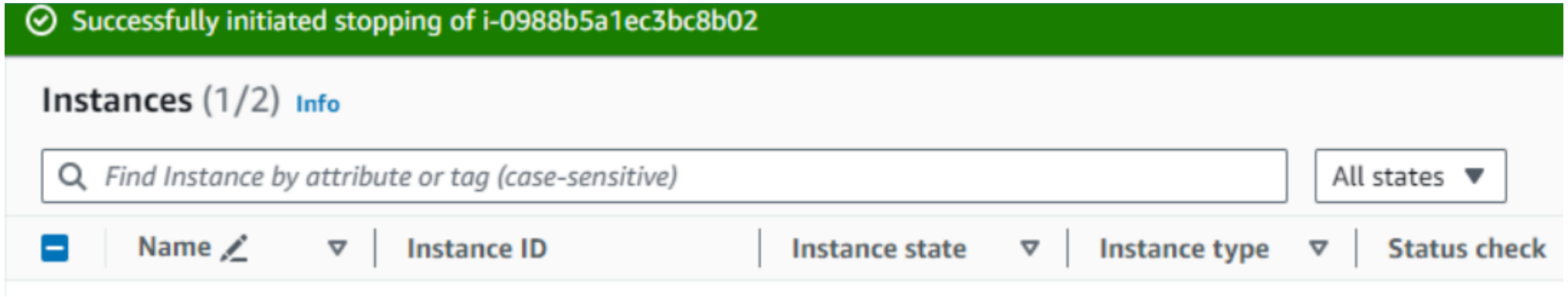
A red fail banner pops up if I stop the production instance

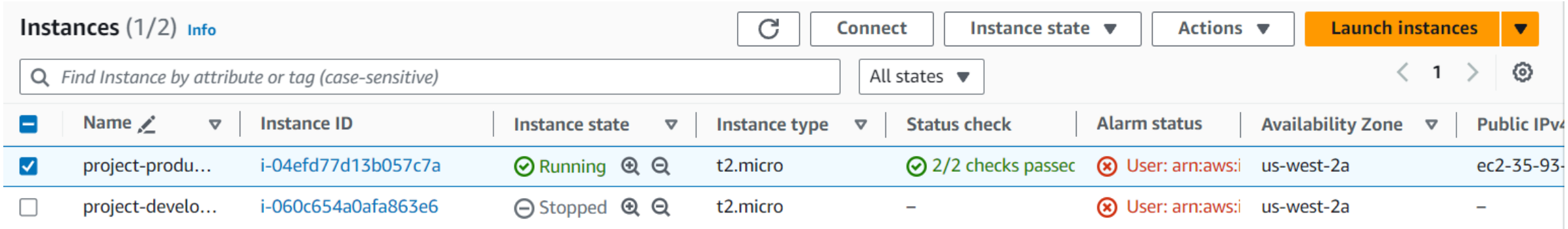
Failed to stop the instance i-04efd77d13b057c7a

You are not authorized to perform this operation. User: arn:aws:iam::738565846221:user/dev-sristi is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-west-2:738565846221:instance/i-04efd77d13b057c7a because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: dsE7vAxLnVNdS2QVBRIt4KULai9P7HCFts3GMUbkMQxI5_CsGY4-fMgRZ8l2gu1h_szhavz71ZV1mO1_n_fy5CgCCRbRjRz-nrN-wAXTqcCXqC0iXTn9GZsMt4POdG0mpR2NG1cSXcNOGWD2VLVdCuXz9SOTtR8mBn2EG_1dVMHD7kCh3xjWUYBzpYogMq2dnPeeElF0OMK6RC5ULrBJQ9FMGexIX3Wrvvd0tA-rQ8UiLaLf1MRKI5u3xokbdsta2rphHQ_jZG8zkOxOed5bVVVMNYkWoykStGKGTU-5XeQWshj8qh27wOdRsroTG2VerTkc-K-PeX-TDGALDzORvFEob_xK5vNSHLcR27O1F_T5BFobSeYRf7MvjUr2EcDj--tAG5VAnk_lDjVsAZpu2GHEAwSpOzJ_1t8GJGABIGjlJTz_Uf6exOZo5lRsm1tD9J8HNO9UG2bAQQ8rVo-rPSEGVLQ-pWM0UXbVC8dfd2S9q8qNwMijKexJ2GydrYXYWGkuRPg_nbNttZp83lFN06vufKeuxGDF7qBkZ5oq4yLsOILYidUixxboISQPelazG06wH-xc9e5Gufim-9VvCpOwUsHKLsTK49EWKLO-goq7xR58UOIrsuVXyud1bpFGwp4Lh6LSvZ3Pvx3oYg1prTJSXOsPB4gov7IUV3T8hPaIHIvMuAN3k9HlLkfkCpTkKL-KGJhaR55JCNfkDmhiALYu8NO35X6lO5FfKGR_LnJLnVjvVrDiriAHlo8ikwShZERmKrtxvhsxKgHyvTTItzesQizi5tZCVLaoT17-YJnaWhWsgsIdLS8DrsTzHvL0H_ba5N0

Next, when I tried to stop the development instance, I had a green popup alert **“Successfully initiated stopped”.** The user was able to stopped the instance from running because of the group policy set which the user was part of.

A green success banner pops up if I stop the development instance

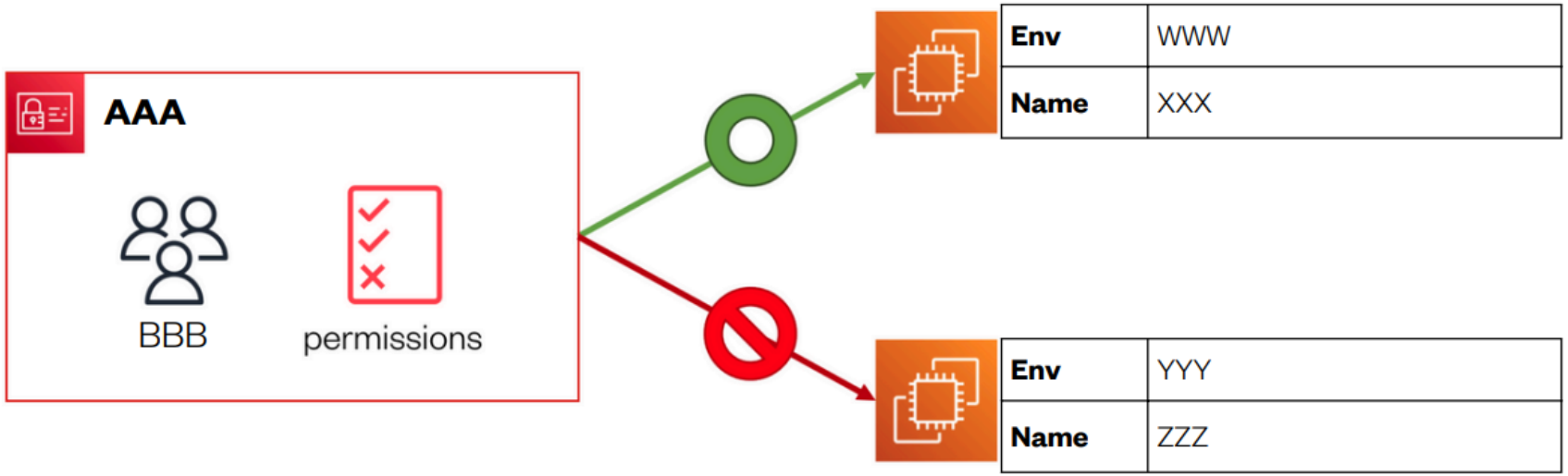




TO SUMMARISE

I created:

- An IAM User Group called **dev-group** with defined permissions using an IAM Policy.
- An IAM User called **dev-sristi** is added to the user group
- An EC2 instance with the Env tag development and Name **project-development-sristi**
- An EC2 instance with the Env tag production and Name **project-production-sristi**



My Key Learnings

- What are IAM Policies are set of rules helps to allow and deny users certain permissions to a resources.

- What is an AWS Account Alias are friendly names created that can be used to access Aws management console instead of using a actual account to login.

- What are IAM Users are entities created and granted permission to perform or access certain resources by a policy. It helps to create and manage by allowing and deny based and rules .

- What are IAM UserGroups is a folder or container that users are managed by setting a group policy which allows or deny what those users under that group can have access to what resources. It is easy to manage a lot of users by just setting a particular policy and all users get affected.

- I have learnt how to create instances ,assigned policies to users and groups, how to stop instances with certain users or group users based on set policy and permission given. Also how to set a JSON policy file.