# AWS Switch IAM Role between Accounts

## Introduction

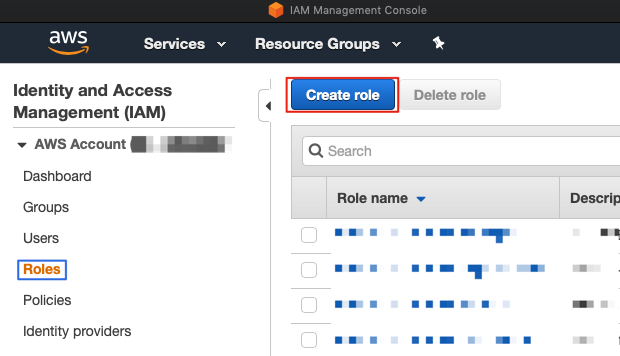
[A role specifies a set of permissions that you can use to access AWS resources that you need. In that sense, it is similar to a user in AWS Identity and Access Management (IAM). When you sign in as a user, you get a specific set of permissions. However, you don’t sign in to a role, but once signed in you can switch to a role. This temporarily sets aside your original user permissions and instead gives you the permissions assigned to the role. The role can be in your own account or any other AWS account. For more information about roles, their benefits, and how to create them, see IAM Roles, and Creating IAM Roles.](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html)

So, the scenario for this walk through is, Mary, an IAM user, from account-A will be managing account-B. Therefore, a role in account-B must be created for Mary to be assumed when switching account. Important! you must use IAM user account, NOT ROOT account, when switching role from account-A to B.

The steps are quite simple,  
1. Create a role with appropriate privileges in **account-B**.  
2. In account-A, setup role switch configuration.  
3. Make sure to use IAM user in account-A, that’s it!

Let’s begin.

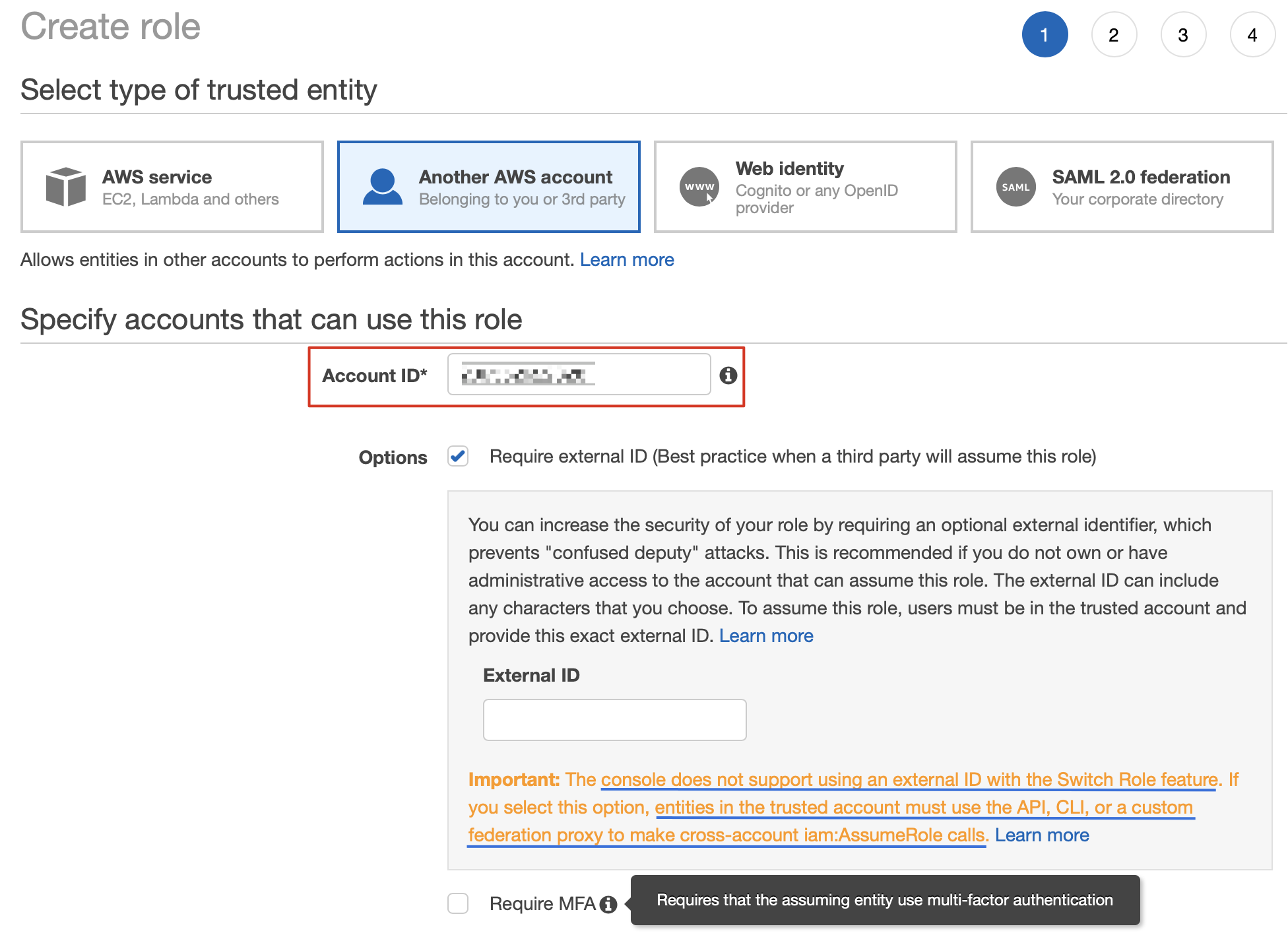
Sign in **account-B**, from IAM service, start by creating role.



AWS IAM SWITCH ROLE

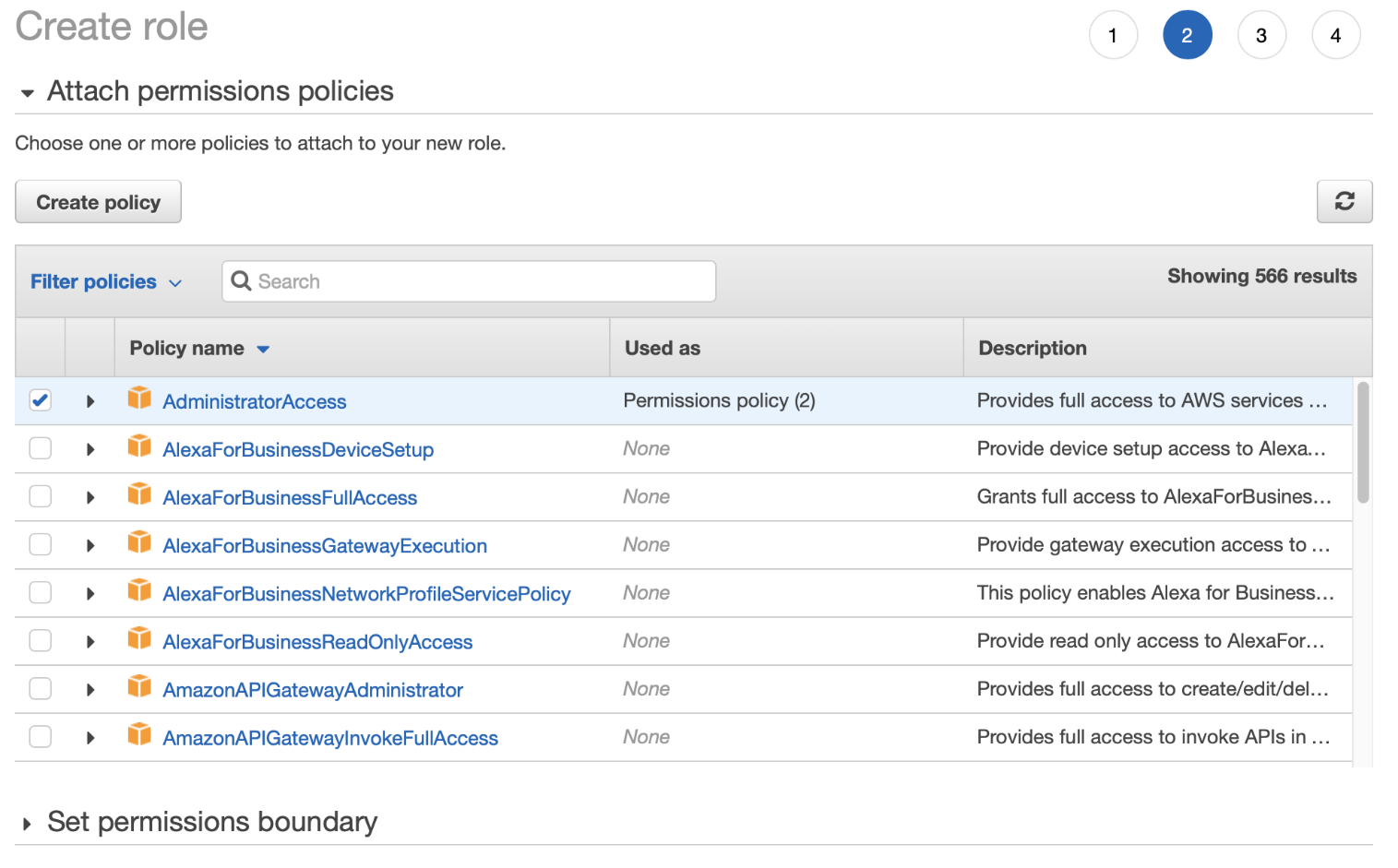
There are four types of trusted entity. Since we are going to allow Mary from account-A to access account-B, so we choose “Another AWS account”. In the Account ID, we input **account-A’s** account ID (We are in account-B’s account now).

There are “require external ID” and “require MFA” options when creating role. Both options are for higher security and in simple words, when using “external ID”, you can only use API, CLI or custom federation proxy calls to switch role. When using “require MFA”, only user authenticated with MFA is allowed to switch role. For this walk through, I will leave both empty.



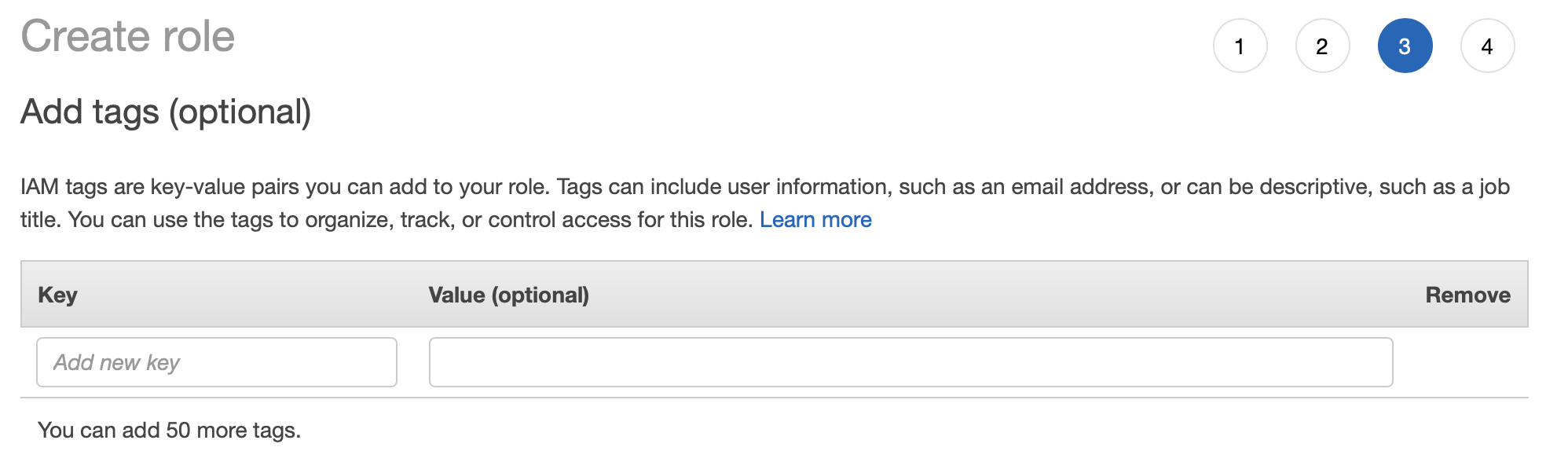
AWS IAM SWITCH ROLE

Next, assign appropriate privilege to the role. Whatever privileges you given here, means that user switching to this account ( account-B ) has those privileges. For this demo, I choose AdministratorAccess.



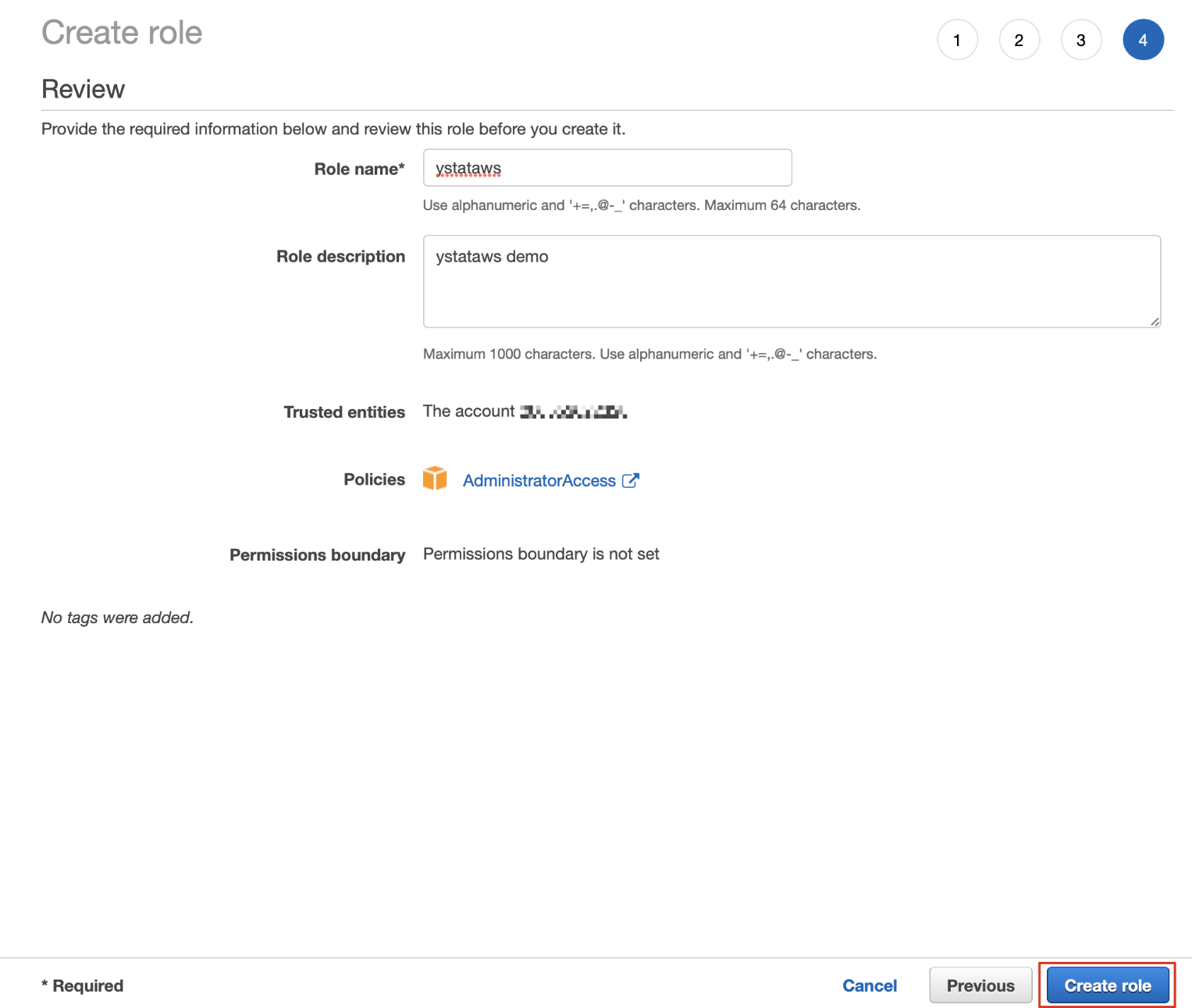
AWS IAM SWITCH ROLE

Add tags at your choice.



AWS IAM SWITCH ROLE

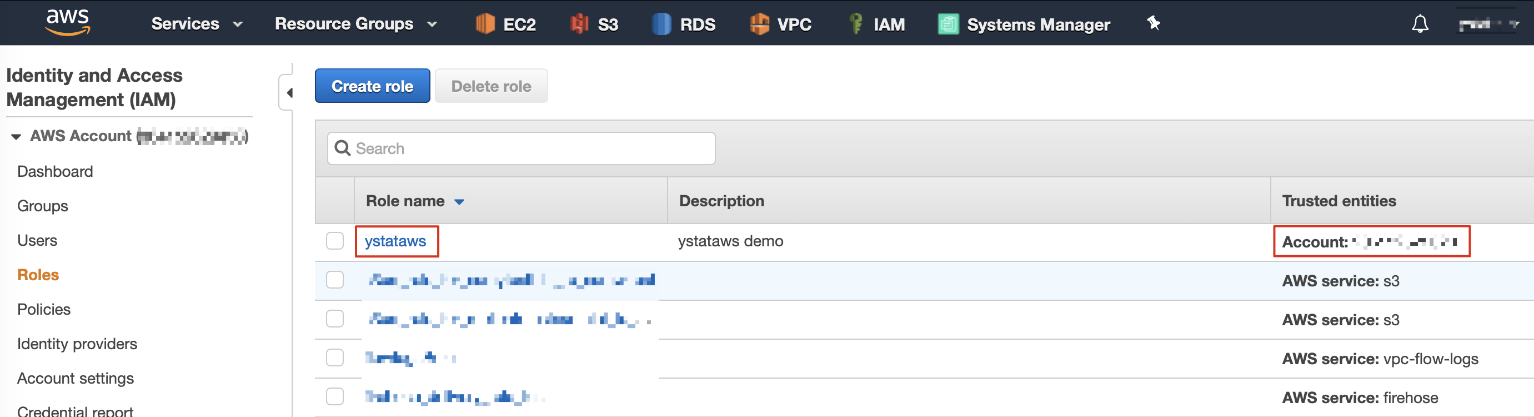
Finally, give your role a name and optionally, a description.



AWS IAM SWITCH ROLE

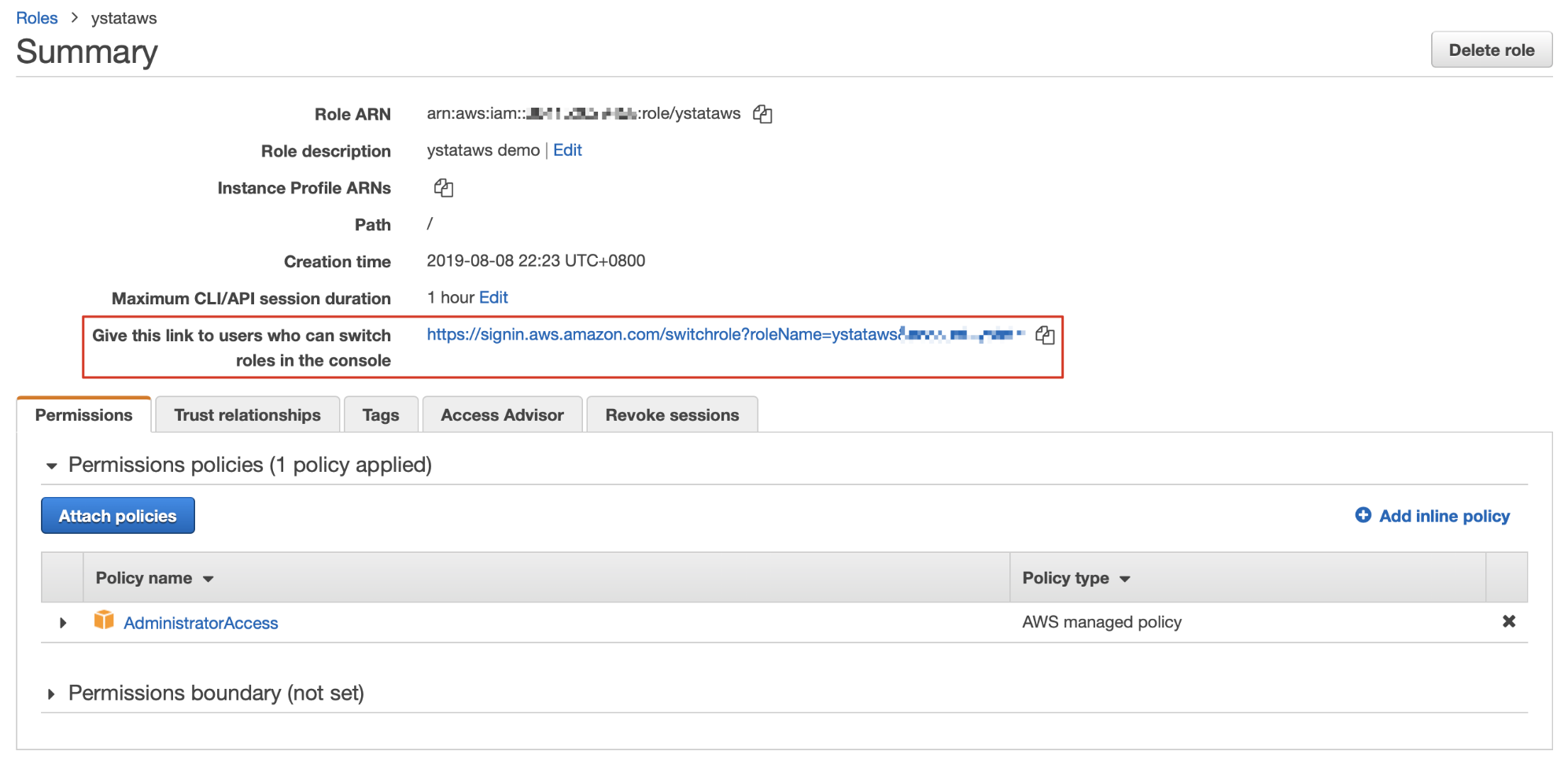
A finish view of role creation. Pay attention that in the “Trusted entities” column, the role we just created is valued with “Account: account-A’s ID”. Click on the role to see more details.

https://miro.medium.com/max/60/1*i3CR_l7WmEHp5xwLojG4hw.png?q=20



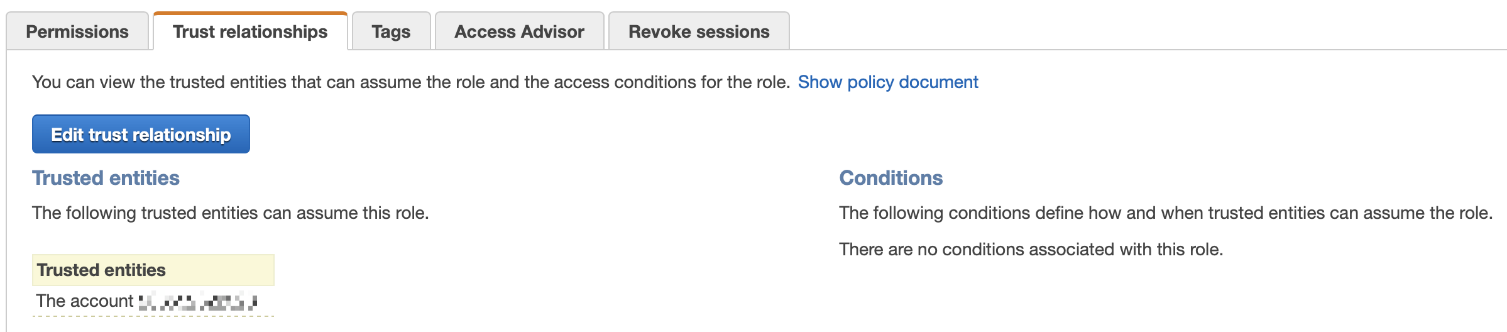
AWS IAM SWITCH ROLE

From here, give the link to Mary in account-A and she can use this link to assume **role ystataws** to switch to account-B.



AWS IAM SWITCH ROLE

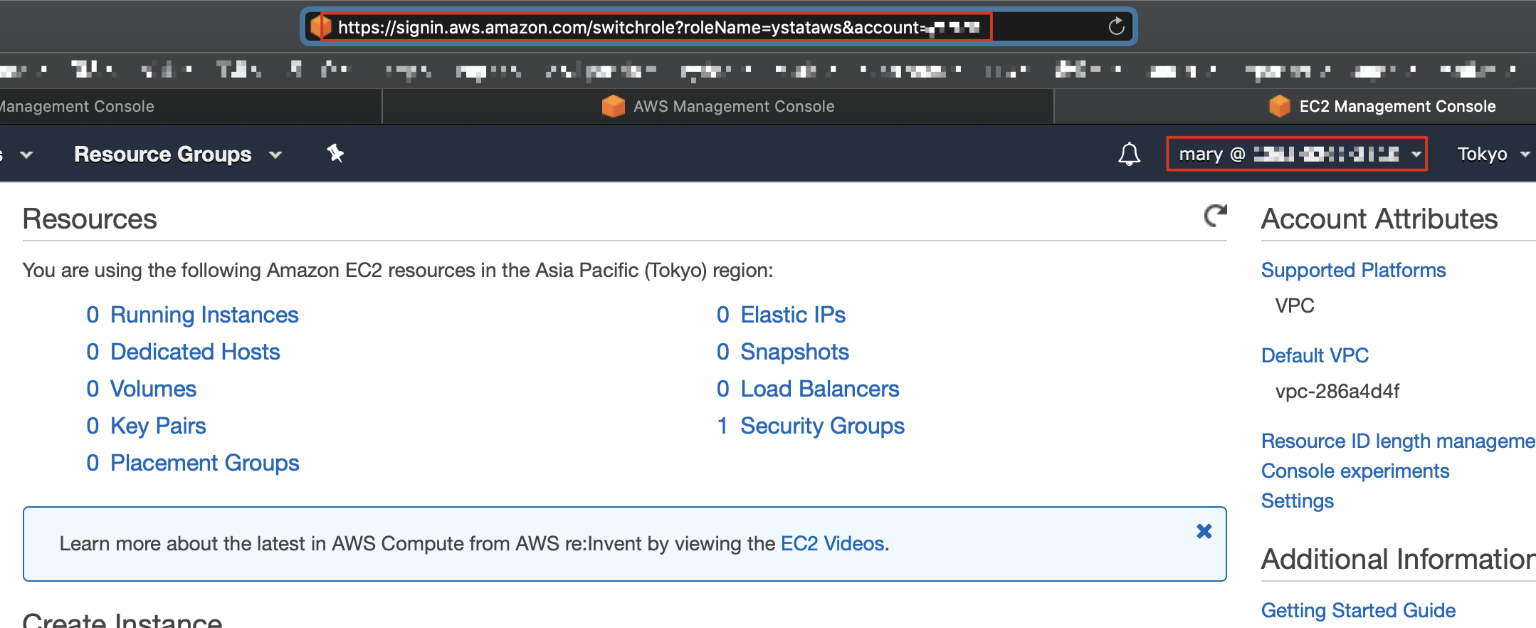
From “Trust relationships”, you will see **Account-A’s** ID here and you can make more detailed modification by using “edit trust relationship”.



AWS IAM SWITCH ROLE

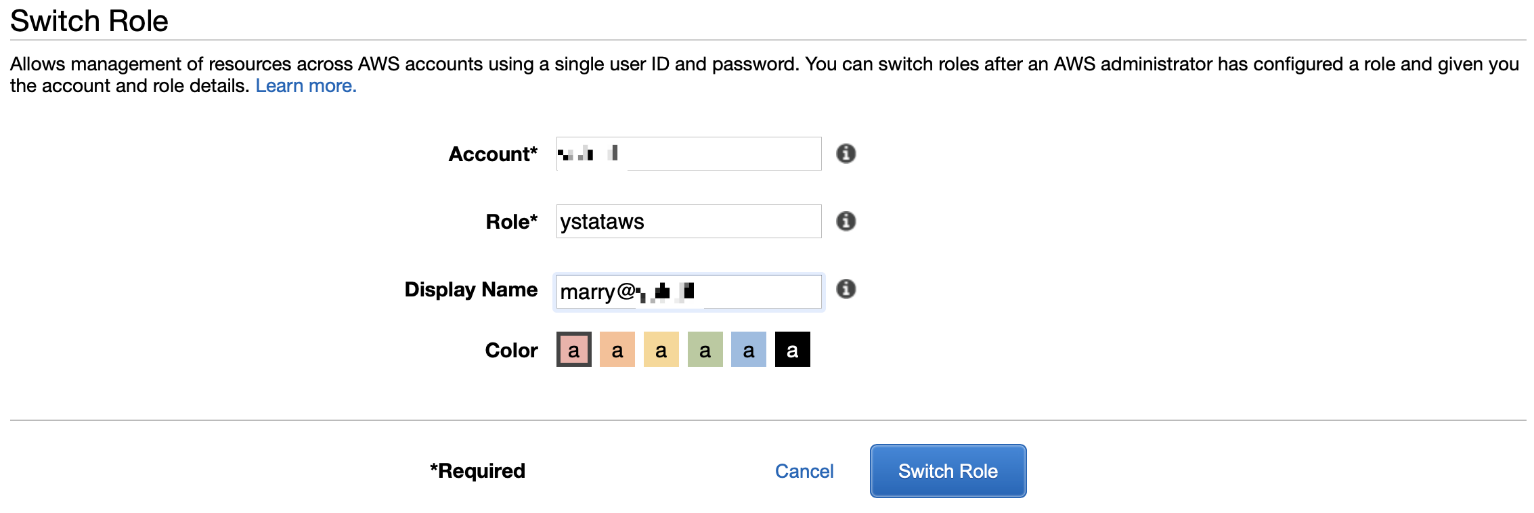
That’s it for account-B, let’s jump to Mary’s account, account-A to setup switching role configuration.

Sign in a**ccount-A** with IAM user Mary. Paste the URL provided by **role ystataws** (Check the second image above) in the browser and hit enter.



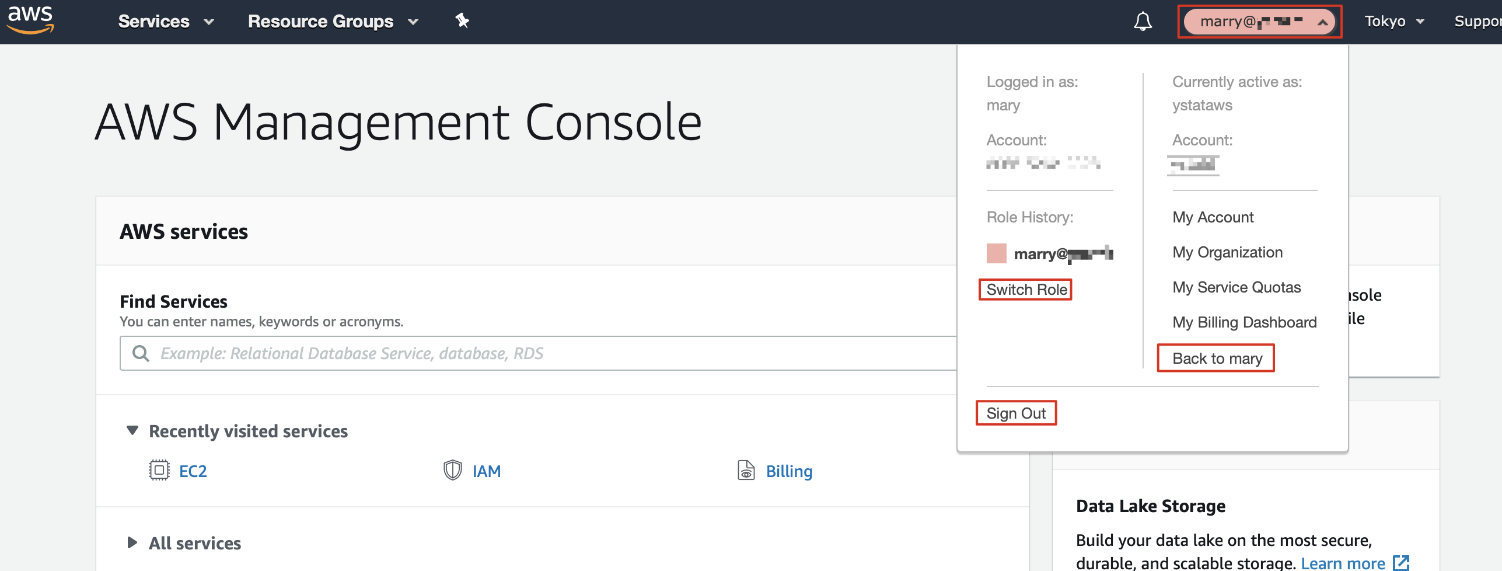
AWS IAM SWITCH ROLE

If everything is setup correctly, you will see this page with appropriate values filled in. Leave **Account** and **Role** untouched. Change Display Name and Color at your choice. Click Switch Role when done.



AWS IAM SWITCH ROLE

After click “Switch Role”, you are now in the account of **account-B**! You can confirm from your account information shown as image below. You login as Mary from **account-A** and Currently active as ystataws (role) in **account-B**. And since role ystataws is given **administratorAccess**, that means you can do anything to account-B now!



AWS IAM SWITCH ROLE

When you have done with whatever you need to, simply Sign out from console or switch back to Mary!