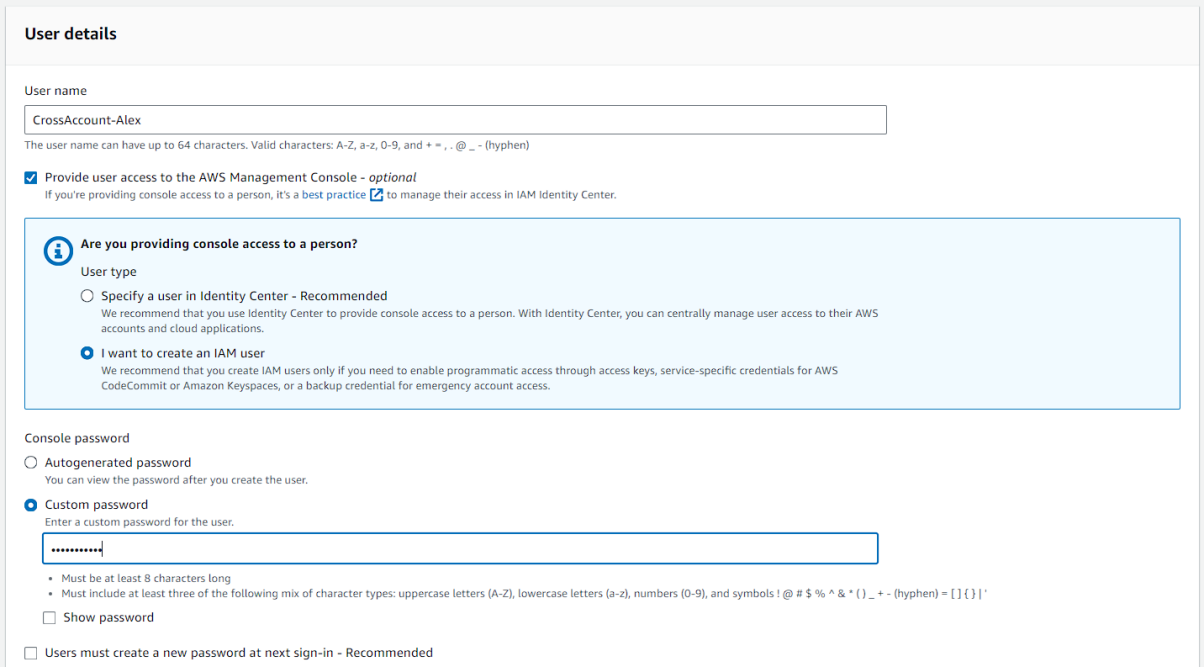
# 😊 Cross Account IAM Roles

1. So basically, you have two sets of accounts. First one is referred as the identity account. So, identity account is where the identities are stored and what are identities. Identities are IAM users and then you have various other accounts where the actual resources are created. It can be S3 bucket, it can be EC2 instances and so on.
2. So, the architecture is the IAM user will log in to this identity account and then depending upon the permission of the user, he can log in to account B account C or whatever AWS accounts are present through the assume role functionality.
3. Now the overall steps that are involved are three.
4. First one is you have to create a user in account A. So, the account A is nothing but the identity account.
5. Then you need to create a cross account role in account B. So, cross account role is where you go ahead and create a IAM role and this IAM role is what the IAM users from the identity account will be assuming.
6. And then the third step is allowing user to switch to account B role. So, the IAM user that has stored in the identity account, that user also needs the permission to assume this role so that permission you'll have to give in the identity account.

## 😄 Step 1: Create User in Account A

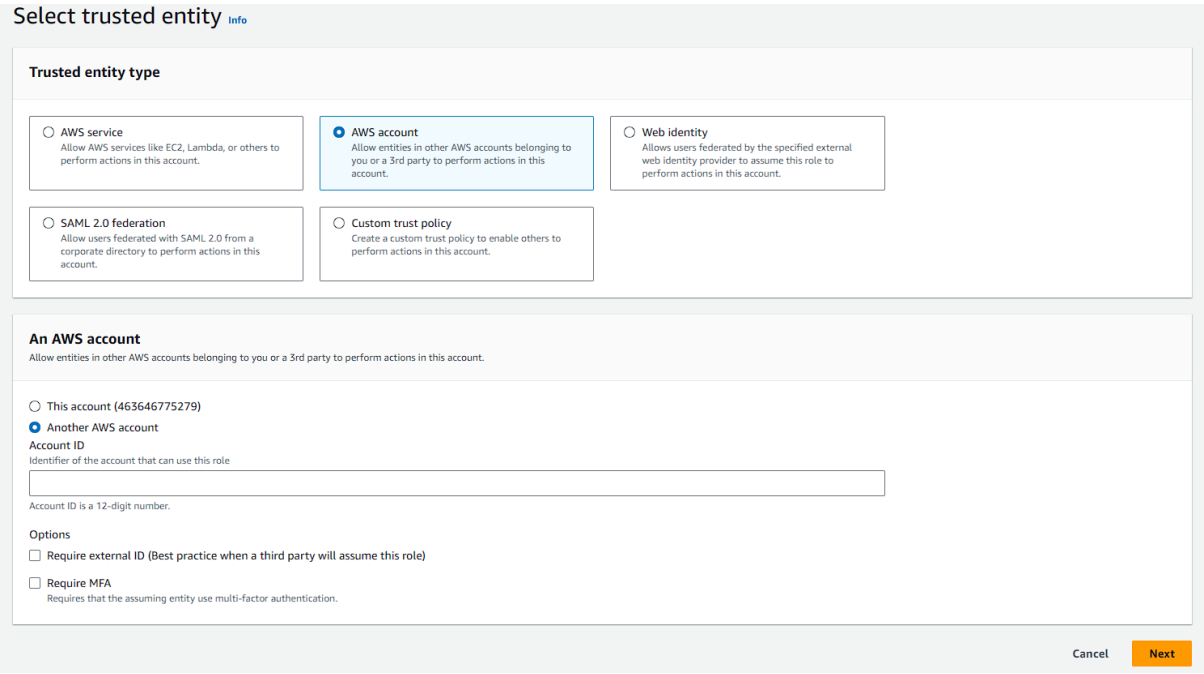
1. Now for this lab you should be having two accounts and you need to login in both of these accounts.
2. Now go whichever you have considered account A, navigate to it. Then go to IAM and create a user.
3. Give your user a name and then provide it with AWS Console access.
4. Then type in your custom password and uncheck for new password at next sign up.
5. Then create your user without attaching any policies.




6. Once your user is created then move to step 2.

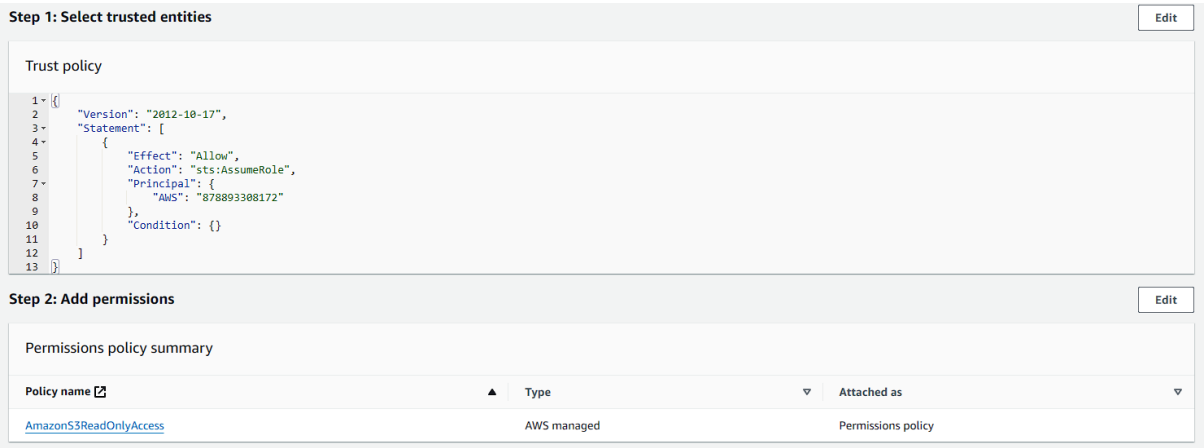
## 😄 Step 2: Create Cross Account Role in Account B

1. Now you need to navigate to your account B and go to IAM.
2. There you are going to create a new role. Now while creating your role, you need to click on AWS account and in that you have to select Another AWS Account.
3. Afterwards go back to your Main account and copy your Account ID. Then click on next.

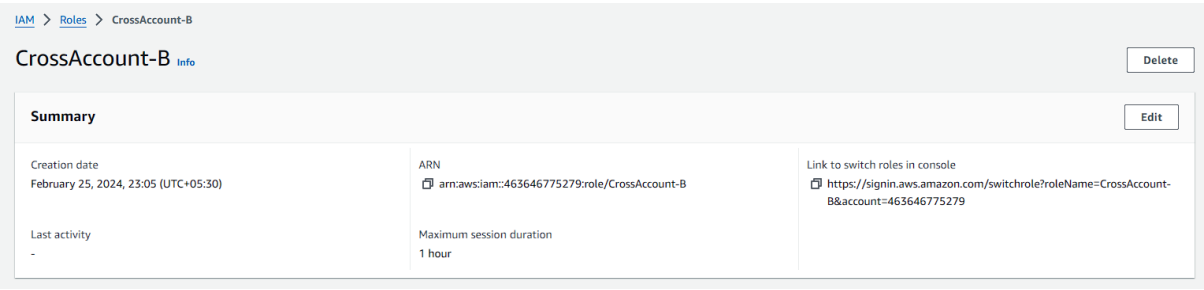



4. On the next page it will ask you for permission.

5. So, what this basically means is that once the IAM user from the identity account assumes this role and connects to the account, B what are the permissions that this user must have, whether he must have access to S3, access to EC2 and so on.
6. Now you can give permission whether to give access to S3 Read only policy or EC2 read only policy. It depends on you. I have given permission for S3 read only access.




7. Now you see for the cross account, IAM role, you basically have one more option which states, give this link to user who can switch the role in the console. So, if a user from the identity account wants to connect to the account B then he has to go ahead and click on this specific link.

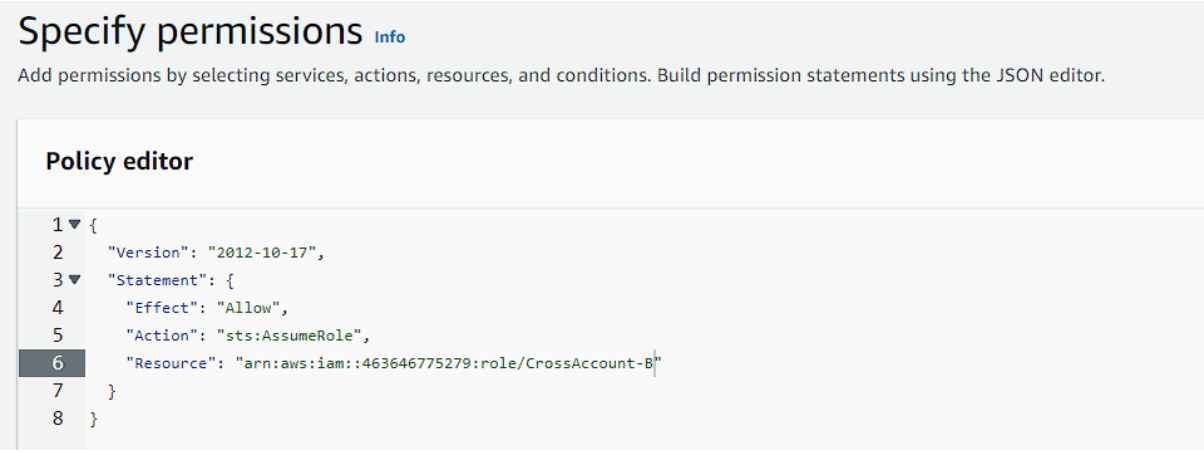



## 😄 Step 3: Allow user to switch to Account B

1. So, currently what has happened is our Alex user is created in identity account and that user does not have any permission. So that means that the Alex user will not even be able to go ahead and connect to the cross account IAM role in account B. So, we have to give minimal permission to Alex user so that he can at least connect to the IAM role of different AWS accounts.
2. Now quickly go back to your main account A and then open up your user and then click on add permission to it.
3. Then select create inline policy.
4. Here you need to switch to JSON and paste this policy over here. In this policy role is to just assume role and you need to paste the ARN of the Role that you have created in your account B.

**{**

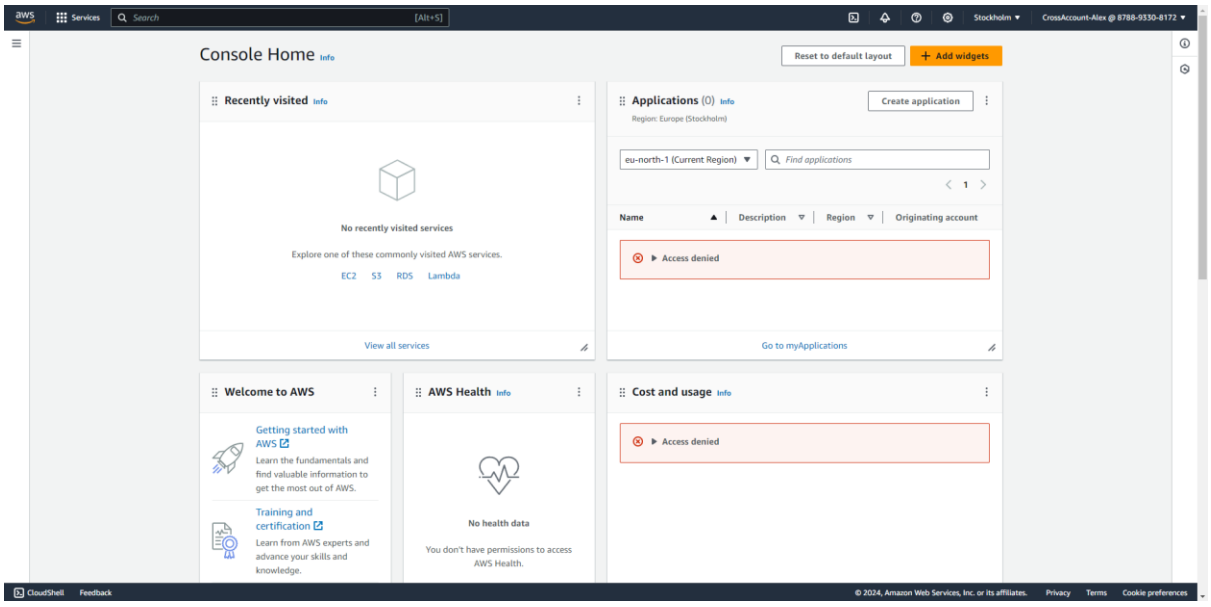
```
"Version": "2012-10-17",
"Statement": {
 "Effect": "Allow",
 "Action": "sts:AssumeRole",
 "Resource": "arn:aws:iam::463646775279:role/CrossAccount-B"
 }
}
```



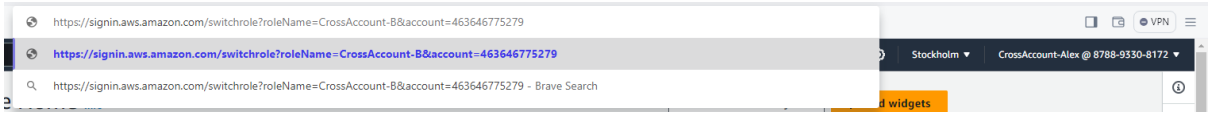

5. Now go to the review page and create your policy.
6. Now our all steps are completed. We just need to login with our Alex user account.

## 😄 Step 4: Trying out the Cross Account.

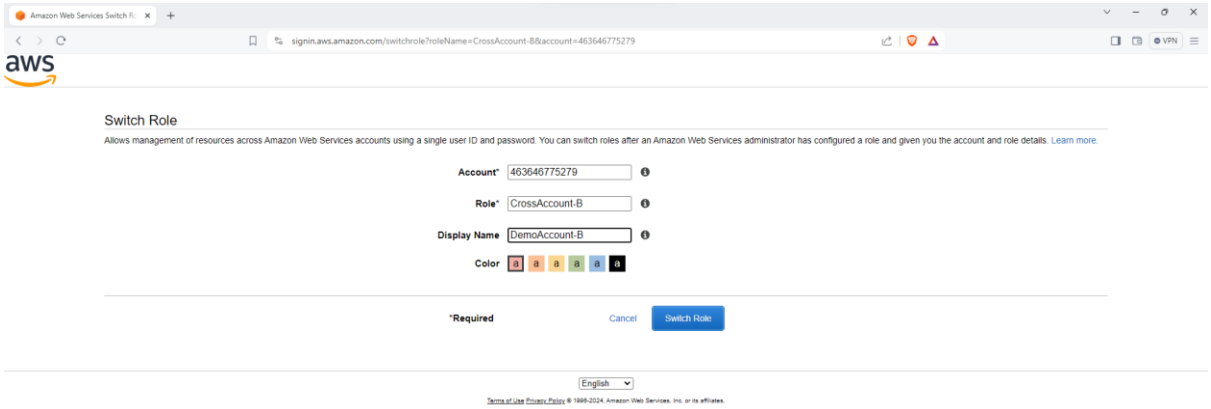
1. Now go back to your main account and login with your Alex user.
2. Once you are logged in then quickly go to you account B and from the roles copy the link to switch roles and paste in the Alex user.



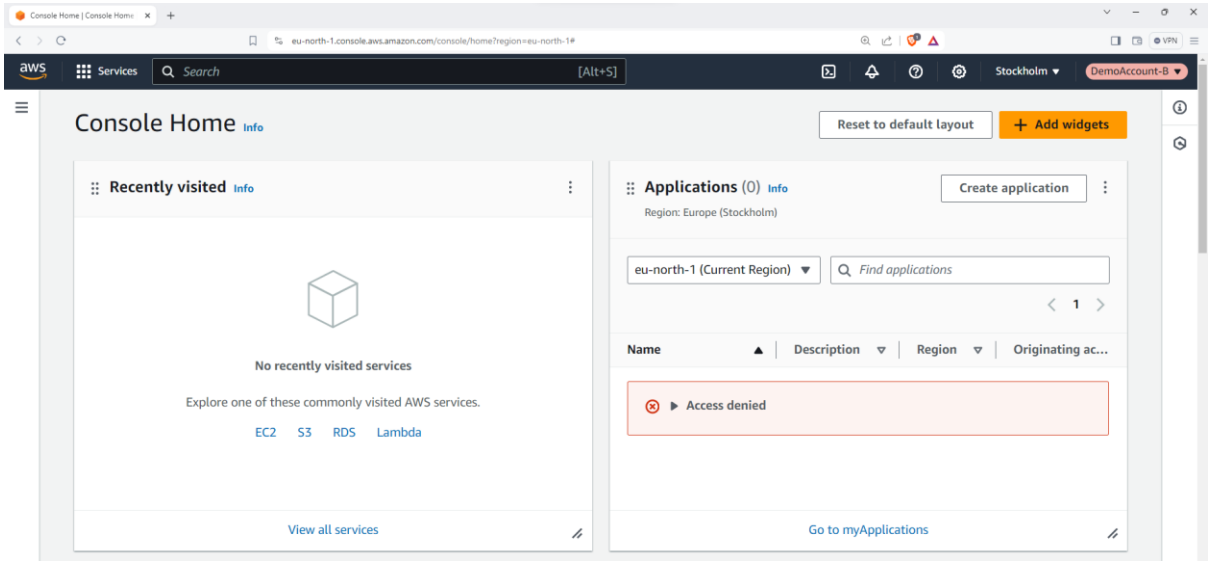

3. Once you have pasted it and press enter you will see a different tab.



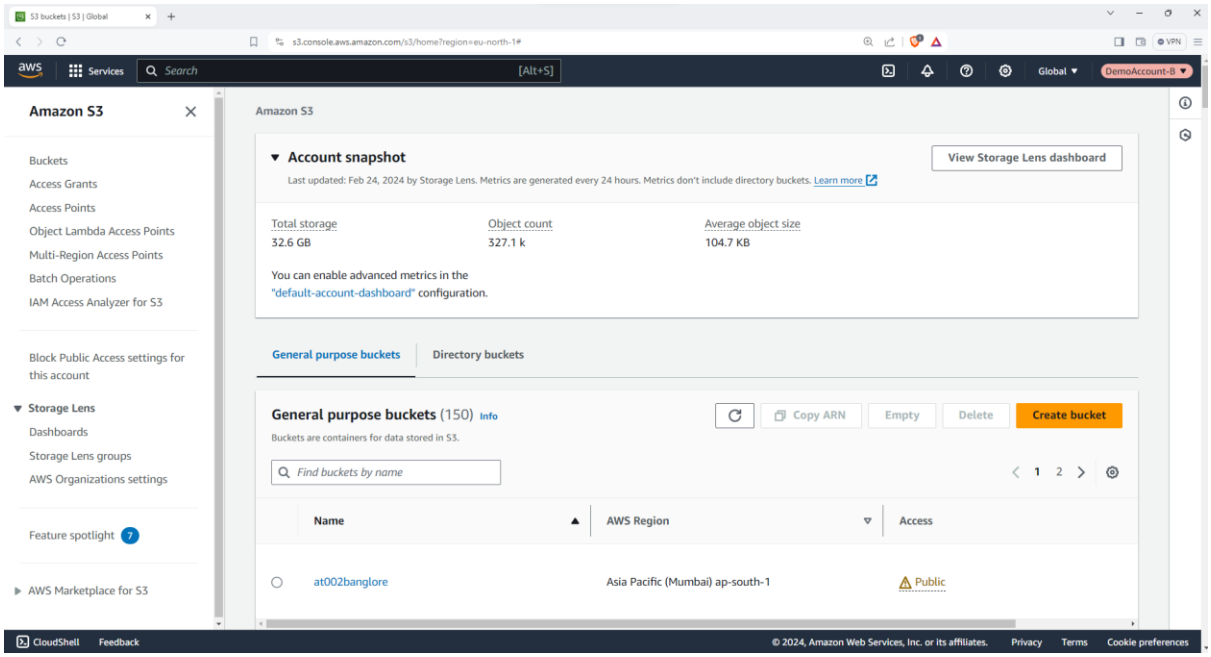

4. Here you are going to give it a display name click on Switch role.



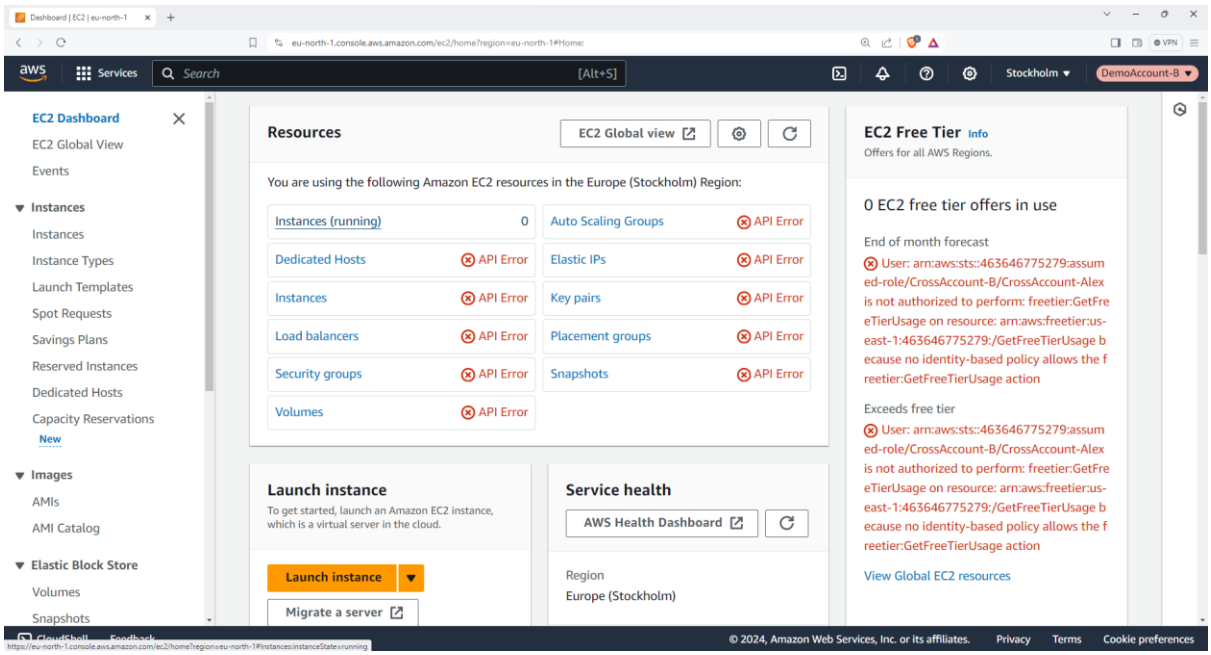

5. Now you can see that Alex user is signed in to Account B. As of now I have provided it with S3 Read only access.
6. So, I will navigate to S3.



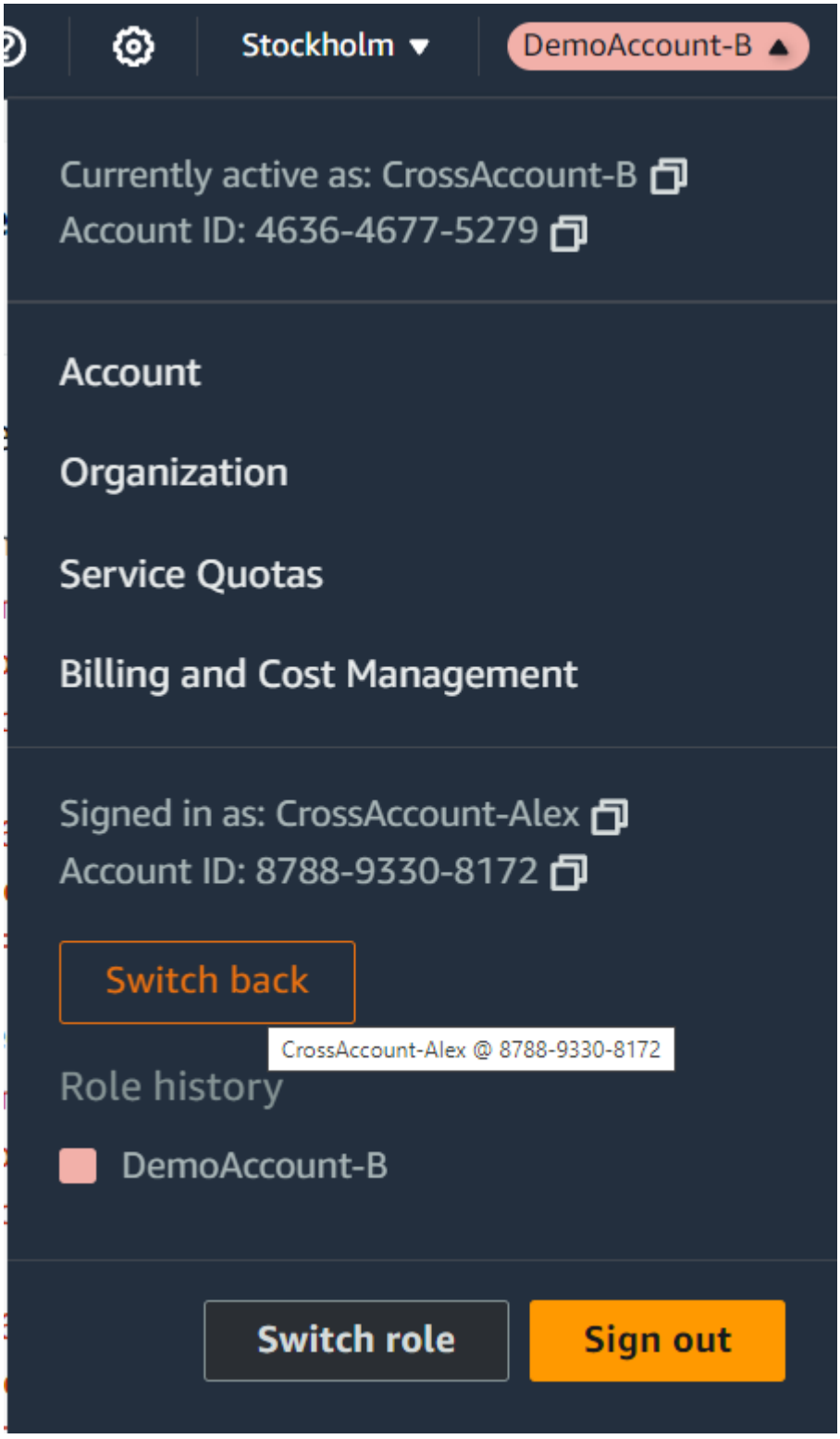

7. I can see all the buckets available as in read only mode using Alex user account.




8. But if this user Alex tries to open EC2 then he will get access denied because there is no permission for it.




9. Now let suppose this user work has been done in this account now he can switch back to his account by clicking on switch back.




10. Now if you will just visit to S3 or EC2 in this account you will get access denied as well because this user Alex does not have sufficient permissions.