Describe the process of setting up cross-account access in AWS IAM

Source account 🡪 target account

**wants to access**

step 1) Create two IAM users known as source account && target account

Target Account 🡪

https://975050134708.signin.aws.amazon.com/console

target-account

Mayur@4279

&& Assign All Administrator access policy.

source account 🡪

https://975050134708.signin.aws.amazon.com/console

source-account

Mayur@4279

&& only Assign {awscloudshellfullaccess } policy. 🡪 for testing perpose

Step2) Create an IAM Role in the Target Account

1. Sign in to the AWS Management Console in the target account.

2. Navigate to the IAM console.

3. Create a New Role.

Go to the "Roles" section and click on "Create role".

Select "Another AWS account" as the type of trusted entity.

4. Specify the Trusted Accounts

Enter the account ID (In this case select for this Aws account)

5. Attach Policies to the Role

Choose the permissions you want to grant to the role.

You can select AWS managed policies or create a custom policy.

For example, to allow full access to S3, attach theAmazonS3 FullAccess policy.

6. Complete the Role Creation

Provide a name and description for the role. - Review and create the role.

Step3) Assign STS Inline policy for source account. (Using root account )

* Select the source account
* In permission click on Add permission
* Select create inline policy
* Select service = STS
* Click on ALL STS actions && click on all resources
* Give name and create the policy

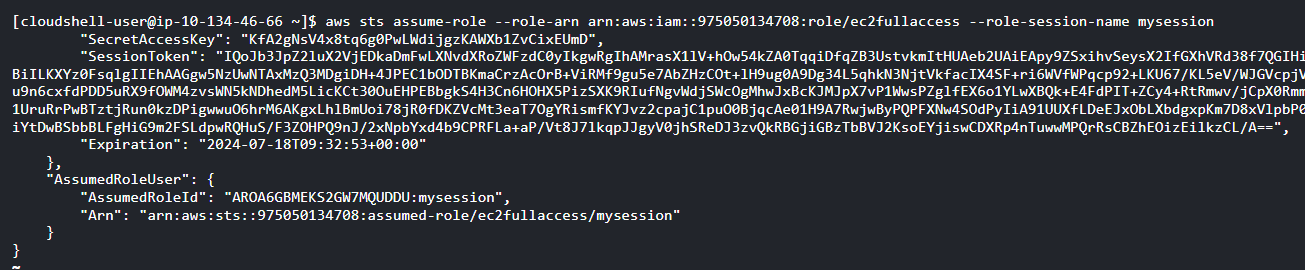
Step4) Navigate to source account and open cloudshell

Use following command to get credentials from another account…

aws sts assume-role --role-arn arn:aws:iam::975050134708:role/ec2fullaccess --role-session-name mysession

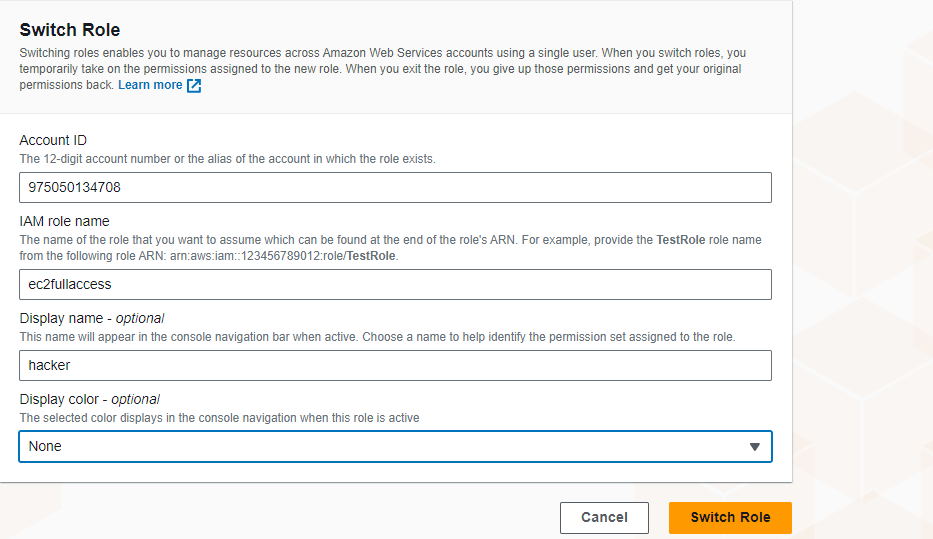
**Note: we can access ec2service using source account without attaching any policy.**

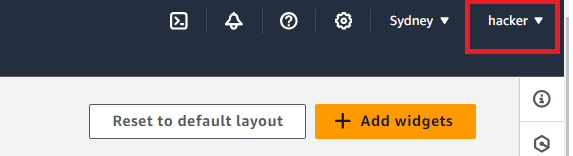
Result:



Step5) for graphically access...

Click on profile 🡪 switch role 🡪 enter account Id 🡪 role name 🡪 click on switch role.





1. Create an IAM role in the target account and specify the trusted accounts that can assume the role.

2. Attach policies to the role defining the permissions.

3. In the source account, use the AWS STS `AssumeRole` API to get temporary credentials for the target account.

Continuous update the