**Steps to create trust relationship policy between accounts and the Master account.**

Step 1: Create an IAM Policy to allow modification of security groups in an account

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"ec2:AuthorizeSecurityGroupEgress",

"ec2:AuthorizeSecurityGroupIngress",

"ec2:RevokeSecurityGroupEgress",

"ec2:RevokeSecurityGroupIngress",

"ec2:DescribeSecurityGroups",

"ec2:DescribeSecurityGroupReferences",

"ec2:DescribeNetworkInterfaces",

"ec2:DescribeVpcs"

],

"Resource": "\*"

}

]}

Step 2: In the navigation pane, choose Roles and then choose Create role and name it as Security\_group\_access.

Step 3: Choose the An AWS account role type.

Step 4:For Account ID, type the Master account ID.

Step 5:Choose Next: Permissions to set the permissions associated with the role.

Step 6:Select the check box next to the policy that you created previously.

Step 7:After reviewing the role, choose Create role.

**Steps to create IAM role in the Master account that have access to modify the security groups in other accounts.**

Step 1: In the navigation pane, choose Roles and then choose Create role and name it as Lambda\_role.

Step 2: Choose Lambda as the service.

Step 3:Choose Next: Permissions to set the permissions associated with the role

Step 4:Select the check box next to the policy and give below inline policy to the role:

{

"Version": "2012-10-17",

"Statement": [{

"Effect": "Allow",

"Action": "sts:AssumeRole",

"Resource": "arn:aws:iam::Account-id-server:role/UpdateApp"

},{

"Effect": "Allow",

"Action": [

"ec2:AuthorizeSecurityGroupEgress",

"ec2:AuthorizeSecurityGroupIngress",

"ec2:RevokeSecurityGroupEgress",

"ec2:RevokeSecurityGroupIngress",

"ec2:DescribeSecurityGroups",

"ec2:DescribeSecurityGroupReferences",

"ec2:DescribeNetworkInterfaces",

"ec2:DescribeVpcs"

],

"Resource": "\*" }]}

Step 7:After reviewing the role, choose Create role.

Finally, attach this role to the Lambda