# 

# **Assessment**

# **IAM**

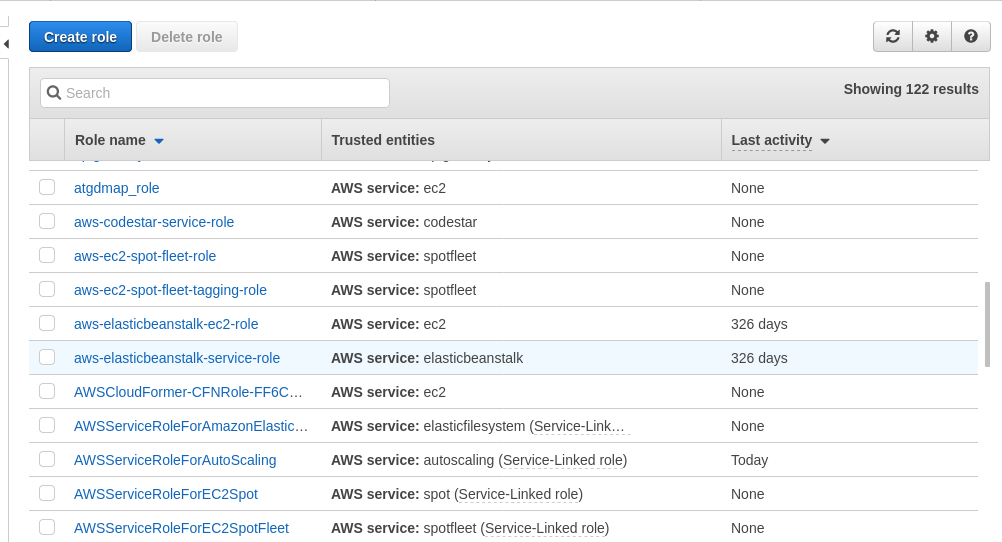
Trainee Name : Aditya Upadhyay

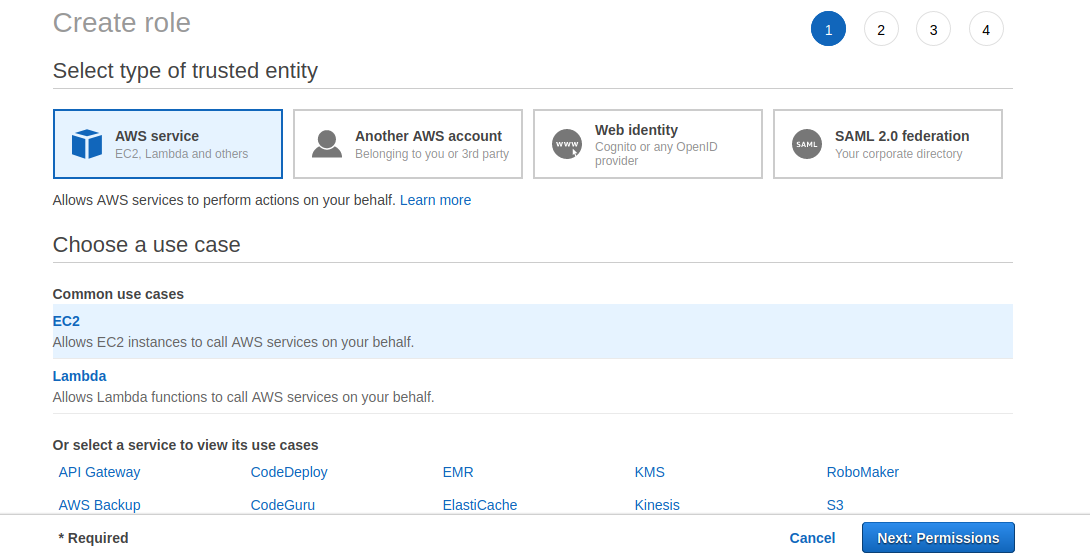
Newers ID : 3978

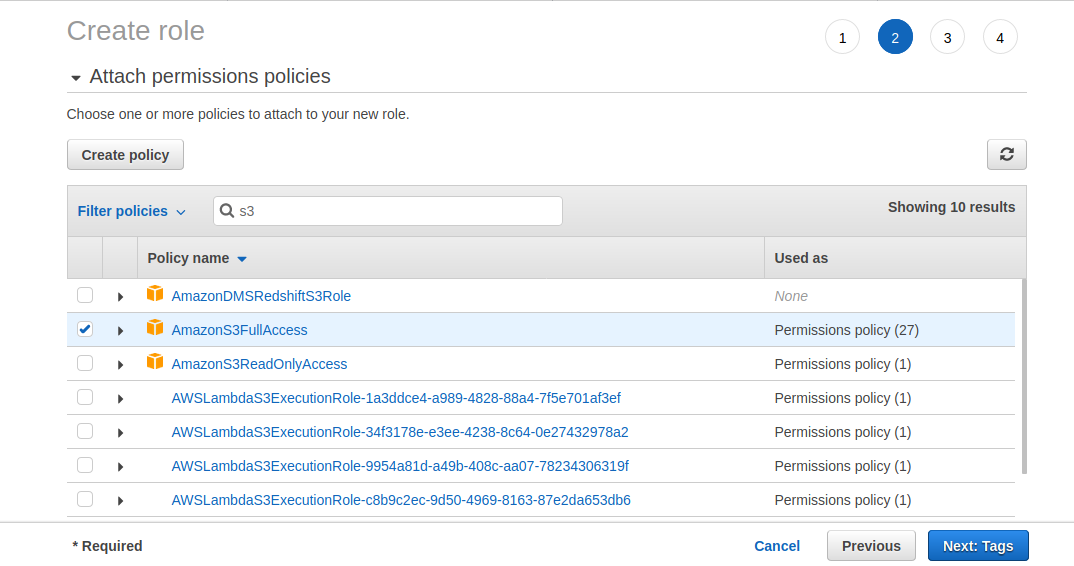
Mentor Name : Tarun Saxena

College : UPES

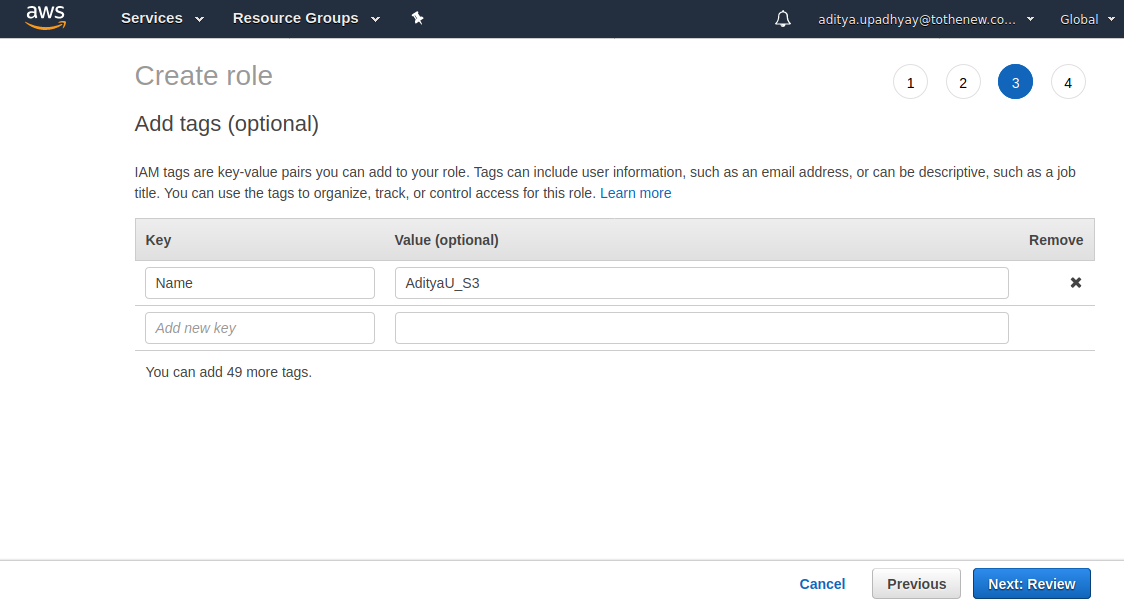
1. Create a Role with full access to S3

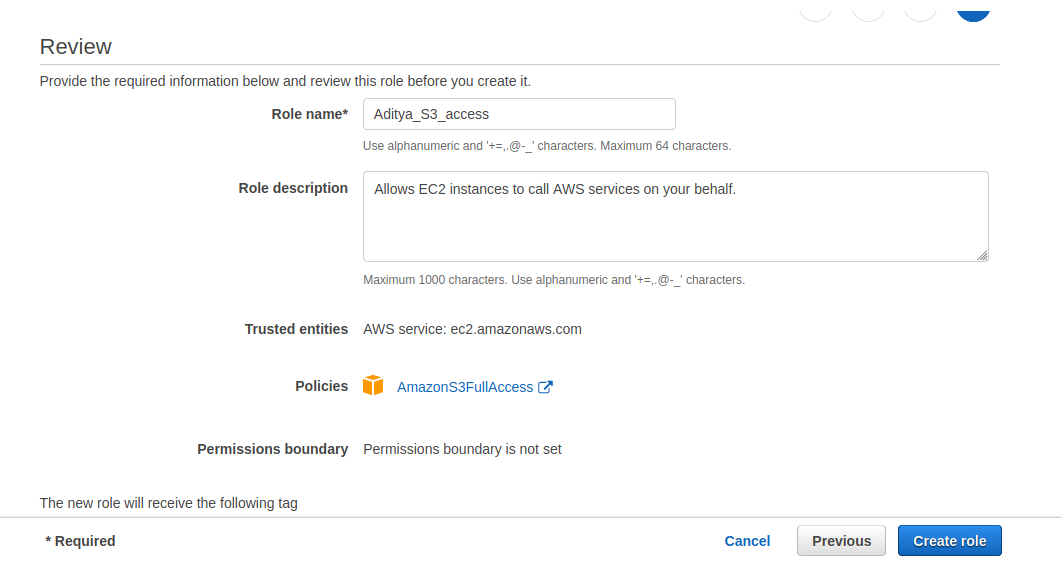


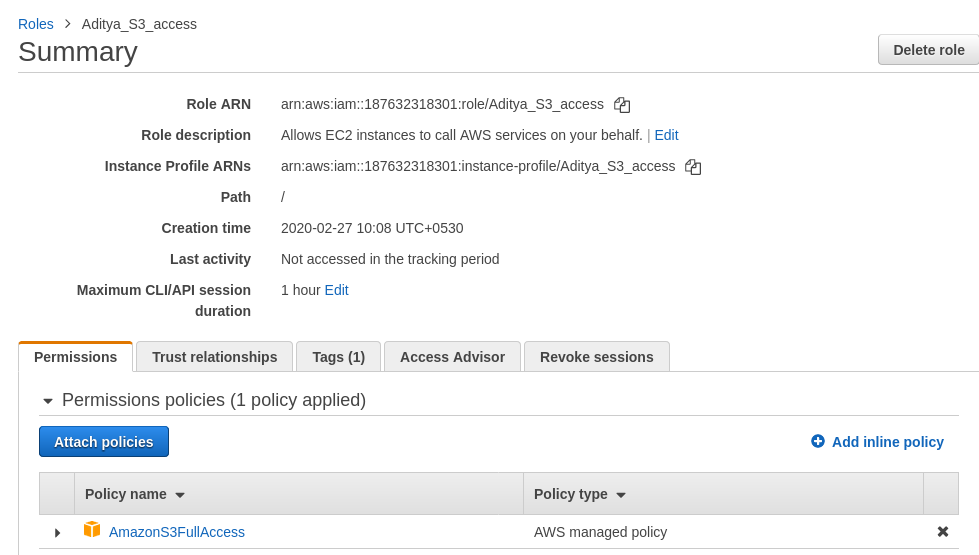




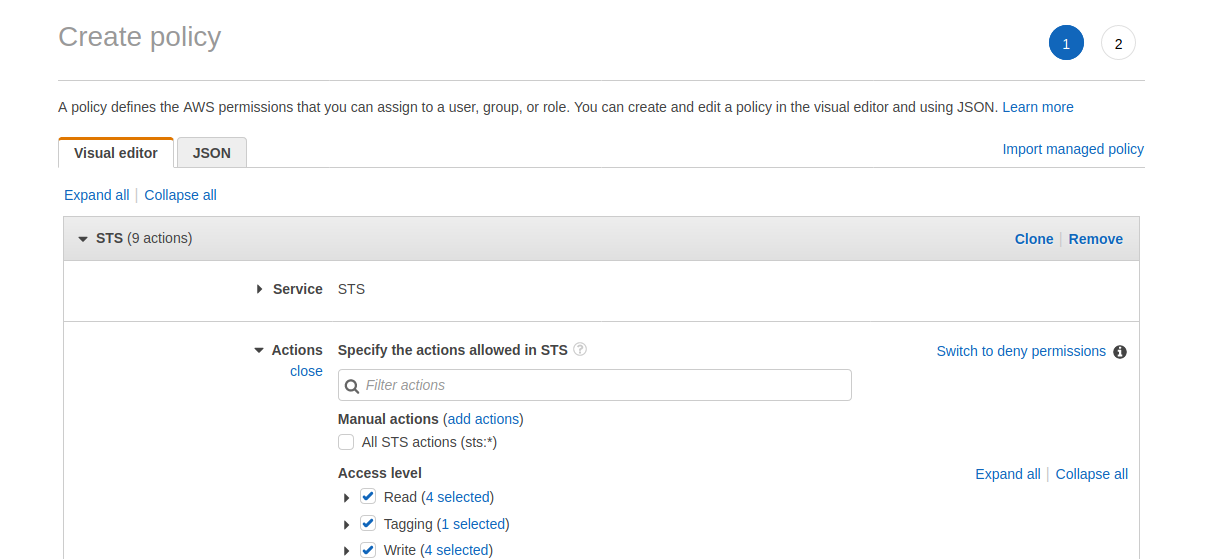


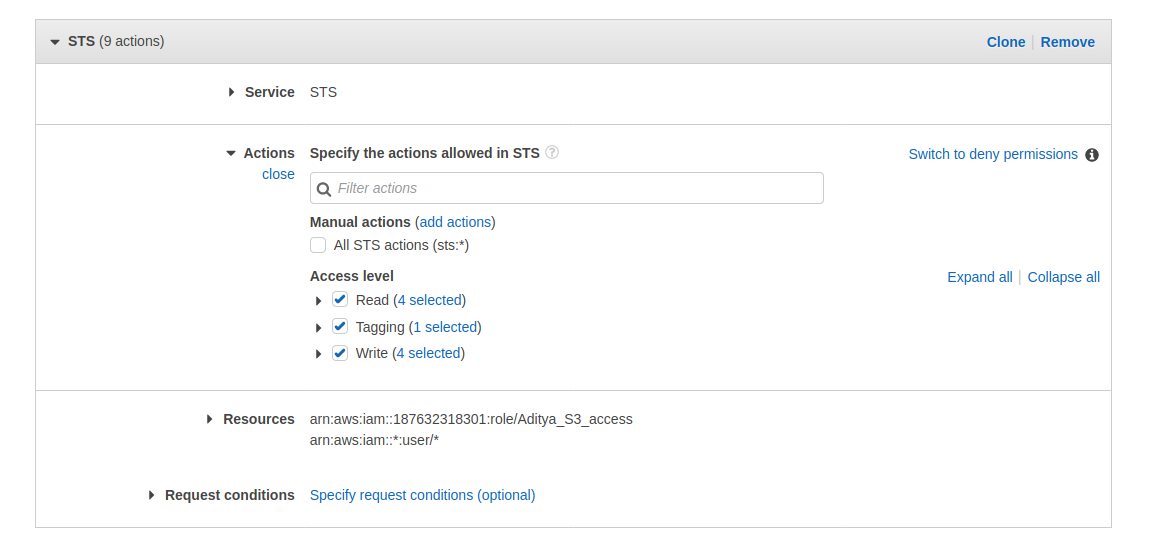


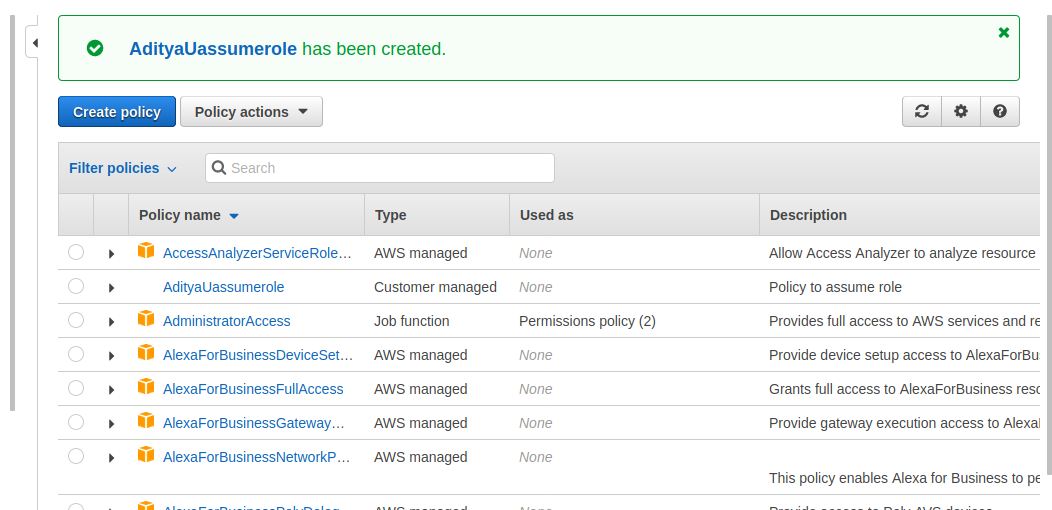


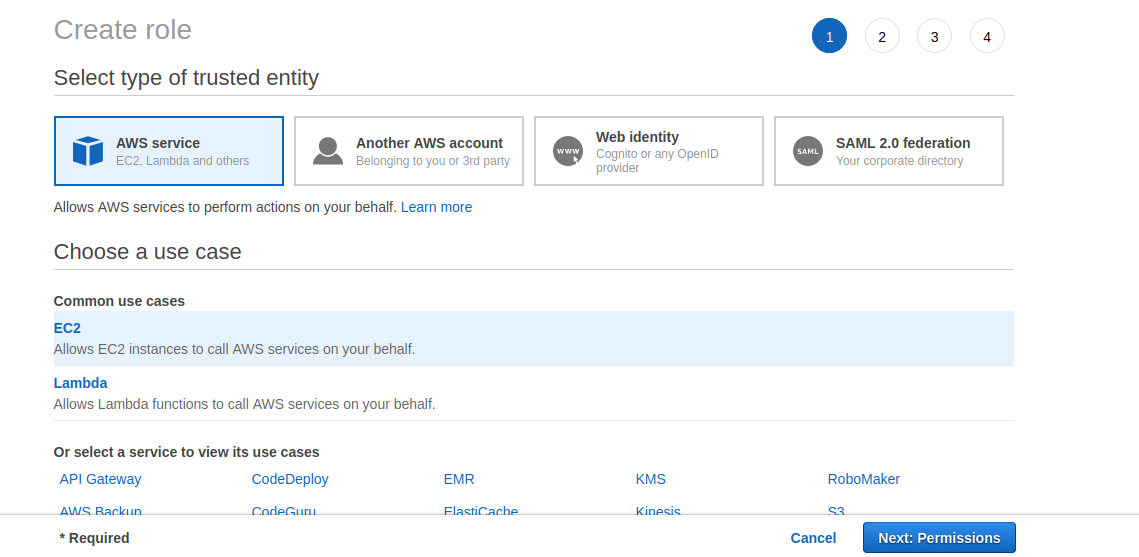


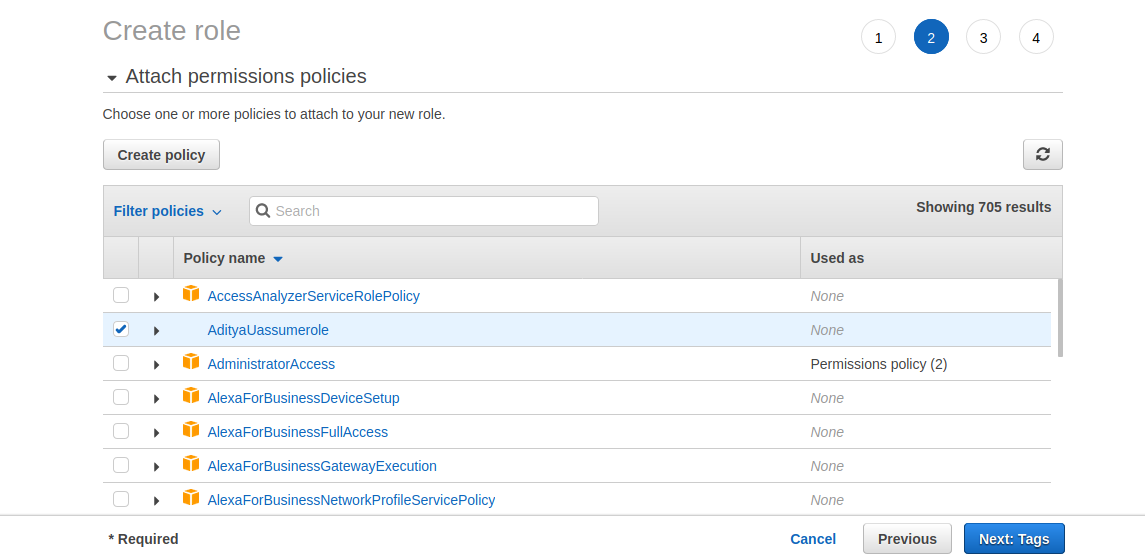
2. Create another which has the policy to assume the previous Role

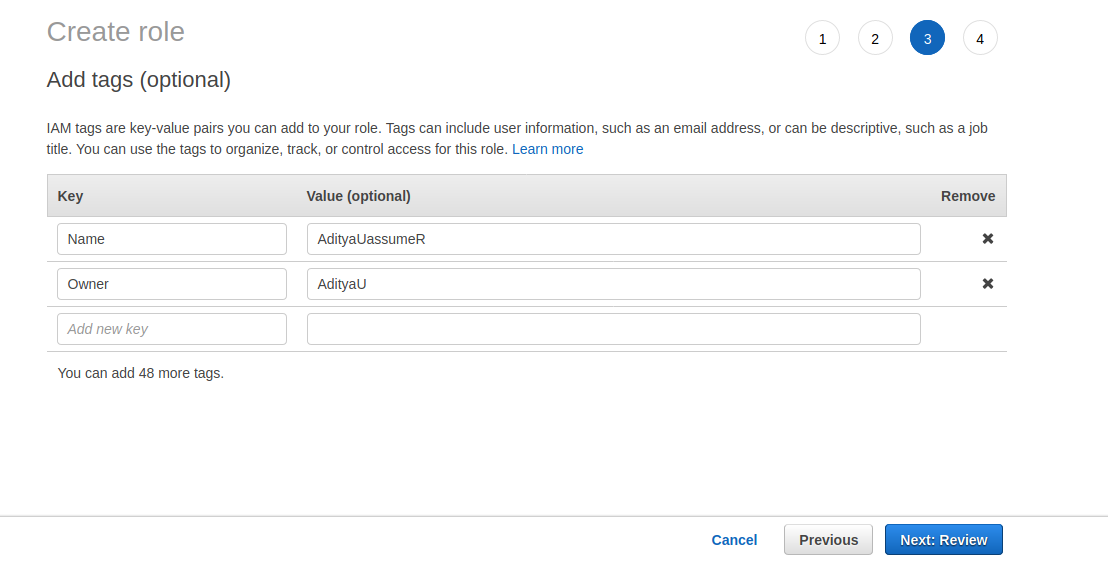


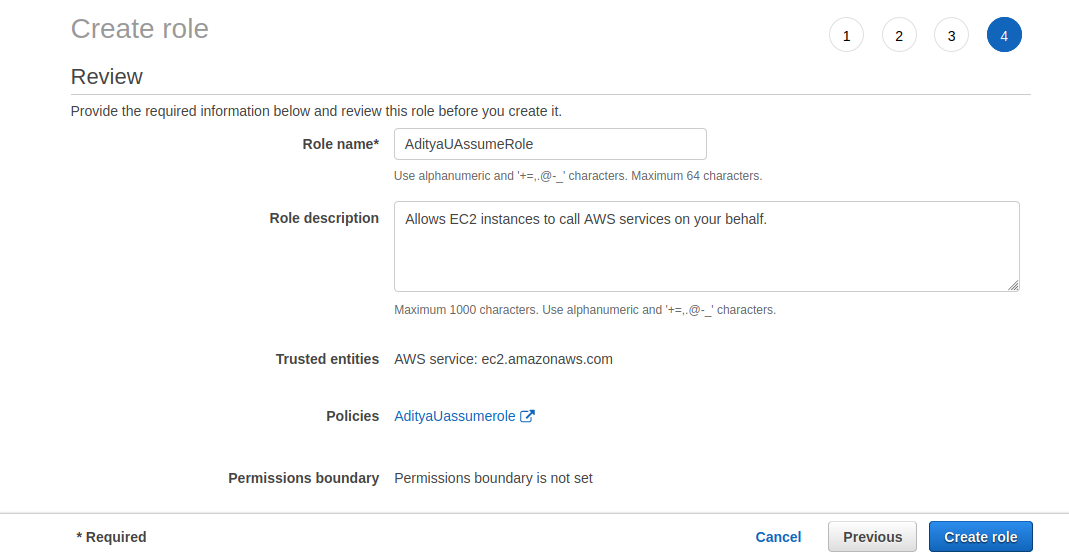


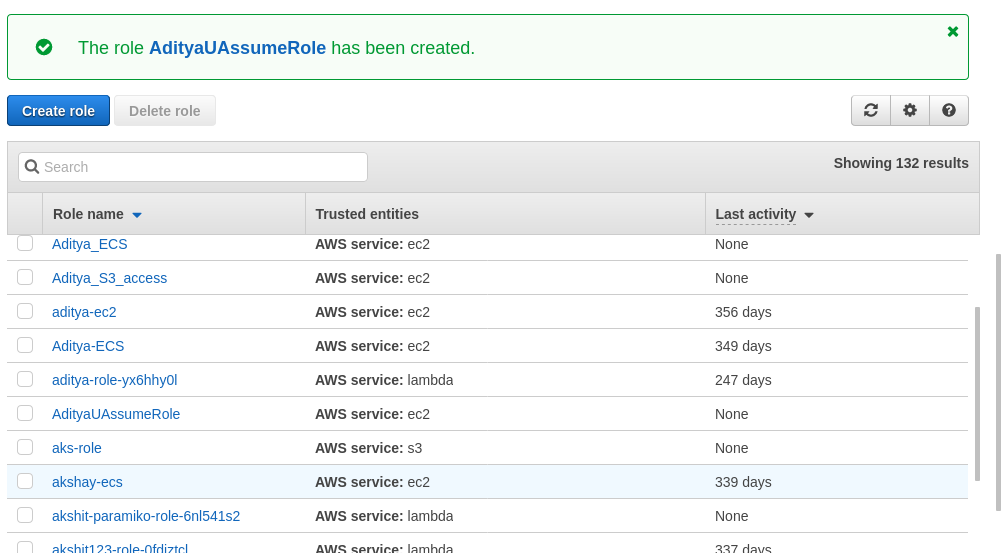


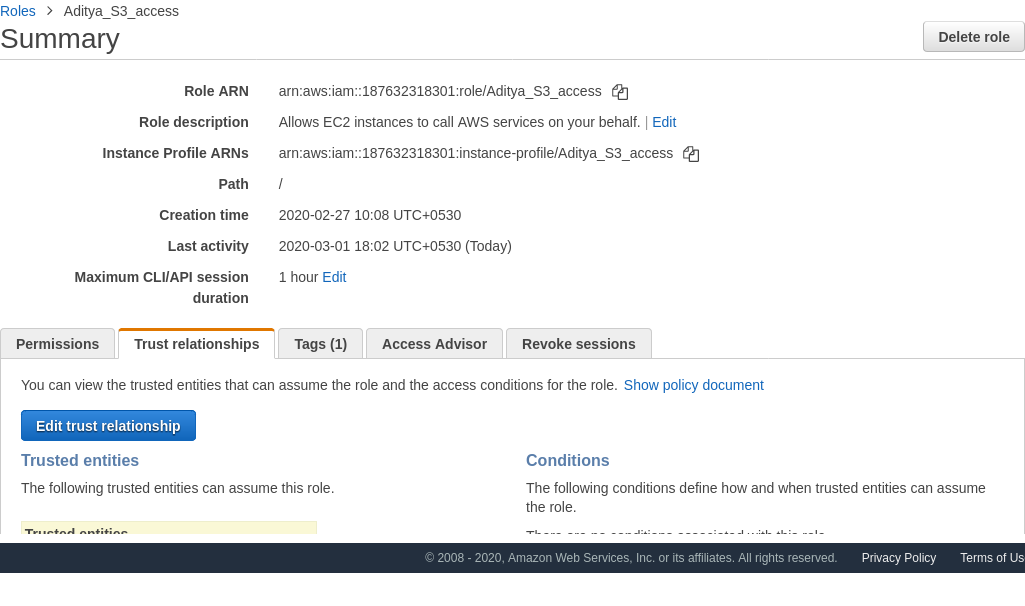


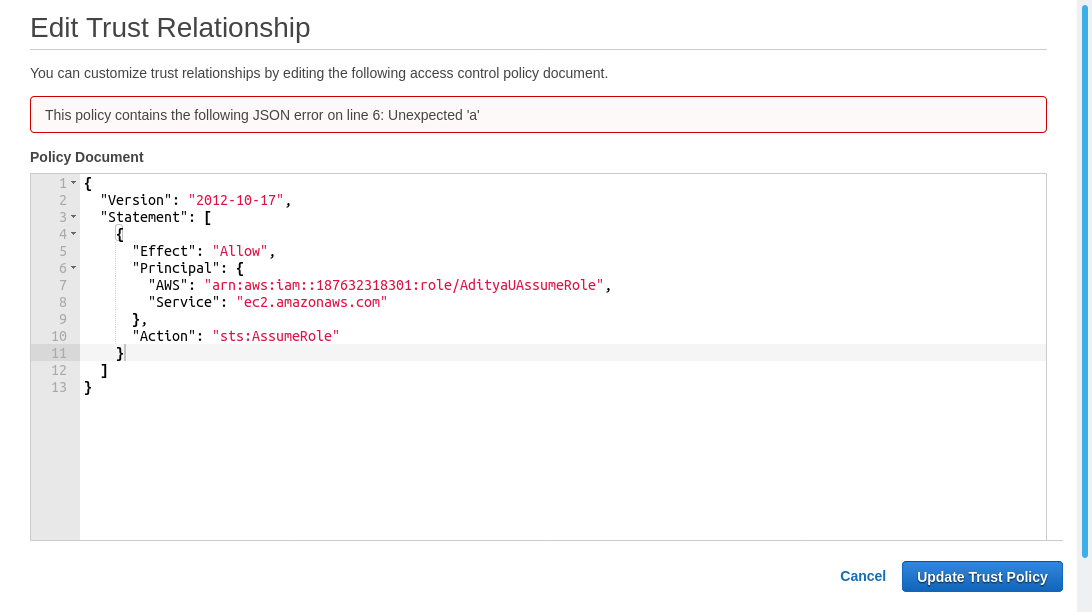


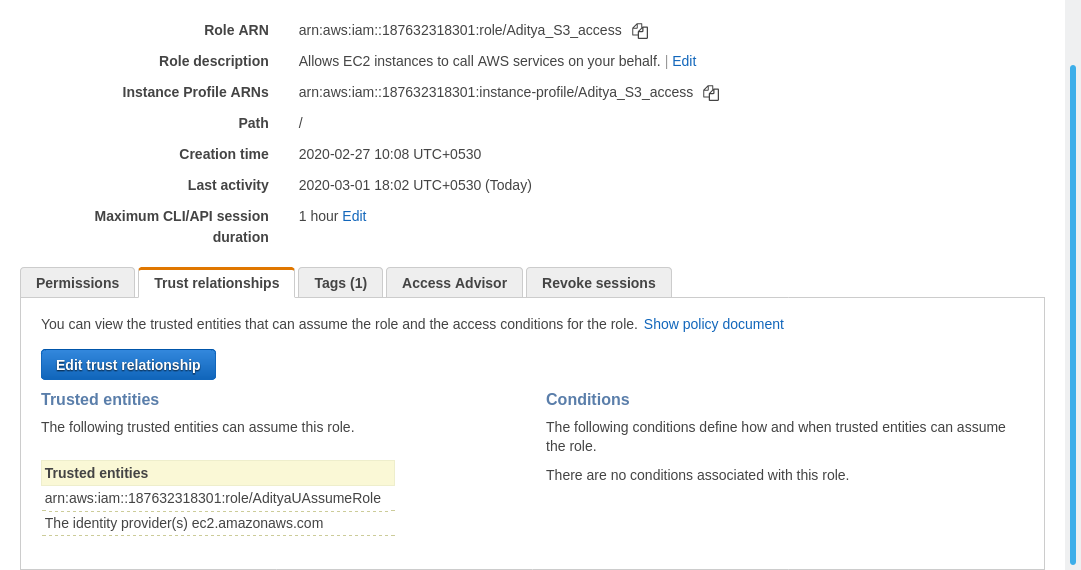




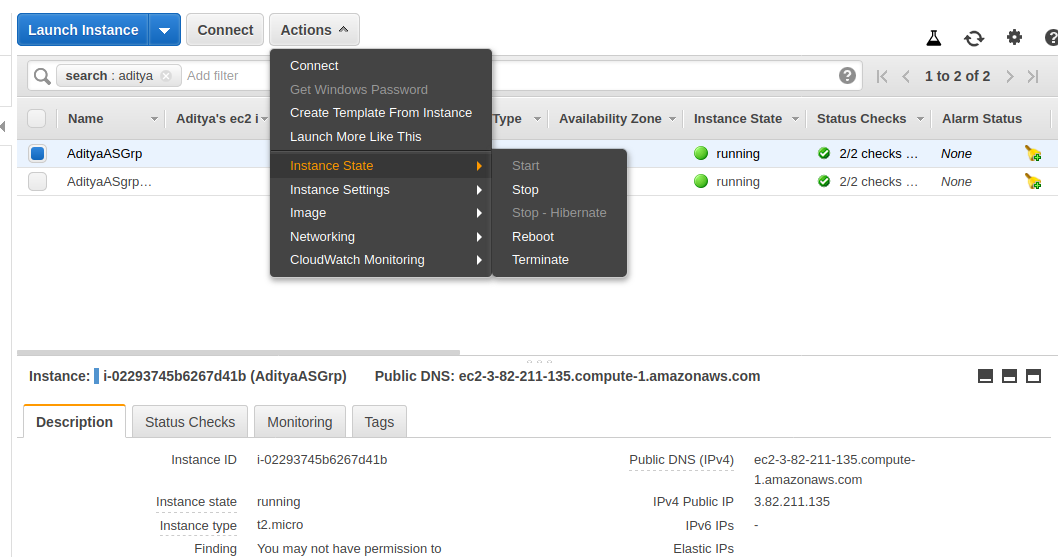


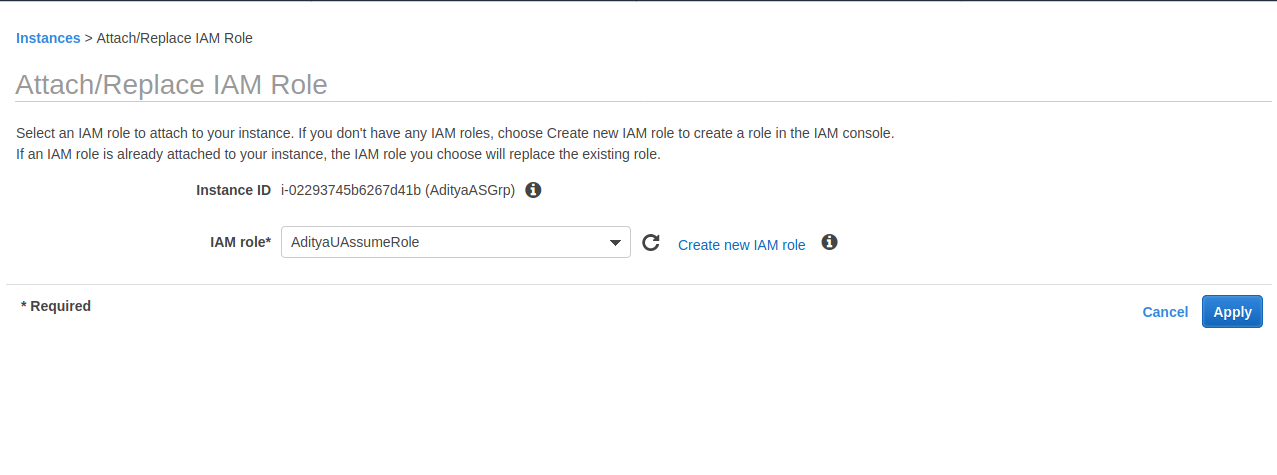


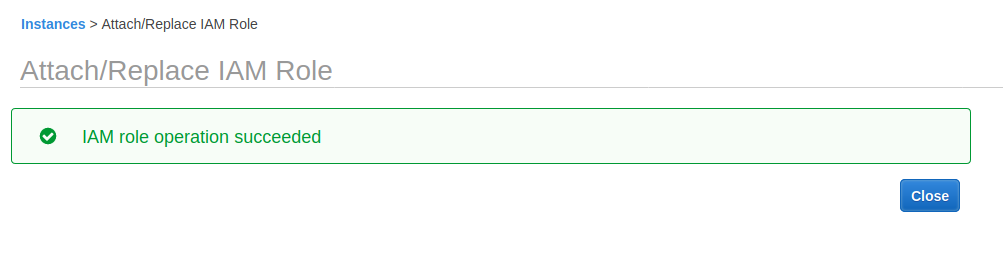


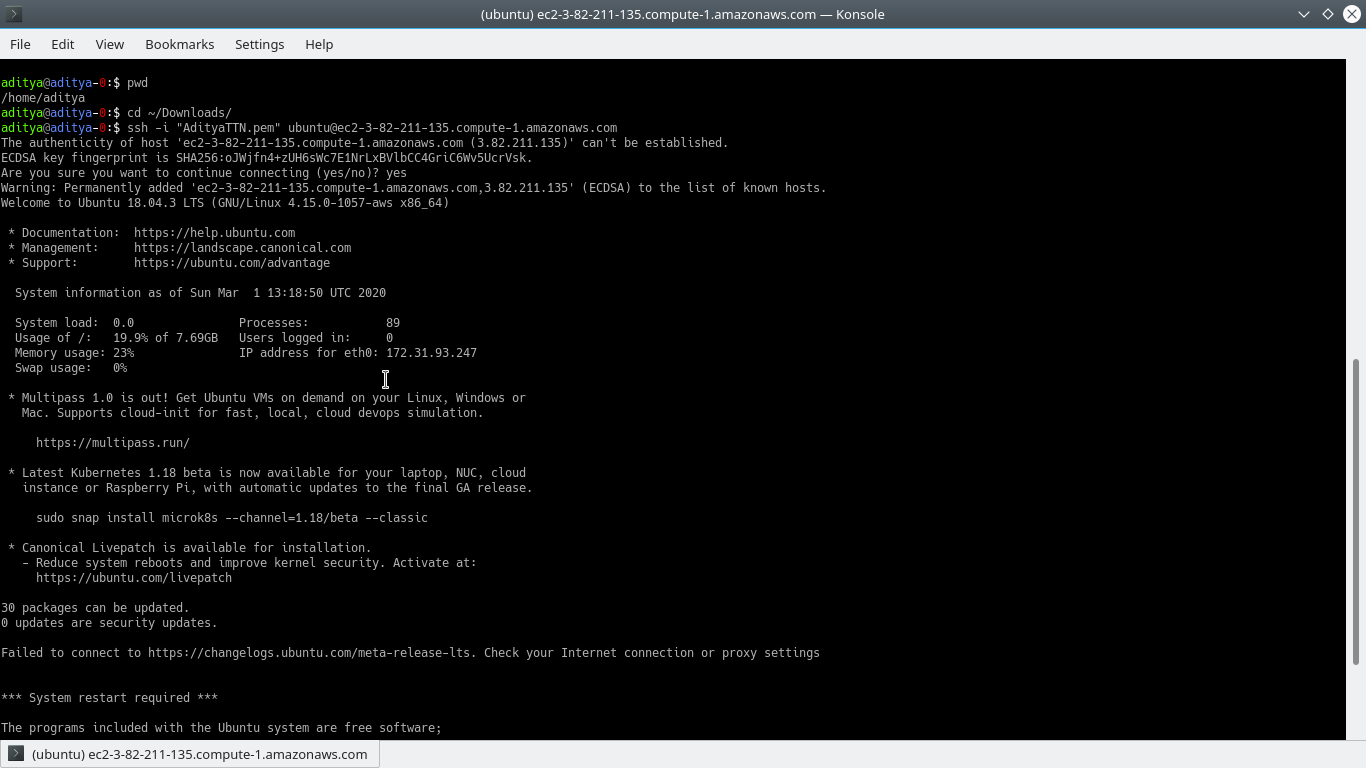


3. Attach this to an instance and get an sts token.











4. Create a group for "Data Administrator" where the user 'Alice' be a member of this group. This group will prepare the data for the analysis. So Provide the following access to the group.

Service: Amazon S3;

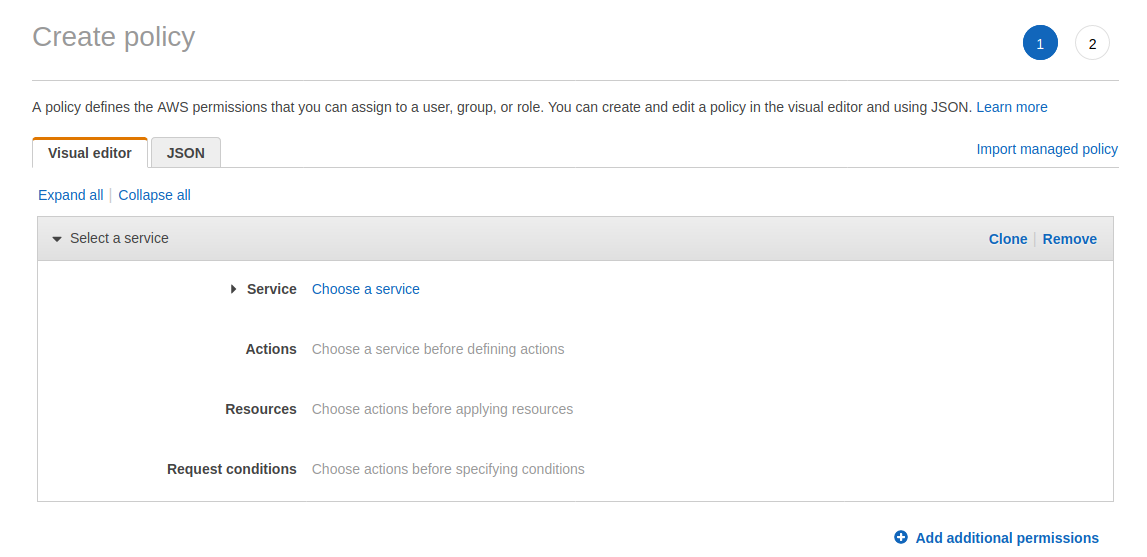
Action:

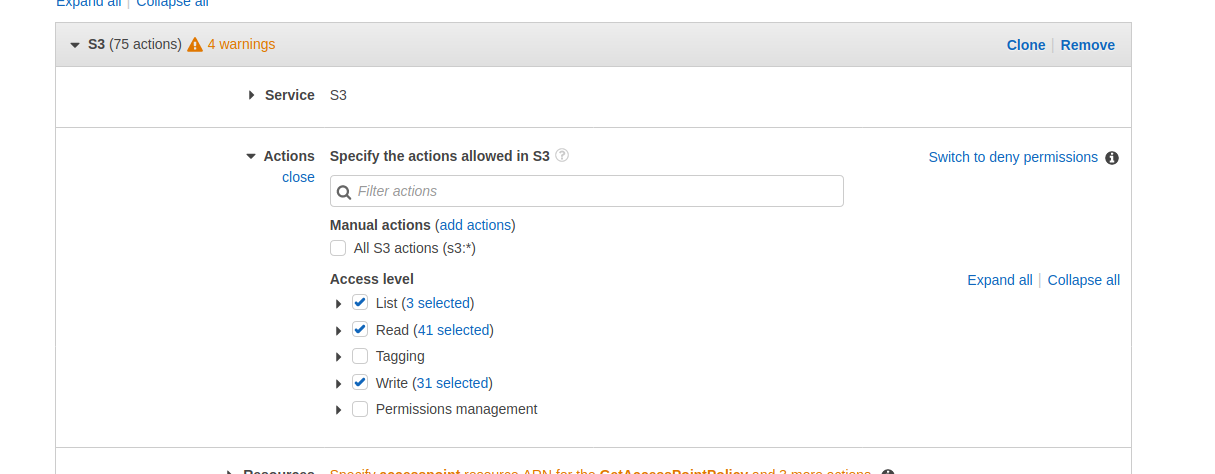
Get\*,

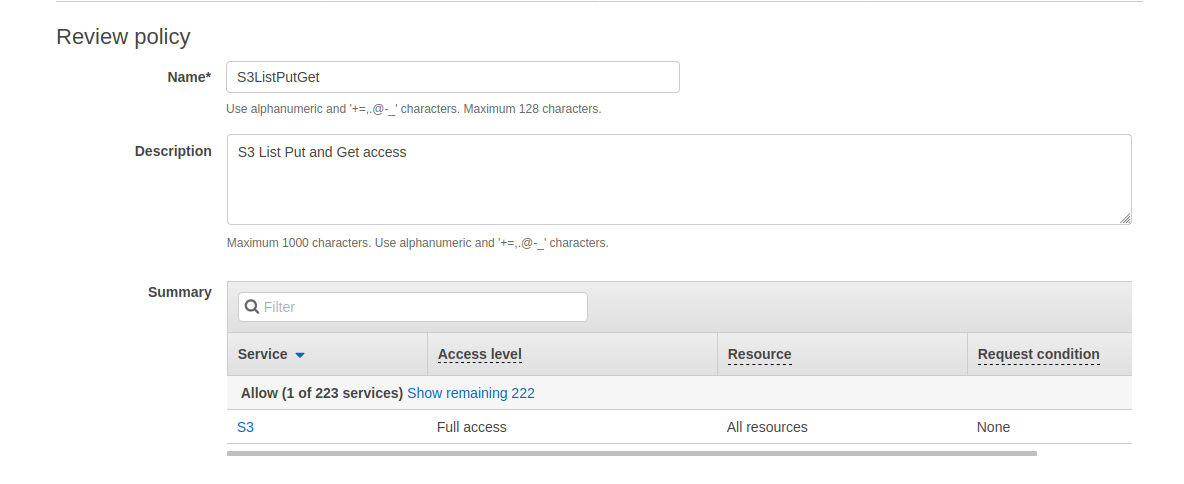
List\*,

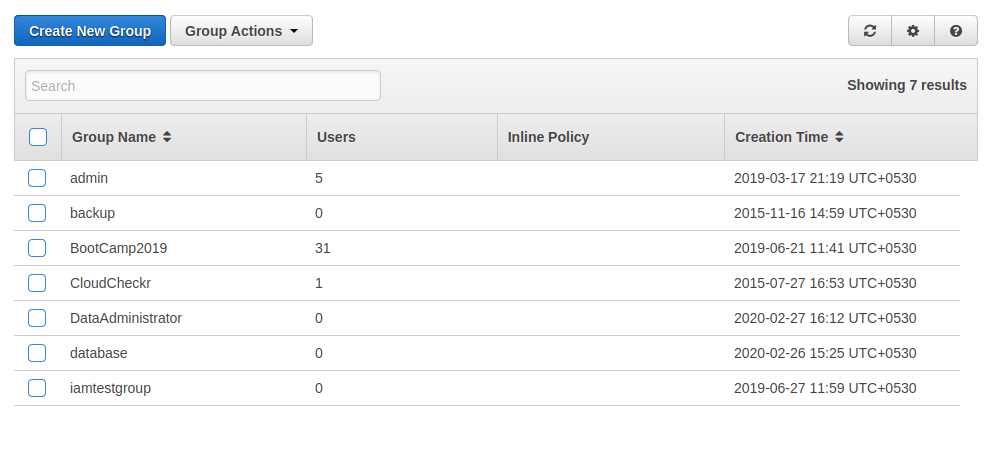
Put\*,

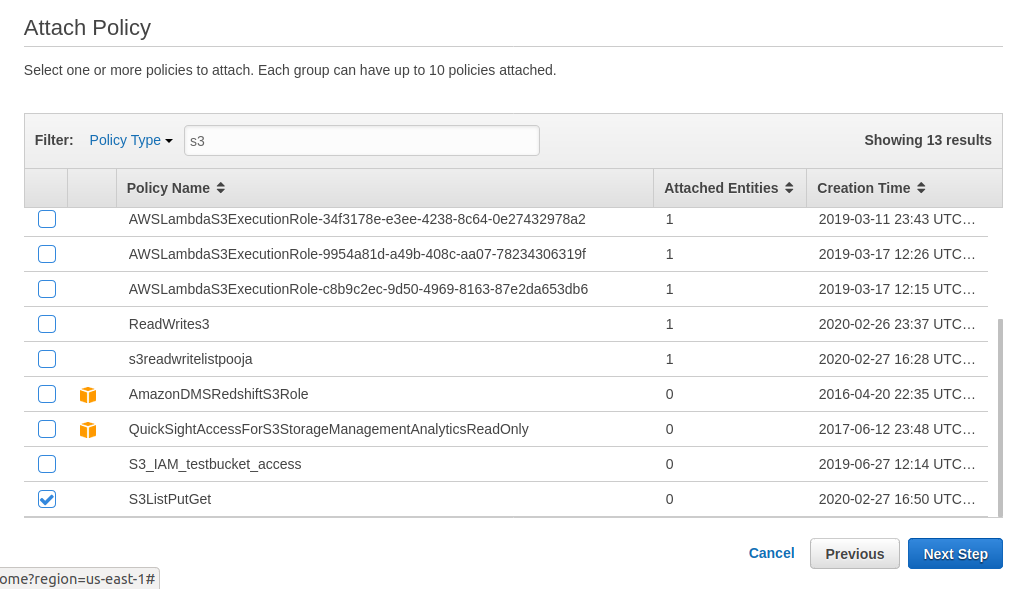
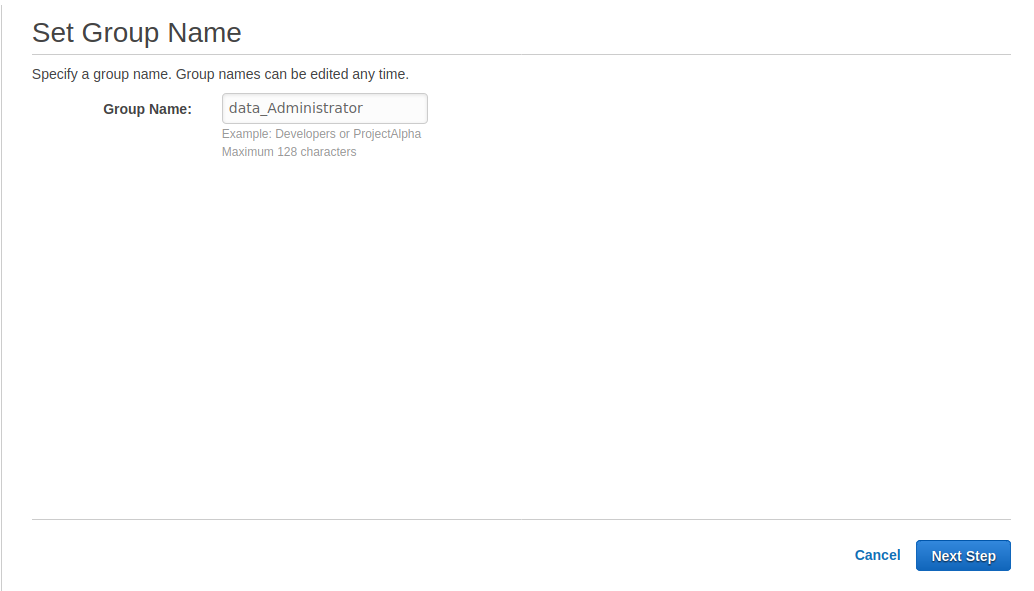
ARN: Input and output Buckets (no conditions)

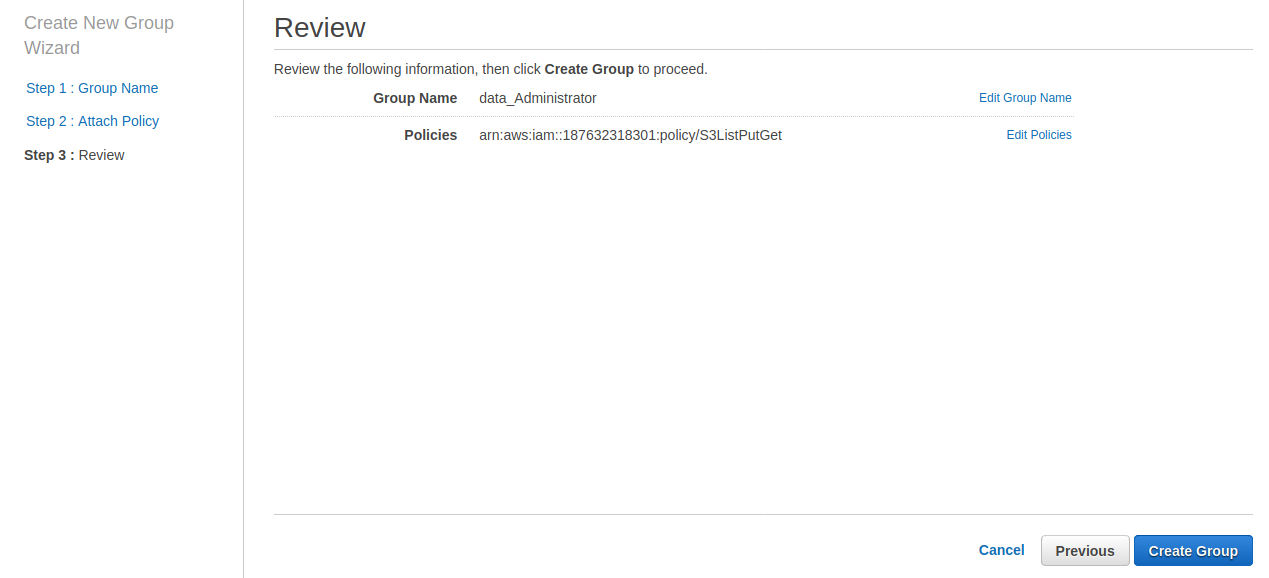


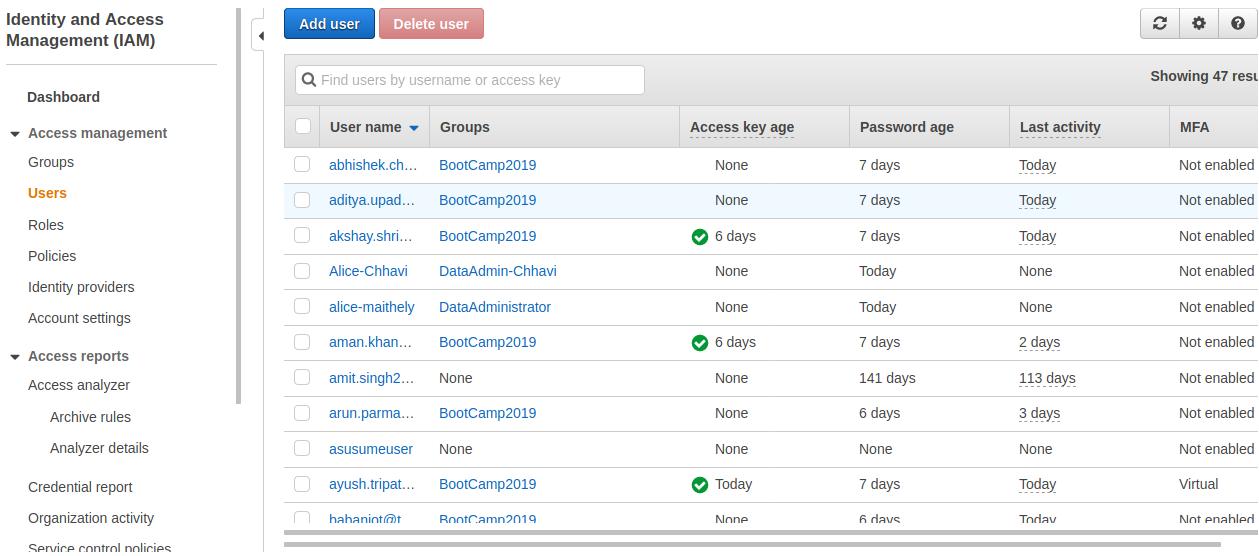


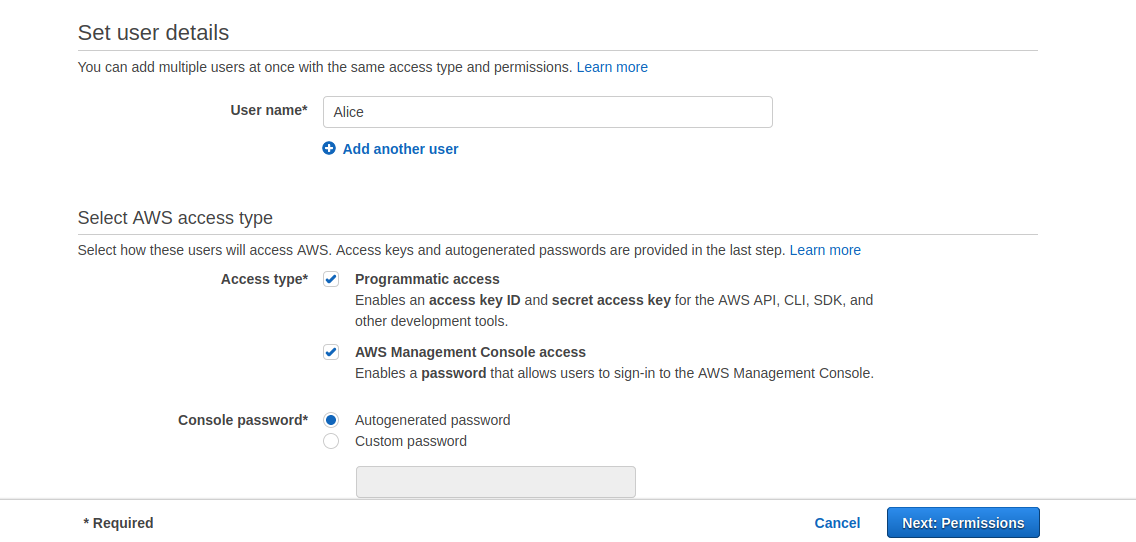


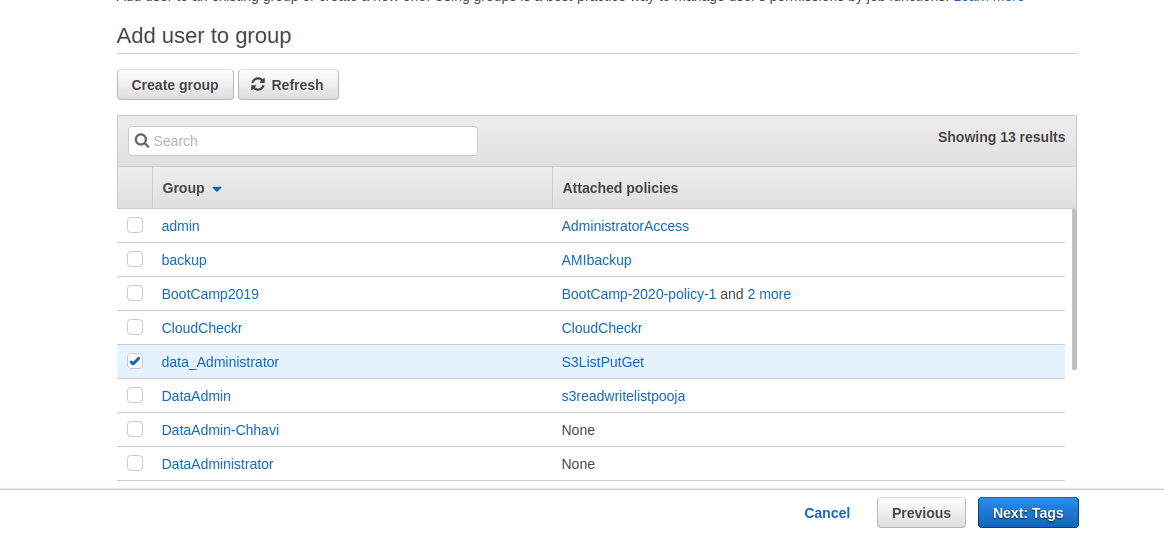


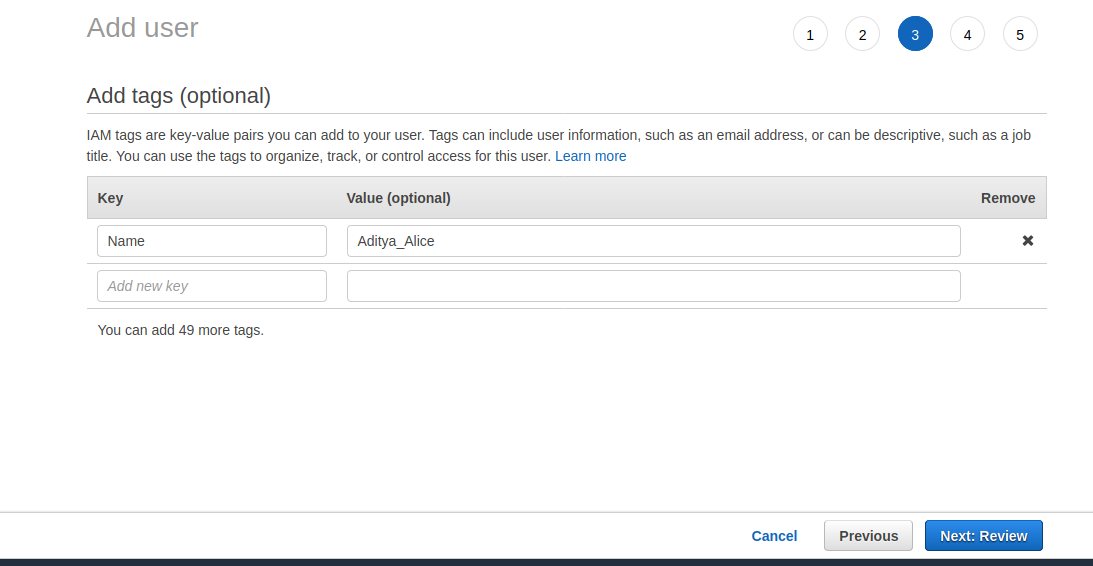


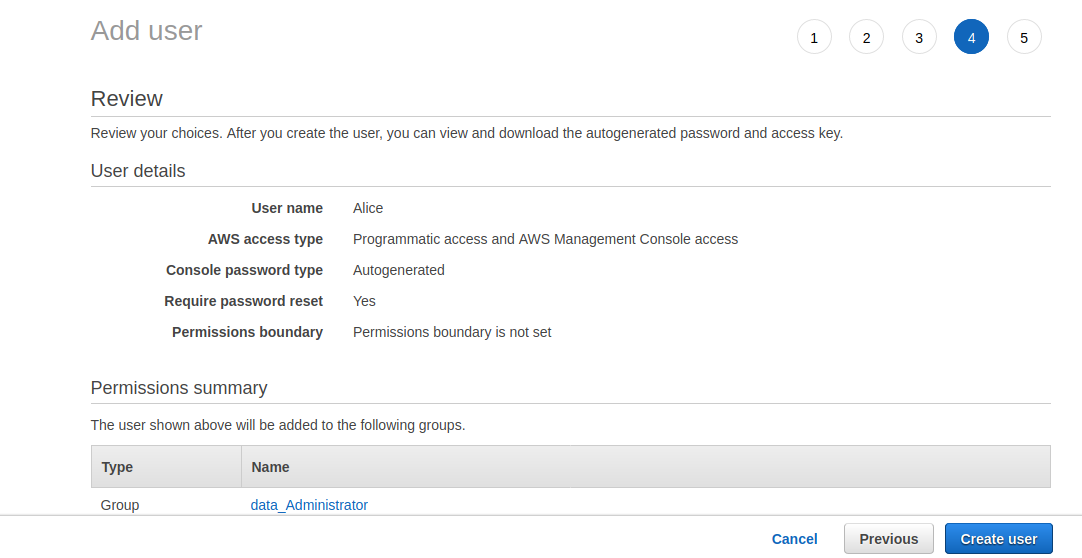


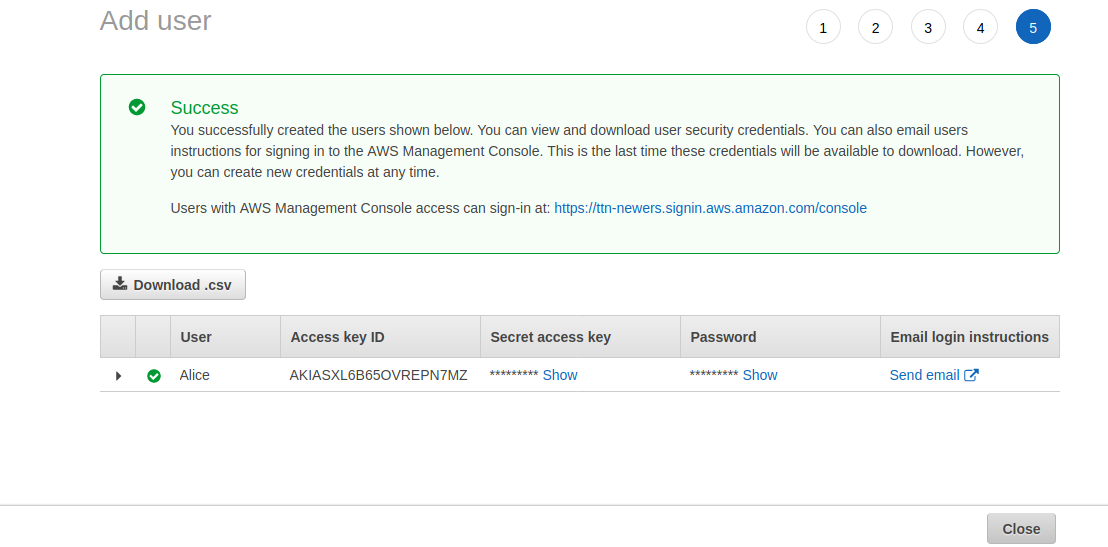










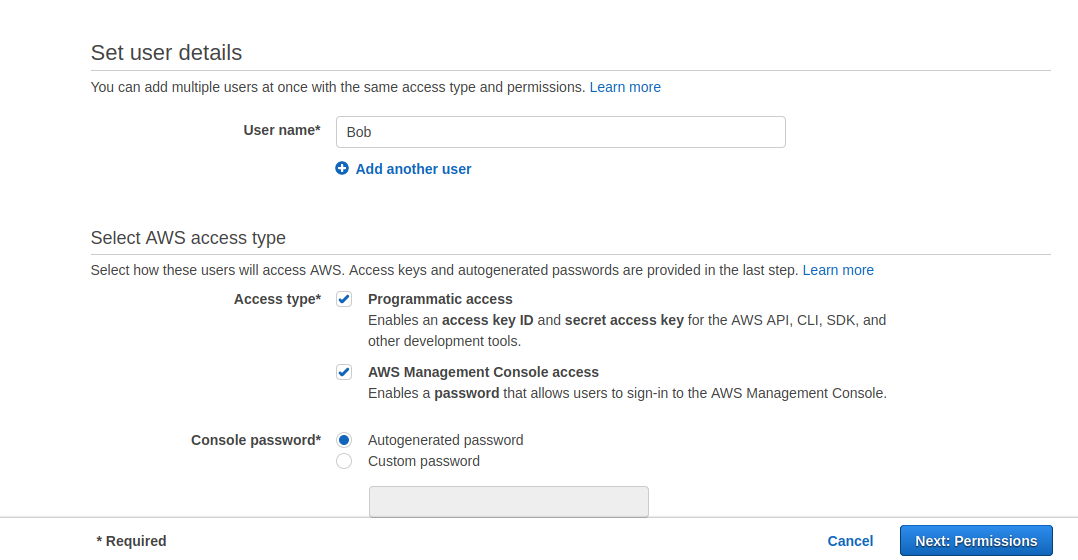


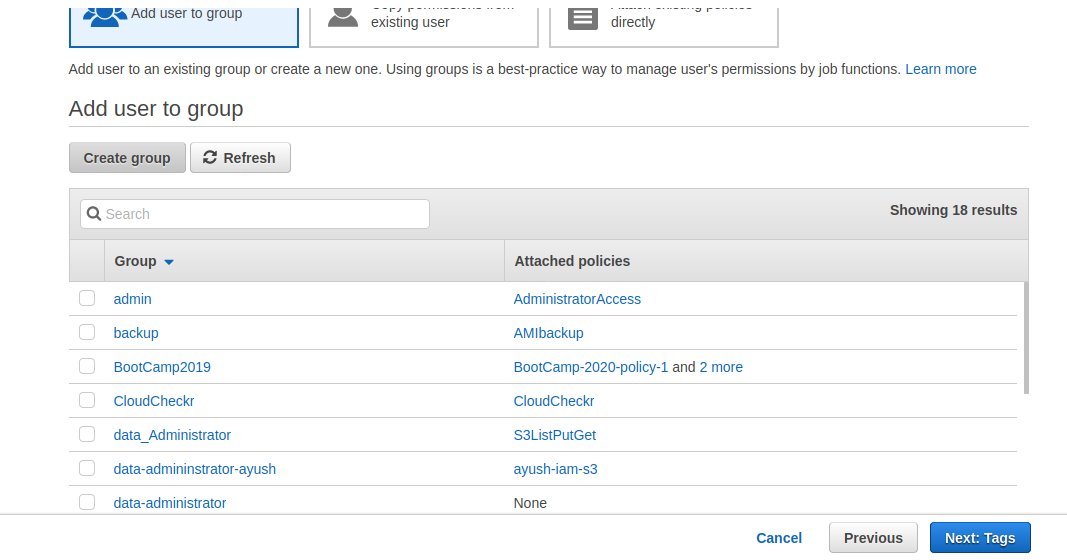
5. Create a group for the "Developer group " where the user 'bob ' is a member of this group. This group with Test Newly Developed Features for which they require access to EC2 instances. Provide the following access to this group:

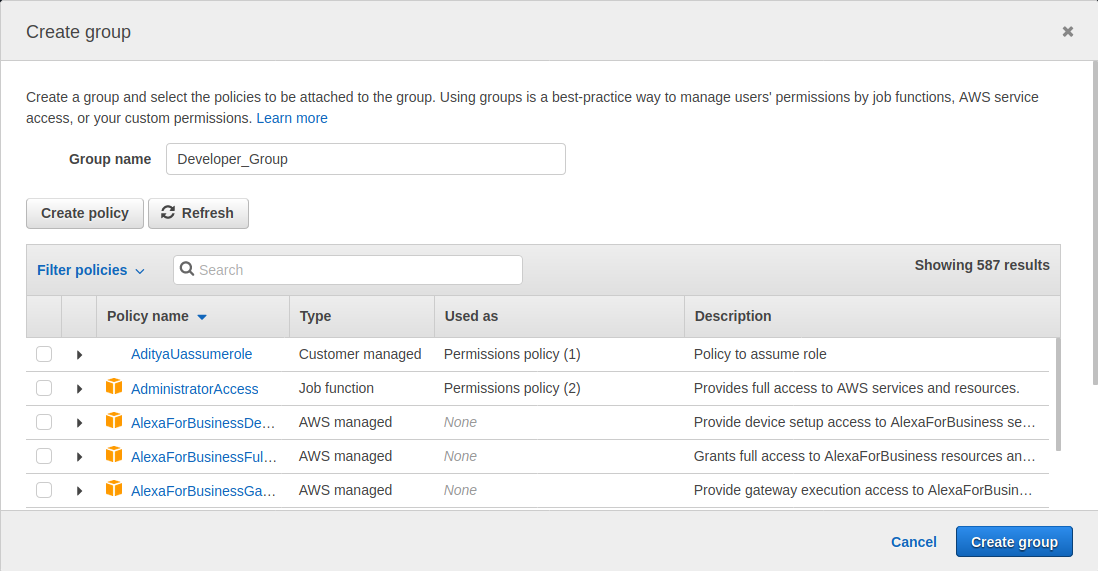
Service: Amazon EC2

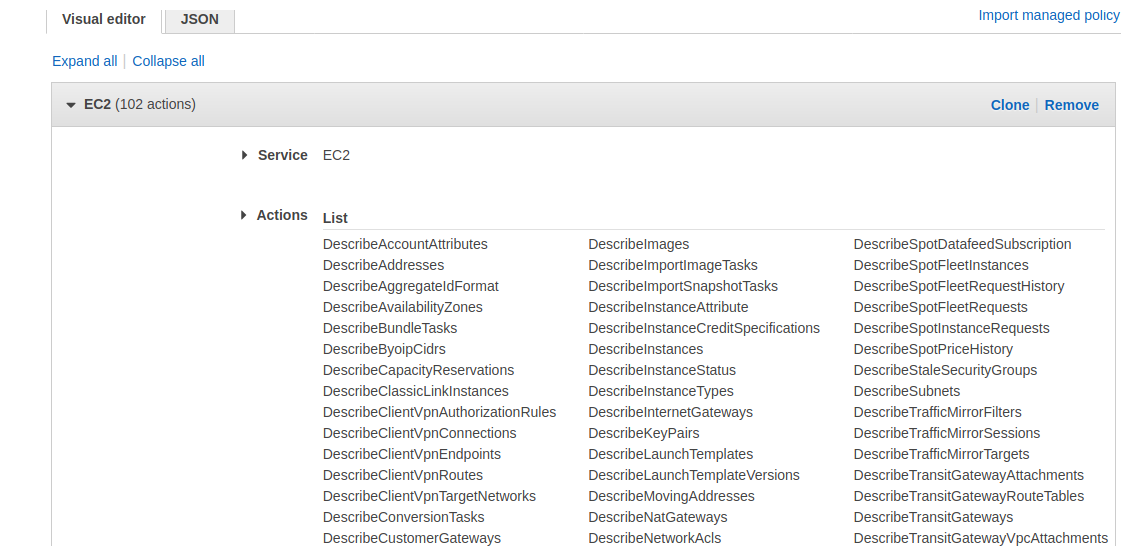
Action: \*Instances, \*Volume, Describe\*, CreateTags;

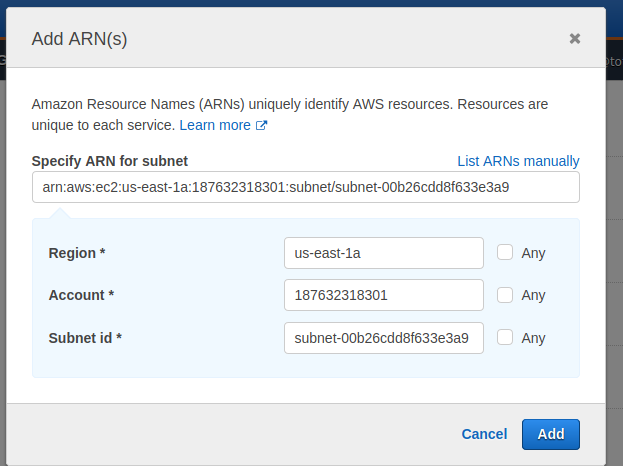
Condition: Dev Subnets only

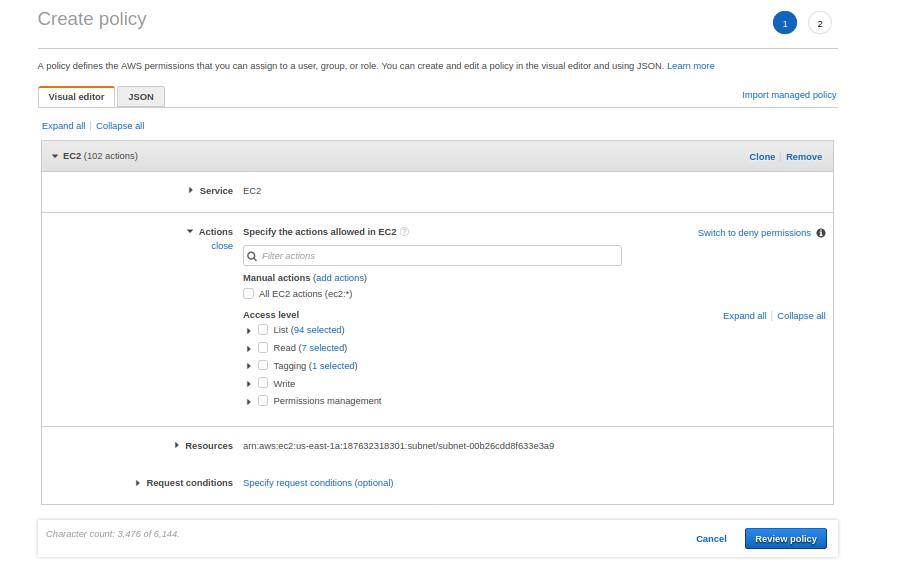


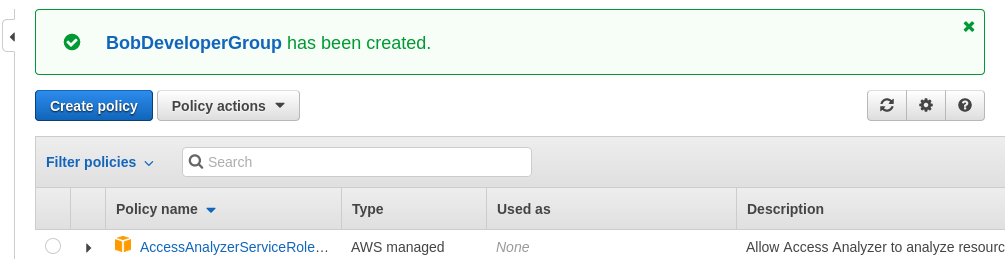


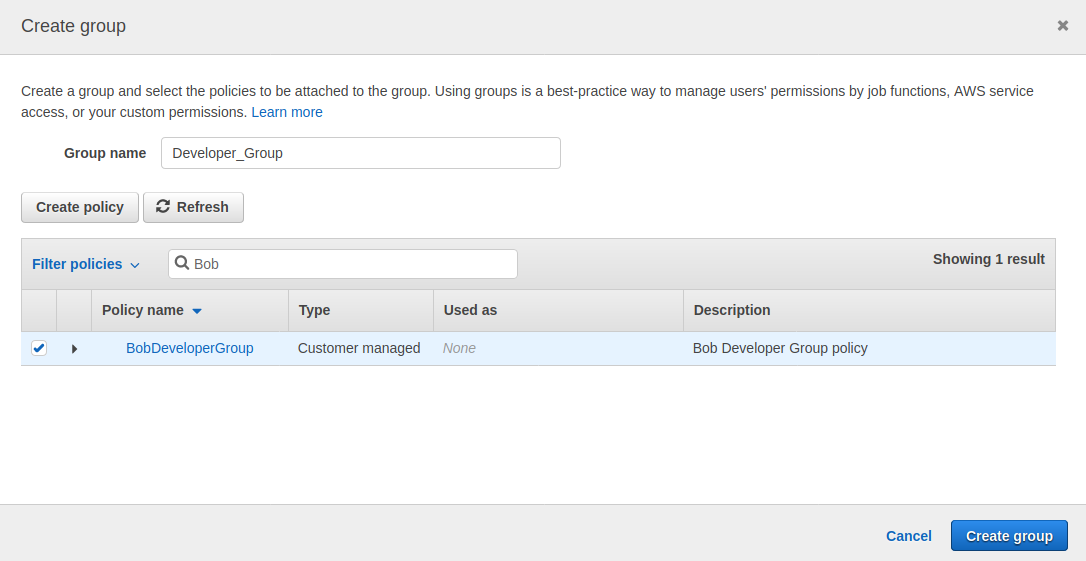


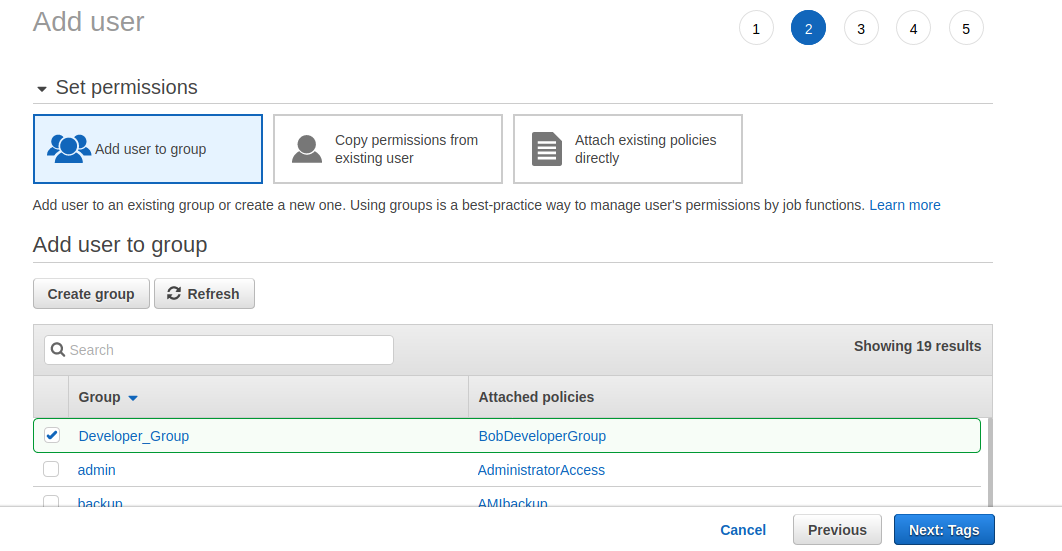


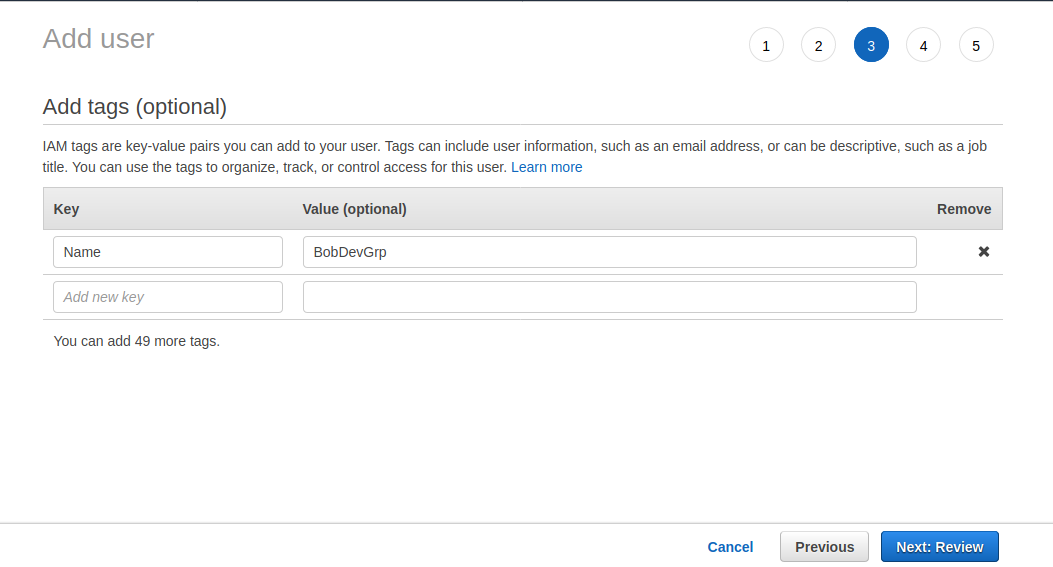


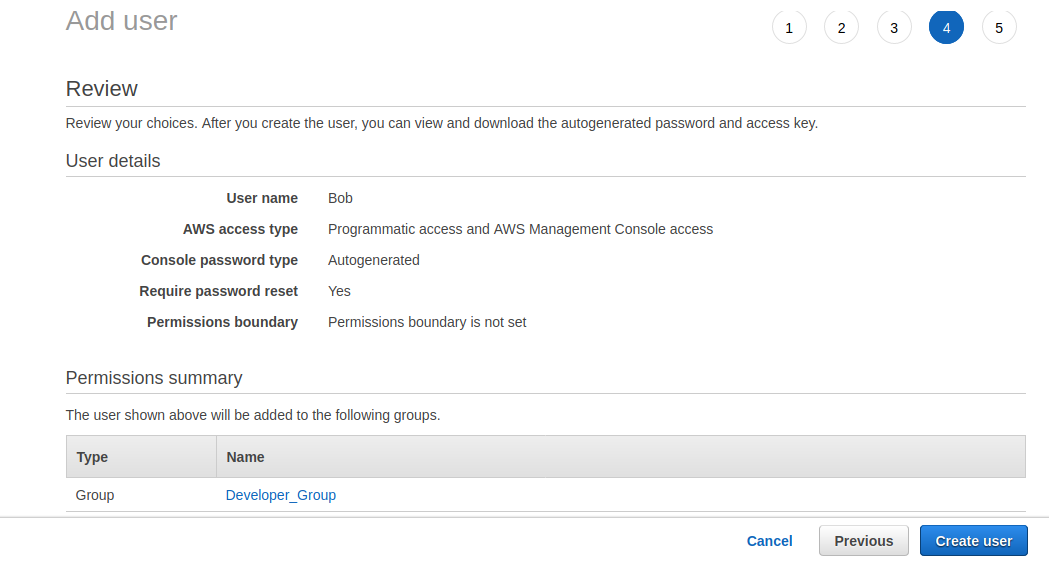


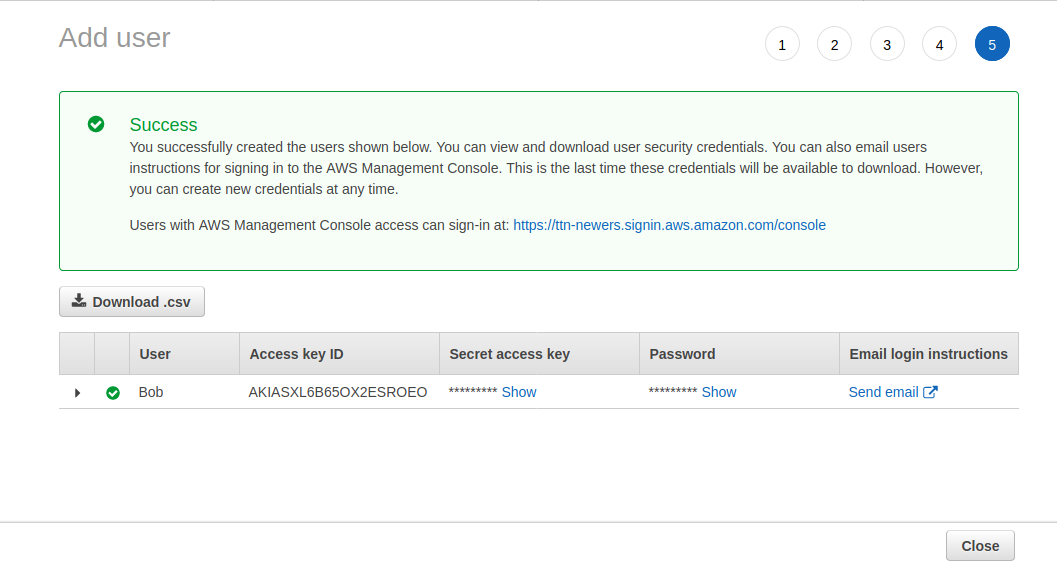




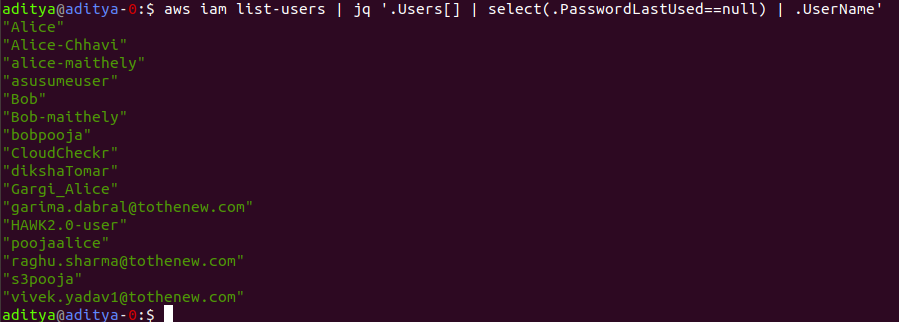








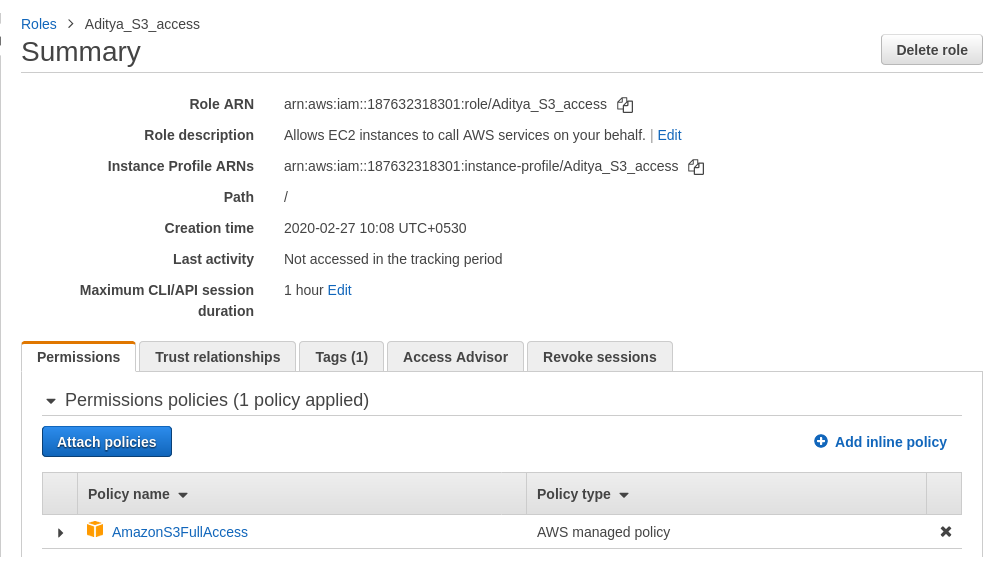
6. Identify the unused IAM users/credentials using AWS CLI.

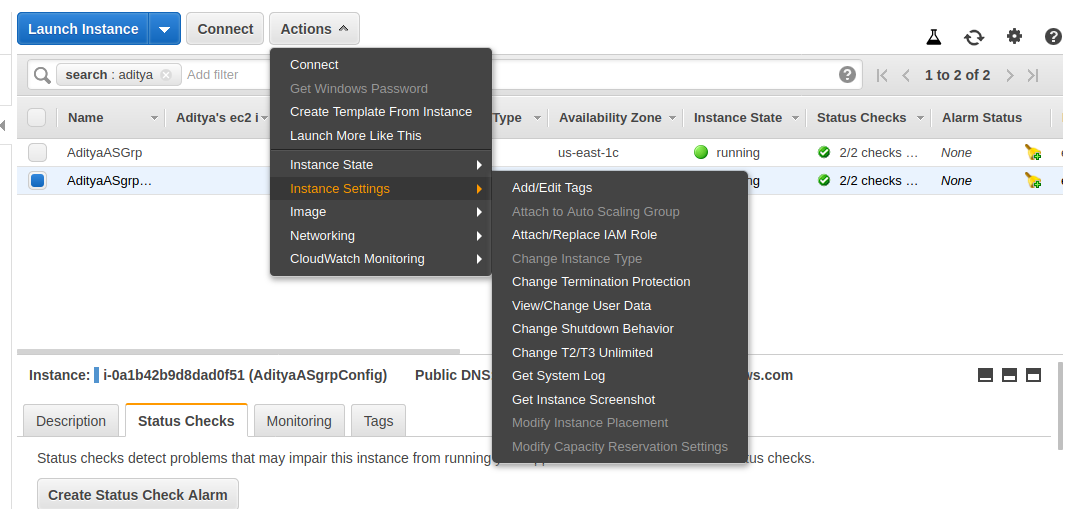


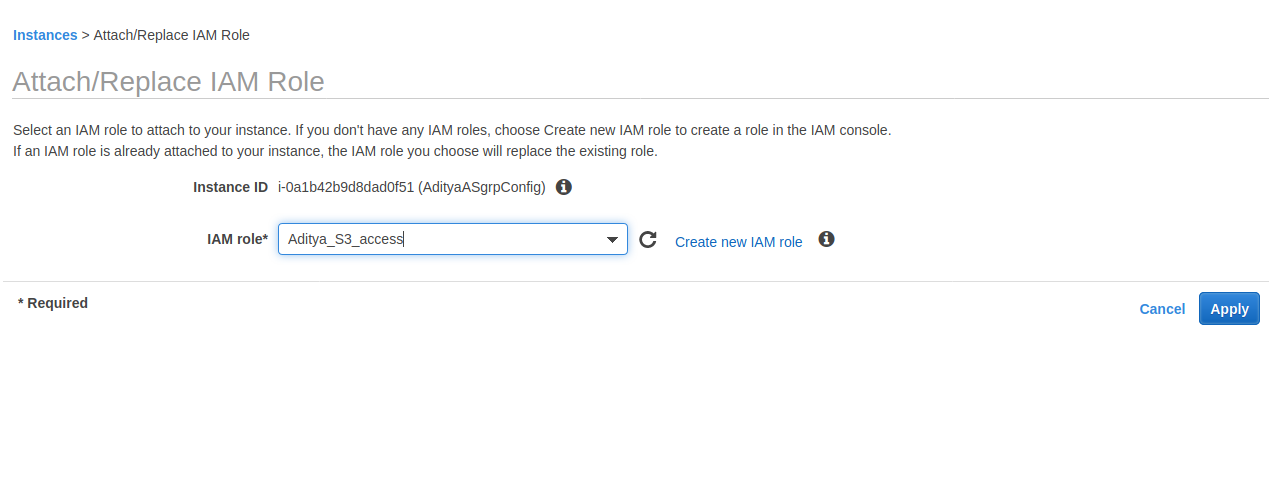
7. Identify all the instances having the tag key-value "backup=true" using AWS CLI.

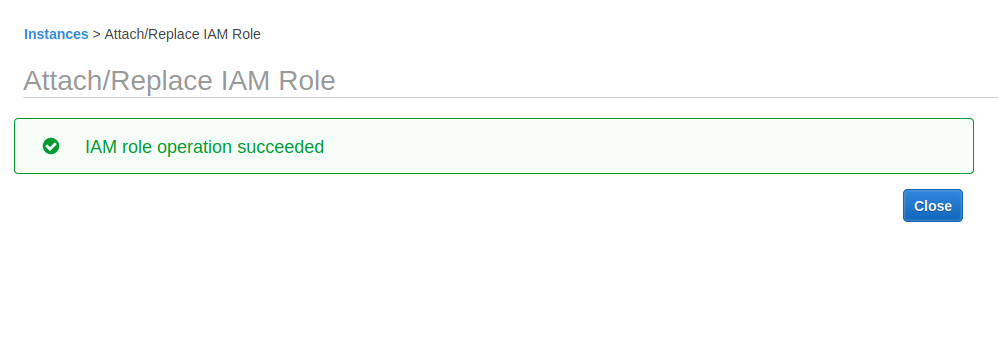


8. An EC2 Instance hosts a Java-based application that accesses an s3 bucket. This EC2 Instance is currently serving production users. Create the role and assign the role to EC2 instance.

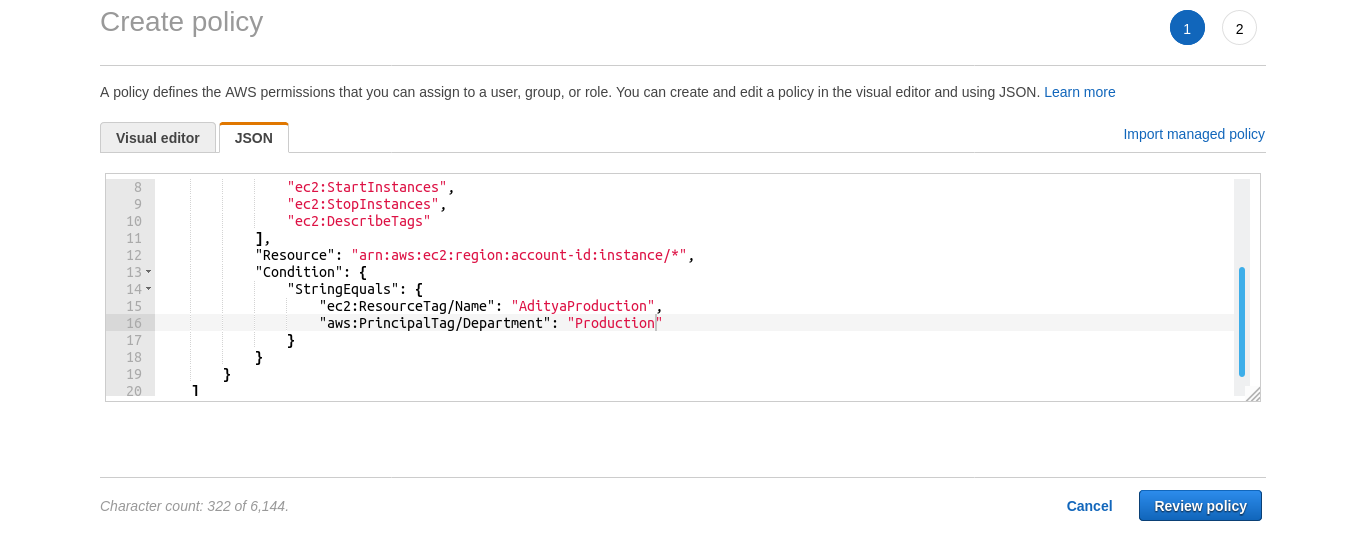


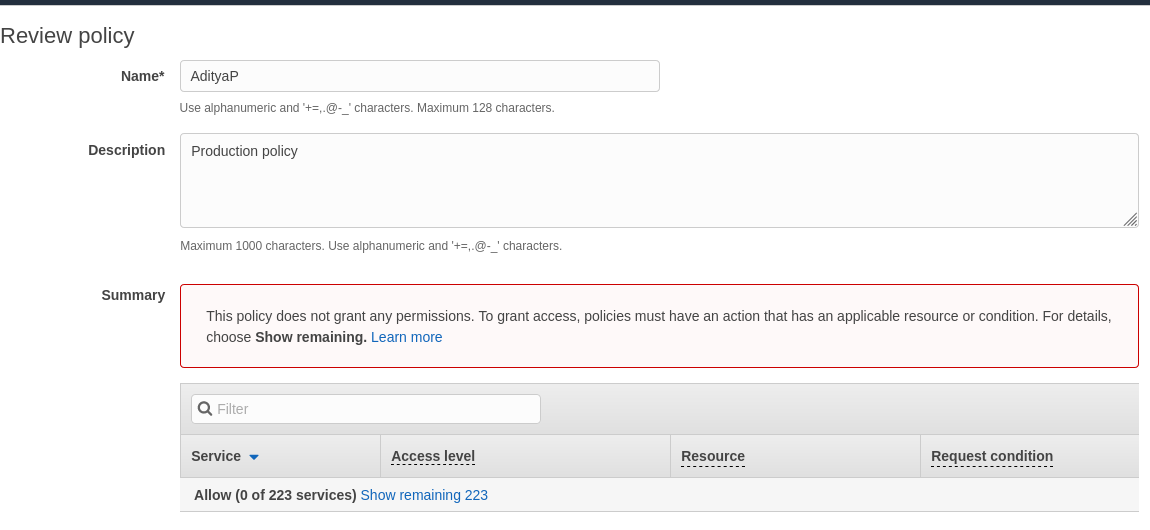


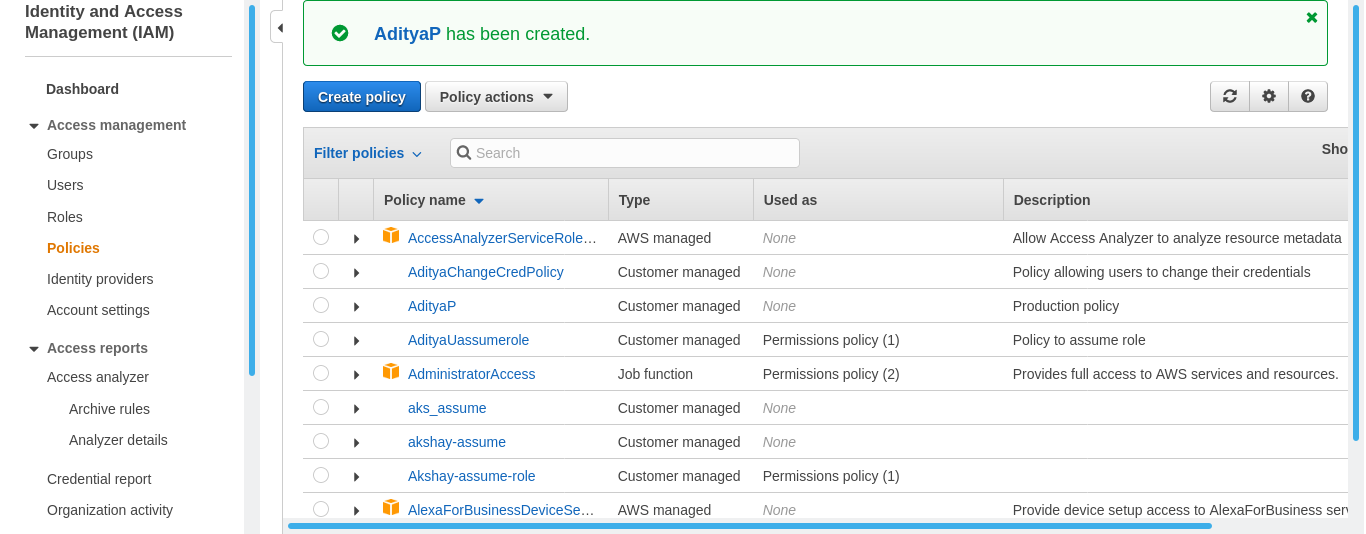




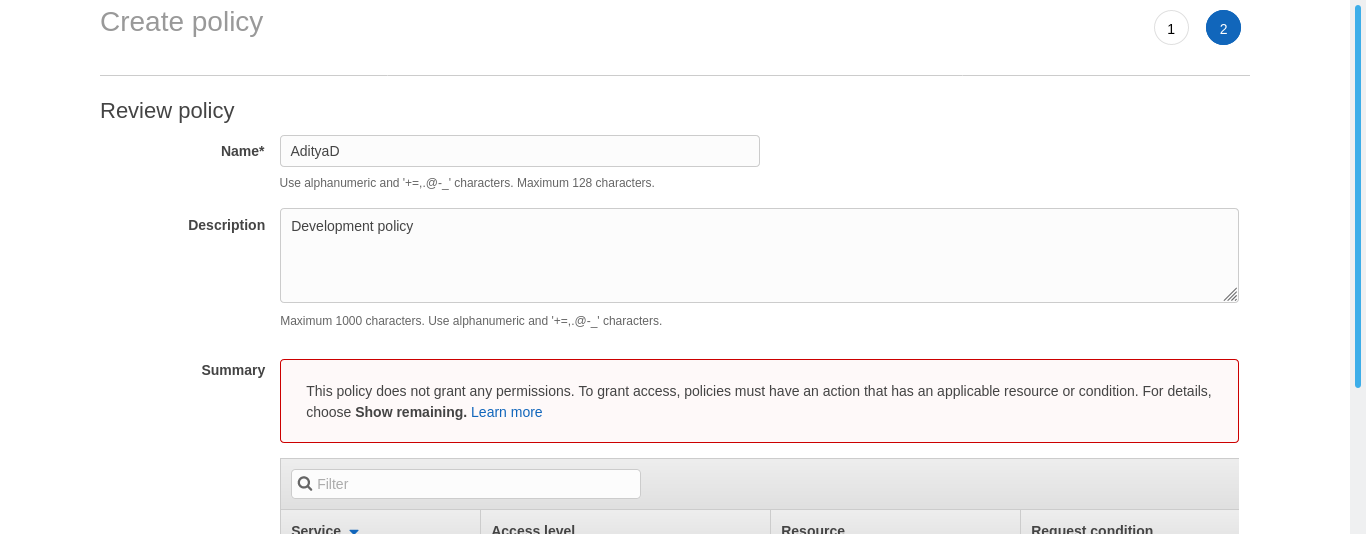
9. You have both production and development based instances running on your VPC. It is required to ensure that people responsible for the development instances do not have access to work on production instances for better security. Define the tags on the test and production servers and add a condition to the IAMPolicy which allows access to specific tags.

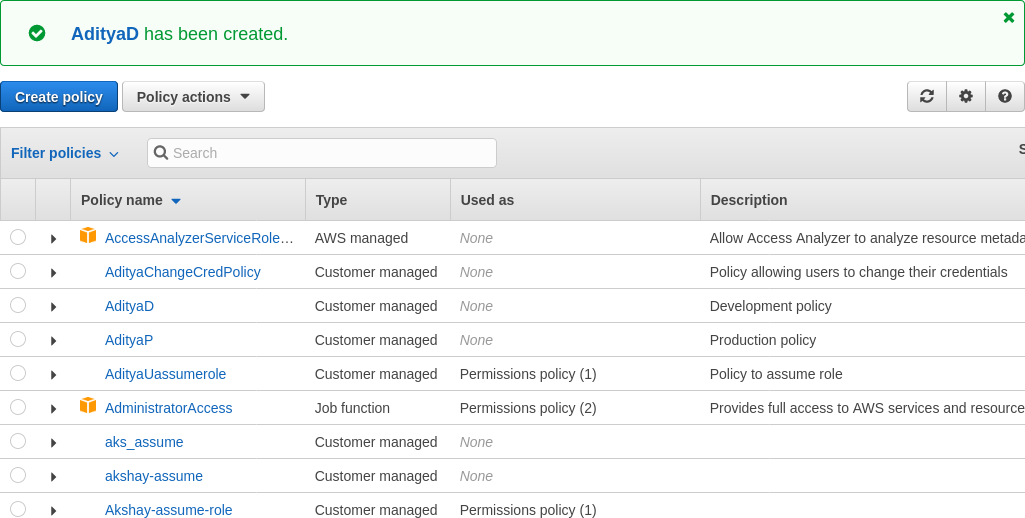












10. Create a policy for allowing users to set or rotate their credentials, such as their console password, their programmatic access keys, and their MFA devices.

