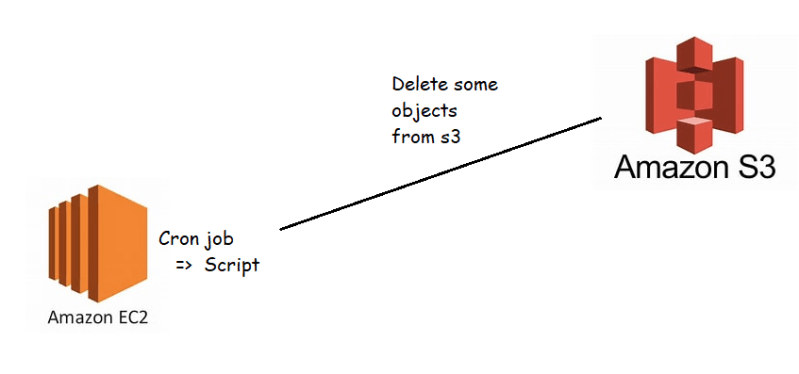
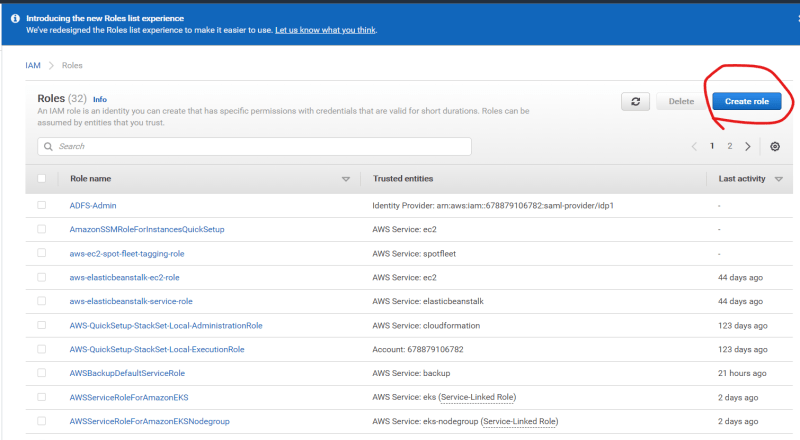
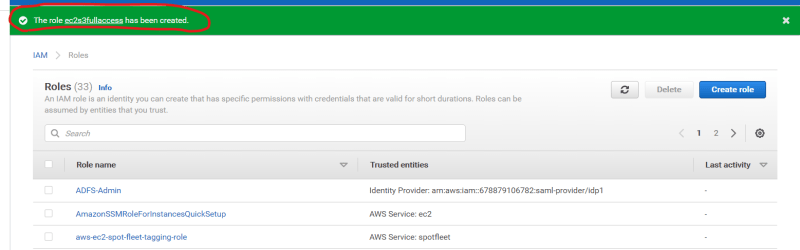
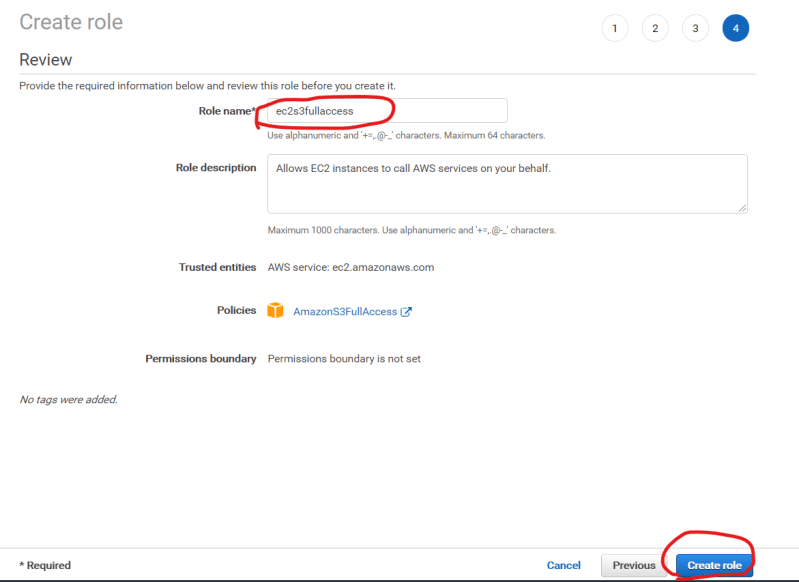
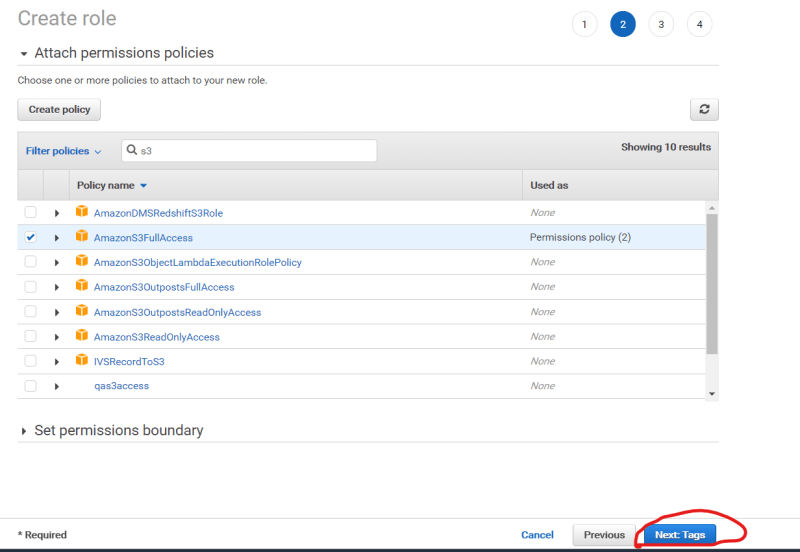
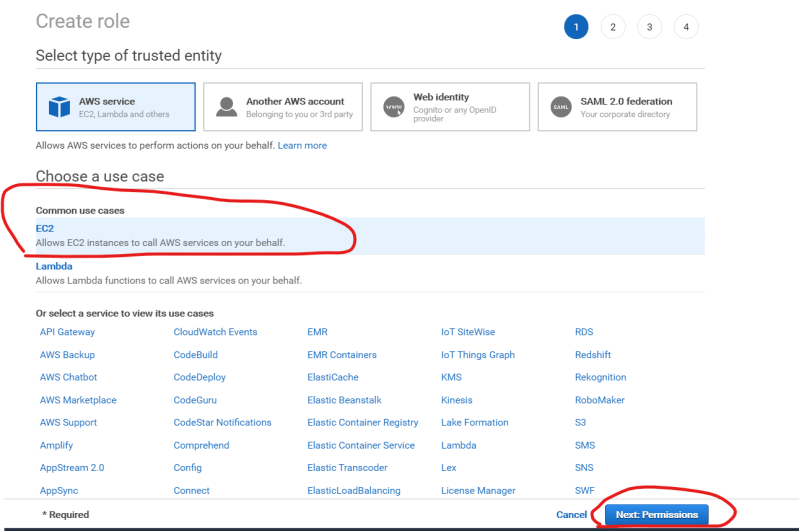
**IAM Roles**

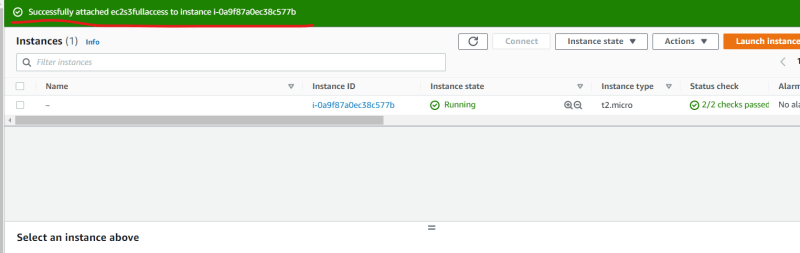
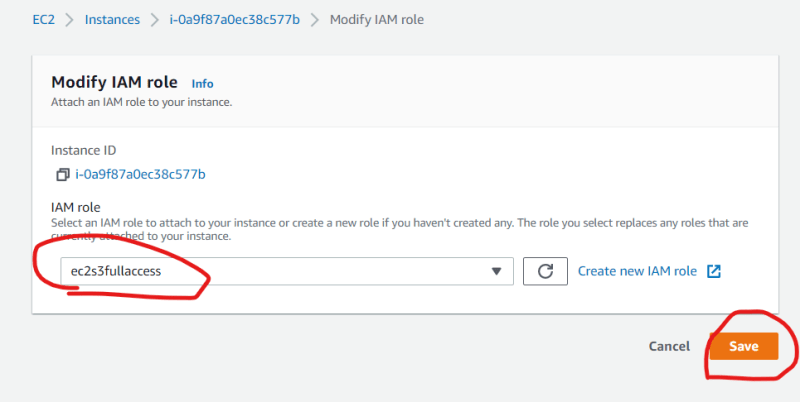
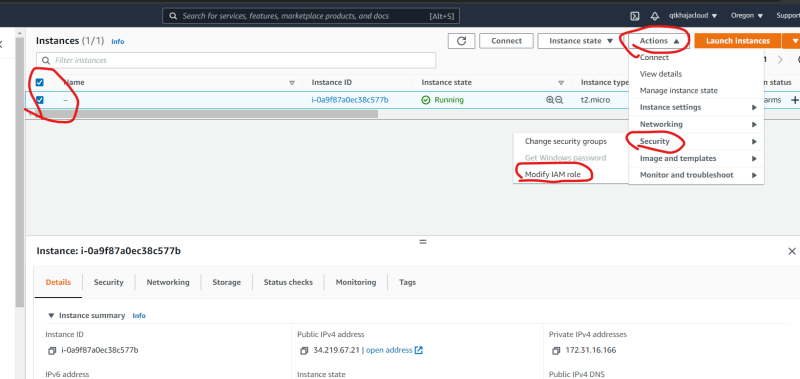
* An IAM Roles is an permission given to the AWS service to access other AWS Services.
* Scenarios
  + Some cron job running on ec2 to delete some s3 objects
    - We need to give permission to ec2 to access s3

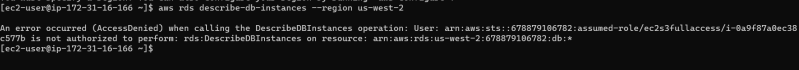
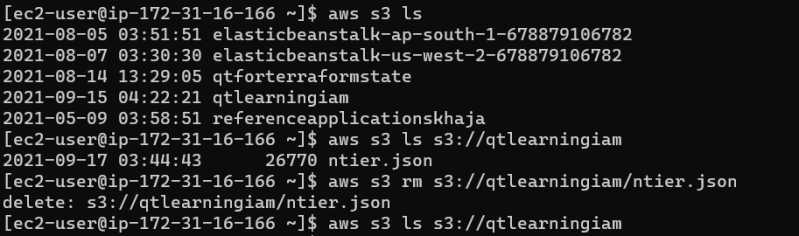
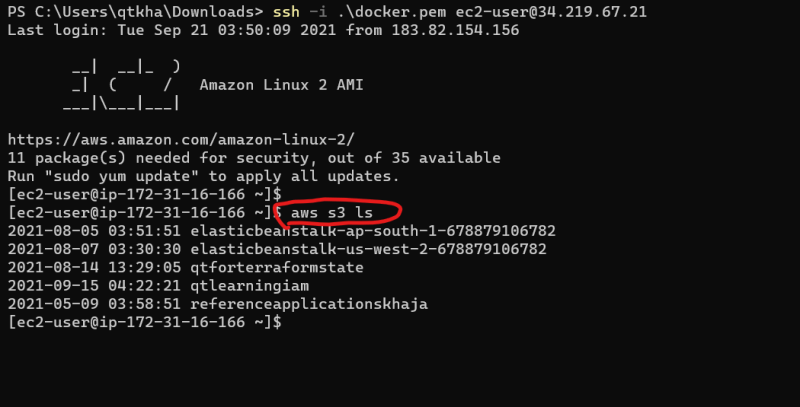


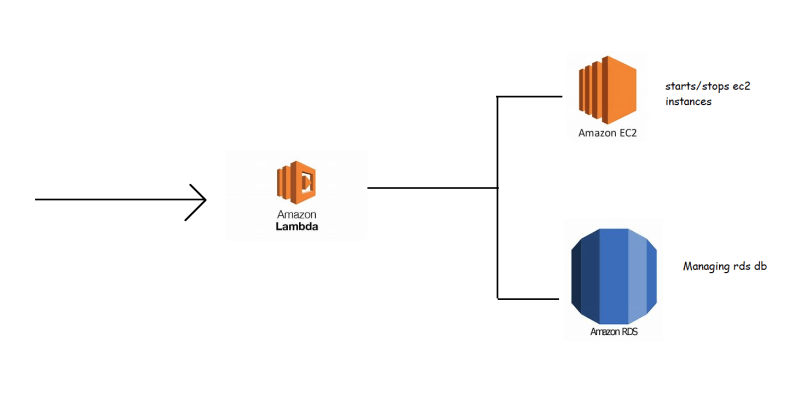
* + - In these kind of scenarios roles help.
    - We can create a role assign some policy to it. Attach role to AWS resource
    - Lets create ec2 instance
    - Now create an IAM role



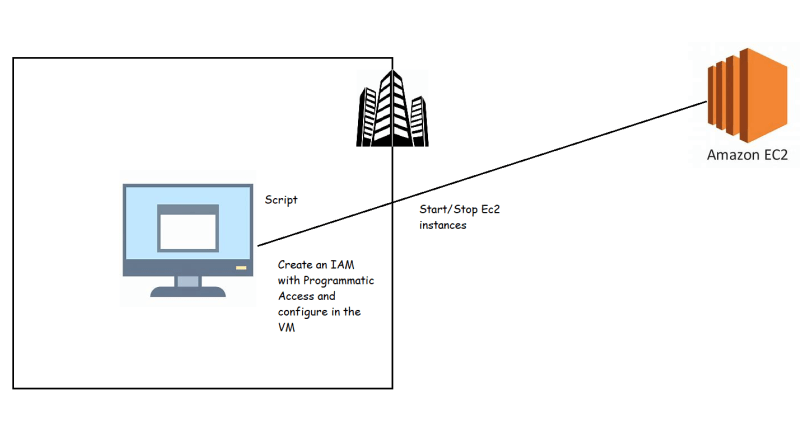


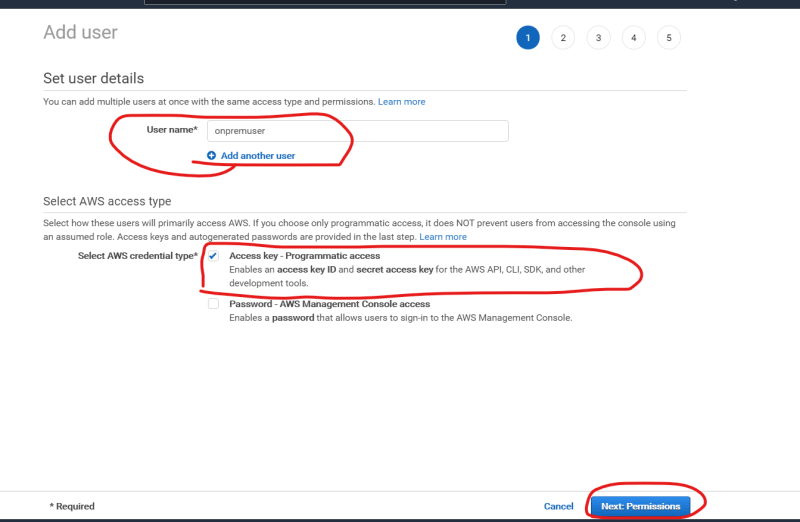
Now lets attach role to ec2 instance 

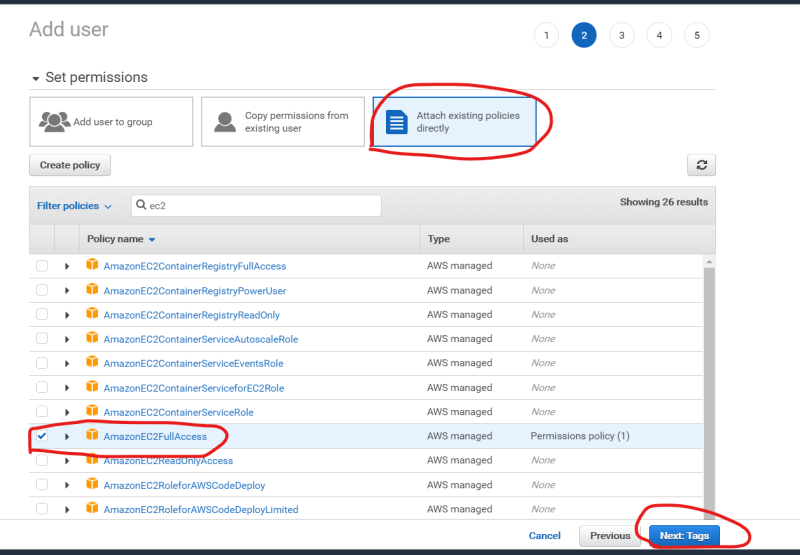
Login into ec2 and verify access 

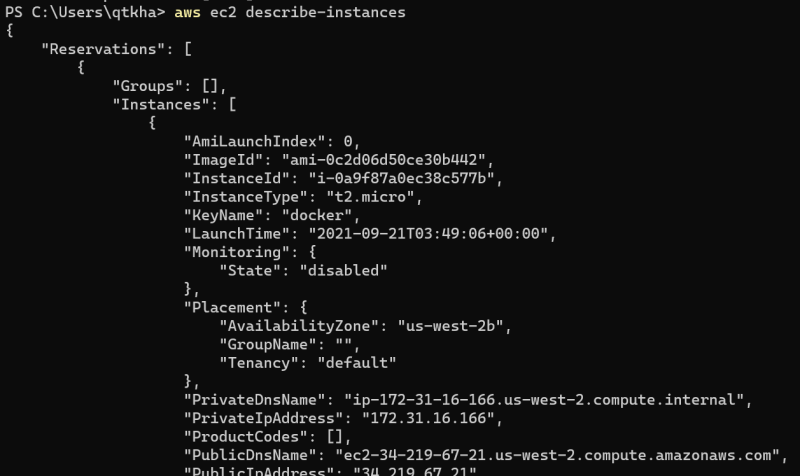
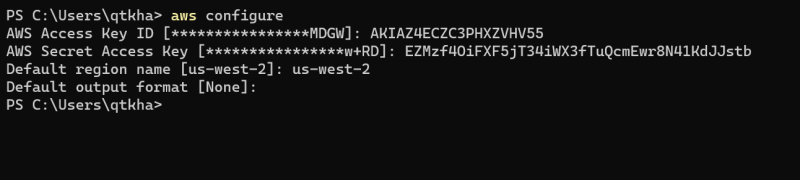
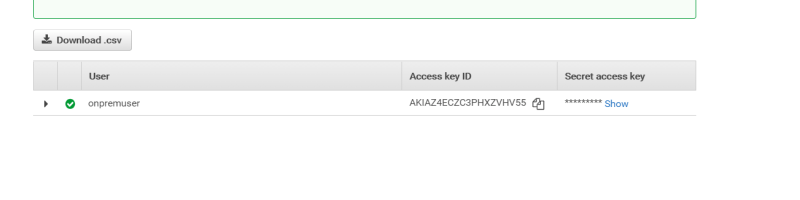
Access to AWS Lambda to start/stop/manage ec2 and rds instances 

Here we create a role for Lambda with iam policies to perform operations and attach it to lambda function

Access to AWS Services from on-premises 

Create an IAM user with programmatic access 

Attach necessary IAM Policy 

* Install AWS CLI on the on-premise vm
* Configure AWS cli with secret access key & id 
* Best Practice: Use CLI profiles to work with multiple AWS accounts or with different user permissions. Please go through the classroom video