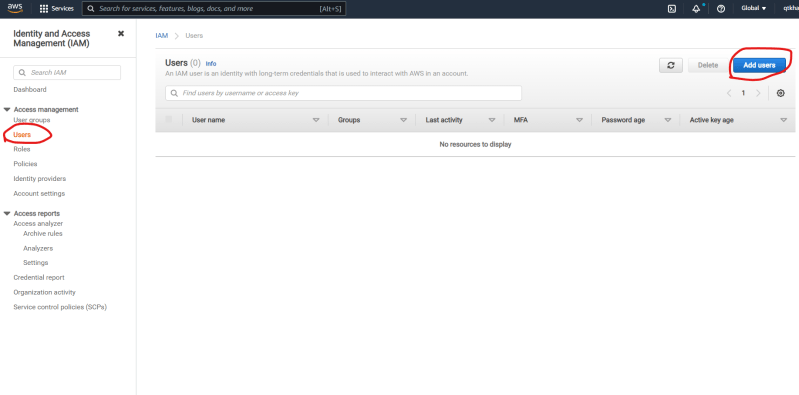
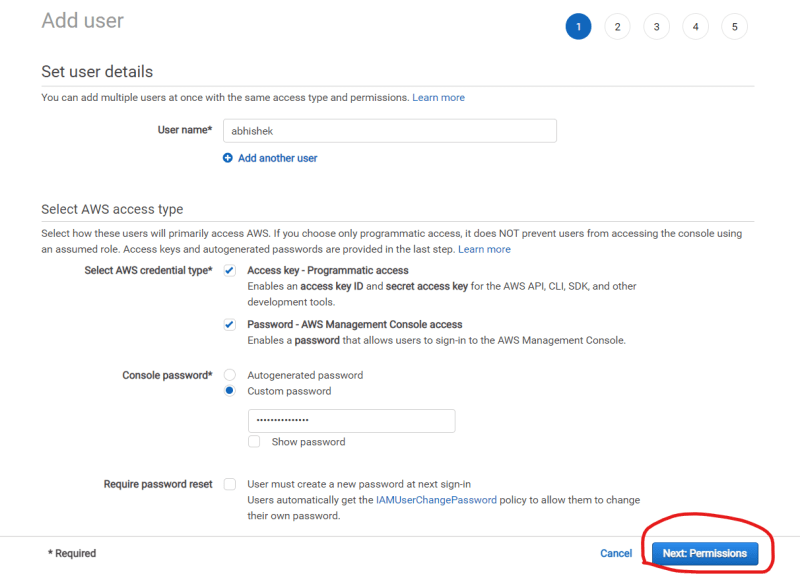
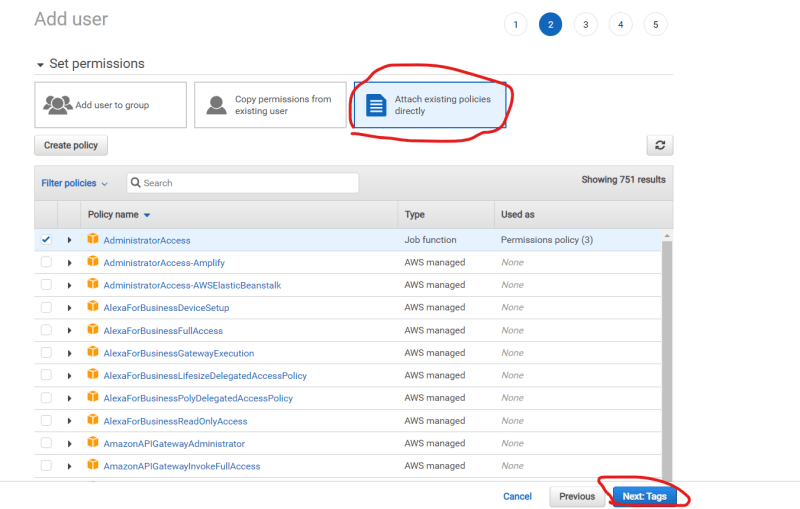
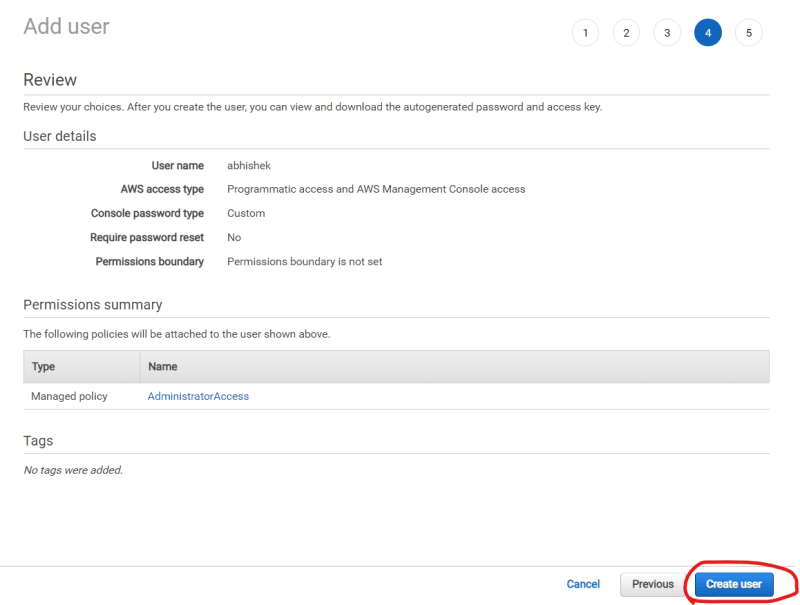
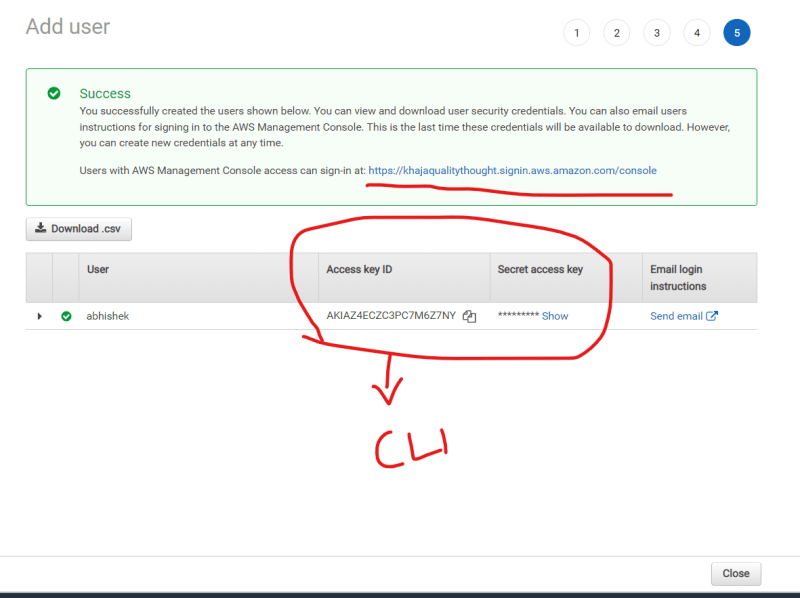
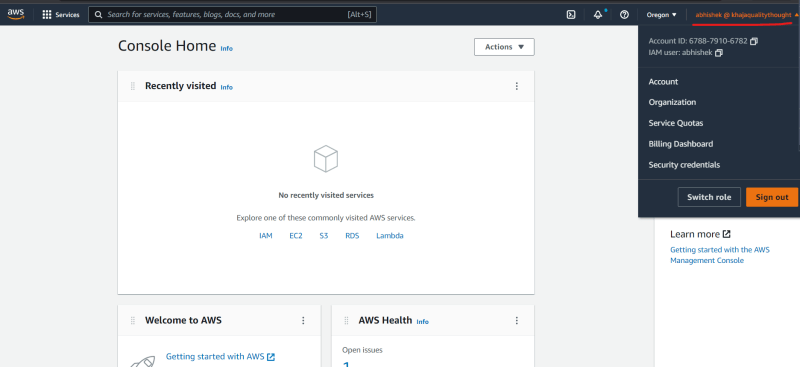
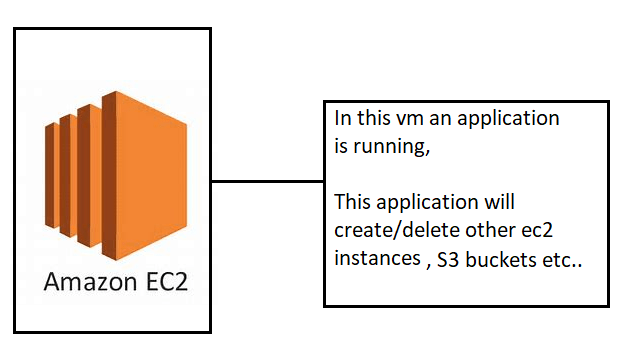
**Scenario1:** A new employee has joined the team who would be responsible for creating infrastructure in AWS

Solution:

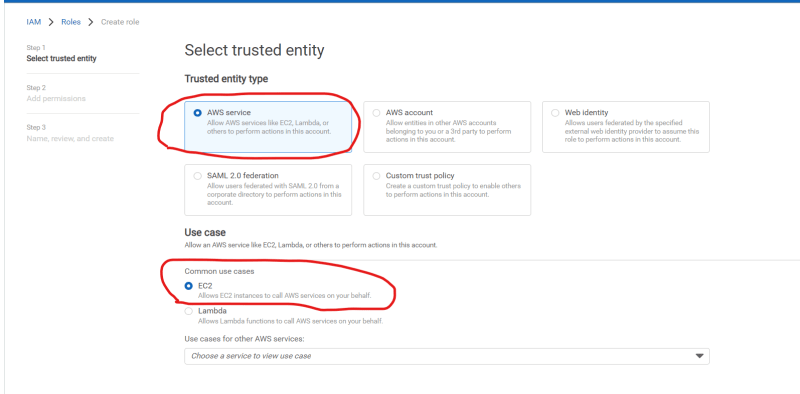
* Create a new IAM User
* Give him Both Programmatic access and Console Access
* Select the right policy for this user.

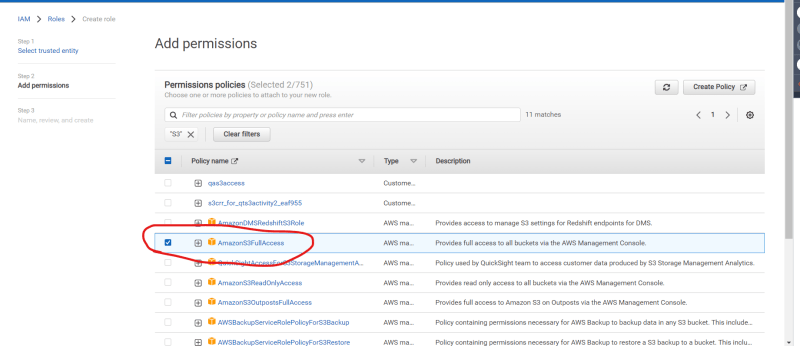
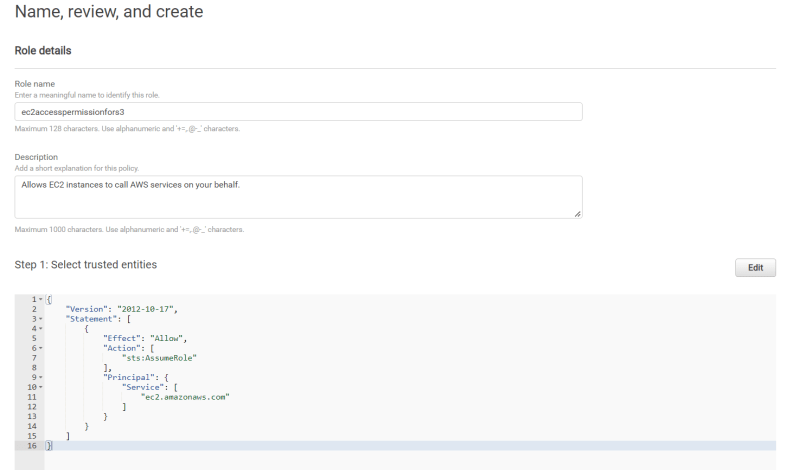
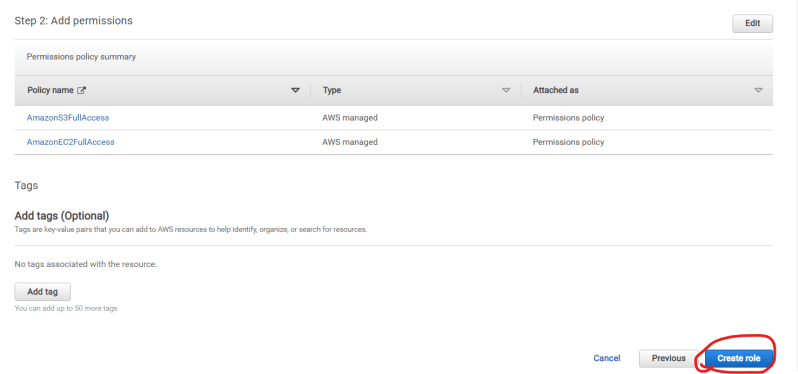
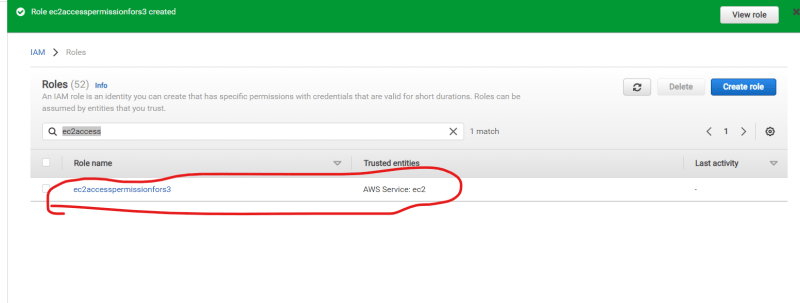
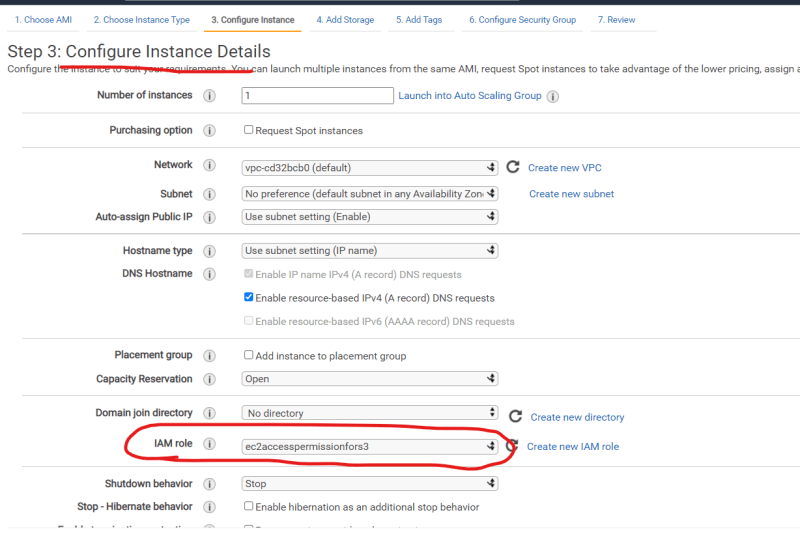
  
  
  
  
  
  


**Scenario 2:** An application running in ec2 requires permissions to create/delete other AWS resources [Example Terraform apply/Terraform destroy]  


* One way of solving this is
  + Create an IAM user with programmatic access
  + Configure this access into the application running on ec2
  + Ensure the IAM User which you have create has necessary permissions.
* Other Way is Role:

Role in AWS is a permission given to AWS Resource/Service to access other AWS Services/Resource



**Scenario 3:** Consider we have 5 admins who require same set of permissions, so rather that managing policy at user level, we manage it at the group level  
