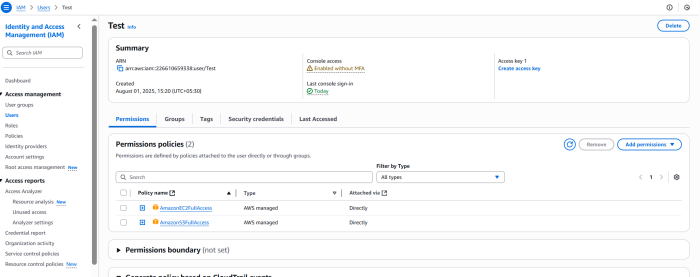
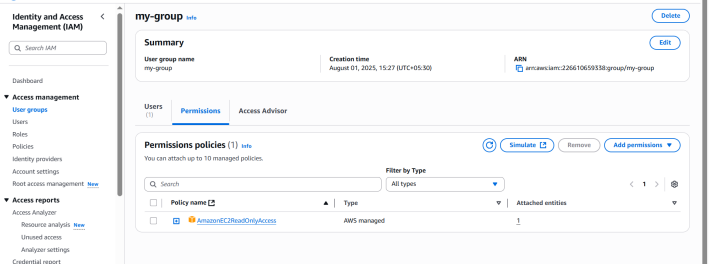
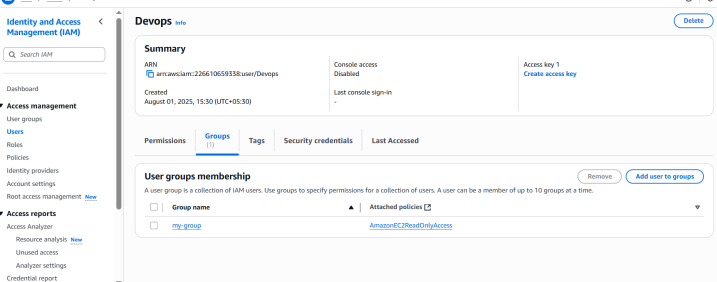
1. Create one IAM user and assign ec2,s3 full access role.



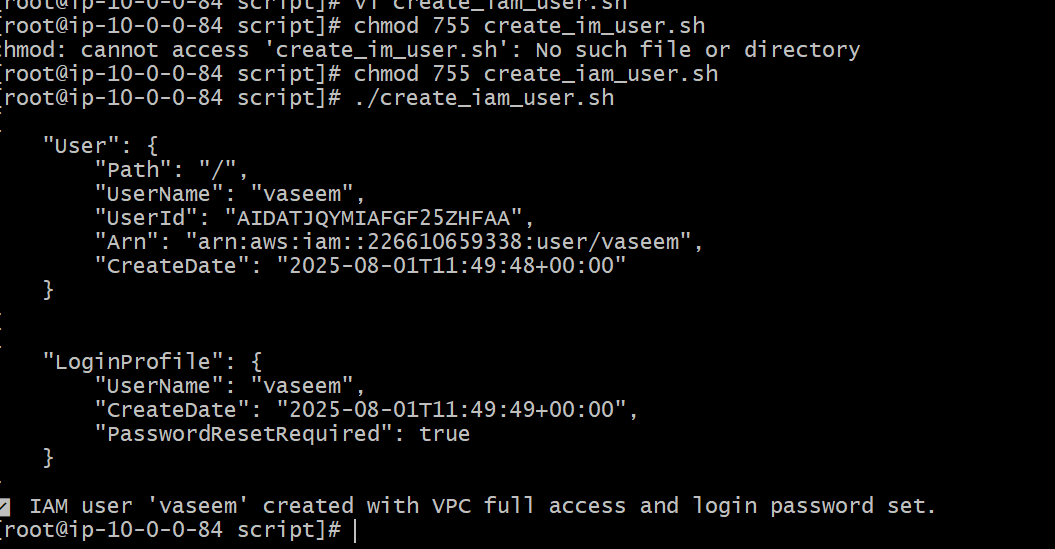
1. Create one Group in IAM and Assign Read access for ec2.

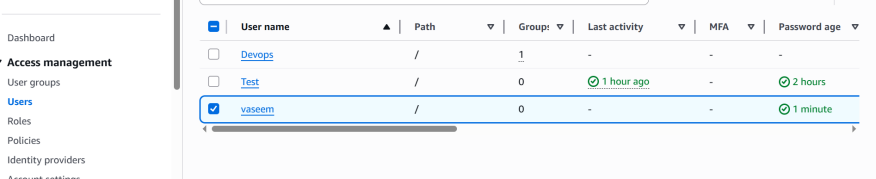


1. Create a new user with name Devops and add to the group created in task2.

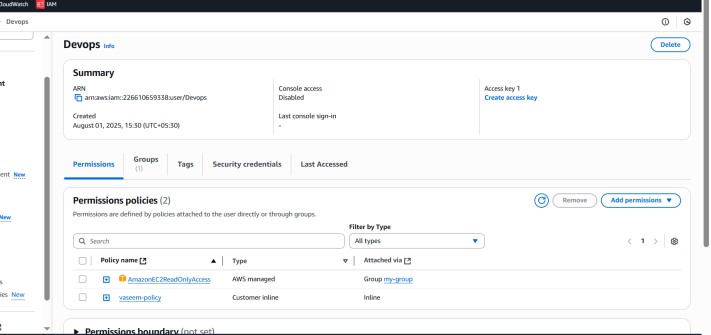


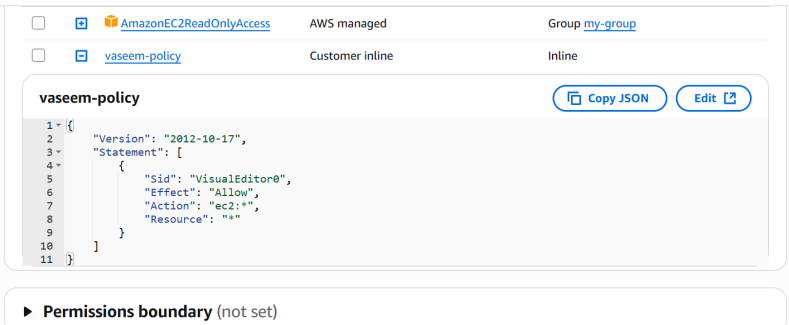
1. Write a bash script to create a IAM user with VPC full access.





1. Create a IAM policy to access ec2 for a specific user in specific regions only.





1. We have two accounts Account A and Account B, Account A user should access s3 bucket in Account B. (Collaborate with team member and execute this.Mostly asked in every interview)

--->We have to create Inline-policy in account-A with name of our bucket name (vaseem.shop) and in account-B need to create bucket policy with account-A account#

User Inline policy:

{  
 "Version": "2012-10-17",  
 "Statement": [  
  {  
   "Sid": "Example",  
   "Effect": "Allow",  
   "Action": [  
    "s3:ListBucket"  
   ],  
   "Resource": [  
    "arn:aws:s3:::vaseem.shop;"  
   ]  
  }  
 ]  
}

In account-B need to create bucket policy with account-A account#

{  
   "Version": "2012-10-17",  
   "Statement": [  
      {  
         "Sid": "Example permissions",  
         "Effect": "Allow",  
         "Principal": {  
            "AWS": "arn:aws:iam::(id of account-A):root"  
         },  
         "Action": [  
            "s3:GetLifecycleConfiguration",  
            "s3:ListBucket"  
         ],  
         "Resource": [  
            "arn:aws:s3:::(bucket name of account-B)"  
         ]  
      }  
   ]  
}

After updating policies in both account need to configure in GIT-bash with commands

> aws configure

> aws s3 ls

> aws s3 ls s3://(account-B bucket name)

It will appear the account-B bucket objects

