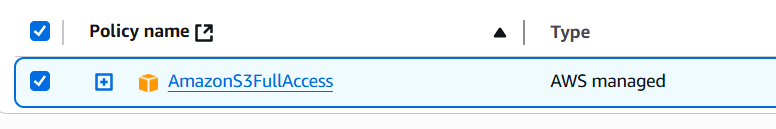
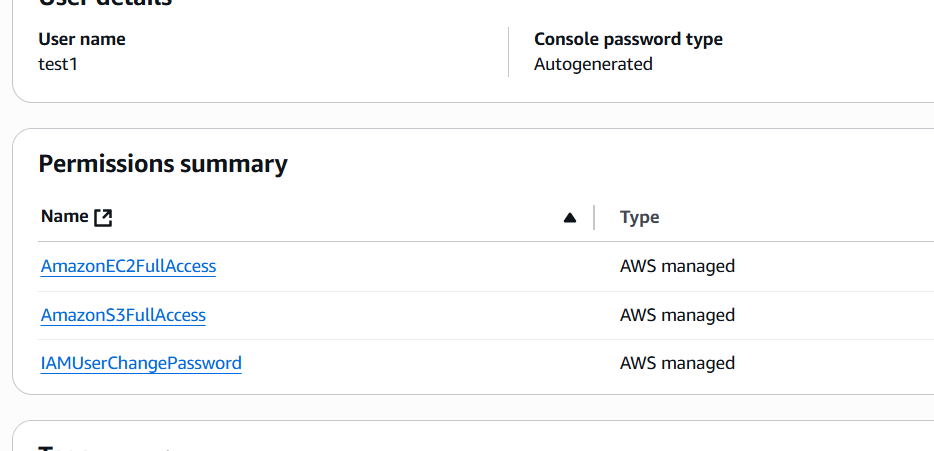
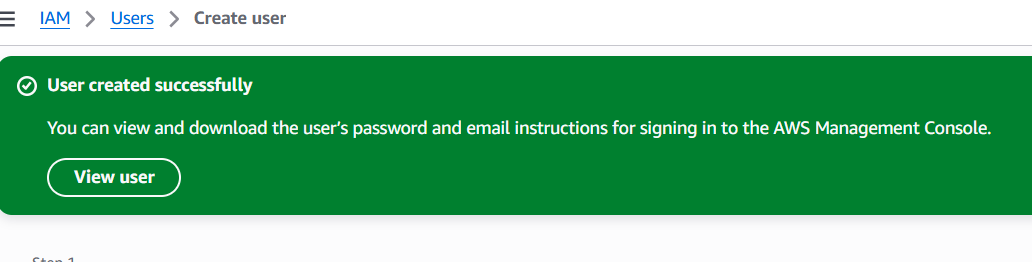
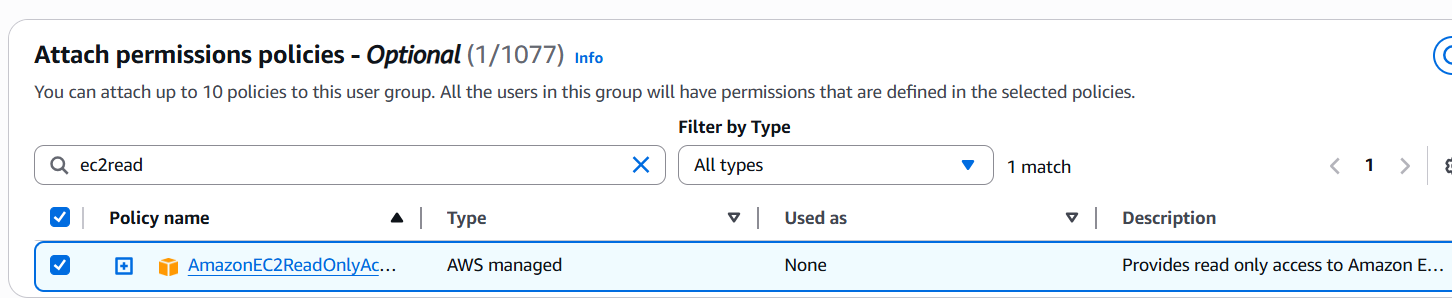
**IAM TASK**

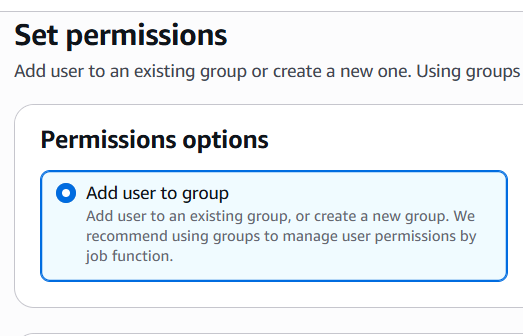
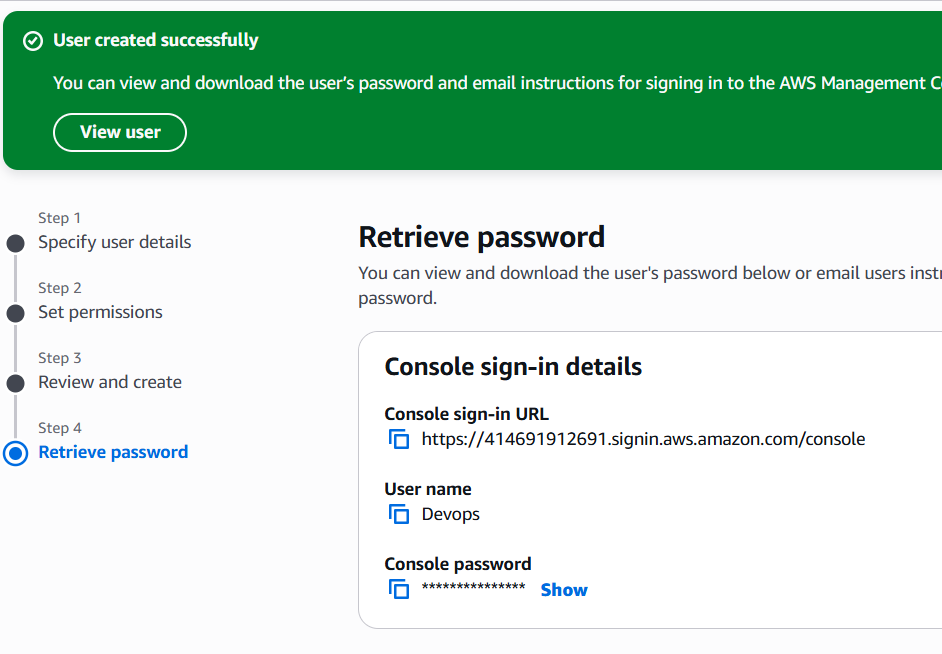
1. **Create one IAM user and assign EC2 and S3 full access roles.**

* Login into aws console
* Navigate to iam
* Create user and add password
* Attach the policy
* Ec2full acess and s3 full access
* ****
* ****
* ****
* user created

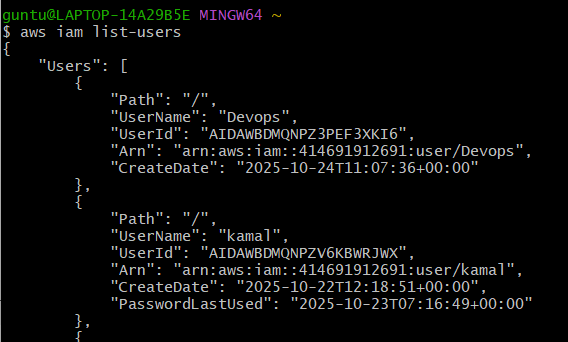
1. **Create one group in IAM and assign read access for EC2.**

* Navigate to iam
* Find groups
* Create a group
* And attach permission read only acces to ec2
* ****

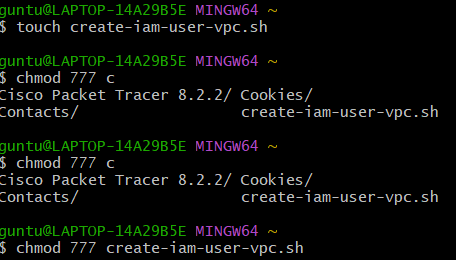
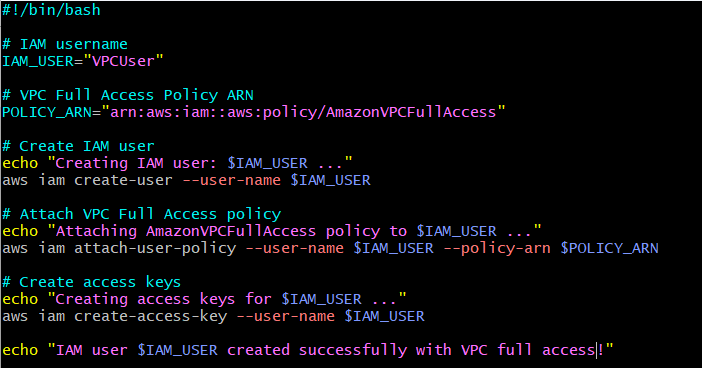
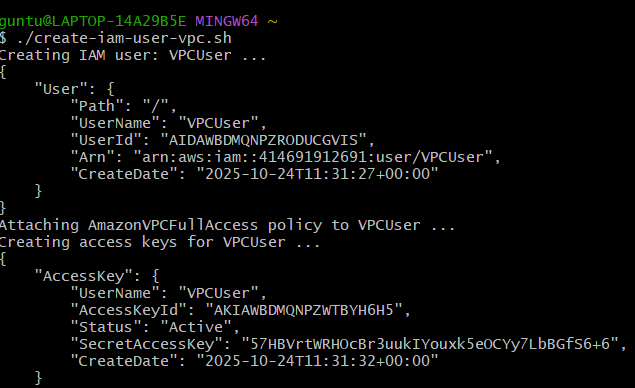
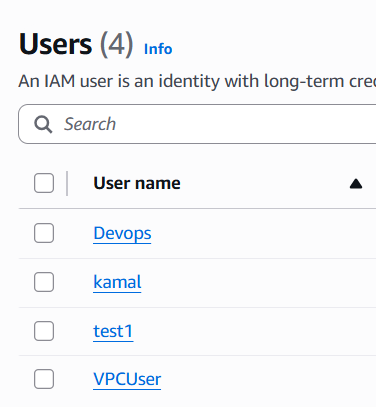
1. **Create a new user named "Devops" and add to the group created in task 2.**

* Create a user with name Devops
* Select autogenrate password
* Select add this user to group
* ****
* ****
* user added to group

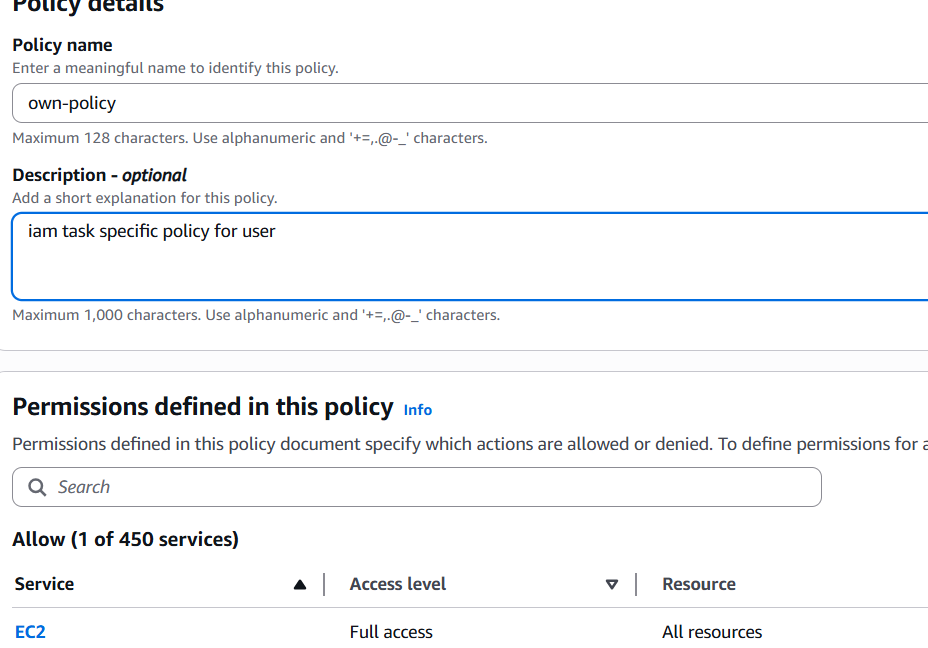
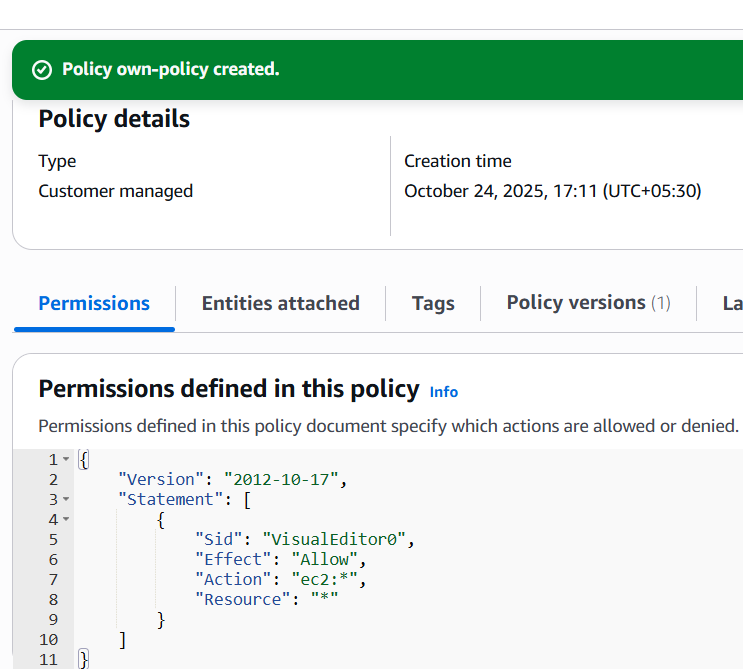
**4 . Write a bash script to create an IAM user with VPC full access.**

* Configure aws cli and gui
* Aws configure give, access key and secret key
* Aws iam list-users – shows all existing users in aws gui
* ****
* Writing a bash script for creating a new user in aws iam through cli

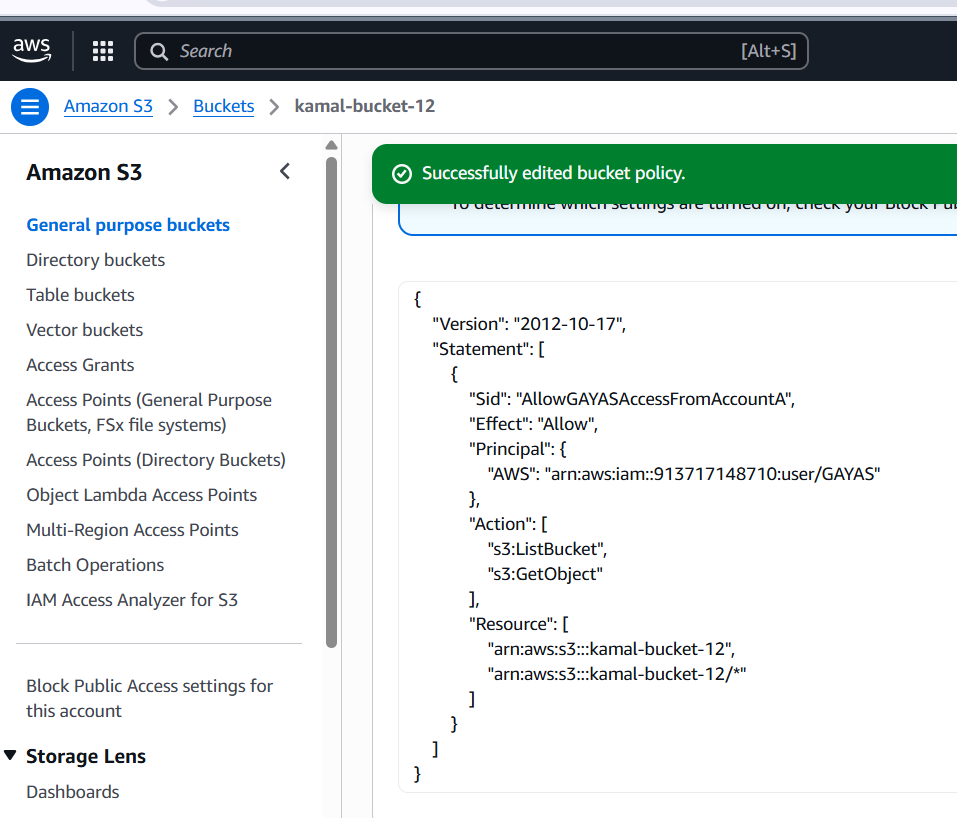
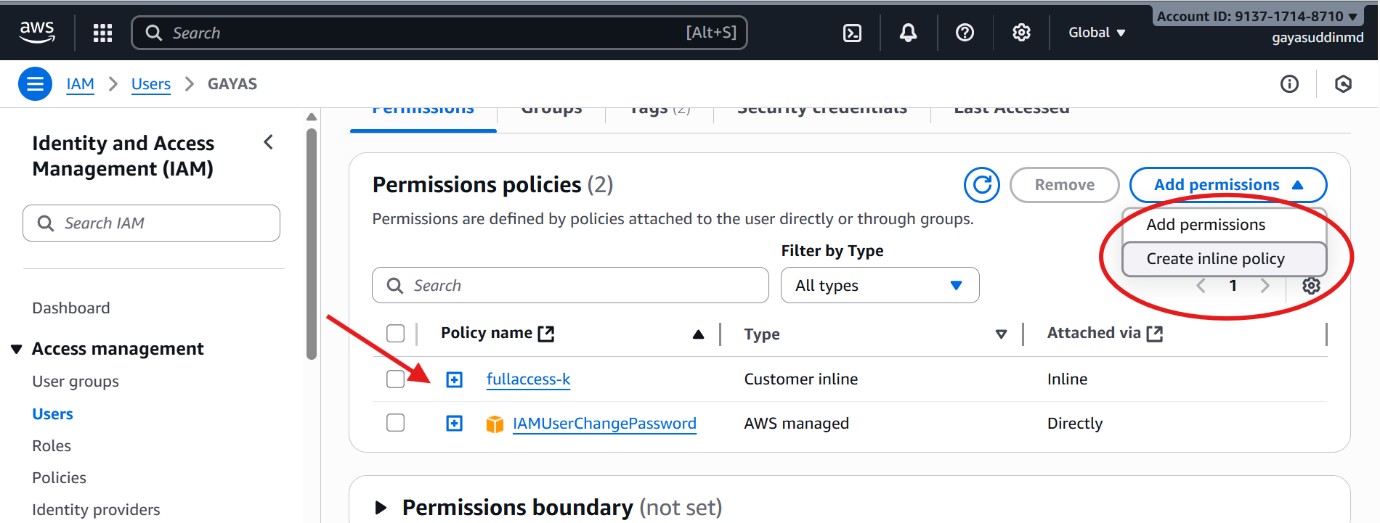
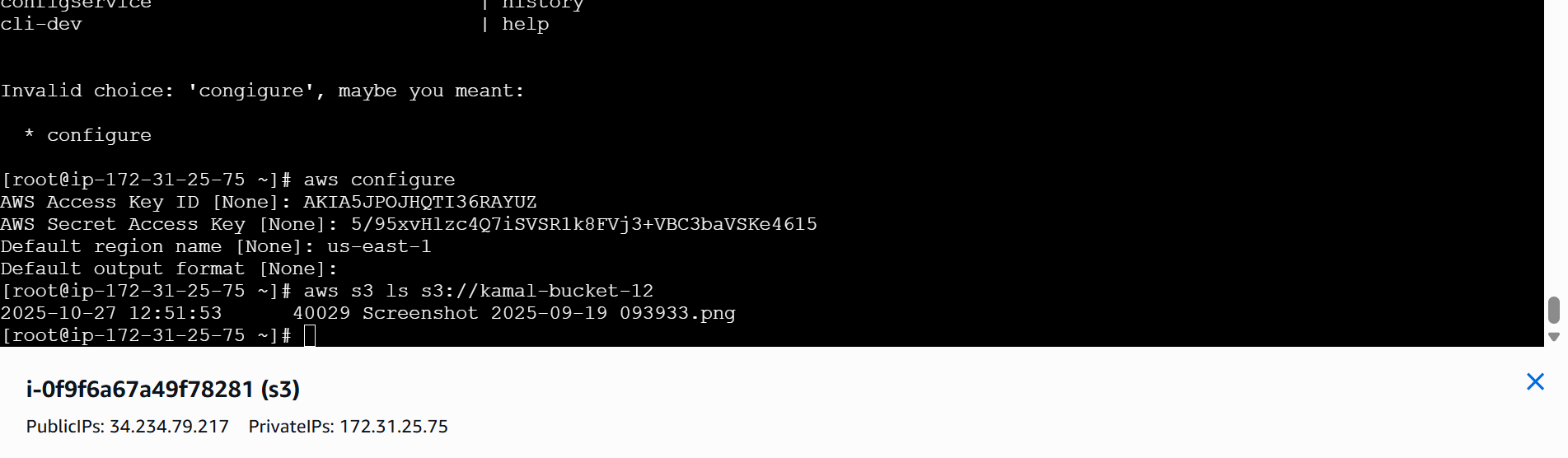
This creates an executable script file.

* touch create-iam-user-vpc.sh
* give permission
* chmod create-iam-user-vpc.sh
* 
* Open the file and start edit
* Vi create-iam-user-vpc.sh
* Add script for creating iam user with vpc full access
* #!/bin/bash
* # IAM username
* IAM\_USER="VPCUser"
* # VPC Full Access Policy ARN
* POLICY\_ARN="arn:aws:iam::aws:policy/AmazonVPCFullAccess"
* # Create IAM user
* echo "Creating IAM user: $IAM\_USER ..."
* aws iam create-user --user-name $IAM\_USER
* # Attach VPC Full Access policy
* echo "Attaching AmazonVPCFullAccess policy to $IAM\_USER ..."
* aws iam attach-user-policy --user-name $IAM\_USER --policy-arn $POLICY\_ARN
* # Create access keys
* echo "Creating access keys for $IAM\_USER ..."
* aws iam create-access-key --user-name $IAM\_USER
* echo "IAM user $IAM\_USER created successfully with VPC full access!"
* 
* Now run the script
* ./create-iam-user-vpc.sh
* 
* 
* Verify in gui
* Check for user called vpcuser
* 

5 . Create an IAM policy to allow EC2 access for a specific user in specific regions only.

* navigate to iam
* select policies
* specify thepermission for ec2 full access
* add json format
* 
* Policy created
* 

**6. We have two accounts: Account A and Account B. Account A user should access an S3 bucket in Account B**

* Created a s3 full access policy in IAM
* Now, navigate to S3 open bucket and permissions
* Edit policy and this script
* {
* "Version": "2012-10-17",
* "Statement": [
* {
* "Sid": "AllowGAYASAccessFromAccountA",
* "Effect": "Allow",
* "Principal": {
* "AWS": "arn:aws:iam::913717148710:user/GAYAS"
* },
* "Action": [
* "s3:ListBucket",
* "s3:GetObject"
* ],
* "Resource": [
* "arn:aws:s3:::kamal-bucket-12",
* "arn:aws:s3:::kamal-bucket-12/\*"
* ]
* }
* ]
* }
* 
* Now go second account GAYAS – user
* 
* Open permission and click inline policy and
* Add this script in gayas account – user
* {
* "Version": "2012-10-17",
* "Statement": [
* {
* "Sid": "AllowGayasReadAccess",
* "Effect": "Allow",
* "Principal": {
* "AWS": "arn:aws:iam::913717148710:user/GAYAS"
* },
* "Action": [
* "s3:ListBucket",
* "s3:GetObject"
* ],
* "Resource": [
* "arn:aws:s3:::kamal-bucket-12",
* "arn:aws:s3:::kamal-bucket-12/\*"
* ]
* }
* ]
* }
* Now connect to instance in gayas account
* Aws configure
* Add access key and secret key
* To verify aws s3 ls s3://kamal-bucket-12
* 
* S3 responded gave the objects which are in my bucket