**Group 3** Members:

Duy Panharith

Keo Kimsong

Sem Khevin

Sin Chanmony

Yoeur Man

Ren Phary

CLI VPC

1. Create VPC

aws ec2 create-vpc --cidr-block 192.168.100.0/24

2. List VPC

aws ec2 describe-vpcs

3. Delete VPC

aws ec2 delete-vpc --vpc-id vpc-073aca7817a43550a

CLI EC2

A. Create key pair

aws ec2 create-key-pair --key-name panharith --query 'KeyMaterial' --output text > panharith.pem

B. Security group

-List VPC

aws ec2 describe-vpcs

-Create security group

aws ec2 create-security-group --group-name Panharith --description "Panharith security group" --vpc-id vpc-90a860f6

- List security group

aws ec2 describe-security-groups --group-names Panharith

- Add security group rule

aws ec2 authorize-security-group-ingress --group-name Panharith --protocol tcp --port 22 --cidr 0.0.0.0/0

- List subnet(get subnet ID)

aws ec2 describe-subnets --filters "Name=vpc-id,Values=vpc-90a860f6”

E. Find AMI list:

https://cloud-images.ubuntu.com/locator/ec2/

1. Run an instance

aws ec2 run-instances --image-id ami-0f6565c3d5328c913 --count 1 --instance-type t2.micro --key-name panharith --security-group-ids sg-0d5cb2b43bbcbcfba --subnet-id subnet-6789242f

2. List instances

aws ec2 describe-instances --filters "Name=instance-type,Values=t2.micro" --query "Reservations[].Instances[].InstanceId”

3. Terminate instance

aws ec2 terminate-instances --instance-ids i-5203422c

CLI RDS

1. Create DB instance

aws rds create-db-instance --db-instance-identifier panharith --db-instance-class db.t3.micro --engine mysql --master-username panharith --master-user-password duypanharith --allocated-storage 20

2. List instance

aws rds describe-db-instances

3. Delete instance

aws rds delete-db-instance --db-instance-identifier panharith --skip-final-snapshot

CLI S3 bucket

Step 1 Create IAM group and assign permission group to S3 full Access

Step 2 Create users (4.1ARN) and assign to group download (4.2 Access Key) and (4.3 Secret Access Key)

Step 3 Install CLI

Step 4 CLI configuration

4.1 assign ARN

vim /Users/panharith/.aws/config

4.2 assign Access Key

4.3 assign Secrete Access Key

vim /Users/panharith/.aws/credentials

1. Create bucket

aws s3 mb s3://web-bucket1111 --profile panharith—region ap-southeast-1

2. Remove bucket

aws s3 rb s3://web-bucket1111 --profile panharith –force

3. Copy bucket from local to AWS bucket

aws s3 cp HR.sql s3://web-bucket1111/ --profile panharith

4. Copy from bucket to bucket

aws s3 cp s3://web-bucket1111/HR.sql s3://web-bucket2222/ --profile panharith

5. Sync object local from/to bucket

aws s3 sync entro/ s3://web-bucket1111/ --profile panharith

6. Sync object in different accounts

-First, we need to assign a policy to grain access permission to destination account and vise versa. (set user ARN of source and destination account)

Bucket Policy:

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "DelegateS3Access",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::872509096394:user/S3User"

},

"Action": "s3:\*",

"Resource": [

"arn:aws:s3:::panharith-bucket",

"arn:aws:s3:::panharith-bucket/\*"

]

}

]

}

aws s3 sync s3://panharith-bucket s3:// MyAnotherAccBucket

References

VPC:https://docs.aws.amazon.com/vpc/latest/userguide/vpc-subnets-commands-example.html/

EC2: https://cloud-images.ubuntu.com/locator/ec2/

EC2:https://docs.aws.amazon.com/cli/latest/userguide/cli-services-ec2-instances.html

EC2:https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-vpcs.html

EC2:https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-subnets.html

RDS:https://docs.aws.amazon.com/cli/latest/reference/rds/create-db-instance.html#examples

RDS:https://docs.aws.amazon.com/cli/latest/reference/rds/describe-db-instances.html

RDS:https://docs.aws.amazon.com/cli/latest/reference/rds/delete-db-instance.html#examples

S3:https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies.html