Government of Karnataka

Department of Collegiate and Technical Education

GOVT. POLYTECHNIC SIDDAPUR

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CLOUD COMPUTING LAB (20CS53I)

CERTIFICATE

This is to certify that Mr/ Mrs ……………………………………….. has satisfactory completed the course of experiments in Practical **CLOUD COMPUTING LAB (20CS53I)** prescribed by the Board of Technical examination, Bangalore for fifth semester 2024-25 Year Diploma in Computer Science Engineering in this polytechnic during the year 2024 to 2025.

INTERNAL ASSESSMENT MARKS

TOTAL OF 5 WRITTEN AND PRACTICE TESTS (150)	ONLINE COURSE WORK (40)	PROFILE BUILDING (20)	ASSIGNEMNT (30)

Total Marks: / 240

Course Cohort

Signature of HOD

TABLE OF CONTENTS

SL NO.	Name of the Experiment/Lab Activity	Signature
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		

21		
22		
23		
24		
25		
26		
27		
28		
29		
30		
31		
32		
33		

Lab Activity -1:
Creating an AWS Account

Steps :-

1. Open the Amazon Web Services home page .
2. Choose Create an AWS account.
3. Enter your account information, and then choose Verify email address. This will send a verification code to your specified email address.
4. Enter your verification code, and then choose Verify.
5. Enter a strong password for your root user, confirm it, and then choose Continue.
6. Choose Business or Personal. Personal accounts and business accounts have the same features and functions.
7. Enter your company or personal information.
8. Read and accept the AWS Customer Agreement. Be sure that you read and understand the terms of the AWS Customer Agreement.
9. Choose Continue. At this point, you'll receive an email message to confirm that your AWS account is ready to use. You can sign in to your new account by using the email address and password you provided during sign up.
10. Enter the information about your payment method, and then choose Verify and Continue. If you want to use a different billing address for your AWS billing information, choose Use a new address. You can't proceed with the sign-up process until you add a valid payment method.
11. Enter your country or region code from the list, and then enter a phone number where you can be reached in the next few minutes.
12. Enter the code displayed in the CAPTCHA, and then submit.
13. When the automated system contacts you, enter the PIN you receive and then

submit.

14. Select one of the available AWS Support plans.

15. Choose complete sign up. A confirmation page appears that indicates that your account is being activated.

16. Check your email and spam folder for an email message that confirms your account was activated. Activation usually takes a few minutes but can sometimes take up to 24 hours. After you receive the activation message, you have full access to all AWS services.

Lab Activity-2:

Demonstrate how to create an EC2 instance in AWS

Steps:-

1. Login to AWS management console.
2. Select EC2 service and then select EC2 dashboard to see any instances running currently.
3. To create a new instance, click launch instance.
4. Choose an Amazon Machine Image (AMI).
5. Choose an Instance Type. (t2. micro)
6. Configure Instance Details. (Keep default network configuration in the beginning).
7. Add storage. (enable the check list saying delete on termination)
8. Add tags(optional)
9. Configure security tag. (Open SSH from source anywhere as default).
10. Review and launch

Lab Activity -3:

Demonstrate how to create security group with least privilege in AWS.

Steps:-

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. From the top navigation bar, select a Region for the security group. Security groups are specific to
3. Region, so you should select the same Region in which you created your key pair.
4. In the left navigation pane, choose Security Groups.
5. Choose Create security group.
6. For Basic details, do the following:
7. Enter a name for the new security group and a description. Use a name that is easy for you to remember.
8. In the VPC list, select your default VPC for the Region.
9. For Inbound rules, create rules that allow specific traffic to reach your instance. For example, use the following rules for a web server that accepts HTTP and HTTPS traffic.
   i. Choose Add rule, For Type, choose HTTP, For Source, choose anywhere.
   ii. Choose Add rule, For Type, choose HTTPS, For Source, choose anywhere.
   iii. For Outbound rules, keep the default rule, which allows all outbound traffic.
10. Choose Create security group

Lab Activity -4:

How to SSH to EC2 Instance.

Steps:-

Connect using the Amazon EC2 Console:-

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose Instances.
3. Select the instance and choose Connect.
4. Choose EC2 Instance Connect.
5. Verify the user name and choose Connect to open a terminal window.

To connect to your instance using PuTTY :-

1. Start PuTTY (from the Start menu, choose All Programs, PuTTY, PuTTY).
2. In the Category pane, choose Session and complete the following fields:
3. In the Host Name box Enter Pulic IP address of a instances
4. Ensure that the Port value is 22.
5. Under Connection type, select SSH.
6. In the Category pane, expand Connection, expand SSH, and then expand Auth then choose Credentials Complete the following:
7. In Private key for authentication: Choose Browse.
8. Select the .ppk file that you generated for your key pair and choose Open.
   a. Choose Open.
   b. If this is the first time you have connected to this instance, PuTTY displays a security alert dialog box that asks whether you trust the host to which you

are connecting.

c. Choose Yes. A window opens and you are connected to your instance.

Lab Activity -5:

Demonstrate how to create EC2 Placement groups in AWS.

Steps:-

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose Placement Groups, Create placement group.
3. Specify a name for the group.
4. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
5. In the navigation pane, choose Placement Groups, Create placement group.
6. Specify a name for the group.
7. Choose the placement strategy for the group.
8. If you choose Partition, choose the numberof partitions within the group.
9. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
10. In the navigation pane, choose Placement Groups, Create placement group.
11. Specify a name for the group.
12. Choose the placement strategy for the group.
13. If you choose Partition, choose the numberof partitions within the group.
14. Choose the placement strategy for the group.
15. If you choose Spread, choose the spread level.
16. Rack - no restrictions
17. Host - only for Outposts
18. If you choose Partition, choose the number of partitions within the group.
19. To tag the placement group, choose Add tag, and then enter a key and value. Choose

20. Add tag for each tag that you want to add.

21. Choose Create group.

Demonstrate how to Launch instances in a placement group

Steps:

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. From the EC2 console dashboard, in the Launch instance box, choose Launch instance, and then choose Launch instance from the options that appear. Complete the form as directed, taking care to do the following:
3. Under Instance type, select an instance type that can be launched into a placement group.
4. In the Summary box, under Number of instances, enter the total number of instances that you need in this placement group, because you might not be able to add instances to the placement group later.
5. Under Advanced details, for Placement group name, you can choose to add the instances to a new or existing placement group. If you choose placement groups with a partition strategy, for Target partition, choose the partition in which to launch the instances.

Lab Activity -6:

Demonstrate how to create ENI and attach and detach it from an EC2 instance.

Steps:-

1. Login to AWS management console.
2. Go to VPC service and check the subnet configurations.
3. Go to EC2 instance and check its primary network interface and private IP.
4. Go to network and security in the page and click create new network interface.
5. Give a name for description and select the subnet to which the EC2 instance belongs to.
6. Enable auto assign.
7. Select any one security group and click create network interface.

To attach / detach ENI to EC2 instance

1. Select the newly created ENI.
2. And click action button and attach option there.
3. Select the EC2 instance from the list and click attach.
4. Now check the ENI details, it show ENI is in use
5. To detach ENI from the same instance, got actions and select detach and click.
6. Select the ENI and click detach and we can see ENI is available to attach to any new instance

Lab Activity -7:

Demonstrate how to create an AMI image from an existed EC2 instance and to launch a new EC2 instance from new AMI image.

Steps:-

1. Login to AWS management Console
2. Navigate to EC2 instance dashboard
3. Select any running instance
4. Go to actions and navigate to ->Image and template-> create image
5. Give a name for AMI image (Ex: amazon Linux Image) and for description.
6. Continue with default settings for instant volumes.
7. By default volume type is EBS and EBS snapshot will be created automatically.
8. Click create image button and will get message as create image request is accepted.
9. Navigate to images->AMI and can see newly created AMI image.
10. Give a new name for AMI image.

Note: for the above newly created AMI image, EBS snapshot will also be created automatically. Use this new AMI image to launch new EC2 instance. select AMI image from my images tab

Lab Activity -8:

Demonstrate how to create EBS snapshot using the console in AWS.

Steps:-

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose Snapshots, Create snapshot.
3. For Resource type, choose Volume.
4. For Volume ID, select the volume from which to create the snapshot.
5. The Encryption field indicates the selected volume's encryption status. If the selected volume is encrypted, the snapshot is automatically encrypted using the same KMS key. If the selected volume is unencrypted, the snapshot is not encrypted.
6. (Optional) For Description, enter a brief description for the snapshot.
7. (Optional) To assign custom tags to the snapshot, in the Tags section, choose Add tag,and then enter the key-value pair. You can add up to 50tags.
8. Choose Create snapshot.

Lab Activity -9:

Demonstrate how to create EFS file system using Amazon EFS Quick Create in AWS.

Steps:-

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Choose Launch instance.
3. (Optional) Under Name and tags, for Name, enter a name to identify your instance.
4. Under Application and OS Images (Amazon Machine Image), choose a Linux operatingsystem, and then for Amazon Machine Image (AMI), select a Linux AMI.
5. Under Instance type, for Instance type, select an instance type or keep the default.
6. Under Key pair (login), for Key pair name, choose an existing key pairor create a new one.
7. Under Network settings, choose Edit (at right), and then for Subnet, select a subnet.
8. Under Configure storage, choose Edit (at bottom right), and then do the following:
9. Make sure that EFS is selected.
10. Choose Add shared file system.
11. For File system, select an existing file system, or choose Create new shared file system and create a file system using Amazon EFS Quick Create.
12. For Mount point, specify a mount point or keep the default.
13. To enable access to the file system, select automatically create and attach security groups. By selecting this check box, the necessary security groups will automatically be created and attached to the instance. You can choose to manually create and attach the security groups. If you want to manually create and attach the security groups,
14. To automatically mount the shared file system when the instance launches, select automatically mount shared file system by attaching required user data script. To view the user data that is automatically generated, expand Advanced details, and scroll down to User data.
15. Configure any other instance configuration settings as needed.
16. In the Summary panel, review your instance configuration, and then choose Launch instance.

To delete the file system

1. Open the Amazon Elastic File System console at https://console.aws.amazon.com/efs/.
2. Select the file system to delete.
3. Choose Actions, Delete file system.
4. When prompted for confirmation, enter the file system ID and choose Delete file system.

Lab Activity -10:

Demonstrate how to create the following architectural setup in AWS

Steps:-

Architecture Explanation:

- Create custom VPC with IP 10.0.0.0/16
- Create public and private subnet in two different availability zone
- Create an Internet Gateway and attach to VPC
- Configure Public (Main) route table and Private route table with correct subnet association.

Create VPC with IP 10.0.0.0/16

1. Log in to AWS, Select your region (For example, Asia Pacific (Mumbai)), Search Service VPC, and go to VPC home page:
2. VPC Home page. Choose, Create VPC
3. Choose Option VPC only to configure VPC only and choose VPC and more to understand more about VPC and Its components and other resources that can be created in the VPC
4. Create VPC
5. VPC created successfully
6. After creation of VPC (i.e. cloudiofy-vpc) by default following components are being created:
7. A default security group
8. A Main Route Table
9. A default network ACL

Create public and private subnet in two different availability zone

1. Go to VPC home page, Choose Subnets from left menu, Click to Create subnet
2. Public Subnet with IP – 10.0.1.0/24 | Availability zone: ap-south-1a
3. By default, “Auto assign public IPv4” is not enabled. To get Public IP assigned to

resources, Select public Subnet(i.e. cloudiofy-public-subnet-aps-1a), Choose "Edit subnet settings" and "Enable auto - assign public IPv4 address"

4. Private Subnet with IP – 10.0.2.0/24 | Availability zone: ap-south-1b
5. Click on Create Subnet button to create Both public and private subnets

Create an Internet Gateway and attach to VPC

1. Go to VPC home page, Choose Internet Gateway from left menu, and Click to Create Internet gateway
2. Create an internet gateway
3. Internet gateway created successfully, Now Attach it to VPC
4. Choose your VPC and attach
5. Configure Public (Main) route table and Private route table with correct subnet association
6. A route table contains a set of rules, called routes, that are used to determine where network traffic from your subnet or gateway is directed.
7. Configure Public Route Table: – We can use the Main route table as a Public Route Table, To allow routing
8. from/to internet, Edit Route, and Add an internet gateway
9. Select Main-Public-Route-Table, Go to tab subnet association, and click to Edit subnet associations (associate
10. public subnet)
11. Configure Private Route Table: - Go to VPC home page, Choose Route Table from left menu, Click to Create route table
12. Associate private subnet, Select Private-Route-Table, Go to tab subnet association and click to Edit subnet associations (associate public subnet)

Lab Activity -11

NACL and Security Groups demonstration

Steps:-

Create a security group

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/
2. In the navigation pane, choose Security Groups.
3. Choose Create Security Group.
4. Enter a name for the security group (for example, my-security-group) and provide a description. Select the ID of your VPC from the VPC menu and choose Yes, Create.

Adding a rules

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/
2. In the navigation pane, choose Security Groups.
3. Select the security group to update.
4. Choose Actions, Edit inbound rules or Actions, Edit outbound rules.
5. For Type, select the traffic type, and then fill in the required information.
6. You can also allow communication between all instances that are associated with this security group. Create an inbound rule with the following options:
7. Type: All Traffic
8. Source: Enter the ID of the security group.
9. Choose Save rules.

Creating a network ACL

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/
2. In the navigation pane, choose Network ACLs.
3. Choose Create Network ACL.
4. In the Create Network ACL dialog box, optionally name your network ACL, and select the ID of your VPC from the VPC list. Then choose Yes, Create.

Add rules to a network ACL

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/
2. In the navigation pane, choose Network ACLs.
3. In the details pane, choose either the Inbound Rules or Outbound Rules tab, depending on the type of rule that you need to add, and then choose Edit.
4. In Rule , enter a rule number. The rule number must not already be in use in the network ACL. AWS process the rules in order, starting with the lowest number.
5. Select a rule from the Type list.
6. In the Source or Destination field, enter the CIDR range that the rule applies to
7. From the Allow/Deny list, select ALLOW to allow the specified traffic or DENY to deny the specified traffic.
8. Choose Save.

Lab Activity -12
VPC Peering

Steps:-

To create a VPC peering connection with VPCs in the same account and Region

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose Peering connections.
3. Choose Create peering connection.
4. Configure the following information, and choose Create Peering Connection when you are done:
   - Peering connection name tag: You can optionally name your VPC peering connection.
   - VPC (Requester): Select the VPC in your account with which you want to create the VPC peering connection.
   - Under Select another VPC to peer with: Ensure My account is selected, and select another of your VPCs.
   - (Optional) To add a tag, choose Add new tag and enter the tag key and value.
5. In the confirmation dialog box, choose OK.
6. Select the VPC peering connection that you've created, and choose Actions, Accept Request.
7. In the confirmation dialog, choose Yes, Accept. A second confirmation dialog displays; choose Modify my route tables now to go directly to the route tables page or choose Close to do this later.

To request a VPC peering connection with VPCs in different accounts and Regions

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose Peering connections.
3. Choose Create peering connection.
4. Configure the information as follows, and choose Create Peering Connection when you are done:
5. Peering connection name tag: You can optionally name your VPC peering connection. Doing so creates a tag with a key of Name and a value that you specify.

This tag is only visible to you; the owner of the peer VPC can create their own tags for the VPC peering connection. VPC (Requester): Select the VPC in your account with which to create the VPC peering connection.

6. Account: Choose Another account.
7. Account ID: Enter the AWS account ID of the owner of the accepter VPC.
8. Region: Choose Another region, select the Region in which the accepter VPC resides.
9. VPC (Accepter): Enter the ID of the VPC with which to create the VPC peering connection.
10. In the confirmation dialog box, choose OK.

Lab Activity -13

Demonstrate how to create an RDS instance.

Steps:-

Following are the steps to create an RDS Instance:

1. Sign into AWS Management Console.
2. Open the RDS console.
3. In the upper-right corner, choose the region where you wish to create your instance.
4. In the navigation pane, click on ‘Databases’.
5. Click on ‘Create database’.
6. Make sure ‘Standard create’ is chosen, then click on MySQL (or the database in which you wish tocreate an RDS database instance).
7. In the ‘Templates’ tab, click on the ‘Dev/Test’ option.
8. In the ‘Setting’ tab, set the following values:

DB instance identifier

Master username

Auto Generate a password

Master password

Confirm password

1. In the ‘DB instance size’ option, give a value for the following variables:

DB instance performance types

DB instance class

1. In the ‘Storage’ and ‘Availability & durability’ section, leave the default values as is.
2. In the ‘Connectivity’ section, click on the ‘Additional connectivity configuration’ and set the below values in it:

Virtual Private Cloud (VPC)

Subnet group

Publicly accessible- No

VPC security groups

Availability zone- No preference

Database port- 3306

The same is displayed in the below screenshot:

1. Click on the ‘Additional configuration tab, and provide a name for the ‘Initial database name’ variable.The default settings for other options need to be kept the same.
2. Now click on ‘Create database’.
3. It takes a few minutes for the instance to get created. It can be seen in the ‘Databases’ list as ‘Creating’.
4. Once it is created, it shows as ‘Available’.
5. The ‘Endpoint’ and ‘Port’ of the database instance can be viewed in the ‘Connectivity & security’section.

Note: Make sure that your database instance is secure, by verifying that sources outside of the VPC can’tconnect to the RDS database instance.

Lab activity-14

Encrypt New AWS RDS Database

Steps:-

1. Open the Amazon RDS console after logging into the AWS Management Console.
2. Select the AWS Region you want to create the DB instance from the top right corner of the Amazon RDSdashboard.
3. Scroll down and Choose Create database.
4. Select Standard Create as the database creation method, and then choose an engine type from MariaDB, Microsoft SQL Server, MySQL, Oracle, PostgreSQL, and Microsoft SQL Server in Engine options.
5. Similarly, choose the Edition, Engine Version, Templates, and customize the parameters as per yourpreference. When it's done, click the Additional Configuration Option
6. Furthermore, scroll down and tick the Enable Encryption Box.
7. At last, click on Create database.

Lab activity -15

Hands On: S3 Buckets and Objects

Steps:-

- **Create a Bucket**
- **Upload an object to your Bucket**
- **Delete the objects Task**
- **Emptying your Bucket**
- **Delete the Buckets Task**

Create a Bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. Choose Create bucket.
3. The Create bucket wizard opens.
4. In Bucket name, enter a DNS-compliant name for your bucket. After you create the bucket, you cannot change its name.
5. In Region, choose the AWS Region where you want the bucket to reside.
6. Under Object Ownership, to disable or enable ACLs and control ownership of objects uploaded in your bucket.
7. In Bucket settings for Block Public Access, choose the Block Public Access settings that you want to apply to the bucket.
8. (Optional) Under Bucket Versioning, you can choose if you wish to keep variants of objects in your bucket.
9. (Optional) Under Default encryption, you can choose to configure your bucket to use server side encryption.
10. (Optional) You can enable/disable S3 Object Lock.
11. Choose Create bucket.

Upload an object to your Bucket

1. Open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the Buckets list, choose the name of the bucket that you want to upload your object to.
3. On the Objects tab for your bucket, choose Upload.
4. Under Files and folders, choose Add files.
5. Choose a file to upload, and then choose Open.
6. Choose Upload. You've successfully uploaded an object to your bucket.

Delete the objects

1. Open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the Buckets list, choose the name of the bucket that you want to delete an object from.
3. Select the check box to the left of the names of the objects that you want to delete.
4. Choose Actions and choose Delete from the list of options that appears. Alternatively, choose Delete from the options in the upper right.
5. Type permanently delete if asked to confirm that you want to delete these objects.
6. Choose Delete objects in the bottom right and Amazon S3 deletes the specified objects.

Emptying your Bucket

1. In the Buckets list, select the bucket that you want to empty, and then choose Empty.
2. To confirm that you want to empty the bucket and delete all the objects in it, in Empty bucket, type permanently delete.
3. To empty the bucket and delete all the objects in it, and choose Empty.
4. To return to your bucket list, choose Exit.

Delete Bucket

1. To delete a bucket, in the Buckets list, select the bucket.
2. Choose Delete.
3. To confirm deletion, type the name of the bucket.
4. To delete your bucket, choose Delete bucket.

Lab activity -16

Enable or Suspend versioning on an S3 Bucket.

Steps:-

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the Buckets list, choose the name of the bucket that you want to enable versioning for.
3. Choose Properties.
4. Under Bucket Versioning, choose Edit.
5. Choose Suspend or Enable, and then choose Save changes.

Lab activity-17

Enable Default Encryption on an S3 Bucket.

Steps:-

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the Buckets list, choose the name of the bucket that you want.
3. Choose Properties.
4. Under Default encryption, choose Edit.
5. To enable or disable server-side encryption, choose Enable or Disable.
6. To enable server-side encryption using an Amazon S3-managed key, under Encryption key type, choose Amazon S3 key (SSE-S3).
7. To enable server-side encryption using an AWS KMS key, follow these steps:
    a. Under Encryption key type, choose AWS Key Management Service key (SSE-KMS).
    b. Under AWS KMS key choose one of the following:
    c. AWS managed key
    d. Choose from your KMS root keys, and choose your KMS root key.
    e. Enter KMS root key ARN, and enter your AWS KMS key ARN.
8. To use S3 Bucket Keys, under Bucket Key, choose Enable.
9. Choose Save changes.

Lab activity -18

Create or edit a bucket policy

Steps:-

1. Sign in to the AWS Management Console and open the Amazon S3 consoleat https://console.aws.amazon.com/s3/.
2. In the Buckets list, choose the name of the bucket that you want to create a bucket policy for orwhose bucket policy you want to edit.
3. Choose Permissions.
4. Under Bucket policy, choose Edit. This opens the Edit bucket policy page.
5. On the Edit bucket policy page, choose Policy generator to generate a policy automatically, oredit the JSON in the Policy section.
6. If you choose Policy generator, the AWS Policy Generator opens in a new window:
   a. On the AWS Policy Generator page, in Select Type of Policy, choose S3 Bucket Policy.
   b. Add a statement by entering the information in the provided fields, and then choose Add Statement.Repeat for as many statements as you would like to add.
   c. After you finish adding statements, choose Generate Policy.
   d. Copy the generated policy text, choose Close, and return to the Edit bucket policy page
   e. in the Amazon S3 console.
7. In the Policy box, edit the existing policy or paste the bucket policy from the Policy generator. Make sure to resolve security warnings, errors, general warnings, and suggestions before you save your policy.
8. Choose Save changes

Lab activity -19

Static Website Hosting

Steps:-

Step 1: Create a S3 Bucket.

1. Choose Create bucket
2. Enter Bucket name and choose region. An S3 bucket name is globally unique.
3. Public access to buckets is blocked by default.
4. In the Object Ownership section, select ACLs enabled, then verify Bucket owner preferred is selected.
5. Clear Block all public access, then select the box that states I acknowledge that the current
6. settings may result in this bucket and the objects within becoming public.
7. Choose Create bucket.

Step 2: Upload objects to your S3 Bucket.

1. Open the bucket created and upload objects.
2. Choose Upload
3. Choose Add files
4. Locate and select all website file that you have developed.
5. Choose Upload Choose Close.

Step 3: Enabling access to the objects

1. Objects that are stored in Amazon S3 are private by default. You need to public all the objects
2. uploaded to bucket. Select all objects.
3. In the Actions menu, choose Make public via ACL.
4. Choose Make public

Step 4: Enable Static Website Hosting

1. Move to the Properties Tab. Scroll to the Static website hosting panel. Choose Edit
2. Configure the following settings:
3. Static web hosting: Enable
4. Hosting type: Host a static website
5. Index document: index.html
6. Error document: error.html
7. Choose Save changes.
8. In the Static website hosting panel, choose the link under Bucket website endpoint.
9. Open browser and paste it in address bar. Tour website has been hosted and now it is accessible.

Lab activity -20

Enable S3 Access logging

Steps:-

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the Buckets list, choose the name of the bucket that you want to enable server accesslogging for.
3. Choose Properties.
4. In the Server access logging section, choose Edit.
5. Under Server access logging, select Enable.
6. For Target bucket, enter the name of the bucket that you want to receive the log recordobjects. The target bucket must be in the same Region as the source bucket.
7. Choose Save changes.

Lab activity -21

Configuration of S3 Replication

Steps:-

1. Go to the AWS S3 management console, sign in to your account, and select the name of the source bucket.
2. Go to the Management tab in the menu, and choose the Replication option. Next, choose Add rule.
3. Under the Set resource configuration, choose the Entire bucket option.
4. Under the Set destination configuration, choose the Buckets in this account option. If you wish to replicate to another account, select this option and specify a bucket policy for the destination.
5. To change the storage class of the object after replication, go to the Destination options configuration, and select a different storage class for the destination objects.
6. You can also set the replication time

Lab activity-22

Generate S3 Pre-signed URL for your object.

Steps:-

1. Sign in to the AWS Management Console and open the Amazon S3 console
2. In the Buckets list, choose the name of the bucket that contains the object that you want a pre signed URL for.
3. In the Objects list, select the object that you want to create a pre-signed URL for.
4. On the Actions menu, choose Share with a pre-signed URL.
5. Specify how long you want the pre-signed URL to be valid.
6. Choose Create pre-signed URL.
7. When a confirmation appears, the URL is automatically copied to your clipboard. You will see a button to copy the pre-signed URL if you need to copy it again.

Lab activity -23

S3 Storage Classes

Steps:-

- **Upload object in a specific storage Class**
- **Change the Storage class of object**

Upload Object in a specific storage class

1. Open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the Buckets list, choose the name of the bucket that you want to upload your object to.
3. On the Objects tab for your bucket, choose Upload.
4. Under Files and folders, choose Add files.
5. Choose a file to upload, and then choose Open.
6. Under Properties, Choose the storage class.
7. Choose Upload. You've successfully uploaded an object to your bucket.

Change the storage class of object

1. Open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the Buckets list, choose the name of the bucket that you want to change the storage class ofan object.
3. Select the check box to the left of the names of the objects that you want to change storage class.
4. Choose Actions and choose edit Storage class.
5. Select the storage class to which you want to change.
6. Choose Save Changes.

Lab Activity -24

Demonstrate how to create classic load balancer.

Steps:-

To create a Classic Load Balancer

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. On the navigation bar, choose a Region for your load balancer. Be sure to select the same Region thatyou selected for your EC2 instances.
3. On the navigation pane, under **LOAD BALANCING**, choose **Load Balancers**.
4. Choose **Create Load Balancer**.
5. For **Classic Load Balancer**, choose **Create.**

To define your load balancer and listener

1. For **Load Balancer name**, type a name for your load balancer.
2. For **Create LB inside**, select the same network that you selected for your instances: EC2-Classic or a specific VPC.
3. [Default VPC] If you selected a default VPC and would like to choose the subnets for your load balancer, select **Enable advanced VPC configuration**.
4. Leave the default listener configuration.
5. [EC2-VPC] For **Available subnets**, select at least one available public subnet using its add icon. The subnetis moved under **Selected subnets**. To improve the availability of your load balancer, select more than onepublic subnet.
6. Choose **Next: Assign Security Groups**.

To assign security group to your load balancer

1. On the **Assign Security Groups** page, select **Create a new security group**.
2. Type a name and description for your security group, or leave the default name and description.
3. Choose **Next: Configure Security Settings**.
4. Choose **Next: Configure Health Check** to continue to the next step.

To configure health checks for your instances

1. On the **Configure Health Check** page, leave **Ping Protocol** set to HTTP and **Ping Port** set to 80.
2. For **Ping Path**, replace the default value with a single forward slash ("/").
3. For **Advanced Details**, leave the default values.
4. Choose **Next: Add EC2 Instances**.
5. Choose **Next** Assign Security Groups.

To register EC2 instances with your load balancer

1. On the **Add EC2 Instances** page, select the instances to register with your load balancer.
2. Leave cross-zone load balancing and connection draining enabled.
3. Choose **Next: Add Tags**.

To add tags to your load balancer

1. On the **Add Tags** page, specify a key and a value for the tag.
2. To add another tag, choose **Create Tag** and specify a key and a value for the tag.
3. After you are finished adding tags, choose **Review and Create**.

To create and test your load balancer

1. On the **Review** page, choose **Create**.
2. After you are notified that your load balancer was created, choose **Close**.
3. Select your new load balancer.
4. On the **Description** tab, check the **Status** row. If it indicates that some of your instances are not inservice, its probably because they are still in the registration process.
5. After at least one of your EC2 instances is in service, you can test your load balancer. Copy the string from **DNS name** (for example, my-load-balancer-1234567890.us-west-2.elb.amazonaws.com) and paste it into the address field of an internet-connected web browser. If your load balancer is working, you see the default page of your server.

To delete your load balancer

1. If you have a CNAME record for your domain that points to your load balancer, point it to a new location and wait for the DNS change to take effect before deleting your load balancer.
2. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
3. On the navigation pane, under **Load Balancing**, choose **Load Balancers**.
4. Select the load balancer.
5. Choose **Actions**, **Delete**.
6. When prompted for confirmation, choose **Yes, Delete**.

Lab Activity -25:

Create An Auto Scaling Group With Application Load Balancer

Steps:-

1. Navigate to **EC2** > **Load Balancers**.
2. Click **Create Load Balancer**.
3. Click the **Create** button under the **Application Load Balancer** and set the following values:
    - *Name*: **HOLALB**
    - *Scheme*: **internet-facing**
    - *IP address type*: **ipv4**
    - *Load Balancer Protocol*: **HTTP**
    - *Port*: **80**
    - Select the VPC.
    - Add the **us-east-1a** and **us-east-1b** AZs to your ALB.
4. Click **Next: Configure Security Settings**
5. Click **Next: Configure Security Groups**.
6. Select to **Create a new security group** for your ALB, and set the following values:
    - *Name*: **ALBSG**
    - *Description*: **ALBSG**
    - The default value allows standard HTTP traffic from 0.0.0.0/0 and ::/0 (IPV6), so leave as it.
7. Click **Next: Configure Routing** and enter the following values:
    - *Name*: **ALBTG**
    - *Target type*: **Instance**

- *Protocol*: **HTTP**
- *Port*: **80**

8. Expand **Advanced health check settings**, and reduce the healthy and unhealthy threshold checks down to **2**.
    - This means the load balancer can respond faster and instances come into service and vice versa.
9. Click **Next: Register Targets**.
10. Click **Next: Review**.

Make a note of the DNS name associated with the load balancer and open in a new browser tab. You should see a 503 error since we don't have any operational EC2 instances associated with the load balancer.

Create an Auto Scaling Group

Note: Make sure the load balancer is ready at this point.

1. **EC2** > **Auto Scaling** > **Auto Scaling Groups**
2. Click **Create Auto Scaling group**.
3. Call the group **HOLASG**.
4. Select **Launch Template**, and choose the template you just created.
5. Select **Adhere to Launch Template**.
6. Pick the VPC from the lab environment, and select us-east-1a and us-east-1b as subnets.
7. Click **Next**.
8. Check **Enable load balancing**.
9. Select target group **ALBTG**.
10. Leave the default for *Health checks*.
11. Select **Enable group metrics collection with CloudWatch**.

12. For *Group Size*, enter the following values:

    - *Desired Capacity*: **2**

    - *Minimum Capacity*: **2**

    - *Maximum Capacity*: **6**

13. For *Scaling Policies*, select **Target tracking scaling policy** and enter the following values:

    - *Scaling Policy Name*: **Target Tracking Policy**

    - *Metric type*: **Average CPU utilization**

    - *Target value*: **30**

    - *Instances need*: **300**

14. Click **Next**.

15. Click **Create Auto Scaling Group**.

Lab Activity -26

How to Configure AWS Database Migration Service.

Steps:-

1. Create 2 RDS one is mariadb and other is mysql from aws console for migration purpose
2. Open another tab and search for DMS click on Database Migration Service
3. Click on create replication instance which acts as bridge for connection
4. Enter the name for replication instance as mydemo or demo then click create replication instance
5. After creation we can check the below tab
6. Create endpoints for both source and target end points by clicking create endpoints option. Specify the source RDS instance name (maria-database-1) and target RDS instance name (mysqldatabase-1).
7. Now both endpoints are created
8. Create task for database migration by Clicking on database migration task. Task is configured to do wholeprocess.
9. Enter the name for task as testdemo then select source database endpoint as maria-database-1 and targetdatabase as mysql-databse and select migration type.
10. In the task setting tab do the following changes
11. In table mapping tab select add new selection rule option to add the rule and enter the schema details. Thenclick the create task button.
12. Migration task starts from here it will be using the replica instances to connect the endpoints from onedatabase to another database. It’s just a basic for how AWS DMS work

Lab Activity -27

Demonstrate how to Configure AWS backup plan.

Steps:-

Create a backup plan based on an existing one

1. Sign in to the AWS Management Console, and open the AWS Backup console athttps://console.aws.amazon.com/backup.
2. From the dashboard, choose Manage Backup plans. Or, using the navigation pane, choose Backup plansand choose Create Backup plan.
3. Choose Start with template, choose a plan from the list (for example, Daily-Monthly,1yr-Retention), andenter a name in the Backup plan name box
4. On the plan summary page, choose the backup rule you want and then choose Edit.
5. Review and choose the values that you want for your rule. For example, you can extend the retention periodof the backup in the Monthly rule to three years instead of one year. If your plan includes Amazon EFS backups, you can configure lifecycle policies that automatically transition these backups from warm storageto cold storage according to a schedule that you define.
6. For the backup vault, choose Default or choose Create new Backup vault to create a new vault.
7. (Optional)- choose an AWS Region from the list in Destination region to copy the backup to differentRegion. To add more Regions, choose Add copy.
8. When you have finished editing the rule, choose Save Backup rule

Create a backup vault

1. On the AWS Backup console, in the navigation pane, choose Backup vaults. Note: If the navigation pane is notvisible on the left side, we can open it by choosing the menu icon in the upper-left corner of the AWS Backup console.
2. Choose Create backup vault
3. Enter a name for your backup vault. You can name your vault to reflect what you will store in it, or to make it easier to search for the backups we need. For example, we could name it as FinancialBackups
4. Select an AWS Key Management Service (AWS KMS) key. we can use either a key that we

already created, orselect the default AWS Backup KMS key.

5. Optionally, add tags that will help us to search for and identify your backup vault. For example, we could add aBackup Type:-Financial tag
6. Choose Create Backup vault
7. In the navigation pane, choose Backup vaults, and verify that your backup vault has been added.

Lab Activity -28

CloudWatch Logs - Viewing Logs:-

Steps:-

1. Open the CloudWatch console.
2. Select the CloudWatch service after that on the left side menu, choose Log groups under Logs. On that screen,enter securitylablogs in the search bar. Click on the log group that appears in the results.
3. You will see these log streams: cw-agent-logs, apache-access-logs, apache-error-logs, yumlogs, and ssh-logs.Click through all of them to view the logs from each of these services
4. You should see a record of log events. This is the data being collected on your EC2 instance, and then sent toCloudWatch by the CloudWatch Agent installed on the instance.
5. You explored log files generated by your EC2 instance in the CloudWatch console. The CloudWatch console provides a unified location to view a variety of logs, enabling you to investigate or monitor security activity ina central location. Using the CloudWatch console illustrates the security best practice of “analyzing logs, findings, and metrics centrally”.

Lab Activity -29

Create a CloudWatch alarm for an instance

Steps:-

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Go to Amazon CloudWatch Management Console and select metrics from the navigation pane.
3. On the metrics page type CPU Utilization in the search bar. From the displayed list of instances choose theinstance for which you want to create an alarm.
4. Creating an alarm to notify when CPU Utilization metric of the instance is greater than 50.
5. Now select the Graphed Metrics option on the same page. Then set the time period according to your need.And choose an alarm icon located beside the selected instance.
6. After clicking the bell icon, alarm creation process started here you can see the metric selected (CPU Utilization), instance id, statistic as average and period equal to 1 minute. In condition section chooses the threshold type as static and CPU Utilization greater than 50 and data points to alarm have 3 out of 5, and then click on next to move.
7. Alarm triggers when its state is in alarm. If you want AWS to send you an email notification whenever the alarm condition is satisfied. The notification is sent through Amazon SNS Topic.
8. Here specific action can also be taken like auto scaling, EC2 action and system manager action.
9. Preview all the details about alarm and click Create Alarm.
10. Congratulations, you have successfully configured Amazon CloudWatch Alarm to monitor your instance. You will receive the notification through an e-mail on the mail-id you have specified when the alarm condition is met.

Lab Activity -30
How to create a trail that applies to all Regions

Steps:-

1. Sign in to the AWS Management Console and open the CloudTrail console athttps://console.aws.amazon.com/cloudtrail/.
2. On the CloudTrail service home page, the Trails page, choose Create trail.
3. On the Create Trail page, for Trail name, type a name for your trail. Then select the storage location (S3 bucket). This can do by creating a new storage location by selecting create new bucket or the existing one.This storage location allows storing the logs for the trail.
4. For Log file SSE-KMS encryption, choose Enabled if you want to encrypt your log files with SSE-KMSinstead of SSE-S3. The default is enabled.
5. If you enable SSE-KMS encryption, choose a New or Existing AWS KMS key. In AWS KMS Alias,specify an alias, in the format alias/MyAliasName.
6. In Additional settings, configure the following.
   - For Log file validation, choose Enabled to have log digests delivered to your S3 bucket.
   - For SNS notification delivery, choose Enabled to be notified each time a log is delivered to yourbucket.
7. Optionally, configure CloudTrail to send log files to CloudWatch Logs by choosing Enabled inCloudWatch Logs.
8. For Tags, add one or more custom tags (key-value pairs) to your trail.
9. On the Choose logevents page, choose the event types that you want to log.
   - Management events: These events are free and can be viewed in the event history for 90 days.
   - Data events:These are not free and cannot be viewed in event history, show only the datamanipulations.
   - Insights events: identifies unusual activity, errors in the AWS account
   - Choose only the management event has it is free.
10. For API activity, choose if you want your trail to log Read events, Write events, or both.
11. On the Review and create page, review your choices. Choose Edit in a section to change the

trail settingsshown in that section. When you are ready to create the trail, choose Create trail.

12. The new trail appears on the Trails page. The Trails page shows the trails in your account from all Regions.In about 15 minutes, CloudTrail publishes log files that show the AWS API calls made in your account.

Lab Activity -31

How to create a AWS Config

Steps:-

1. Sign in to the AWS Management Console and open the CloudTrail console athttps://console.aws.amazon.com/cloudtrail/.
2. Search and select Config from the panel.
3. Click on Get Started.
4. Note: If you are creating Config first time you can follow the steps mentioned below else click on settings from the left-hand side navigation panel then proceed with the steps.To get the records of the resources running in your account click on the record specific resource types.
5. Under Resource, category Select AWS resources than search for EC2 Instance. Also, select Create AWSConfig service-linked role.
6. For Amazon S3 Bucket, choose the Amazon S3 bucket to which Config sends configuration history andconfiguration snapshot files or create a new bucket for Bucket Name, type a name for your Amazon S3 bucket.
7. For Amazon SNS topic, choose Stream configuration changes and notifications to an Amazon SNS topic to have AWS Config send notifications such as configuration history delivery, configuration snapshot delivery, and compliance. Click on next.
8. Rules-If you are setting up AWS Config in a region that supports rules, choose next
9. Review your AWS Config set up details. You can go back to edit changes for each section. ChooseConfirm to finish setting up AWS Config.

Lab Activity -32

Demonstrate how to create Code Commit in AWS

Steps:-

1. Access the CodeCommit console. You can use this URL: https://console.aws.amazon.com/codecommit/.
2. Navigate to the Repositories page and click Create repository. Type a name for the repo and click Create
3. On the Create repository page, in Repository name, enter a name for your repository (for example, myrepo).
4. Select Enable Amazon Code Guru Reviewer for Java and Python if this repository will contain Java or Python code, and you w ant to have Code Guru Re viewer analyze that code. Code Guru Reviewer uses multiple machinelearning models to find code defects and to automatic ally suggest improvements and fixes in pull requests.
5. Choose Create.

Add files to your repository

1. In the navigation bar for the repository, choose Code.
2. Choose Add file, and then choose whether to create a file or upload a file from your computer. This tutorial showsyou how to do both.
3. To add a file, do the following:
    - In the drop-down list of branches, choose the branch where you want to add the file. The default branchis selected automatically for you. In the example shown here, the default branch is named main. If you want to add the file to a different branch, choose a different branch.
    - In File name, enter a name for the file. In the code editor, enter the code for the file.
    - In Author name, enter the name you want displayed to other repository users.
    - In Email address, enter an email address.
    - (Optional) In Commit message, enter a brief message. Although this is optional, we recommend that you add a commit message to help your team members understand

why you added this file. If you donot enter a commit message, a default message is used.

- Choose Commit changes.

To upload a file, do the following:

1. If you're uploading a file, choose the file you want to upload.
2. A view of uploading a file in the Code Commit console
3. In Author name, enter the name you want displayed to other repository use
4. In Email address, enter an email address
5. (Optional) In Commit message, enter a brief message. Although this is optional, we recommend that you add a commit message to help your team members understand why you added this file. If you do not entera commit message, a default message is used.
6. Choose Commit changes.

To delete the CodeCommit repository

1. Open the CodeCommit console at https://console.aws.amazon.com/codesuite/codecommit/home.
2. In Repositories, choose the repository you want to delete. If you followed the naming convention in thistopic, it is named MyRepo.
3. Type delete, and then choose Delete. The repository is permanently deleted.

Lab Activity -33

Demonstrate how to create a cluster in AWS

Steps:-

1. Open the Amazon ECS console at https://console.aws.amazon.com/ecs/.

2. From the navigation bar, select the Region to use.

3. In the navigation pane, choose Clusters.

4. On the Clusters page, choose Create Cluster.

5. For Select cluster compatibility, choose Networking only, then choose Next Step.

6. On the Configure cluster page, enter a Cluster name. Up to 255 letters (uppercase and lowercase),numbers, hyphens, and underscores are allowed.

7. In the Networking section, configure the VPC for your cluster. You can keep the default settings, oryou can modify these settings with the following steps.

- (Optional) If you choose to create a new VPC, for CIDR Block, select a CIDR block for yourVPC.
- For Subnets, select the subnets to use for your VPC. You can keep the default settings or youcan modify them to meet your needs.

8. In the CloudWatch Container Insights section, choose whether to turn on Container Insights for thecluster.

9. Choose Create.