

G. Nandini
20A31A05D6

PRACTICAL IMPLEMENTATION OF AWS SERVICES

CONTENTS

- 1) AWS Command Line Interface (CLI)
- 2) Elastic Cloud Compute (EC2)
- 3) Virtual Private Cloud (VPC)
- 4) Elastic Load Balancer (ELB)
- 5) Identity and Access Management (IAM)
- 6) Relational Database System (RDS)
- 7) Elastic Block Service (EBS)
- 8) AWS Lightsail
- 9) Simple Storage Service (S3)
- 10)Cloud Watch

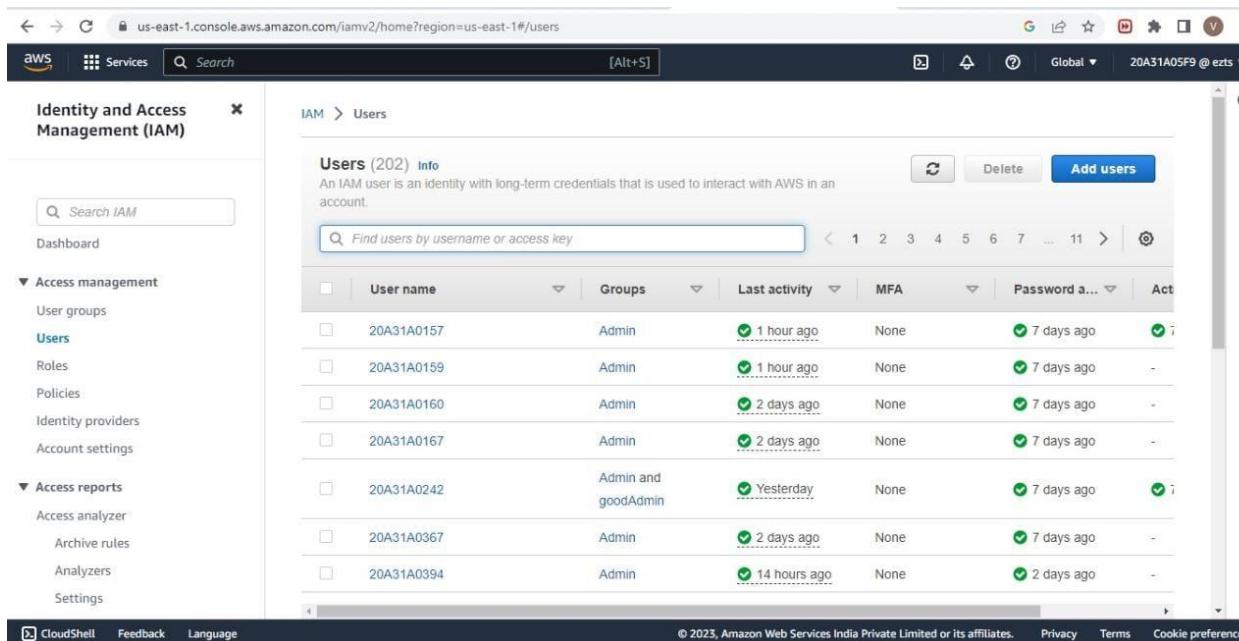
AWS COMMAND LINE INTERFACE

Lab - Configuring AWS CLI

STEP 1 - Download and install AWS CLI and complete the installation steps

STEP 2 - Login to AWS Management Console and search for IAM.

STEP 3 - In the navigation pane ,select Users



The screenshot shows the AWS IAM Management Console. The left sidebar is collapsed, and the main area displays the 'Users' page. The title bar says 'IAM > Users'. The page header includes a search bar, a 'Delete' button, and a 'Add users' button. Below the header is a table with 202 rows, each representing an IAM user. The columns are: User name, Groups, Last activity, MFA, Password a..., and Action. The 'Last activity' column shows various time intervals from '1 hour ago' to '14 hours ago'. The 'Groups' column shows most users are 'Admin' and one is 'Admin and goodAdmin'. The 'Action' column contains small icons for each user entry.

User name	Groups	Last activity	MFA	Password a...	Action
20A31A0157	Admin	1 hour ago	None	7 days ago	
20A31A0159	Admin	1 hour ago	None	7 days ago	
20A31A0160	Admin	2 days ago	None	7 days ago	
20A31A0167	Admin	2 days ago	None	7 days ago	
20A31A0242	Admin and goodAdmin	Yesterday	None	7 days ago	
20A31A0367	Admin	2 days ago	None	7 days ago	
20A31A0394	Admin	14 hours ago	None	2 days ago	

STEP 4 - In the users select the name of the user whose access keys you want to create.

STEP 5 - Click on Security Credentials tab.

The screenshot shows the AWS IAM console interface. The left sidebar is collapsed, showing the main navigation menu. The main content area displays the details for a user named "20A31A05D2".

User Details:

- Created: March 21, 2023, 14:51 (UTC+05:30)
- Last console sign-in: Today
- Access key 2: Not enabled

Security Credentials Tab:

- Permissions
- Groups (1)
- Tags
- Security credentials** (selected)
- Access Advisor

Console sign-in:

- Console sign-in link: <https://ezts.signin.aws.amazon.com/console>
- Console password: Updated 7 days ago (2023-03-27 09:57 GMT+5:30)
- Last console sign-in: 27 minutes ago (2023-04-03 20:58 GMT+5:30)

Multi-factor authentication (MFA): (0)
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Buttons: Remove, Resync, Assign MFA device

Footer:

- Device type
- Identifier
- Created on
- © 2023, Amazon Web Services India Private Limited or its affiliates.
- Privacy
- Terms
- Cookie preferences

STEP 6 - In the access Keys section , choose Create access key -> Command Line Interface -> Create Access Key

The screenshot shows the AWS IAM Access Keys page. The URL is `us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/details/20A31A05D2?section=security_credentials`. The left sidebar shows the IAM navigation menu. The main content area displays the 'Access keys' section with one item listed:

AKIATR4OXV3QNPAMUQBM	
Description	-
Last used	Created
7 days ago	7 days ago
Last used region	Last used service
us-east-1	iam

Below this, there is a section for 'SSH public keys for AWS CodeCommit (0)'.

Page footer: CloudShell, Feedback, Language, © 2023, Amazon Web Services India Private Limited or its affiliates., Privacy, Terms, Cookie preferences

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#users/details/20A31A05D2/create-access-key

Services Search [Alt+S] Global 20A31A05F9 @ ects

Step 1 Access key best practices & alternatives

Step 2 - optional Set description tag

Step 3 Retrieve access keys

Access key best practices & alternatives

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

- Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.
- Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.
- Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.
- Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.
- Application running outside AWS

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#users/details/20A31A05D2/create-access-key

Services Search [Alt+S] Global 20A31A05F9 @ ects

IAM > Users > 20A31A05D2 > Create access key

Step 1 Access key best practices & alternatives

Step 2 - optional Set description tag

Step 3 Retrieve access keys

Set description tag - optional

The description for this access key will be attached to this user as a tag and shown alongside the access key.

Description tag value

Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . / + = @

Cancel Previous Create access key

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#users/details/20A31A05D2/create-access-key

Services Search [Alt+S] Global 20A31A05F9 @ ects

Access key created

This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

IAM > Users > 20A31A05D2 > Create access key

Step 1 Access key best practices & alternatives

Step 2 - optional Set description tag

Step 3 Retrieve access keys

Retrieve access keys

Access key

If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIATR4OXV3QD5GD6MZZ	***** Show

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

STEP 7 - Now you can use this access key to configure CLI

STEP 8 - Open Command Line Interface and run the following command

```
>aws configure
```

After entering this command AWS CLI prompts us with four pieces of information

1. Access Key ID: (enter your ID)
2. Secret Access Key: (enter your key)
3. AWS Region: (enter the desired region)
4. Output Format: (enter the desired output)

```
Microsoft Windows [Version 10.0.22621.1413]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sivas>aws configure
AWS Access Key ID [None]: AKIATR40XV3QD5GD6MZZ
AWS Secret Access Key [None]: vMQP4GL99CbDSxsPWSgiTkkozMiRsUUZ0i+hDdNT
Default region name [None]: us-east-1
Default output format [None]: json
```

Finally we get Javascript Object Notation of all the users as output.

ELASTIC CLOUD COMPUTE (EC2)

Lab - Creating an EC2 Instance

Step-1: Go to AWS services, click EC2, and then select 'launch instances'.

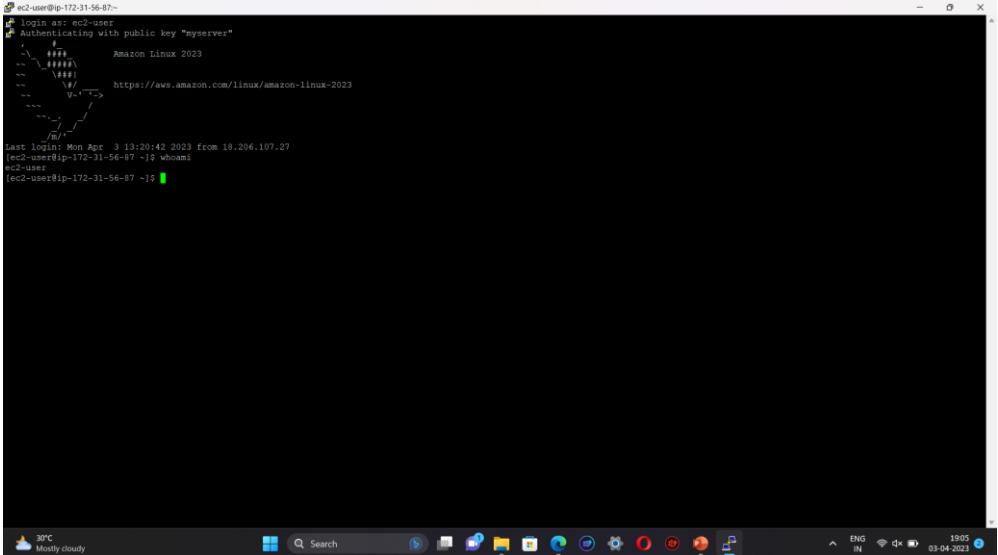
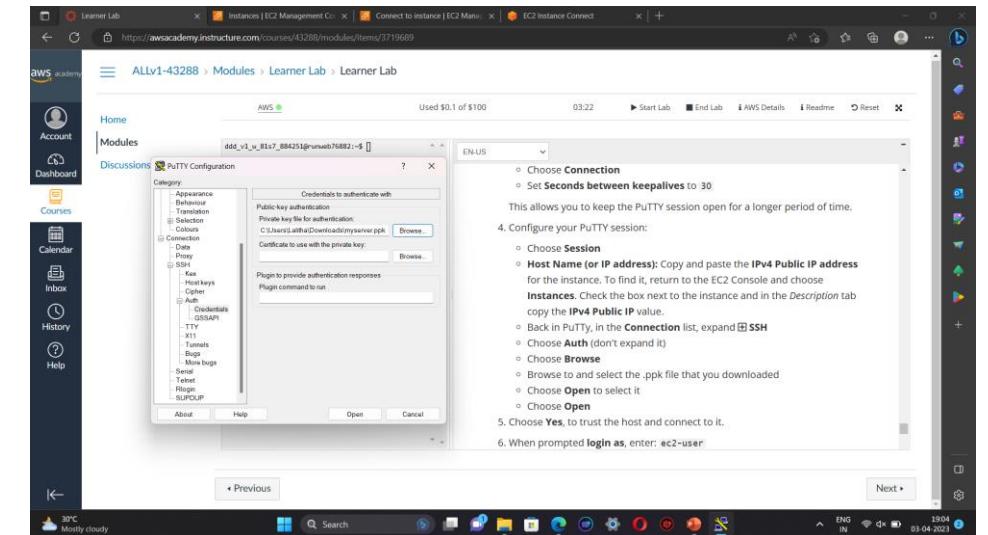
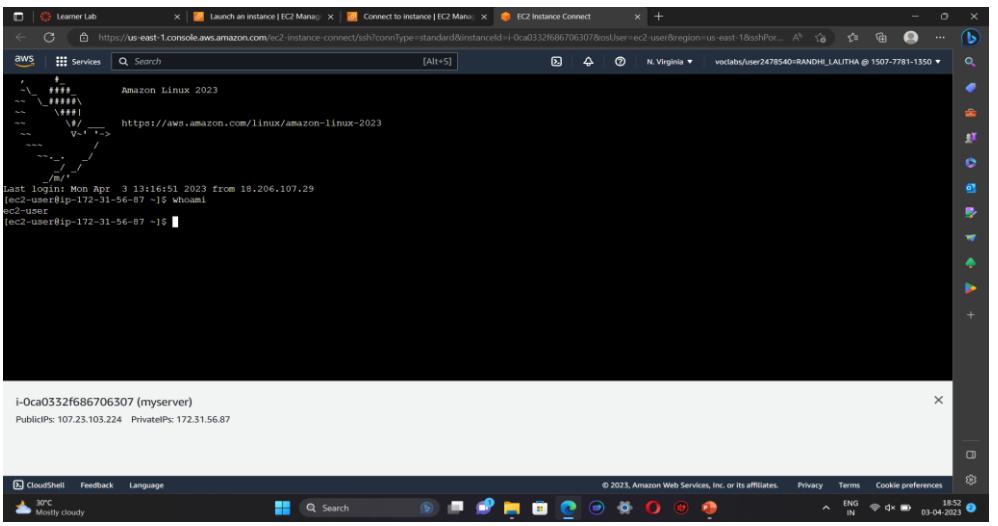
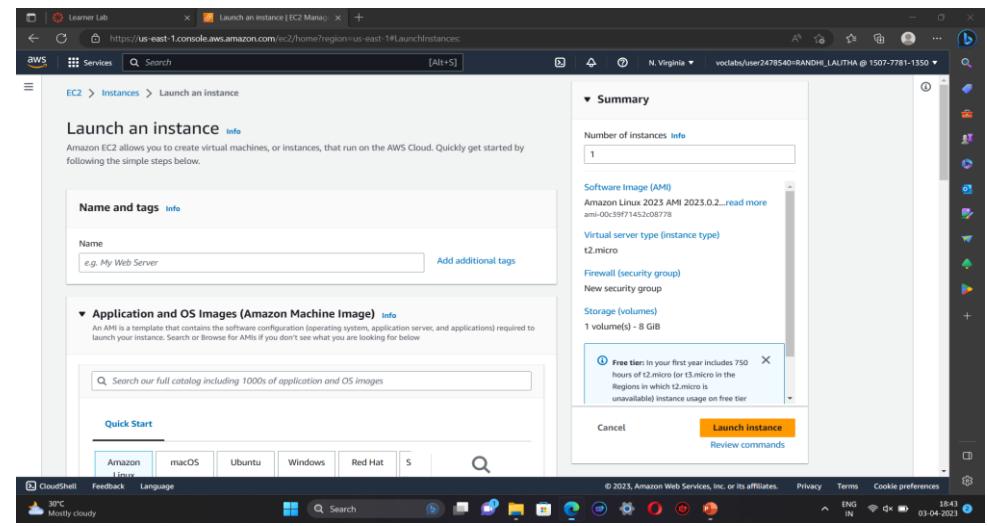
Step-2: Name the instance, select an AMI(LINUX, WINDOWS server), select a key pair, and click launch instance.

Step-3: For Linux-select the PPK key and for windows server-select the pem key.

Step-4: If a key pair is not available create a new key.

Step-5: For Linux-click connect to instance you will be redirected to the CLI (or) open the putty file configure it to not timeout, and configure the putty session. This will redirect you to the CLI.

For windows server-click connect → RDP client → get password → upload private key → decrypt password. Open the RDP file and enter the password. This will redirect you to the windows server. Now terminate instances.





A screenshot of the Amazon EC2 Management Console. The main view shows a table of instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
myserver	i-0ca0332f686706307	Running	t2.micro	2/2 checks passed	No alarms	us-east-1e	ec2-107-
windows-server	i-0c37769ef85c932d7	Running	t2.micro	2/2 checks passed	No alarms	us-east-1c	ec2-52-

The left sidebar shows navigation links for EC2 Dashboard, Global View, Events, Tags, Limits, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, Images (AMIs, AMI Catalog), and Elastic Block Store (CloudShell, Feedback, Language).

VIRTUAL PRIVATE CLOUD (VPC)

Lab – Building a VPC and Launching a Web server

Step 1: First start the lab, when the lab status gets ready, it redirects to the AWS management console.

Step 2: Go to AWS services, search, and choose VPC to open the VPC console.

Step 3: Verify that your regions remain in the N-Virginia(us-east-1). Choose to create VPC in the VPC dashboard

Step 4: Choose VPC and more, in name tag auto-generation, keep auto-generate select and change it to a lab.

Step 5: Keep the IPv4 CIDR block to 10.10.0.0/16 and next for a number of availability zones select 1, number of public subnets select 1 , number of private subnets select 1

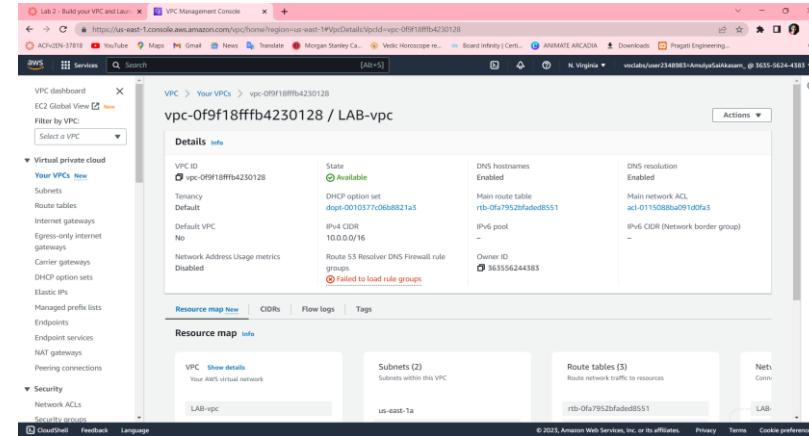
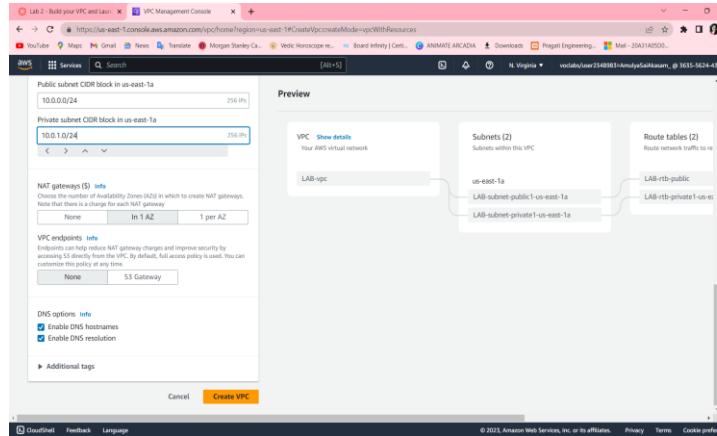
Step 6: Now customize subnets CIDR blocks, change public subnet(us-east-1a) to 10.10.0.0/24, and change private subnet (us-east-1a) to 10.0.1.0/24

Step 7: Set the NAT gateways to 1AZ and set VPC endpoints to none and keep both DNS hostnames and DNS resolutions enabled

Step 8: Check on the preview panel on the right side whether they match with the given regions or not

The image consists of three screenshots of the AWS VPC Management Console, each showing a different step in the configuration process:

- Screenshot 1 (Top Left):** Shows the "Create VPC" wizard. It displays various AWS services like EC2 Instances, NAT Gateways, and Route Tables. The "Additional Information" section includes links to VPC Documentation, Forums, and Report an Issue. A "AWS Network Manager" section is also present.
- Screenshot 2 (Top Right):** Shows the "VPC settings" page. It includes fields for "Name tag auto-generation" (set to "LAB"), "IPv4 CDR block" (set to "10.0.0.0/16"), and "IPv6 CDR block" (set to "No IPv6 CDR block"). The "Preview" section shows a network diagram with subnets (us-east-1a, us-east-1b) and route tables (LAB-rtb-public, LAB-rtb-private1-us-east-1a).
- Screenshot 3 (Bottom):** Shows the "Preview" section of the configuration. It includes sections for "Number of Availability Zones (AZs)" (set to 1), "Number of public subnets" (set to 1), "Number of private subnets" (set to 2), "NAT gateways (S)" (set to "In 1 AZ"), and "VPC endpoints" (set to "None"). The "Preview" diagram remains the same, showing the network structure.



CREATING ADDITIONAL SUBNETS :

Step 1: Choose subnets in the left panel, choose to CREATE SUBNET

Step 2: in this, choose VPC ID: LAB-vpc and choose subnet name to lab-subnet-public2, choose availability zone to us-east-1b and choose IPv4 block to 10.0.2.0/24

Step 3: choose to create a subnet and again create the same subnet with lab-subnet-private2, change the IPv4 block to 10.0.2.0/24, and then create a subnet

Step 4: Choose the routing table in the left panel, select lab-rtb-private1-us-east-1a, in the lower panel, choose routes note destination, choose the subnet association tab, in the explicit subnet associations panel choose EDIT SUBNET

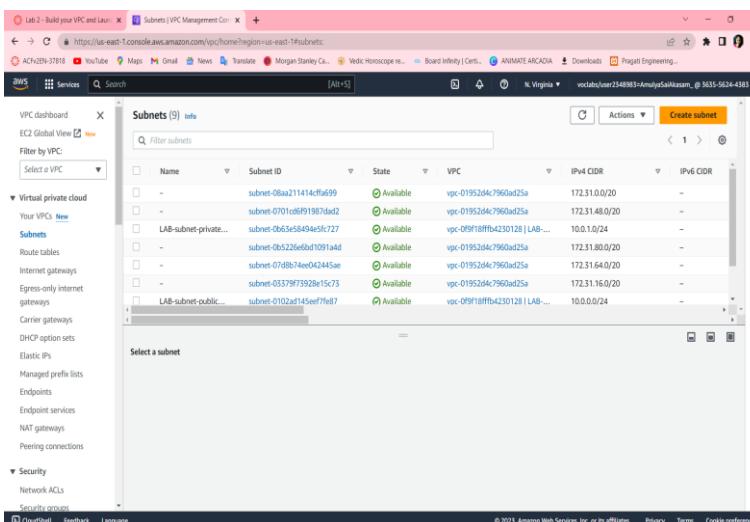
Step 5 : Leave lab-subnet-private1-us-east-1a and also select lab-subnet-private2

Step 6: Choose SAVE ASSOCIATIONS

Step 7: Select lab-rtb-public route table and deselect any other subnet

Step 8: In the lower panel, again repeat from step 4 but here we select lab-subnet-public2 also

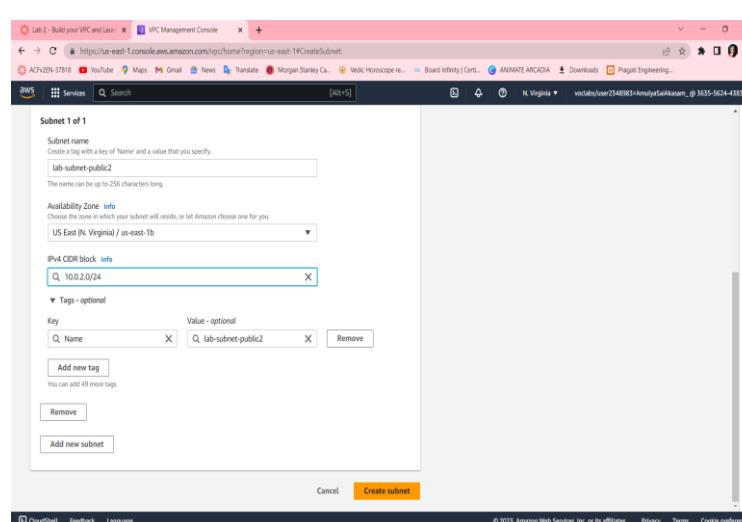
Step 9: Choose SAVE ASSOCIATIONS



Subnets (9) Info

Name	Subnet ID	VPC	IPv4 CIDR	IPv6 CIDR
subnet-08aa211414cffa699	vpc-01952d4c7960ad25a	172.31.0.0/20	-	
subnet-07010ef91987ad2	vpc-01952d4c7960ad25a	172.31.48.0/20	-	
LAB-subnet-private...	vpc-0653e584945fc727	10.0.1.0/24	-	
subnet-0b5226fe6fb10911ad	vpc-01952d4c7960ad25a	172.31.80.0/20	-	
subnet-07bb814ee02445ae	vpc-01952d4c7960ad25a	172.31.64.0/20	-	
subnet-03379f73928e15c73	vpc-01952d4c7960ad25a	172.31.16.0/20	-	
LAB-subnet-public...	vpc-0f918fffb42301281	10.0.0.0/24	-	

Select a subnet



Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

lab-subnet-public2

Availability Zone info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1b

IPv4 CIDR block info
10.0.2.0/24

Tags - optional

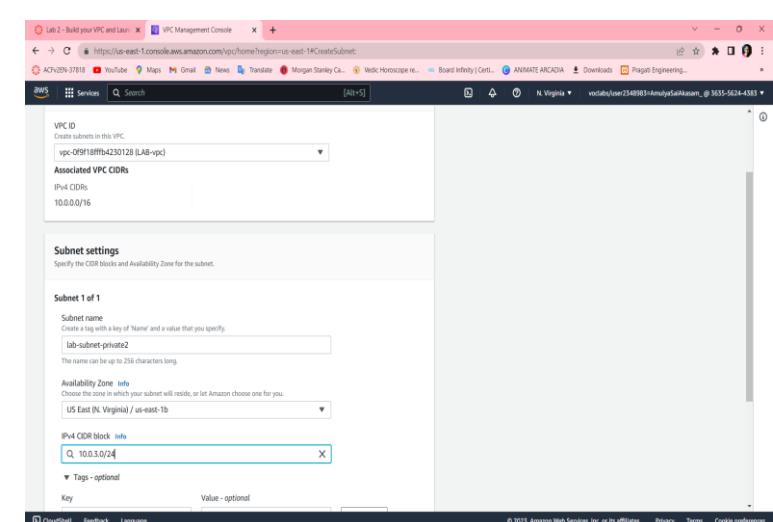
Key Name Value - optional

Add new tag

Remove

Add new subnet

Create subnet!



VPC ID
Create subnets in this VPC

vpc-0f918fffb4230128 (lab-vpc)

Associated VPC CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR block and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

lab-subnet-private2

Availability Zone info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1b

IPv4 CIDR block info
10.0.3.0/24

Tags - optional

Create subnet!

Lab 2 - Build your VPC and Lan... Subnets (VPC Management Con... +

You have successfully created 1 subnet: subnet-0de9853ca1053843c

Subnets (1) Info Actions Create subnet

Subnet ID: subnet-0de9853ca1053843c X Clear filters

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
lab-subnet-private2	subnet-0de9853ca1053843c	Available	vpc-0f5918fffb4230128 LAB...	10.0.0.0/24	-

Select a subnet

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Lab 2 - Build your VPC and Lan... VPC Management Console +

VPC Management Console https://us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#subnets:SubnetId=subnet-0de9853ca1053843c

Subnets Subnet ID: subnet-0de9853ca1053843c X Actions Create subnet

Filter subnets

Available subnets (2/4)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
LA8-subnet-private1-us-east-1a	subnet-0b63e58d94e5f727	10.0.1.0/24	-	rtb-0d578d819939ba1c / LA8-rtb-pr...
lab-subnet-private2	subnet-0de9853ca1053843c	10.0.3.0/24	-	Main (rtb-0fa7952faded8551)

Selected subnets

subnet-0b63e58d94e5f727 / LA8-subnet-private1-us-east-1a X subnet-0de9853ca1053843c / lab-subnet-private2 X

Cancel Save associations

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Lab 2 - Build your VPC and Lan... Route tables | VPC Management ... +

You have successfully updated subnet associations for rtb-0895a23740a50765 / LAB-rtb-public.

Route tables (5) Info Actions Create route table

Route table ID Name Explicit subnet assoc... Edge associations Main VPC

Route table ID	Name	Explicit subnet assoc...	Edge associations	Main	VPC
rtb-0352820de91af822e	Work Public Route...	subnet-0267afdf31dc7e...	-	No	vpc-0f8fad1cb0fd9d53b Wo...
rtb-0d67952faded8551	-	-	-	Yes	vpc-0f91ffbf4230128 LAB...
rtb-0d077ac50aa4769ad	-	-	-	Yes	vpc-0f8fad1cb0fd9d53b Wo...
rtb-0bb91f63678f62fe	-	-	-	Yes	vpc-01952d4c7960a25a

Select a route table

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

CREATING A VPC SECURITY GROUP

Step 1: Choose to create a security group and in this choose the security group name to a web security group, have a description as enable HTTP access and choose vpc to lab-vpc

Step 2: In inbound rules choose to add rule and then in this chosen type to HTTP, source to Anywhere ipv4 and description to permit web requests

The image consists of three side-by-side screenshots of the AWS VPC Management Console.

Screenshot 1: Create security group
This screenshot shows the "Create security group" wizard. Under "Basic details", the "Security group name" is set to "Web Security Group". The "Description" field contains "Enable HTTP access". Under "Inbound rules", there is one rule: "HTTP" (Protocol), "80" (Port range), "Anywhere" (Source), and "Permit web requests" (Description).

Screenshot 2: Outbound rules
This screenshot shows the "Outbound rules" section. It lists a single rule: "All traffic" (Type), "All" (Protocol), "All" (Port range), "Custom" (Destination), and "0.0.0.0/0" (Description). Below this, there is a "Tags - optional" section with a note about adding tags to resources.

Screenshot 3: Security group details
This screenshot shows the "sg-0f15c53fab20c8729 - Web Security Group" details page. It displays the security group name, ID, and description ("Enable HTTP access"). It also shows the owner (363555244383), inbound rules count (1), and outbound rules count (1). The "Inbound rules" tab is selected, showing one rule: "HTTP" (Protocol), "80" (Port range), "Anywhere" (Source), and "Permit web requests" (Description). A success message at the top states "Security group (sg-0f15c53fab20c8729 | Web Security Group) was created successfully".

LAUNCH A WEB SERVER INSTANCE

Step 1 : Choose EC2 to open EC2 console , from instances click launch instance and give name as web server 1

Step 2 : Keep Amazon Linux selelct and select amazon linux 2023 AMI , Choose t2.micro

Step 3 : Choose key pair name to vockey , in network settings choose edit select network to lab-vpc ,subnet to lab-subnet-public2 and auton assign to enable

Step 4 : Under firewall choose select existing security group , for common security groups select web security group

Step 5 : Expand the advanced details panel , scroll down upto the user data box appear .

```
#!/bin/bash
# Install Apache Web Server and PHP
sudo dnf install -y httpd wget php mariadb105-server
# Download Lab files get https://aws-tc-largeobjects.s3.us-west-
2.amazonaws.com/CUR-TF-100-ACCLFO-2-9026/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
```

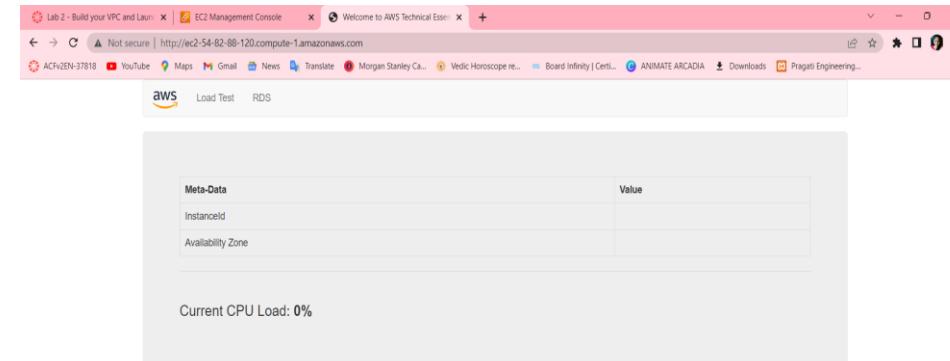
Step 6: At the bottom SUMMARY panel choose launch instance ,click on view instances

Step 7 : Wait until web server 1 shows 2/2 checks passed

Step 8 : Copy the public ipv4 dns value present in details tab

Step 9 : Open a new browser , copy the public dns

Step 10 : Finally we see a web page displaying the AWS logo and instances meta-data values



Finally, a web page opens displaying the AWS logo and instances of metadata values

ELASTIC LOAD BALANCER (ELB)

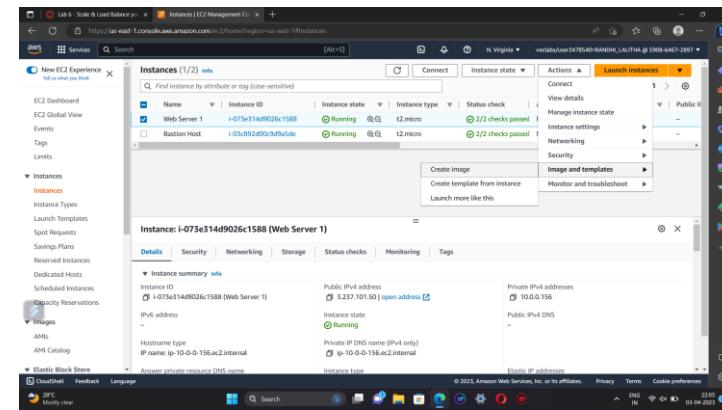
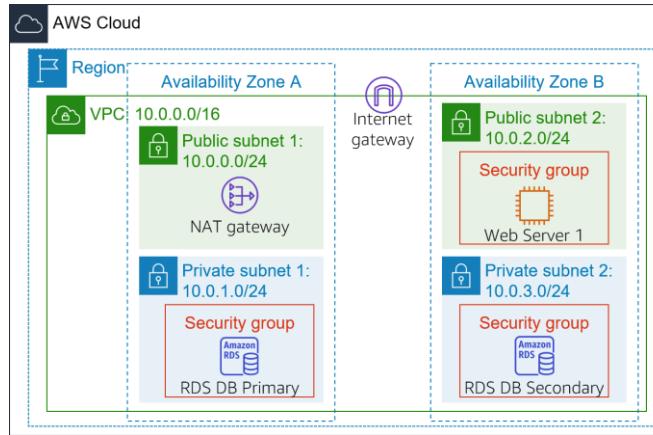
Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances.

In this lab, We are provided with the given infrastructure.

Procedure:

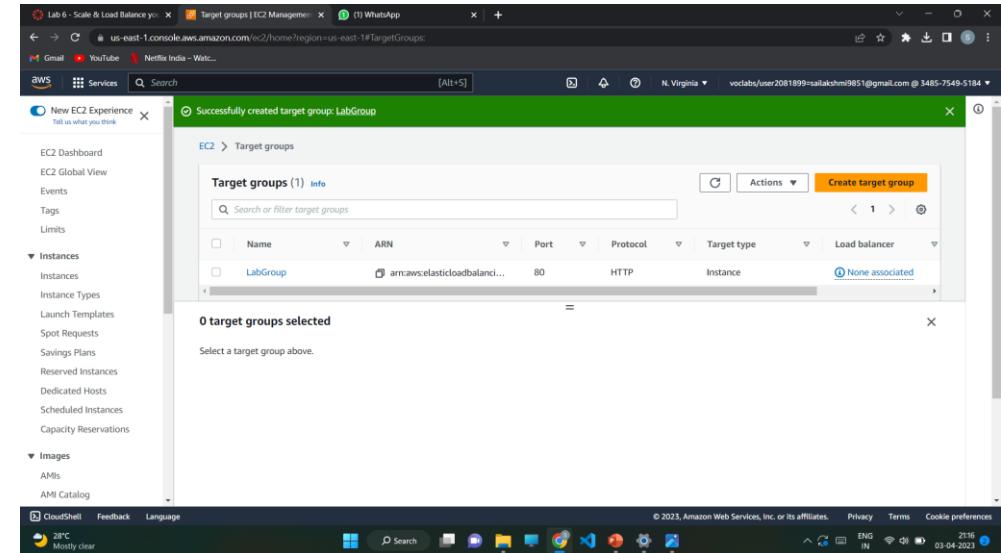
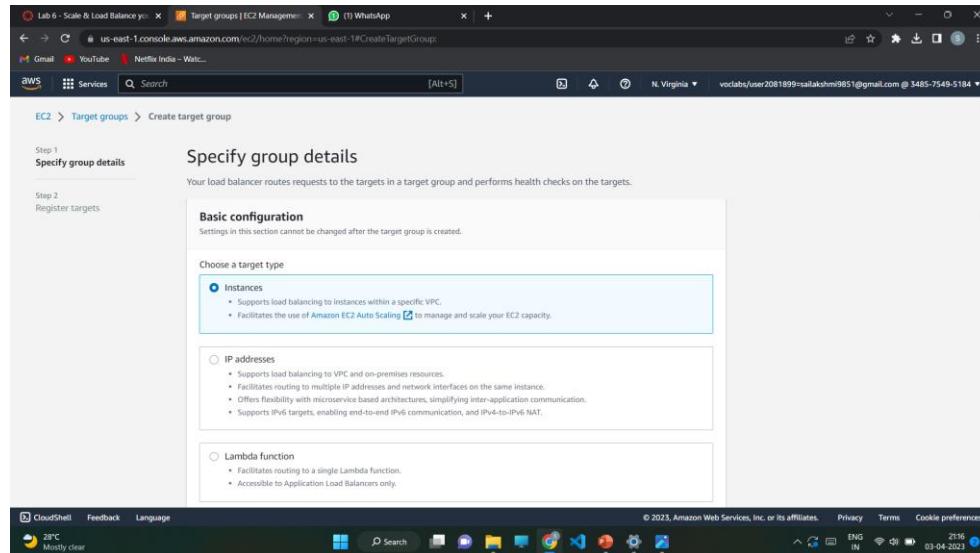
Task1: Creating an AMI for Auto Scaling

- ❖ Click start lab then click on AWS.
- ❖ You will navigate to AWS management console. Click on services and select EC2.
- ❖ Click instances. Make sure that **Status Checks** for **Web Server 1** displays 2/2 checks.
- ❖ Select Web Server 1 and in actions click images and templates > create image. Name the image and give the description.
- ❖ Click create image.

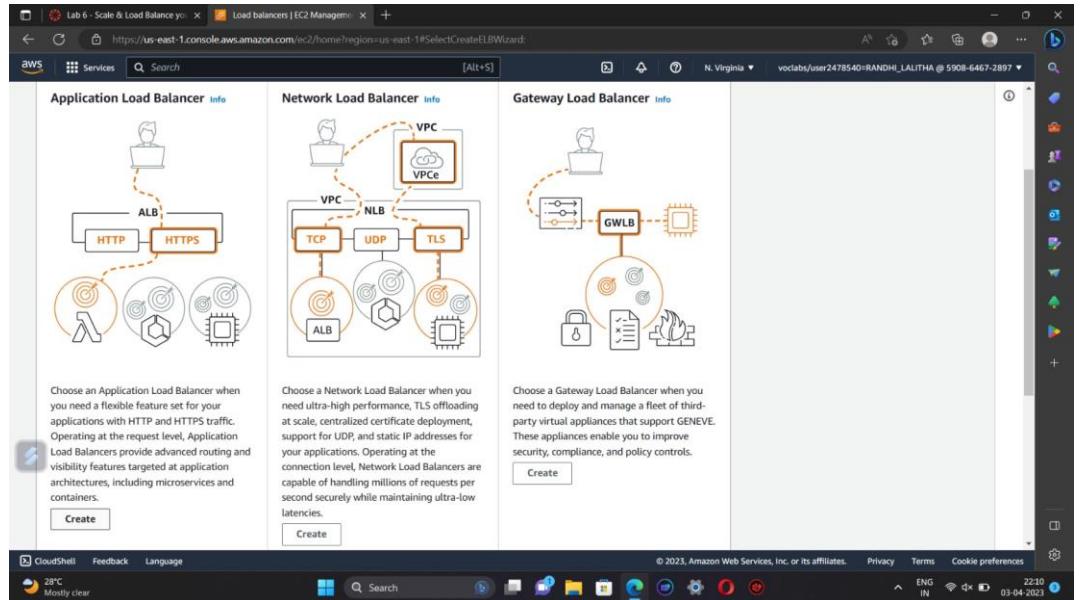


Task 2: Creating a load balancer

- ❖ Choose Target Groups and then click on create target group.
- ❖ Select target type as instances. Name the target group. Select Lab VPC under VPC that is we are creating load balancer in Lab VPC .
- ❖ Choose next and then click on create target group.



- ❖ From the left navigation pane , select Load Balancers. Click create load balancer.
- ❖ To create a application balancer, click create under Application Load Balancer and Name it.
- ❖ In Networking mapping, select Lab VPC and specify the subnets that the load balancer should use.
- ❖ In security groups, select only Web Security Group and deselect all other than it .
- ❖ For the Listener HTTP:80 row, set the Default action to forward to **LabGroup**.



Security groups Info

A security group is a set of firewall rules that control the traffic to your load balancer.

Select up to 5 security groups
Create new security group

Web Security Group sg-03c9de7e3a2fb85 X
VPC-vpc-0dec0fa646139b177

Listeners and routing Info

A Listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

Listener HTTP:80

Protocol	Port	Default action
HTTP	: 80 1-65535	Forward to LoadGroup Target type: Instance, IPv4 HTTP

Create target group

Listener tags - optional

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

Add-on services Edit

None

Attributes

Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.

Create load balancer

Recommendation to not use launch configurations

Amazon EC2 Auto Scaling no longer adds support for new EC2 features to launch configurations and will stop supporting new EC2 instance types after December 31, 2022. We recommend that customers using launch configurations migrate to launch templates. For more information, see the documentation.

Launch configurations (0) Info

Actions Copy to launch template Create launch configuration

Name AMI ID Instance type Spot price Creation time

No launch configurations found in this region.

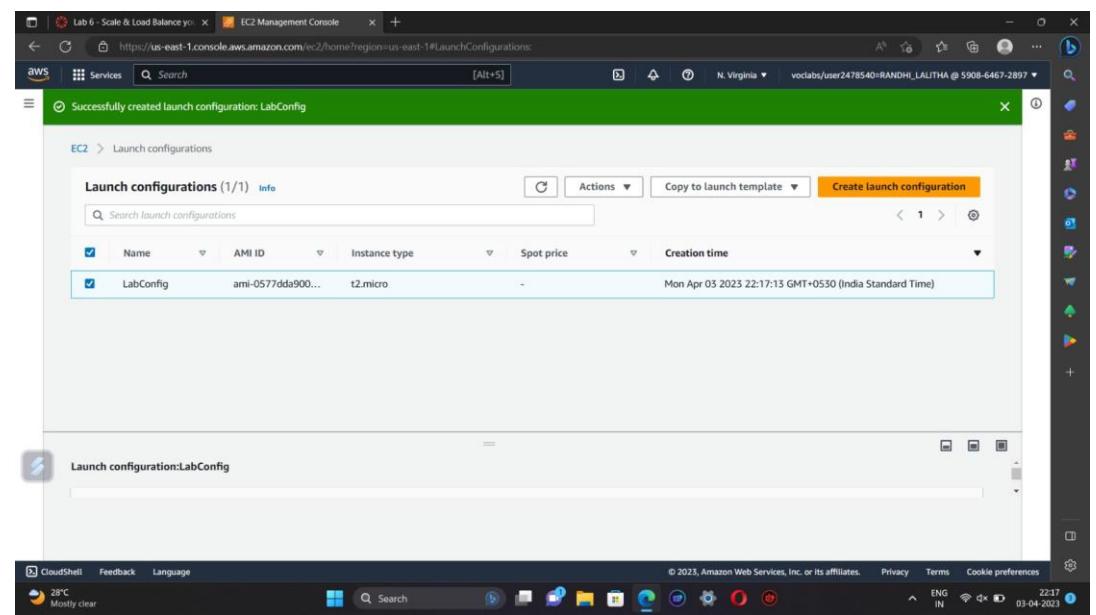
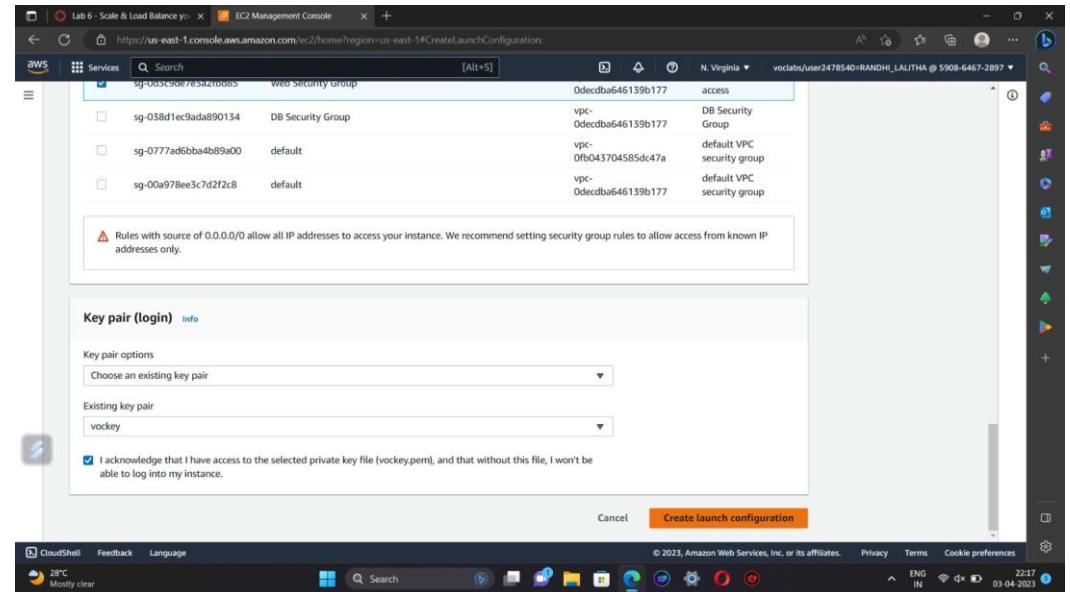
Create launch configuration

Select a launch configuration above

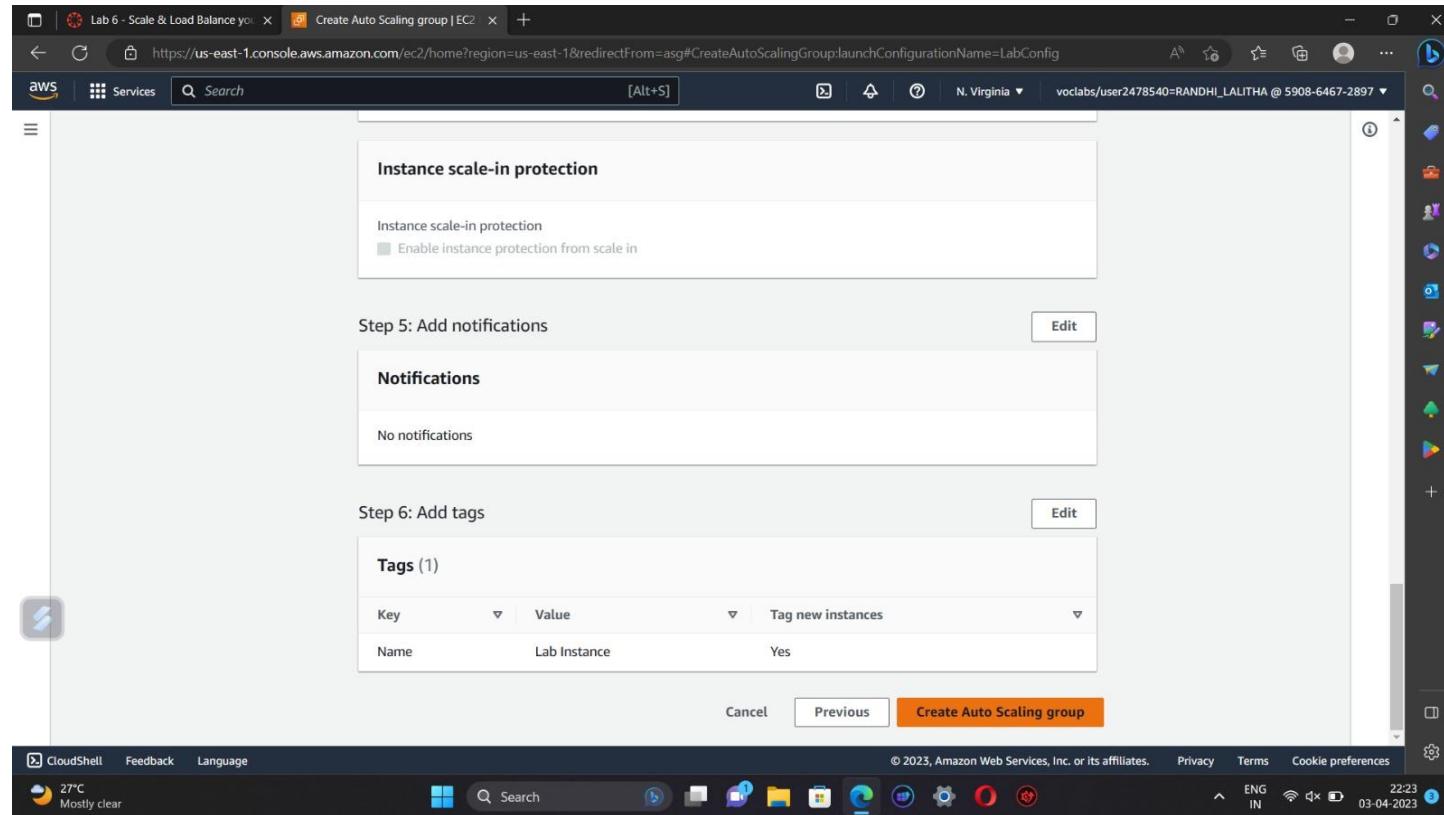
- ❖ Click create load balancer.

Task 3: Create a Launch Configuration and an Auto Scaling Group

- ❖ In Launch Configurations, click create launch configuration.
- ❖ Name the configuration and for AMI choose web server AMI that you created in task 1.
- ❖ Select the instance type.
- ❖ Under Additional Configuration, for monitoring select Enable EC2 instance detailed monitoring within CloudWatch.
- ❖ Under security groups , choose an existing security group Web Security Group.
- ❖ Under key pair, choose an existing key pair vockey. Check I acknowledge...
- ❖ Click Create launch configuration.
- ❖ For created launch configuration, select create auto scaling group from actions.
- ❖ Name it and select Lab VPC under VPC, select the private subnets.
- ❖ Select an existing load balancer which was created earlier.
- ❖ In the **Additional settings - optional** pane, select **Enable group metrics collection within CloudWatch**

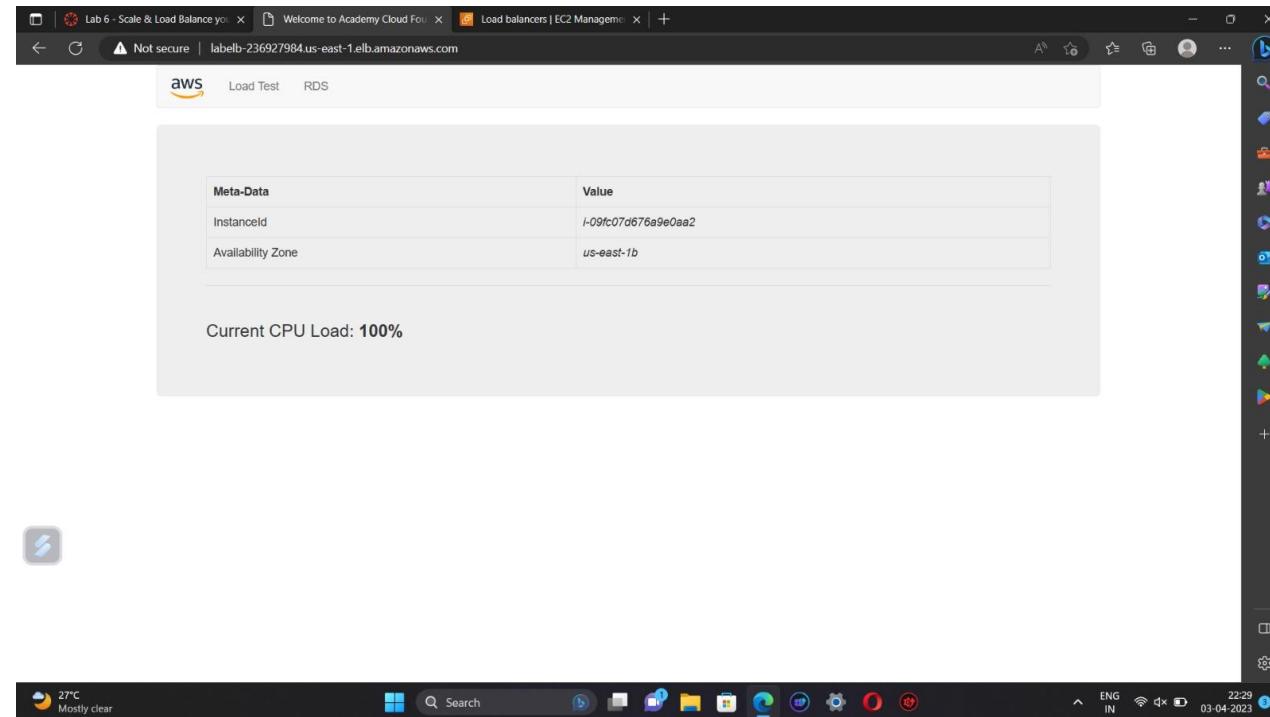


- ❖ Specify the values under Group size.
- ❖ Under **Scaling policies**, choose *Target tracking scaling policy* and name the policy. Specify metric type and target value. Then add a tag and click create auto scaling group.



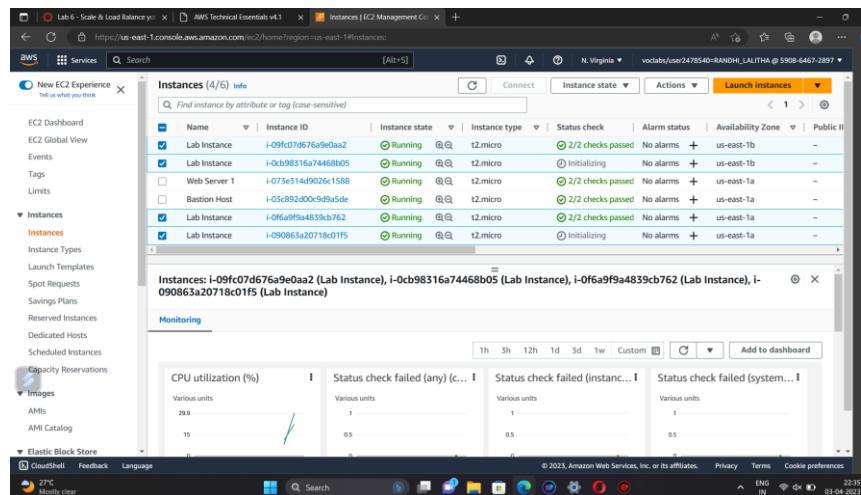
Task 4: Verify that Load Balancing is Working

- ❖ click **Instances**. You should see two new instances named **Lab Instance**. These were launched by Auto Scaling.
- ❖ In the labgroup target group, two **Lab Instance** targets should be listed for this target group. Wait until the **Status** of both instances transitions to *healthy*.
- ❖ Now copy the DNS name of the created load balancer making sure to omit "(A Record)". and paste it in a new browser
- ❖ The application should appear in your browser. This indicates that the Load Balancer received the request, sent it to one of the EC2 instances, then passed back the result.



Task 5: Test Auto Scaling

- ❖ On the **Services** menu, click **CloudWatch**. In the left navigation pane, choose **All alarms**. Two alarms will be displayed. These were created automatically by the Auto Scaling group.
- ❖ From services select EC2 and choose Auto Scaling Groups and select Lab Auto Scaling Group which you created.
- ❖ choose the **Automatic Scaling** tab. Select **LabScalingPolicy** and from actions change the target value to 50.click update.
- ❖ To go cloudwatch and click all alarms and verify.
- ❖ Click the **OK** alarm, which has *AlarmHigh* in its name.Return to the browser tab with the web application. Click **Load Test** beside the AWS logo.This will cause the application to generate high loads.
- ❖ You should see the **AlarmHigh** chart indicating an increasing CPU percentage. Once it crosses the 60% line for more than 3 minutes, it will trigger Auto Scaling to add additional instances.
- ❖ In EC2 instances , you notice that more than two instances labeled **Lab Instance** should now be running.
- ❖ Finally terminate the Web Server 1.



IDENTITY AND ACCESS MANAGEMENT

AWS Identity and Access Management (IAM) is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. With IAM, you can centrally manage **users, security credentials** such as access keys, and ~~permissions that control which AWS resources users can access~~.



Steps to create IAM User and User Groups

1.On the **Console Home** page, select the IAM service. 2.In the navigation pane, select **Users** and then select **Add users**.

The screenshot shows the AWS Management Console search results for 'iam'. The left sidebar lists various services and features under 'Services' and 'Features'. The main search results page displays the IAM service, which is highlighted with a blue border. Other results include IAM Identity Center, Resource Access Manager, and Serverless Application Repository.

The screenshot shows the IAM Management Console with the 'Users' list open. The left sidebar shows the 'Identity and Access Management (IAM)' navigation pane with 'Users' selected. The main area displays a table of existing users, each with columns for User name, Groups, Last activity, MFA, Password age, and Active key age. At the top right of the user list, there is a blue 'Add users' button.

3. For Username, enter EmergencyAccess and , Select the check box next to **Provide user access to the AWS Management Console- optional** and then choose **I want to create an IAM user**.

4. Under **Console password**, select **Custom Password** and create your own password.

5. Clear the check box next to **User must create a new password at next sign-in (recommended)**. Then click on **Next**.

Specify user details

User details

User name
EmergencyAccess

Provide user access to the AWS Management Console - optional

Are you providing console access to a person?

Custom password

Console password

Users must create a new password at next sign-in (recommended)

User details

User name
EmergencyAccess

Provide user access to the AWS Management Console - optional

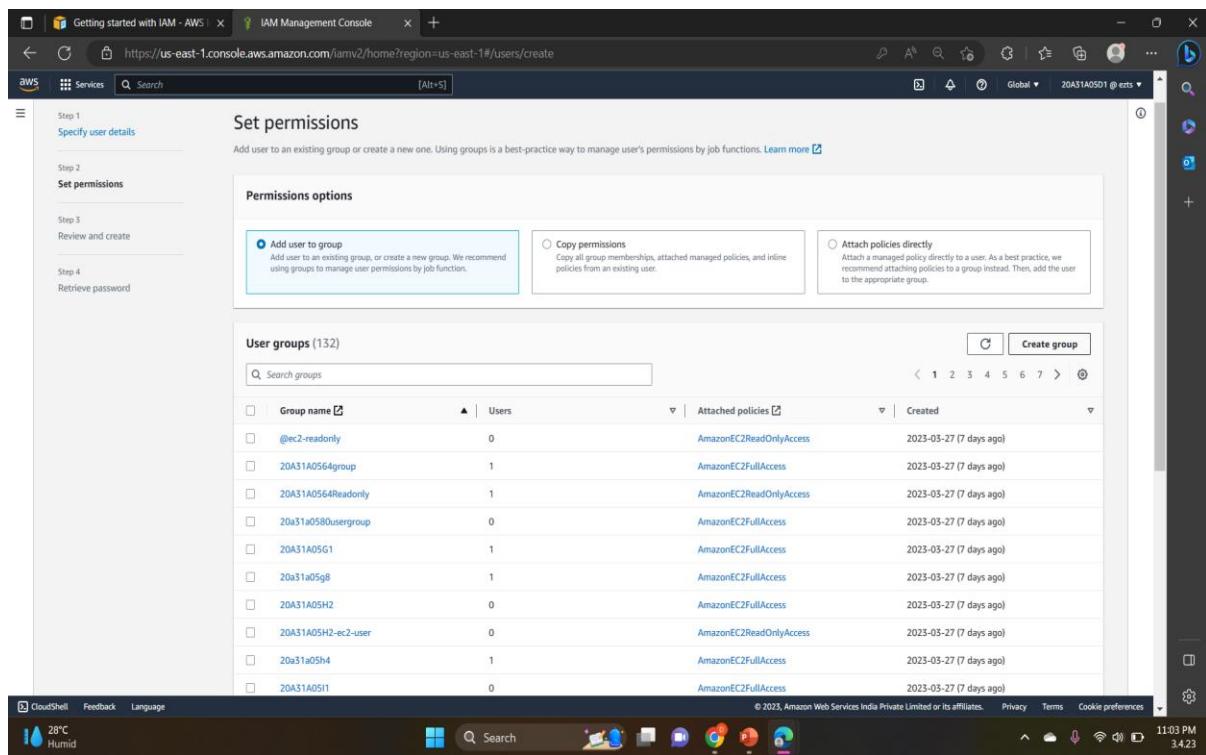
Are you providing console access to a person?

Custom password

Console password

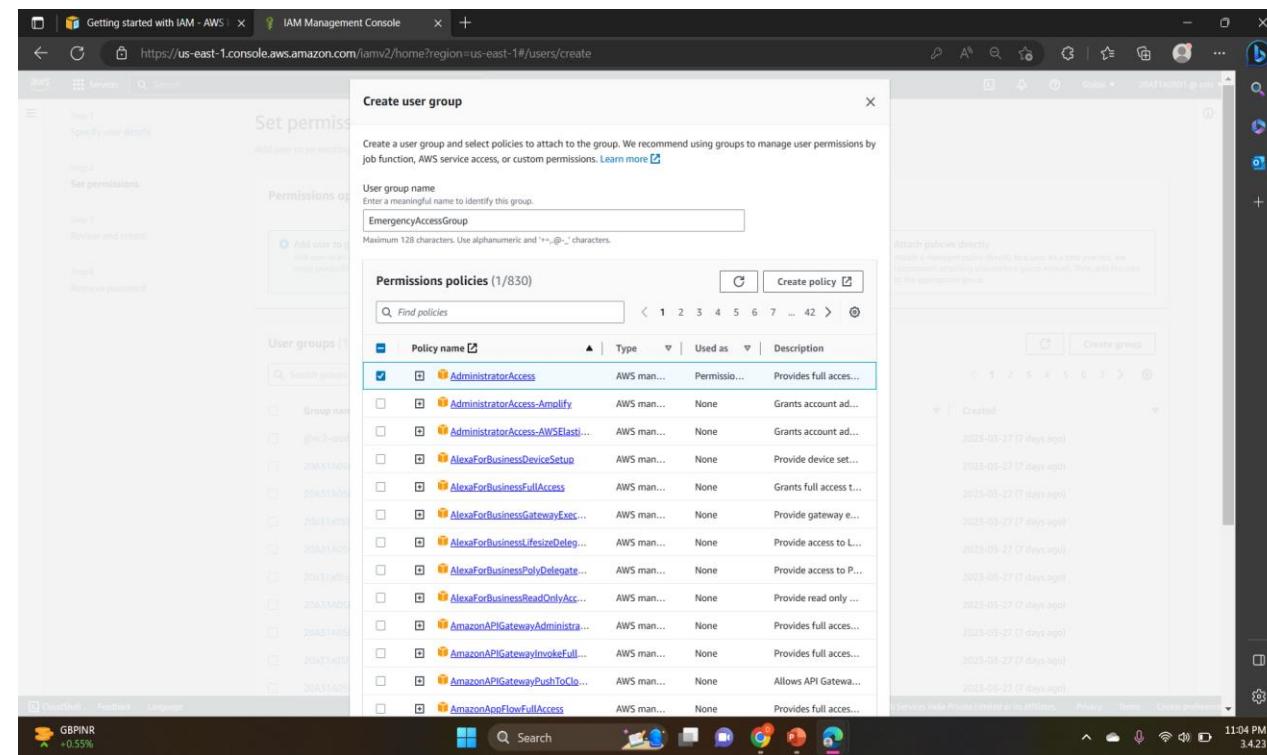
If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more

6. On the Set permissions page, under Permissions options, select Add user to group. Then, under User groups, select Create group.



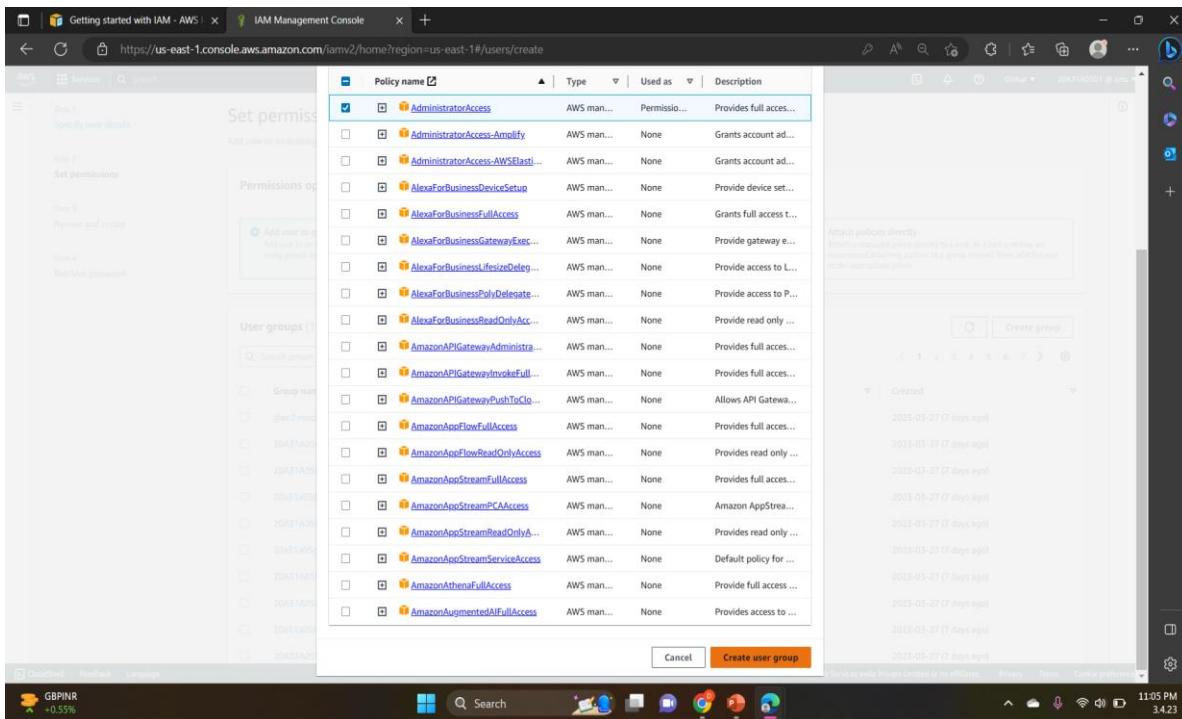
The screenshot shows the 'Set permissions' step in the IAM Management Console. The 'Permissions options' section is open, with the 'Add user to group' radio button selected. Below it, there are three other options: 'Copy permissions', 'Attach policies directly', and 'Add user to existing group'. A 'Create group' button is visible at the bottom right of this section. To the right, a 'User groups (132)' table lists various groups with their details like users, attached policies, and creation date. The table has columns for Group name, Users, Attached policies, and Created.

7. On the Create user group page, in User group name, enter EmergencyAccessGroup. Then, under Permissions policies, select AdministratorAccess.

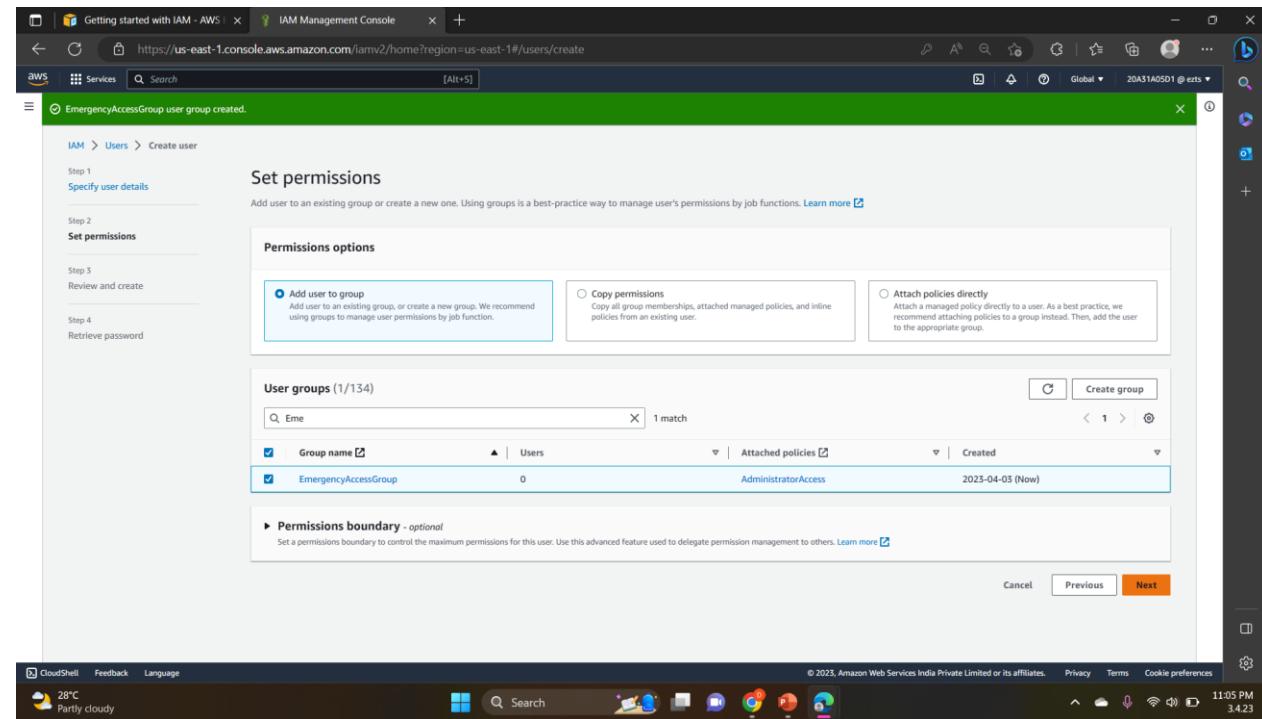


The screenshot shows the 'Create user group' step in the IAM Management Console. In the 'User group name' field, 'EmergencyAccessGroup' is typed. Below it, the 'Permissions policies' section shows a table with one item: 'AdministratorAccess'. This table includes columns for Policy name, Type, Used as, and Description. The 'AdministratorAccess' policy is highlighted with a checkmark. The background shows the 'Set permissions' step from the previous screenshot.

8. Select **Create user group** to return to the **Set permissions** page.



9. Select **Next** to proceed to the **Review and create** page.



10. On the **Review and create** page, review the list of user group memberships to be added to the new user. When you are ready to proceed, select **Create user**.

11. On the **Retrieve password** page, select **Download .csv file** to save a .csv file with the user credential information (Connection URL, user name, and password).

12. Save this file to use if you need to sign-in to IAM and do not have access to your federated identity provider.

The screenshot shows the AWS IAM Management Console interface. The top navigation bar includes the AWS logo, Services menu, and search bar. The main content area has a green header bar stating "User created successfully" and "You can view and download the user's password and email instructions for signing in to the AWS Management Console." Below this, the breadcrumb trail shows "IAM > Users > Create user". The left sidebar lists four steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The "Step 4" section is currently active, titled "Retrieve password". It contains a sub-section "Console sign-in details" which lists the "Console sign-in URL" as <https://ezts.sigin.aws.amazon.com/console>, the "User name" as "EmergencyAccess", and the "Console password" as a masked string followed by a "Show" link. To the right of this section are two buttons: "Email sign-in instructions" and "Download .csv file". At the bottom right of the main content area are "Return to users list" and "Create user" buttons. The footer of the browser window includes standard links like CloudShell, Feedback, Language, and various system status icons.

13. If you want to add permissions to the user group, then go to **User groups** and click on the respective **User group**.

The screenshot shows the AWS IAM Management Console with the URL <https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/groups>. The left sidebar is collapsed, and the main area displays the 'User groups' page. The title bar says 'Identity and Access Management (IAM)'. The page shows a table with one row: 'EmergencyAccessGroup'. The table has columns: Group name, Users, Permissions, and Creation time. The 'EmergencyAccessGroup' row has a status of 'Defined' and was created '5 minutes ago'. A search bar at the top says 'Filter User groups by property or group name and press enter'. The bottom status bar shows the URL and the AWS CloudWatch Metrics icon.

14. Go to **Permissions** → **All permissions** → **Attach policies**

The screenshot shows the AWS IAM Management Console with the URL [https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/groups/details/EmergencyAccessGroup\)section=permissions](https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/groups/details/EmergencyAccessGroup)section=permissions). The left sidebar is collapsed, and the main area displays the 'EmergencyAccessGroup' page under 'User groups'. The title bar says 'Identity and Access Management (IAM)'. The page shows a 'Summary' section with details: User group name 'EmergencyAccessGroup', Creation time 'April 03, 2023, 23:05 (UTC+05:30)', and ARN 'arn:aws:iam:244575612640:group/EmergencyAccessGroup'. Below this is a 'Permissions' section. It shows a table with one row: 'AdministratorAccess'. The table has columns: Policy name, Type, and Description. The 'AdministratorAccess' row is described as 'AWS managed - job function' and 'Provides full access to AWS services and resources'. A search bar at the top says 'Filter policies by property or policy name and press enter'. The bottom status bar shows the URL and the AWS CloudWatch Metrics icon.

15. Add the permission policy and the policy is attached to the User group.

The screenshot shows the AWS IAM Management Console with the URL <https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/groups/details/EmergencyAccessGroup/attach-policies>. The left sidebar is collapsed, and the main area displays a list of "Other permission policies" under the heading "Attach permission policies to EmergencyAccessGroup". A search bar at the top of the list allows filtering by policy name or type. One policy, "AmazonEC2FullAccess", is selected and highlighted in blue. At the bottom of the list, there are buttons for "Create policy" and "Simulate". The status bar at the bottom right shows the time as 11:11 PM and the date as April 3, 2023.

The screenshot shows the AWS IAM Management Console with the URL <https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/groups/details/EmergencyAccessGroup?section=permissions>. The left sidebar is collapsed, and the main area displays a summary of the "EmergencyAccessGroup" and its attached permissions. Under the "Permissions" tab, a table lists two policies: "AmazonEC2FullAccess" and "AdministratorAccess". The status bar at the bottom right shows the time as 11:11 PM and the date as April 3, 2023.

AWS RDS

Step 1: Create a Security Group for the RDS DB Instance.

aws management console → vpc → security groups → choose create security group → add inbound rule → create security group.

The screenshot shows the AWS VPC Management Console with the 'Security groups' section selected. The left sidebar includes options like Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, Peering connections, Security (Network ACLs, Security groups), DNS firewall (Rule groups, Domain lists), and Network Firewall (Firewalls, Firewall policies, Network Firewall rule). The main area displays a table of existing security groups:

Name	Security group ID	Security group name	VPC ID	Description
Web Security Group	sg-01d39ed3846f1fb22	Web Security Group	vpc-0a63c938af50af6dd	Enable HTTP access
-	sg-0df5c92e11cf2e061	default	vpc-0e59d72d284adab5a	default VPC security gr...
-	sg-0924aa7436e12708c	default	vpc-0a63c938af50af6dd	default VPC security gr...
-	sg-0de814af15ac8f2c0	WorkEc2SecurityGroup	vpc-0a130348b7d35abd3	VPC Security Group
-	sg-06c2bd13f5ecc2d5d	default	vpc-0a130348b7d35abd3	default VPC security gr...

The screenshot shows the 'Create security group' wizard. The first step, 'Basic details', has the security group name set to 'DB Security Group' and a description of 'Permit access from Web Security Group'. The second step, 'Inbound rules', shows a single rule for MySQL/Aurora on port 3306 from the 'Web Security Group'. The bottom status bar indicates the session is at 21:53 on 03-04-2023.

Step 2 : Create a DB Subnet Group.

Rds → subnet groups → choose create DB subnet group → add subnets → create DB subnet group.

The screenshot shows the AWS RDS Subnet Groups list page. The left sidebar has 'Subnet groups' selected under 'Amazon RDS'. The main area displays a table titled 'Subnet groups (1)'. The table has columns: Name, Description, Status, and VPC. One entry is listed: 'db-subnet-group' (DB Subnet Group), 'Complete', and 'vpc-0f6f7faaf6c154fc2'. A 'Create DB subnet group' button is located at the top right of the table area.

The screenshot shows the 'Create DB subnet group' wizard. The left sidebar has 'Subnet groups' selected under 'Amazon RDS'. The main area is titled 'Create DB subnet group' with the sub-section 'Subnet group details'. It includes fields for 'Name' (set to 'DB-Subnet-Group'), 'Description' (set to 'DB Subnet Group'), and 'VPC' (set to 'Lab VPC (vpc-0a63c938af50af6dd)'). A note states: 'To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.'

Step 3: In the left navigation pane, choose Databases → choose create database → MySQL

This screenshot shows the AWS RDS Management Console. The left sidebar includes options like Dashboard, Databases (which is selected), Query Editor, Performance insights, Snapshots, Exports in Amazon S3, Automated backups, Reserved instances, Proxies, Subnet groups, Parameter groups, Option groups, Custom engine versions, and Events. The main content area is titled 'Databases' and shows a table with columns for DB identifier, Role, Engine, Region & AZ, Size, Status, and Action. A modal window titled 'Consider creating a Blue/Green Deployment to minimize downtime during upgrades' provides information about using Amazon RDS Blue/Green Deployments to minimize downtime during upgrades. It includes links to the RDS User Guide and Aurora User Guide.

This screenshot shows the 'Create database' page for MySQL. The top navigation bar includes tabs for Services, Search, and AWS. The main title is 'Create database'. Below it, a section titled 'Choose a database creation method' offers two options: 'Standard create' (selected) and 'Easy create'. The 'Standard create' option allows users to set all configuration options, including ones for availability, security, backups, and maintenance. The 'Easy create' option uses recommended best-practice configurations. To the right, a sidebar titled 'MySQL' lists features: supports database size up to 64 TiB, supports General Purpose, Memory Optimized, and Burstable Performance instance classes, supports automated backup and point-in-time recovery, and supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region. The 'Engine options' section shows three choices: Aurora (MySQL Compatible), Aurora (PostgreSQL Compatible), and MySQL (selected). The MySQL icon features a hand holding a wrench.

Step 4: In Availability and durability ,choose Multi -AZ DB instance then configure settings , DB instance class, Storage, connectivity, choose existing vpc security group and setup additional configuration.

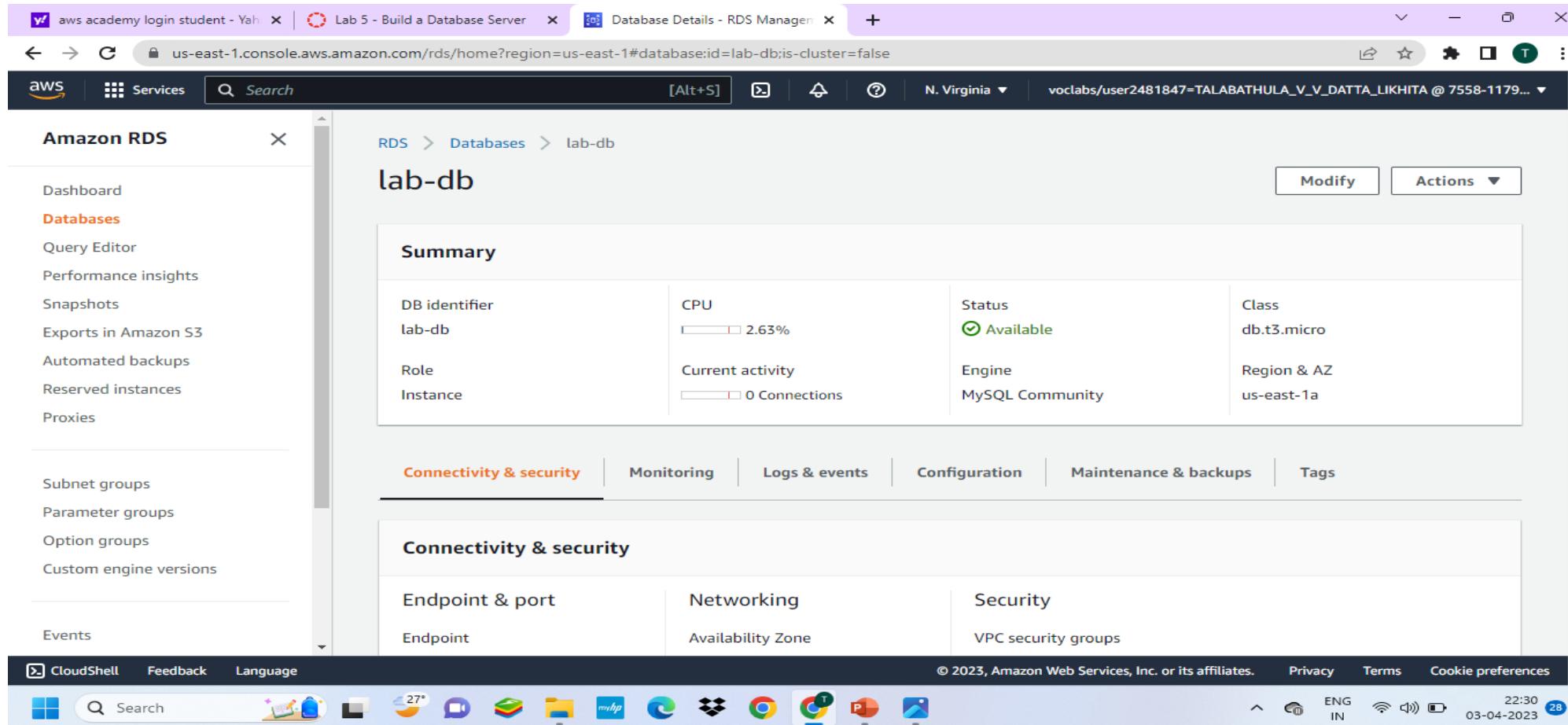
The screenshot shows the 'Availability and durability' section of the AWS RDS MySQL creation wizard. It includes:

- Deployment options:** A radio button for "Multi-AZ DB Cluster - new" is selected, with a note that it creates a DB cluster with a primary DB instance and two readable standby DB instances in different Availability Zones (AZ). It also provides high availability, data redundancy, and capacity to serve read workloads.
- Multi-AZ DB instance:** A radio button for "Multi-AZ DB instance" is selected, noting that it creates a primary DB instance and a standby DB instance in a different AZ, providing high availability and data redundancy but without support for read connections.
- Single DB instance:** A radio button for "Single DB instance" is shown, which creates a single DB instance with no standby instances.
- DB instance identifier:** The identifier "database-1" is entered into the input field.
- MySQL details:** A summary of MySQL features, including support for up to 64 TiB, General Purpose, Memory Optimized, and Burstable Performance instance classes, automated backup, point-in-time recovery, and up to 15 Read Replicas per instance.

The screenshot shows the configuration details for the MySQL DB instance, specifically for Amazon RDS Optimized Writes:

- Amazon RDS Optimized Writes:** A note that MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity.
- DB instance class:** The "Burstable classes (includes t classes)" option is selected, showing the "db.t3.micro" class with 2 vCPUs, 1 GiB RAM, and Network: 2,085 Mbps.
- Storage:** The "Provisioned IOPS SSD (io1)" storage type is selected, with notes on its flexibility in provisioning I/O and allocated storage.
- Additional settings:** Includes options for previous generation classes and other MySQL configuration parameters.

Step 5: Wait until Info changes to Modifying or Available.
Scroll down to the Connectivity & security section and copy the Endpoint field.



The screenshot shows the AWS RDS Database Details page for a database named 'lab-db'. The 'Summary' section displays the following information:

DB identifier	CPU	Status	Class
lab-db	2.63%	Available	db.t3.micro
Role	Current activity	Engine	Region & AZ
Instance	0 Connections	MySQL Community	us-east-1a

The 'Connectivity & security' tab is selected, showing the 'Endpoint & port' section with the 'Endpoint' field containing the value 'Endpoint'. Below the table, the status message 'Status: Available' is displayed.

Step 6 : Interact with Your Database.

On Details , copy the WebServer IP address. Open a new web browser tab, paste the WebServer IP address and press Enter. The web application will be displayed, showing information about the EC2 instance.

The screenshot shows the AWS Academy interface. On the left is a sidebar with icons for Account, Dashboard, Courses, Calendar, Inbox, History, and Help. The main area displays a course navigation path: ACFv2EN... > Modules > Module 8 ... > Lab 5 - Build a Database Server. Below this, there's a table with the following data:

	EN-US
private:	10.0.0.119
SSH key	Show Download PEM Download PPK
AWS SSO	Download URL
SecretKey	qwLdR6kIW1E9YvExD2WvazVmlAmzLhhN2GW4EWRX
WebServer	54.226.213.62
BastionHost	44.195.42.104
Region	us-east-1
AccessKey	AKIA276PEWWVAXXXS4H

Below the table, a note says: "32. To copy the WebServer IP address, choose on the Details drop down menu show these instructions, and then choose Show". At the bottom are 'Previous' and 'Next' buttons.

The screenshot shows a web browser window titled "AWS Technical Essentials v4.1" with the URL "54.226.213.62/load.php". The page displays the following content:

Under High CPU Load! (auto refresh in 5 seconds)

Current CPU Load: **100%**

At the bottom, the Windows taskbar shows various open applications and the system clock at 22:34 on 03-04-2023.

Step 7 : Choose the RDS link at the top of the page and configure the settings.

The screenshot displays a web browser window with the following details:

- Browser Tabs:** aws academy login student - Yah, Lab 5 - Build a Database Server, Database Details - RDS Manager (active), AWS Technical Essentials v4.1.
- Address Bar:** Not secure | 54.226.213.62/rds.php
- Content Area:** A form titled "Database Details - RDS Manager" with the following fields:
 - Endpoint
 - Database
 - Username
 - PasswordA "Submit" button is located at the bottom of the form.
- Taskbar:** Shows various application icons including File Explorer, Task View, Control Panel, Weather (27°), Mail, File History, File Explorer, Microsoft Edge, Google Chrome, and others. It also displays system status: ENG IN, battery level, and the date/time (22:36 03-04-2023).

Step 8: After a few seconds the application will display an **Address Book**.
The Address Book application is using the RDS database to store information.

The screenshot shows a web browser window with four tabs at the top: "aws academy login student - Yah", "Database Details - RDS Manager", "Lab 5 - Build a Database Server", and "AWS Technical Essentials v4.1". The main content area displays the "Address Book" application. The interface includes the AWS logo and navigation links for "Load Test" and "RDS". The "Address Book" title is centered above a table. The table has columns for "Last name", "First name", "Phone", "Email", and "Admin". It contains two rows of data: one for "Doe" (Jane) and one for "Johnson" (Roberto). Each row includes "Edit" and "Remove" buttons under the "Admin" column. A blue "Add Contact" link is positioned above the table. The browser's address bar shows the URL "54.226.213.62/rds.php".

Last name	First name	Phone	Email	Admin
Doe	Jane	010-110-1101	janed@someotheraddress.org	Edit Remove
Johnson	Roberto	123-456-7890	robertoj@someaddress.com	Edit Remove



ELASTIC BLOCK SERVICE (EBS)

1. Open Management Console, on the services menu open Ec2
2. In the left navigation pane choose instances and create a instance with a name
3. Next, In the left navigation pane choose Volumes
4. Click on Create Volume
5. Select volume type, size(Gib),Availability Zone and in Add tag section add key and value names.
6. Then click on create volume
7. Click on volumes on left navigation pane select the created volume and attach a previously created instance to it.
8. Then, go to “Details” drop down, choose “show”
9. Download the ppk file
10. Download putty
11. Open putty set the fields (such as Host name, public key, private key) as per the requirement.
12. The putty shell will open , then login into it and run the commands.
13. The commands looks like:
`df -h
sudo mkfs -t ext3/dev/sdf etc.,`
14. Create a EBS snapshot by giving the necessary fields.
15. Create a volume using snapshot.
16. Attach the volume to the created EC2 instance

Lab 4 - Working with EBS | **Dashboard | EC2 Management**

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Home

N. Virginia vocabs/user2346228@Nandini_Gampala @ 4815-1185-8137

EC2 Dashboard

- EC2 Global View
- Events
- Tags
- Limits
- Instances**
 - Instances
 - Instance Types
 - Launch Templates
 - Spot Requests
 - Savings Plans
 - Reserved Instances
 - Dedicated Hosts
 - Scheduled Instances
 - Capacity Reservations
- Images**
 - AMIs
 - AMI Catalog
- Elastic Block Store**
 - CloudShell
 - Feedback
 - Language

30°C Mostly clear

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	2	Auto Scaling Groups	API Error	Dedicated Hosts	0
Elastic IPs	0	Instances	2	Key pairs	1
Load balancers	0	Placement groups	0	Security groups	5
Snapshots	0	Volumes	2		

Account attributes

Supported platforms

- VPC

Default VPC vpc-0d53b0f60743f36e6

Settings

EBS encryption

Zones

EC2 Serial Console

Default credit specification

Console experiments

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Service health

Region: US East (N. Virginia)

Status: This service is operating normally

Explore AWS

Amazon GuardDuty Malware Protection

GuardDuty now provides agentless malware detection in Amazon EC2 & EC2 container workloads. Learn more

Save up to 90% on EC2 with Spot Instances

Optimizes price-performance by combining EC2 purchase options in a single EC2 ASCI Learning resource

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

CloudShell Feedback Language

30°C Mostly clear

Search ENG IN 8:47 PM 4/3/2023

Lab 4 - Working with EBS | **Instances | EC2 Management**

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances

N. Virginia vocabs/user2346228@Nandini_Gampala @ 4815-1185-8137

Instances (2) Info

Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Bastion Host	i-0fe2bad3517160e0	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-54-210-99-1
Lab	i-0cede73494135f0ff	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-34-238-176-

Select an instance

Instances

- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts
- Scheduled Instances
- Capacity Reservations

Images

- AMIs
- AMI Catalog

Elastic Block Store

CloudShell Feedback Language

30°C Mostly clear

CloudShell Feedback Language

ENG IN 8:48 PM 4/3/2023

Lab 4 - Working with EBS | **Create volume | EC2 Management**

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateVolume

N. Virginia vocabs/user2346228@Nandini_Gampala @ 4815-1185-8137

EC2 > Volumes > Create volume

Create volume

Create an Amazon EBS volume to attach to any EC2 instance in the same Availability Zone.

Volume settings

Volume type: General Purpose SSD (gp2)

Size (GiB): 1

IOPS: 100 / 3000

Throughput (MiB/s): Not applicable

Availability Zone: us-east-1a

Snapshot ID - optional: Don't create volume from a snapshot

Encryption: Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.

Encrypt this volume:

CloudShell Feedback Language

29°C Mostly clear

CloudShell Feedback Language

ENG IN 8:56 PM 4/3/2023

Lab 4 - Working with EBS | **Volumes | EC2 Management**

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Volumes

N. Virginia vocabs/user2346228@Nandini_Gampala @ 4815-1185-8137

Volumes (1/2)

Actions

Create volume

Modify volume

Create snapshot

Create snapshot lifecycle policy

Delete volume

Attach volume

Detach volume

Force detach volume

Manage auto-enabled I/O

Manage tags

Fault injection

Name	Volume ID	Type	Size	IOPS	Throughput
My Volume	vol-022f1f239cc2da05a	gp2	1 GiB	100	-
	vol-088b8ff07838675838	gp3	8 GiB	3000	125

Volume ID: vol-022f1f239cc2da05a (My Volume)

Details Status checks Monitoring Tags

CloudShell Feedback Language

CloudShell Feedback Language

ENG IN 9:01 PM 4/3/2023

Lab 4 - Working with EBS Course Modules: AWS Academy Attach volume | EC2 Management

us-east-1.console.aws.amazon.com/e2/home?region=us-east-1#AttachVolumeVolumeId=vol-022f1f239cc2da05a

N. Virginia volatis/user2346228-Nandini_Gampala @ 4815-1185-8157

EC2 > Volumes > vol-022f1f239cc2da05a > Attach volume

Attach volume

Attach a volume to an instance to use it as you would a regular physical hard disk drive.

Basic details

Volume ID: vol-022f1f239cc2da05a (My Volume)

Availability Zone: us-east-1a

Instance Info: i-0e177f61a0d16fd2

Device name: /dev/sdf

Recommended device names for Linux: /dev/sda1 for root volume. /dev/sdf(p) for data volumes.

Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvd(p) internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.

CloudShell Feedback Language 29°C Mostly clear 9:01 PM 4/3/2023

Lab 4 - Working with EBS Course Modules: AWS Academy Volumes | EC2 Management

awsacademy.instructure.com/courses/37818/modules/items/3224414

ACFv2EN-37818 > Modules > Module 7 - Storage > Lab 4 - Working with EBS

Home Announcements Modules Discussions Grades Calendar Inbox History Help

EN_US

Accumulated lab time: 01:21:00 (81 minutes)
No running instance

SSH key Show Download PEM Download PPK
AWS SSO Download URL

SecretKey UICINNYWWTjV12flRtc477+1SFsywFkTH05KsK0M
BastionHost 54.210.99.175
Region us-east-1
AvailabilityZone us-east-1a
AccessKey AKIAXANCX37HURWN4PUP
LabInstance 34.238.176.253

Then exit the Docker prompt by pressing the X.

Next < Previous 29°C Mostly clear 9:02 PM 4/3/2023

Lab 4 - Working with EBS Course Modules: AWS Academy Volumes | EC2 Management

awsacademy.instructure.com/courses/37818/modules/items/3224414

ACFv2EN-37818 > Modules > Module 7 - Storage > Lab 4 - Working with EBS

Home Announcements Modules Discussions Grades

EN_US

PutTY Configuration

Category: EN_US

18. Configure PuTTY

- Choose Connection type: SSH
- Set Seconds: 2

This allows you to have a longer period of inactivity before the session times out.

19. Configure your PuTTY session

- Choose Session Name: labuser
- Host Name: 54.210.99.175
- Port: 22
- Connection type: SSH
- Save Session

Launch Terminal

Details AWS Start Lab End Lab 7:44 Instructions Actions

File README Terminal Source

labuser (1).ppk 29°C Mostly clear 9:03 PM 4/3/2023

Lab 4 - Working with EBS Instances | EC2 Management Course Modules: AWS Academy Lab 4 - Working with EBS README

labs.vocareum.com/web/2366056/1506157.0/ASLIB/public/docs/lang/en_us/README.html#ssh-after

PutTY (inactive)

Key: Name: Value: Mu_Snapshot

```
login as: ec2-user
root's password: 
[...]
idling, which means that the snapshot is being created. It will
blocks do not occupy any snapshot storage space.

Your file has been deleted.
```

Task 6: Restore the Amazon EBS Snapshot

labuser (1).ppk 29°C Mostly clear 9:24 PM 4/3/2023

Lab 4 - Working with EBS | Instances | EC2 Manager | Course Modules: AWS Acc... | Lab 4 - Working with EBS | README | Volumes | EC2 Manager | + | - | X

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Volumes: N. Virginia vocabs/user2366056-Suneetha @ 7318-6515-7149 [Alt+S]

New EC2 Experience Tell us what you think

EC2 Dashboard EC2 Global View Events Tags Limits

Instances Instances Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts Scheduled Instances Capacity Reservations

Images AMIs

CloudShell Feedback Language labuser (1).ppk Show all 29°C Mostly clear

Volumes (1/3)

Name	Volume ID	Type	Size	IOPS	Throughput
vol-007cd1f098f77c1	gp2	8 GiB	100	-	-
vol-0c318f4765849149	gp2	8 GiB	100	-	-
My Volume	vol-0d10d525f2f83a0c5	gp2	1 GiB	100	-

Actions Create volume Modify volume Create snapshot Create snapshot lifecycle policy Delete volume Attach volume Detach volume Force detach volume Manage auto-enabled I/O Manage tags Fault injection

AMI Catalog Volumes Snapshots Lifecycle Manager Network & Security Security Groups Elastic IPs Placement Groups Key Pairs Network Interfaces Load Balancing Load Balancers Target Groups Auto Scaling Launch Configurations Auto Scaling Groups

Snapshots (1/1) Owned by me Search

Name	Snapshot ID	Size	Description	Storage...	Snapshot status
My Snapshot	snap-013c8ef099b54ee35	1 GiB	-	Standard	Completed

Actions Create snapshot Create image from snapshot Copy snapshot Modify permissions Manage fast snapshot restore Archive snapshot Restore snapshot from archive Change restore period Delete snapshot Manage tags

Snapshot ID: snap-013c8ef099b54ee35 (My Snapshot)

Details Permissions Storage tier Tags CloudShell Feedback Language labuser (1).ppk Show all 29°C Mostly clear

Lab 4 - Working with EBS | Instances | EC2 Manager | Course Modules: AWS Acc... | Lab 4 - Working with EBS | README | Create volume | EC2 Manager | + | - | X

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#createVolumeFromSnapshot:snapshotId=snap-013c8ef099b54ee35: N. Virginia vocabs/user2366056-Suneetha @ 7318-6515-7149 [Alt+S]

Availability Zone Info us-east-1a

Fast snapshot restore Info Not enabled for selected snapshot

Encryption Info Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances. Encrypt this volume

Tags - optional Info A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key Value - optional Name Restored Volume Remove Add tag You can add 49 more tags. Cancel Create volume

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences CloudShell Feedback Language labuser (1).ppk Show all 29°C Mostly clear

Lab 4 - Working with EBS | Instances | EC2 Manager | Course Modules: AWS Acc... | Lab 4 - Working with EBS | README | Attach volume | EC2 Manager | + | - | X

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#attachVolume:volumeId=vol-032d6ef213670b26: N. Virginia vocabs/user2366056-Suneetha @ 7318-6515-7149 [Alt+S]

Basic details

Volume ID vol-032d6ef213670b26 (Restored Volume)

Availability Zone us-east-1a

Instance Info i-0229dfc7ee6522a7b Only instances in the same Availability Zone as the selected volume are displayed.

Device name Info /dev/sdg Recommended device names for Linux: /dev/sda1 for root volume. /dev/sdf[0-9] for data volumes.

Never Linux kernels may rename your devices to /dev/xvdf through /dev/xvd internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.

Cancel Attach volume

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences CloudShell Feedback Language labuser (1).ppk Show all 29°C Mostly clear

AWS S3 (SIMPLE STORAGE SERVICE)

TASKS FOR CONFIGURING S3:

- 1.Log into the AWS Management Console.
- 2.Create an S3 bucket.
- 3.Upload an object to S3 Bucket.
- 4.Access the object on the browser.
- 5.Change S3 object permissions.
- 6.Setup the bucket policy and permission and test the object accessibility.

STEPS :

Step 1: Click on **create group**.

Step 2: Set up the bucket name. S3 bucket name are globally unique, choose a name which is available. Leave other settings as default and click on **create group**.

Step 3: Click on your bucket name.

Step 4: Click Upload.

Step 5: Click on Add Files , and choose a file from your computer.

Step 6: After choosing your file, click on Next.

Step 7: Click on Upload.

Step 8:Now you have a private S3 bucket with a private object uploaded, which means you cannot visit it through Internet.

Step 9:Now you have a private S3 bucket with a private object uploaded, which means you cannot visit it through Internet.

CHANGE BUCKET PERMISSIONS:

Step 10:Go back to your bcket and click on Permissions.

Step 11:Click on Everyone under the Public access, and click on Read object on the right of pop-up window. Then click on Save.

Step 12 :Now its state switches to Read Object - Yes

Step 13:Click on Overview, and click on your Object URL again .

Step 14:Notice the URL on your browser

S3 Management Console

Identity and access management

Amazon S3 > Buckets

Buckets (1) Info

Name AWS Region Access Creation date

samplebucket-458case0 US East (N. Virginia) us-east-1 Insufficient permissions April 3, 2023, 22:25:09 (UTC+05:30)

View Storage Lens dashboard

C Copy ARN Empty Delete Create bucket

Find buckets by name

CloudShell Feedback Language

27°C Mostly clear

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

ENG IN 03-04-2023 22:47

Step 1

S3 bucket

Identity and access management

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name mynewbucket

Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming.

AWS Region US East (N. Virginia) us-east-1

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

Choose bucket

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

ACLs disabled (recommended) All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using bucket policies.

ACLs enabled Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be controlled using ACLs.

CloudShell Feedback Language

27°C Mostly clear

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

ENG IN 03-04-2023 22:47

Step 2

Amazon S3

Identity and access management

Learn how to effectively use the S3 Storage Classes. Learn more

We've temporarily re-enabled the previous version of the S3 console while we continue to improve the new S3 console experience. Switch to the new console.

S3 buckets

Search for buckets

All access types

Create bucket Edit public access settings Empty Delete

2 Buckets 1 Regions

Bucket name	Access	Region	Date created
organization03	Error	US East (N. Virginia)	Dec 16, 2018 9:42:03 PM GMT-GB00
s3bucket180	Error	US East (N. Virginia)	Oct 8, 2020 4:22:24 PM GMT-0700

CloudShell Feedback Language

27°C Mostly clear

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Policy Terms of Use

ENG IN 03-04-2023 22:47

Step 2

Step 3

This bucket is empty. Upload new objects to get started.

Upload

Create folder

Actions

Upload an object

Set object properties

Set object permissions

Select files

Set permissions

Set properties

Review

Drag and drop files and folders here

Add files

permissions

Step 4

Upload

Next

Step 5

Manage users

User ID

Object permissions

organizationAdmin

organizationWhitelistOwner

Read

Write

Access for other AWS account

Add account

Account

Objects

Object permissions

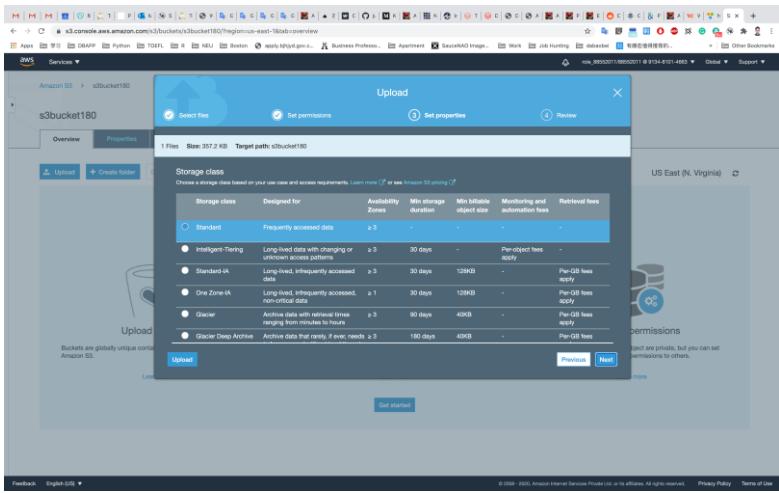
Manage public permissions

Do not grant public read access to this object (Recommended)

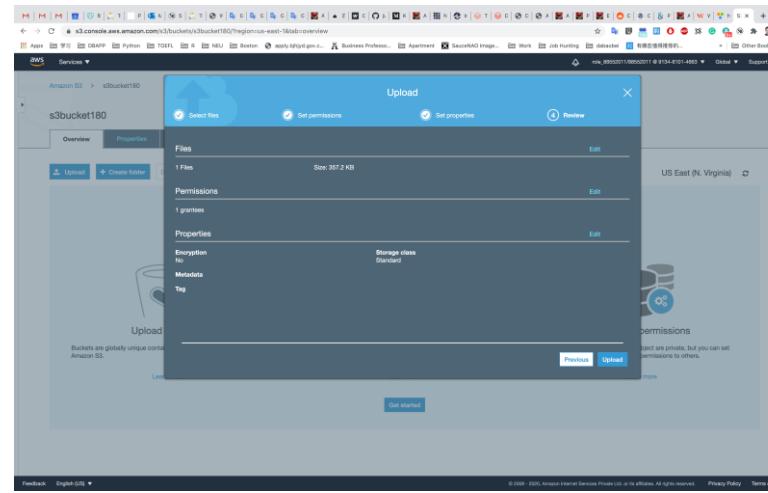
Next

Step 6

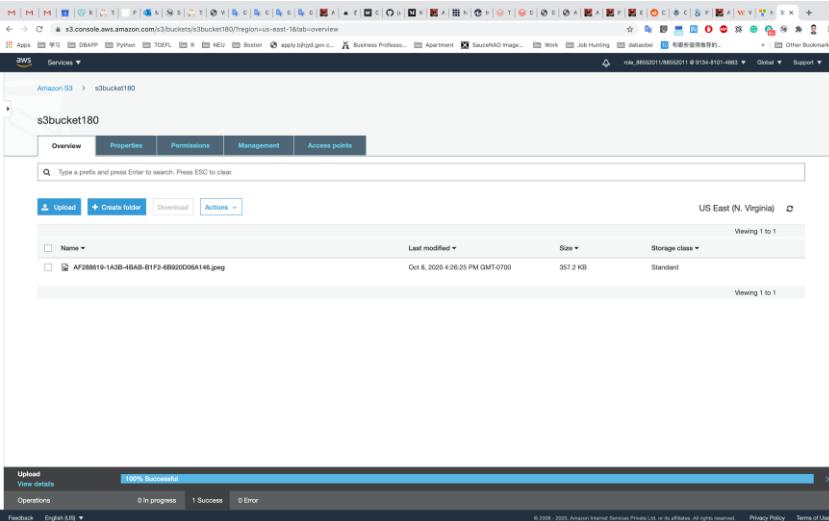
Step 7



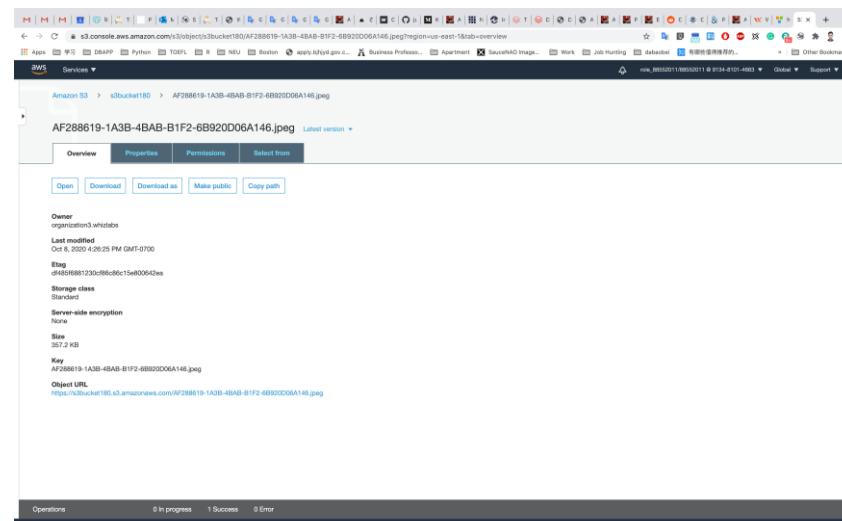
Step 8



Step 9



Step 10



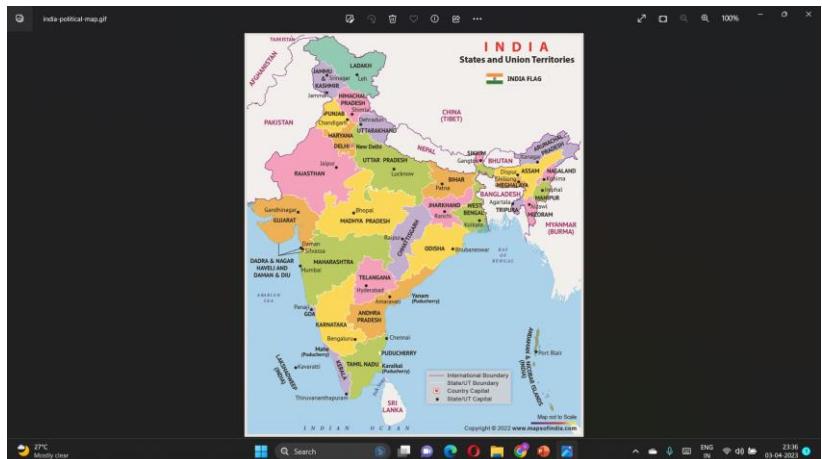
Step 11

The screenshot shows the AWS S3 console with the path `s3://s3bucket1180/AF288619-1A3B-4BAB-B1F2-6B920D06A146.jpeg`. The main content area displays the object's details, including its name, size (1.14 MB), and type (image/jpeg). Below this, the 'Permissions' tab is selected, showing access controls for the object owner and other AWS accounts. The object owner has full permissions (Read object, Read object permissions, Write object permissions) for the canonical ID `asf1156cd5374ecfe0c300ec0395ecfa0587ff02016a94cd38c2fa1d2296`. Other AWS accounts can also be granted permissions via the 'Add account' button. The 'Public access' section shows that the object is accessible by everyone. At the bottom, there are tabs for 'Overview', 'Properties', and 'Permissions', along with a 'Select from' dropdown.

Step 12

This screenshot shows the same AWS S3 object permissions page as the previous one, but with different access settings. The object owner now has full permissions, while other AWS accounts have restricted permissions (Read object, Read object permissions, Write object permissions). The 'Public access' section remains the same, showing it is accessible by everyone. The interface is identical to Step 12, with tabs for 'Overview', 'Properties', and 'Permissions'.

Step 13

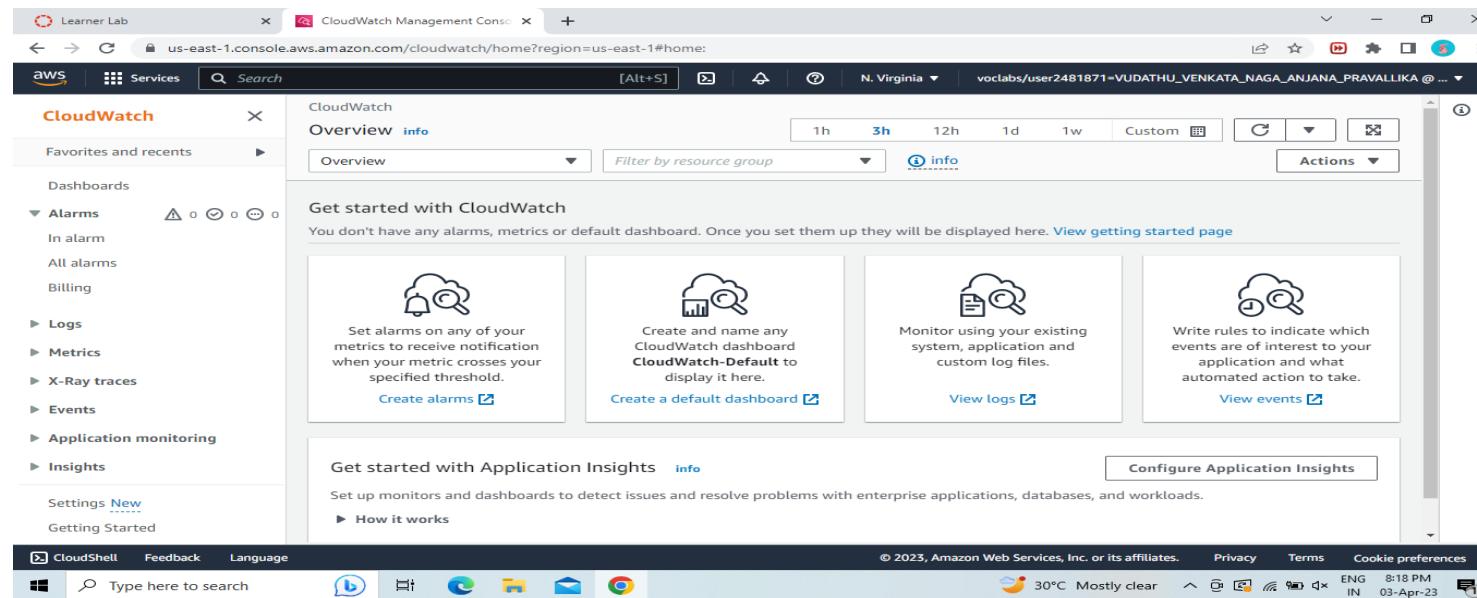


Step 14

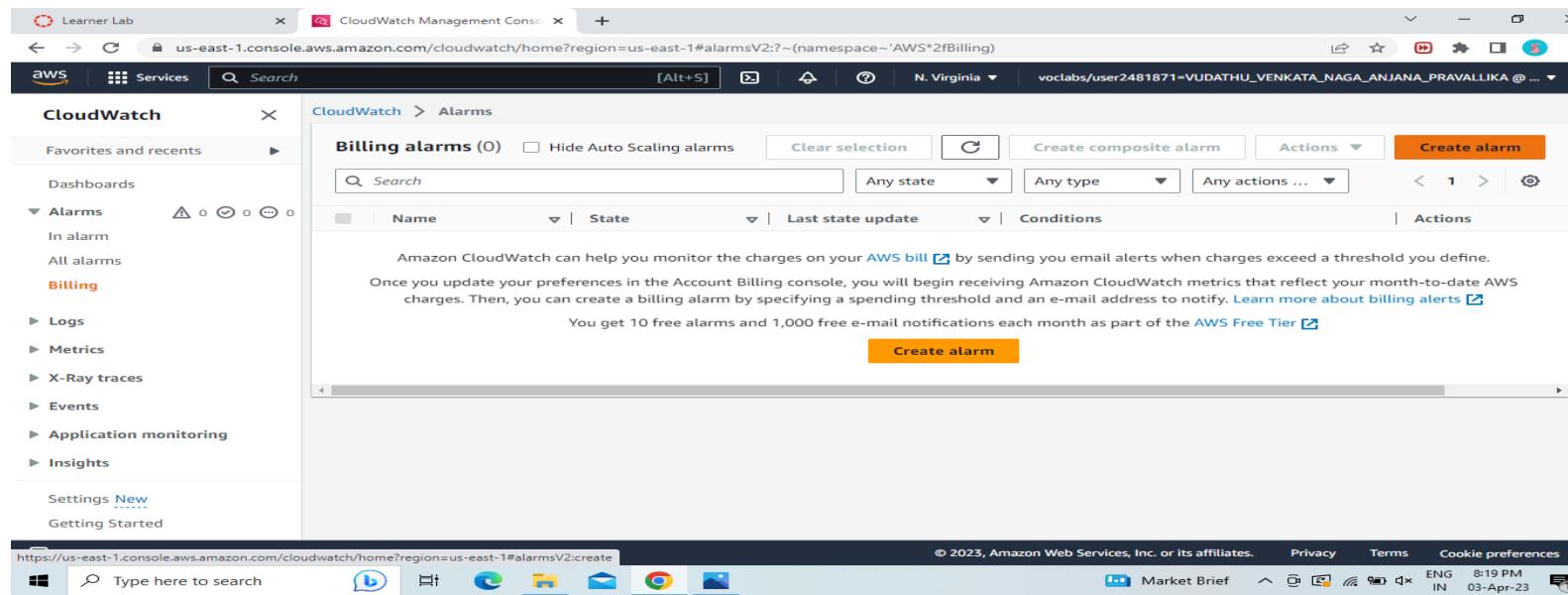
AWS CLOUDWATCH

PROCEDURE

1.Go to AWS Services,Click on CloudWatch and then in the Dashboard go to Alarms section and select Billings.



2.Then Click on CREATE ALARM.



3.Then follow the steps.

In the first step it will ask us to Specify metric and conditions.Click on Select Metric.

Change the Currency to Rupee.

In the Conditions section choose the EstimatedCharges like

Greater/GreaterEqual/Lowerequal/Lower and also define the threshold value.

4.Click on Next.

The image contains two side-by-side screenshots of the AWS CloudWatch Management Console. Both screenshots show the 'Create alarm' wizard.

Screenshot 1 (Left): Shows the 'Specify metric and conditions' step. It displays a graph of 'EstimatedCharges' over time (03/28 to 04/02) with a red threshold line at 1.0. The 'Metric' section shows 'Namespace: AWS/Billing', 'Metric name: EstimatedCharges', 'Currency: USD', and 'Statistic: Maximum'. The 'Conditions' section is collapsed.

Screenshot 2 (Right): Shows the 'Conditions' step. It defines a static threshold of 100 Rupee (Greater than threshold). Other options like Anomaly detection and various comparison operators (> threshold, >= threshold, <= threshold, < threshold) are also shown. The 'Additional configuration' section is collapsed.

5. Now for Configure Actions choose Create new topic. Give a name to the topic and enter your email to receive a notification. Click on Create Topic, then Next.

The screenshot shows the 'Step 4: Preview and create' screen of the CloudWatch Management Console.

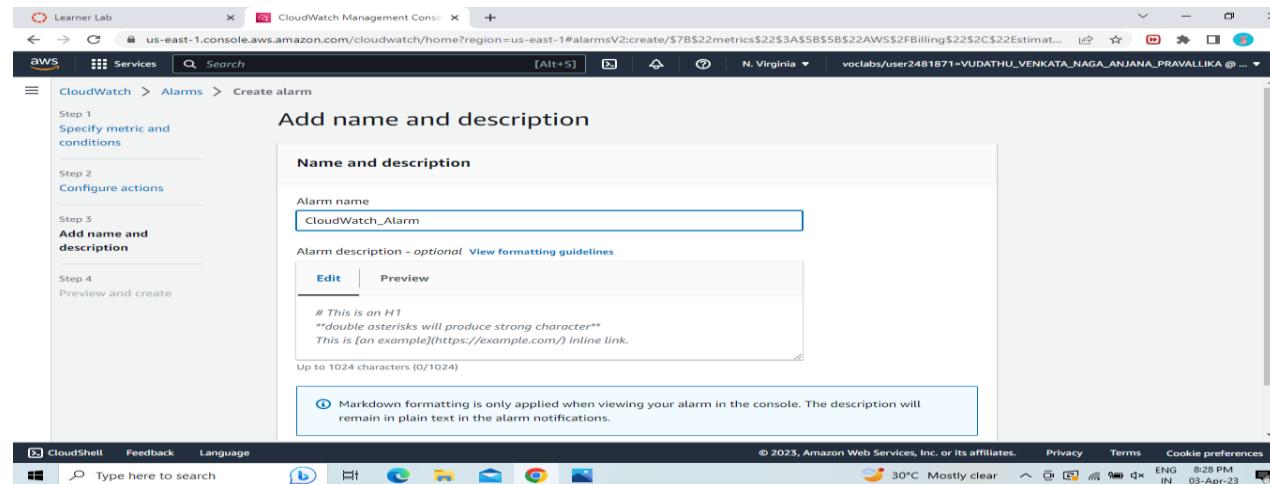
Send a notification to the following SNS topic: This section is expanded. It shows three options: 'Select an existing SNS topic' (radio button), 'Create new topic' (radio button, selected), and 'Use topic ARN to notify other accounts'. Below this, a text input field 'Create a new topic...' contains 'CloudWatch_Alarms'. A note states: 'The topic name must be unique.' and 'CloudWatch topic names can contain only alphanumeric characters, hyphens (-) and underscores (_)'.

Email endpoints that will receive the notification... This section shows an input field containing 'pravallikavudathu2003@gmail.com' and 'user1@example.com, user2@example.com'.

Action: Buttons for 'Create topic' and 'Add notification' are visible.

Auto Scaling action: This section is collapsed.

6.Give a name to your Alarm and Click on next.



7.You will get a AWS Notification-Subscription Confirmation mail to the email which you have provided.Click on Confirm Subscription.Then it will open a window showing Subscription Confirmed.

The left screenshot shows an email from 'AWS Notifications' with the subject 'AWS Notification - Subscription Confirmation'. The message body contains:

You have chosen to subscribe to the topic:
arn:aws:sns:us-east-1:265498189509:CloudWatch_Alarms

To confirm this subscription, click or visit the link below. (If this was in error no action is necessary.)
[Confirm subscription](#)

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [sns@amazon.com](#).

The right screenshot shows a browser window with the URL 'sns.us-east-1.amazonaws.com/confirmation.html?TopicArn=arn:aws:sns:us-east-1:265498189509:CloudWatch_Alarms&Token=2336412f7fb687f5d51e5e2425...'. The page displays:

Subscription confirmed!

You have successfully subscribed.
Your subscription's ID is:
arn:aws:sns:us-east-1:265498189509:Cloudwatch_Alarms:be0de541-e7d9-4bc1-ad93-dc94a2972d8b

If it was not your intention to subscribe, [click here to unsubscribe](#).

8.Preview the details you have entered .

9.Click on Create alarm.This will Create your Alarm.

The screenshot shows the AWS CloudWatch Management Console interface. The left sidebar is titled "CloudWatch" and includes sections for Favorites and recents, Dashboards, Alarms (selected), Logs, Metrics, X-Ray traces, Events, Application monitoring, Insights, Settings, and Getting Started. The main content area is titled "CloudWatch > Alarms" and displays a table for "Billing alarms". The table has columns for Name, State, Last state update, Conditions, and Actions. There is one entry: "CloudWatch_Alarm" (State: Insufficient data, Last state update: 2023-04-03 20:30:53, Conditions: EstimatedCharges > 1000 for 1 datapoints within 6 hours, Actions: Actions enabled). A green banner at the top of the main content area says "Successfully created alarm CloudWatch_Alarm." A "Create alarm" button is visible in the top right of the main content area. The browser address bar shows the URL: us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:~(Page~MetricSelection~AlarmType~MetricAlarm~AlarmData~Metrics...).

1)In the search box to the right of Services, search for and choose Lambda to open the AWS Lambda console.

2)Choose Create function.

3)In the Create function screen, configure these settings:

>Choose Author from scratch

>Function name: myStopinator

>Runtime: Python 3.8

>Choose Change default execution role

>Execution role: Use an existing role

>Existing role: From the dropdown list, choose myStopinatorRole

4)Choose Create function.

5) Choose Add trigger.

6)Choose the Select a trigger dropdown menu, and select EventBridge (CloudWatch Events).

7)For the rule, choose Create a new rule and configure the settings and click add.

Below the Function overview pane, choose Code, and then choose `lambda_function.py` to display and edit the Lambda function code.

In the Code source pane, delete the existing code. Copy the following code, and paste it in the box:

```
import boto3
region = '<REPLACE_WITH_REGION>'
instances = ['<REPLACE_WITH_INSTANCE_ID>']
ec2 = boto3.client('ec2', region_name=region)

def lambda_handler(event, context):
    ec2.stop_instances(InstanceIds=instances)
    print('stopped your instances: ' + str(instances))
```

9) Replace the `<REPLACE_WITH_REGION>` placeholder with the actual Region that you are using. To do this:

10) Choose on the region on the top right corner and use the region code. For example, the region code for US East (N. Virginia) is `us-east-1`.

11) Verify that an EC2 instance named `instance1` is running in your account, and copy the `instance1` instance ID.

12) Return to the AWS Lambda console browser tab, and replace `<REPLACE_WITH_INSTANCE_ID>` with the actual instance ID that you just copied.

13) Choose the File menu and Save the changes. Then, in the top-right corner of the Code source box, choose Deploy.

The screenshot shows two windows side-by-side. On the left is the AWS Management Console search results page for 'lambda'. It lists various services like Lambda, CodeBuild, AWS Signer, and Amazon Inspector. On the right is a code editor window titled 'lambda_function.py' containing the following Python code:

```
1 import boto3
2 region = 'us-east-1'
3 instances = ['i-0317320fde6661814']
4 ec2 = boto3.client('ec2', region_name=region)
5
6 def lambda_handler(event, context):
7     ec2.stop_instances(InstanceIds=instances)
8     print('stopped your instances: ' + str(instances))
```

The screenshot shows the AWS Lambda service landing page. It features a dark header with the AWS logo and 'Lambda' text. Below the header, there's a main section with the heading 'AWS Lambda' and the subtext 'lets you run code without thinking about servers.' It includes a 'Create a function' button and a 'Get started' section with a 'Create a function' button. At the bottom, there's a 'How it works' section showing a code snippet for a Node.js runtime:

```
1 exports.handler = async (event) => {
2     console.log(event);
3     return 'Hello from Lambda!';
4 }
```