

M.Suneetha

20A31A04E0

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

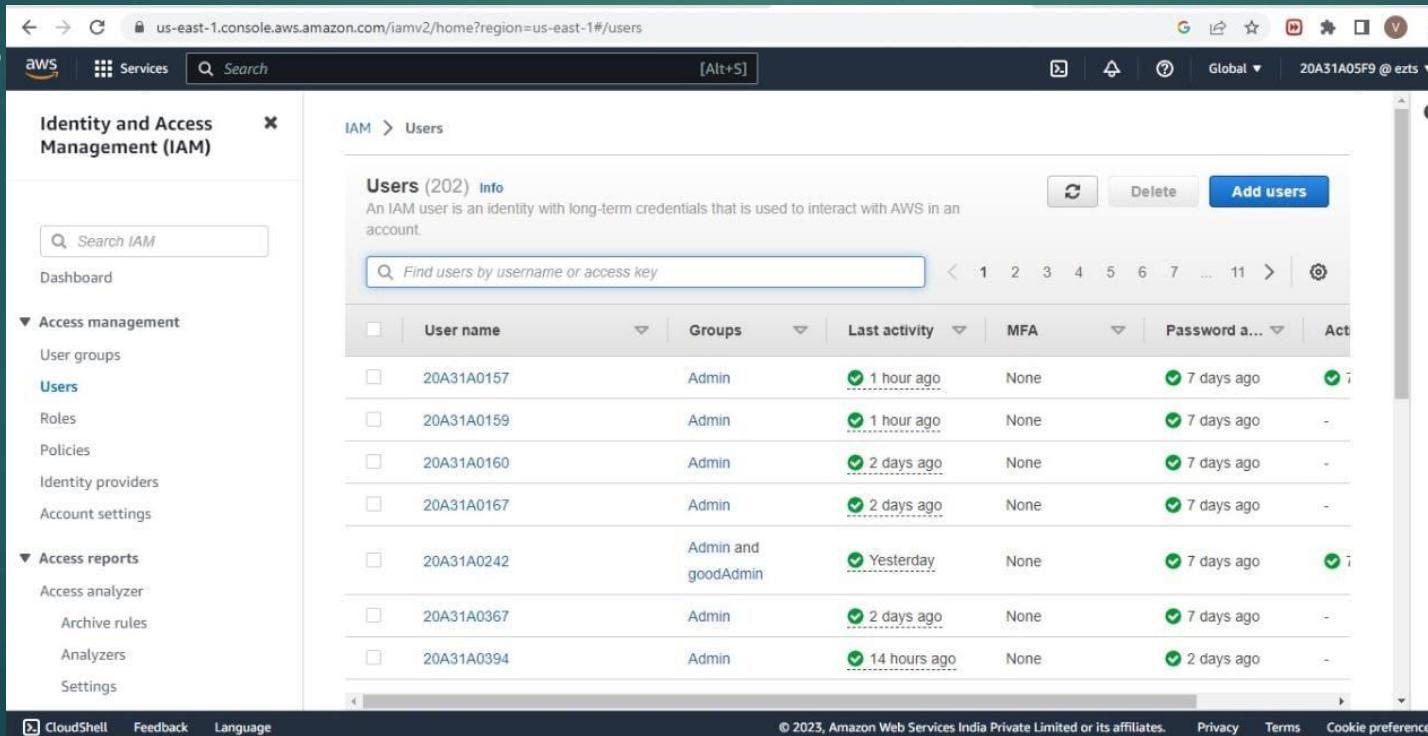
AWS COMMAND LINE INTERFACE

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



The screenshot shows the AWS Management Console interface for the Identity and Access Management (IAM) service. The left sidebar has a 'Search IAM' bar and sections for 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings), 'Access reports' (Access analyzer, Archive rules, Analyzers, Settings), and links for CloudShell, Feedback, Language, and cookie preferences. The main content area is titled 'Users (202)' and includes a search bar, a table of user details, and pagination controls. The table columns are: User name, Groups, Last activity, MFA, Password a..., and Action. The table lists several users, each with a checkbox, their group (Admin or Admin and goodAdmin), their last activity time (e.g., 1 hour ago, Yesterday, 2 days ago, 14 hours ago), and their password status (7 days ago). The 'Action' column contains a small green checkmark icon.

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 Identity and Access Management (IAM) service in a web browser. The URL is `us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/details/20A31A05D2?section=security_credentials`. The page displays details for a user named "20A31A05D2".

Identity and Access Management (IAM)

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

Permissions: Groups (1), Tags, **Security credentials** (highlighted), 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](#)

Actions: Remove, Resync, Assign MFA device

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 Identity and Access Management (IAM) service interface. The left sidebar is titled "Identity and Access Management (IAM)" and includes sections for "Dashboard", "Access management" (User groups, Users, Roles, Policies, Identity providers, Account settings), and "Access reports" (Access analyzer, Archive rules, Analyzers, Settings). The main content area is titled "Access keys (1)". It displays a single access key named "AKIATR4OXV3QNPAMUQBM". The key details are as follows:

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

Below the access key table, there is a section titled "SSH public keys for AWS CodeCommit (0)".

At the bottom of the page, there are links for CloudShell, Feedback, Language, © 2023, Amazon Web Services India Private Limited or its affiliates., Privacy, Terms, and Cookie preferences.

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

AWS Services Search [Alt+S] Global 20A31A05F9 @ eztv

IAM > Users > 20A31A05D2 > Create access key

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

AWS Services Search [Alt+S] Global 20A31A05F9 @ eztv

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

AWS Services Search [Alt+S] Global 20A31A05F9 @ eztv

IAM > Users > 20A31A05D2 > Create access key

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.

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]: AKIATR4OXV3QD5GD6MZZ
AWS Secret Access Key [None]: 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
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.

Learner Lab

Launch an instance | EC2 Manag...

EC2 > Instances > Launch an instance

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name: e.g. My Web Server

Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat S

Software Image (AMI)

Amazon Linux 2023 AMI 2023.0.2... [read more](#)

ami-0c997f1452d08778

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GB

Free tier: In your first year includes 750 hours of t2.micro (or t2.micro in the Regions in which t2.micro is unavailable) instance usage on free tier

Cancel Launch instance Review commands

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

CloudShell Feedback Language 30°C Mostly cloudy 03-04-2023

Learner Lab

Launch an instance | EC2 Manag...

Connect to instance | EC2 Manag...

EC2 Instance Connect

EC2 > Instances > Launch an instance

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.0.2... [read more](#)

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GB

Last login: Mon Apr 3 13:16:51 2023 from 18.206.107.29
[ec2-user@ip-172-31-56-87 ~]\$ whoami
ec2-user
[ec2-user@ip-172-31-56-87 ~]\$

i-Oca0332f686706307 (myserver)
PublicIPs: 107.23.105.224 PrivateIPs: 172.31.56.87

CloudShell Feedback Language 30°C Mostly cloudy 03-04-2023

Learner Lab

Instances | EC2 Management Co...

Connect to instance | EC2 Manag...

EC2 Instance Connect

ALLv1-43288

Allv1-43288 > Modules > Learner Lab > Learner Lab

Used \$0.1 of \$100 03:22 Start Lab End Lab AWS Details Readme Reset

Home Modules Discussions Putty Configuration

Putty Configuration

Category: Appearance Behaviour Translation Selection Colours

Connections: Data Proxy SSH

SSH: Key Host keys Open Auth Credentials (GSSAPI) TTY X11 Tunnels Bugs Mac bugs Serial Telnet Rsync SUDO/P

Public-key authentication with C:\Users\lalitha\Downloads\myserver.ppk

Certificate to use with the private key:

Page to provide authentication responses:

Plugin command to use:

Choose Connection Set Seconds between keepalives to 30

This allows you to keep the Putty session open for a longer period of time.

Configure your Putty session:

Choose Session Host Name (or IP address): Copy and paste the IPv4 Public IP address for the instance. To find it, return to the EC2 Console and choose Instances. Check the box next to the instance and in the Description tab copy the IPv4 Public IP value.

Back in Putty, in the Connection list, expand SSH Choose Auth (don't expand it) Choose Browse Browse to and select the .ppk file that you downloaded Choose Open to select it Choose Open

Choose Yes, to trust the host and connect to it.

When prompted login as, enter: ec2-user

Next < Previous

CloudShell Feedback Language 30°C Mostly cloudy 03-04-2023

ec2-user@ip-172-31-56-87:

login as: ec2-user
Authenticating with public key "myserver"
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
Last login: Mon Apr 3 13:20:42 2023 from 18.206.107.29
[ec2-user@ip-172-31-56-87 ~]\$ whoami
ec2-user
[ec2-user@ip-172-31-56-87 ~]\$

CloudShell Feedback Language 30°C Mostly cloudy 03-04-2023



A screenshot of the AWS EC2 Management Console. The main view shows a table of running 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 screenshot shows the AWS VPC Management Console with the 'Service Health' tab selected. It displays various resources and their counts across different regions. Key sections include:

- Resources by Region:** Shows counts for VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, Peering connections, Security, Network ACLs, and Security groups.
- Settings:** Includes links to EC2 Instances, Zones, and Console Experiments.
- Additional Information:** Links to VPC Documentation, All VPC Resources, Forums, and Report an Issue.
- AWS Network Manager:** Provides tools and features to help manage and monitor your network on AWS.
- Site-to-Site VPN Connections:** Information about Amazon VPC enabling users to use their own isolated resources.

This screenshot shows the 'Create VPC' wizard. The 'VPC settings' step is displayed, where the user has chosen 'VPC and more'. The 'Preview' panel on the right shows the network architecture:

- VPC:** LAB-vpc
- Subnets (2):** us-east-1a (with subnets LAB-subnet-public1-us-east-1a and LAB-subnet-private1-us-east-1a) and us-east-1b (with subnets LAB-subnet-public1-us-east-1b and LAB-subnet-private1-us-east-1b).
- Route tables (2):** LAB-rtb-public and LAB-rtb-private1-us-east-1b.

This screenshot continues the 'Create VPC' wizard. The 'Preview' panel now includes configuration for NAT gateways and VPC endpoints:

- NAT gateways (0):** None, In 1 AZ, 1 per AZ.
- VPC endpoints (0):** None, S3 Gateway.

The left screenshot shows the 'Create VPC' wizard step 2. It displays two CIDR blocks: 'Public subnet CIDR block in us-east-1a' (10.0.0.0/24) and 'Private subnet CIDR block in us-east-1a' (10.0.1.0/24). A new subnet 'LAB-subnet-public1-us-east-1a' is being created with CIDR 10.0.2.0/24. The right screenshot shows the 'Your VPCs' page for 'LAB-vpc'. It lists the subnet 'LAB-subnet-public1-us-east-1a' and its associated route table 'rtb-lab-public1-us-east-1a'.

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

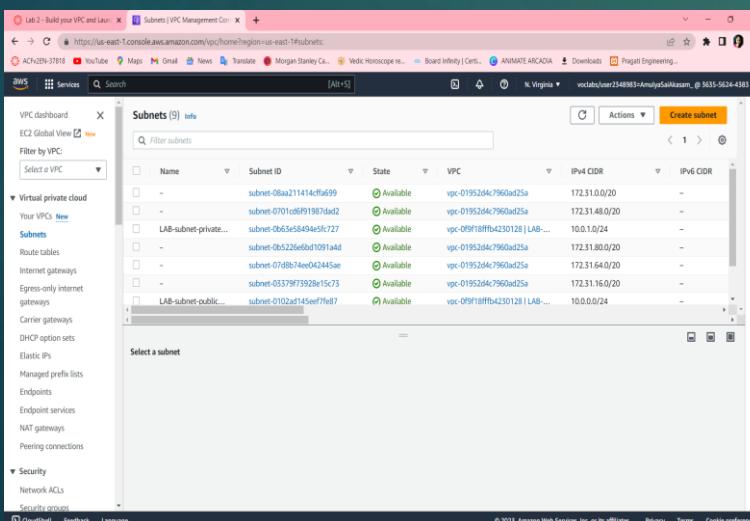
Step 5 : Leave lab-subnet-private1-us-east-1a and also select lab-subnet-private2

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

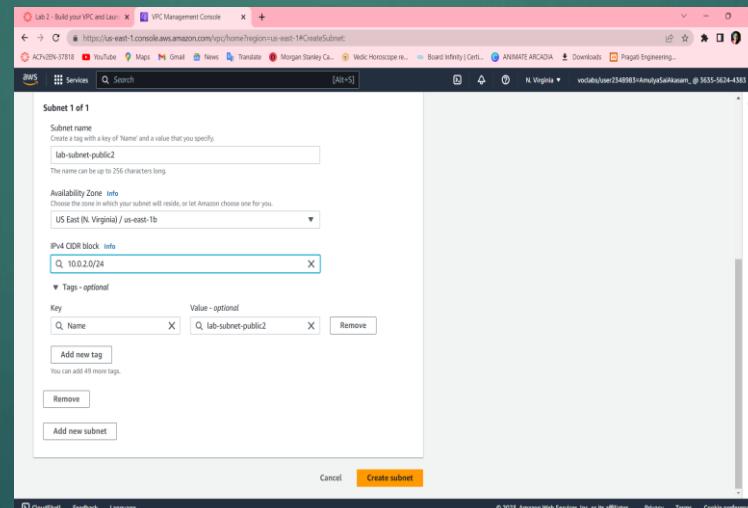
Step 9: Choose SAVE ASSOCIATIONS



Subnets (9) Info

Name	Subnet ID	VPC	State	IPv4 CIDR	IPv6 CIDR
subnet-08aa211414cffa699	vpc-01952d4c7960ad25a	Available	172.31.0.0/20	-	-
subnet-07010ef9f1987ad2	vpc-01952d4c7960ad25a	Available	172.31.48.0/20	-	-
LAB-subnet-private...	subnet-0653e58454e5fc727	Available	vpc-0591ff8fffb423012b [LAB-...]	10.0.1.0/24	-
subnet-085226febf10911ad	vpc-01952d4c7960ad25a	Available	172.31.80.0/20	-	-
subnet-078864ee02445ae	vpc-01952d4c7960ad25a	Available	172.31.64.0/20	-	-
subnet-0337973928e15c73	vpc-01952d4c7960ad25a	Available	172.31.16.0/20	-	-
LAB-subnet-public...	subnet-0102ad7145eef7fe7	Available	vpc-0591ff8fffb423012b [LAB-...]	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.

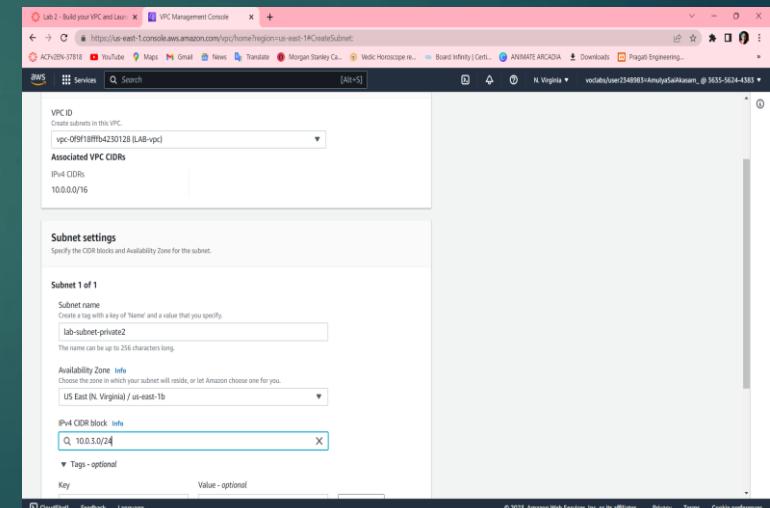
Availability Zone info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1b

IPv4 CIDR block info

Tags - optional

Add new tag
Key Name Value - optional
Add new tag
Remove
Add new subnet

Create subnet!



Subnet settings

Subnet 1 of 1

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

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

Tags - optional

Cancel Create subnet!

Lab 2 - Build your VPC and Lab 1 Subnets | VPC Management Console

You have successfully created 1 subnet: subnet-0de9853ca1053843c

Subnets (1) Info Actions Create subnet

Subnet ID: subnet-0de9853ca1053843c

Name: lab-subnet-private2 Subnet ID: subnet-0de9853ca1053843c State: Available VPC: vpc-0f9f18ffbd4230128 | LAB... IPv4 CDR: 10.0.0/24 IPv6 CDR: -

Select a subnet

Available subnets (2/4)

Name Subnet ID IPv4 CDR IPv6 CDR Route table ID

LA8-subnet-private1-us-east-1a	subnet-0b63e58d94e5f727	10.0.1.0/24	-	rtb-0d57b819393ba1c / LAB-rtb-pr...
lab-subnet-private2	subnet-0de9853ca1053843c	10.0.3.0/24	-	Main (rtb-0fa7952bfaded8551)

Selected subnets

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

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

Lab 2 - Build your VPC and Lab 1 Route tables | VPC Management Console

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)

Name Subnet ID IPv4 CDR IPv6 CDR Route table ID

LA8-subnet-private1-us-east-1a	subnet-0b63e58d94e5f727	10.0.1.0/24	-	rtb-0d57b819393ba1c / LAB-rtb-pr...
lab-subnet-private2	subnet-0de9853ca1053843c	10.0.3.0/24	-	Main (rtb-0fa7952bfaded8551)

Selected subnets

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

Cancel Save associations

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

Lab 2 - Build your VPC and Lab 1 Route tables | VPC Management Console

You have successfully updated subnet associations for rtb-0895a2f3740a50765 / LAB-rtb-public.

Route tables (5) Info Actions Create route table

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

rtb-0352820691af822e	Work Public Route Table	subnet-0267afdf31dc7e...	-	No	vpc-0f8fad1cb0fd053b Wo...
rtb-0d67952bfaded8551	-	-	-	Yes	vpc-0f9f18ffbd4230128 LAB...
rtb-0d0077a50aa1769ad	-	-	-	Yes	vpc-0f8fad1cb0fd053b Wo...
rtb-0b891f616578f82fe	-	-	-	Yes	vpc-01952d4c7960ad25a

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 screenshots of the AWS VPC Management Console, illustrating the steps to create a security group and add an inbound rule.

Screenshot 1: Create security group
The first screenshot shows the "Create security group" page. The security group name is "Web Security Group", with a description "Enable HTTP access". Under "Basic details", there is a VPC named "vpc-0f9f18fffb4230128". The "Inbound rules" section shows one rule: "HTTP" on port "80" from "Anywhere" with the description "Permit web requests".

Screenshot 2: Add rule
The second screenshot shows the "Add rule" dialog for the "Outbound rules" tab. It shows a single rule: "All traffic" on port "0.0.0.0/0". Below it, the "Tags - optional" section indicates "No tags associated with the resource".

Screenshot 3: Security group details
The third screenshot shows the "sg-0f15c53fab20c8729 - Web Security Group" details page. It lists the security group name, ID, description, owner, and inbound/outbound rule counts. The "Inbound rules" tab is selected, showing the rule added in the previous step: "HTTP" on port "80" from "Anywhere" with the description "Permit web requests".

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
```

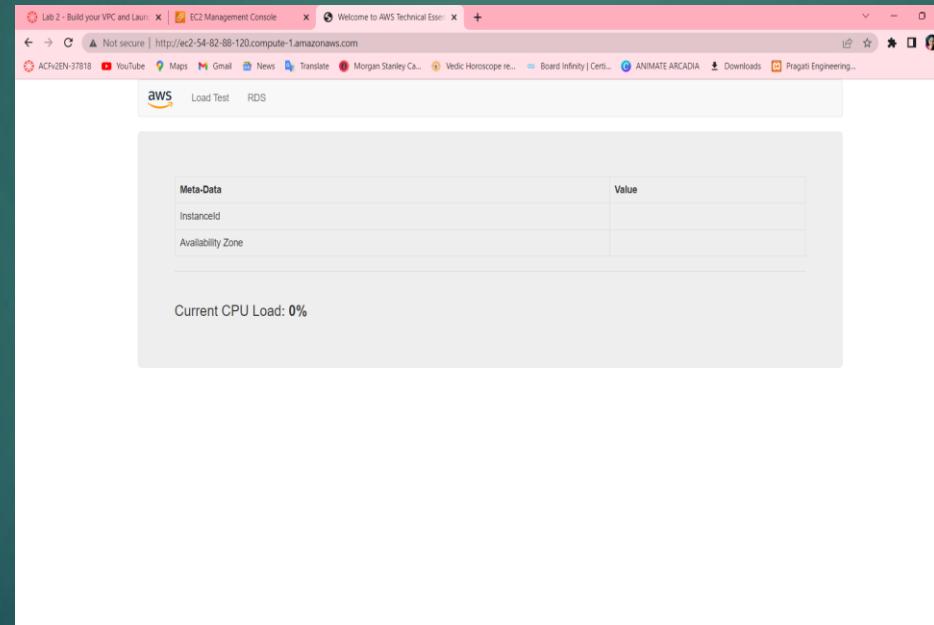
Step 6: At the bottom SUMMARY panel choose launch instance ,click on view instances

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)

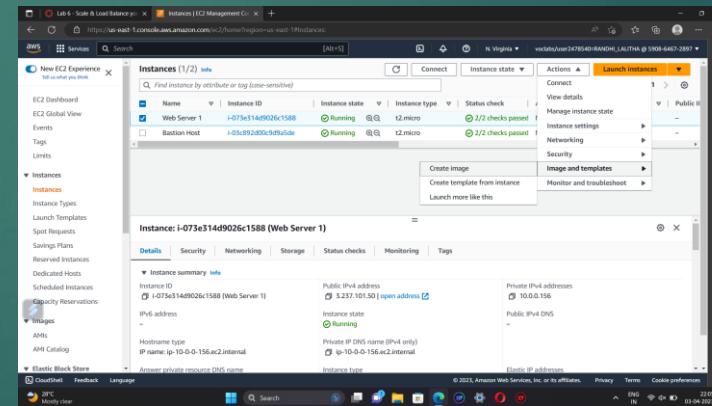
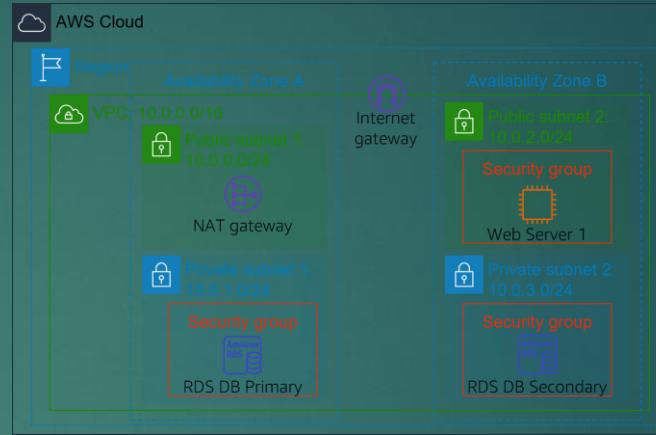
Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances.

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

Procedure:

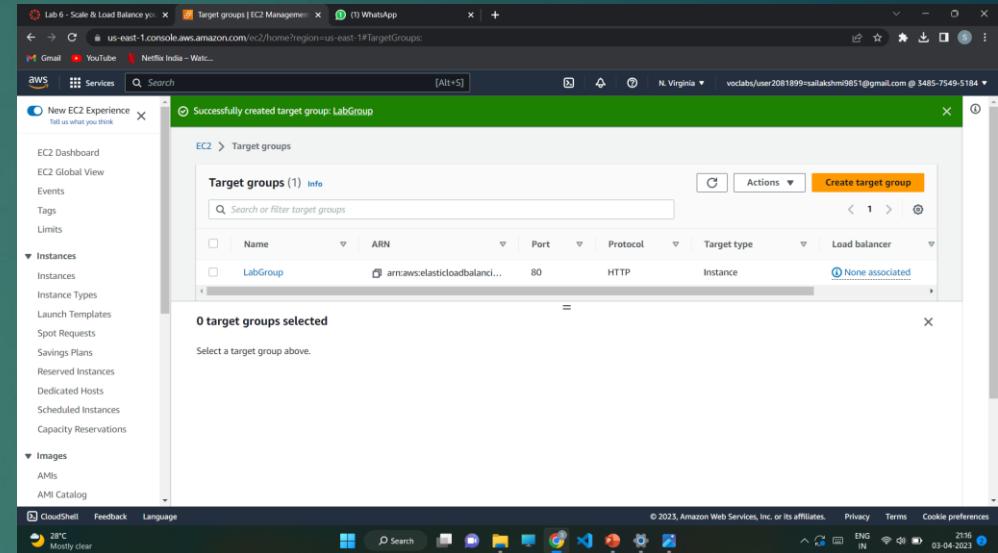
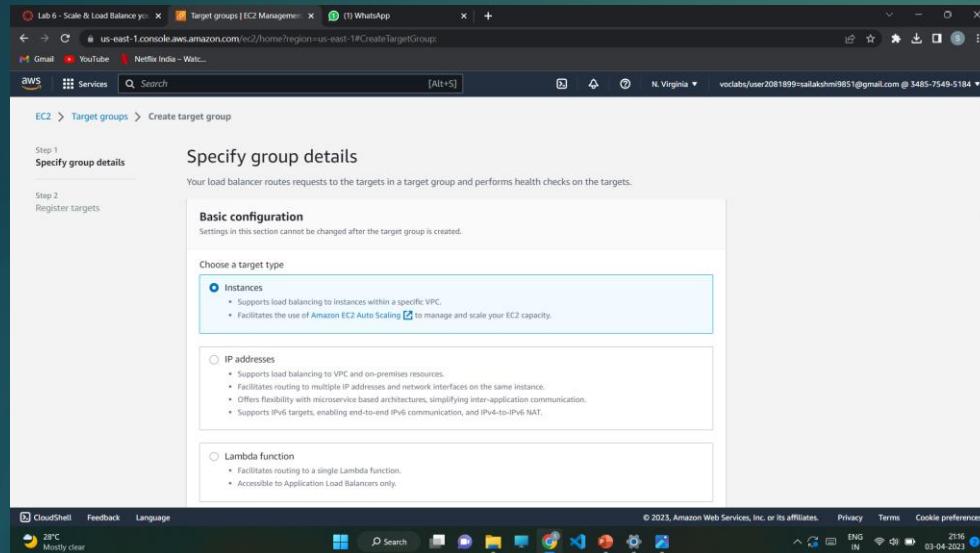
Task1: Creating an AMI for Auto Scaling

- ❖ 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.

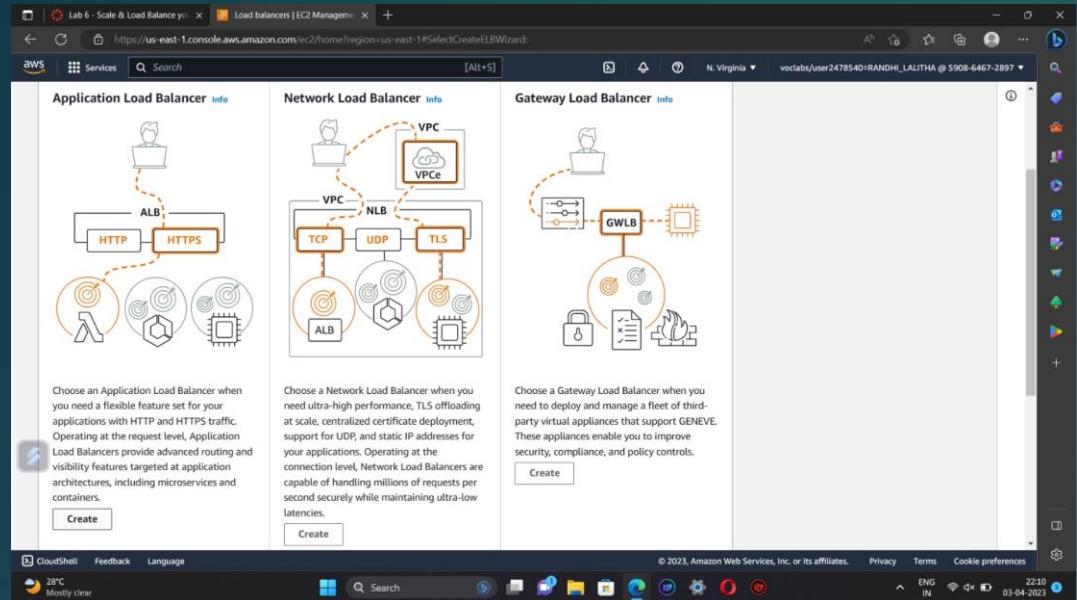


Task 2: Creating a load balancer

- ❖ 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-0dec0cta646139b177

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	Info
HTTP	: 80 1-65535	Forward to	LabGroup 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

Tags Edit

None

Attributes

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

Cancel 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.

EC2 > Launch configurations

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.

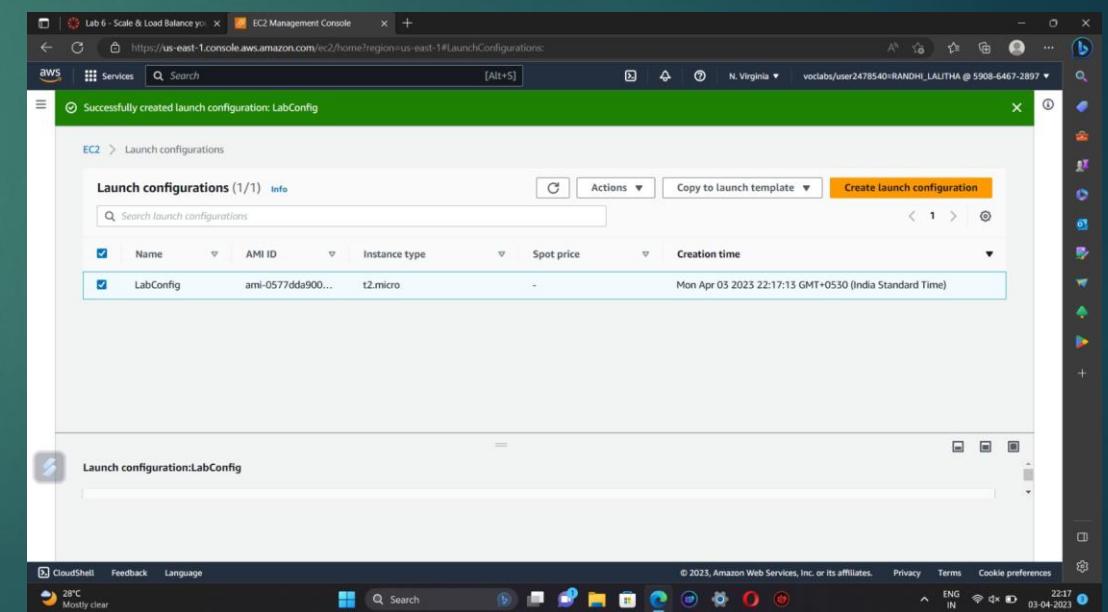
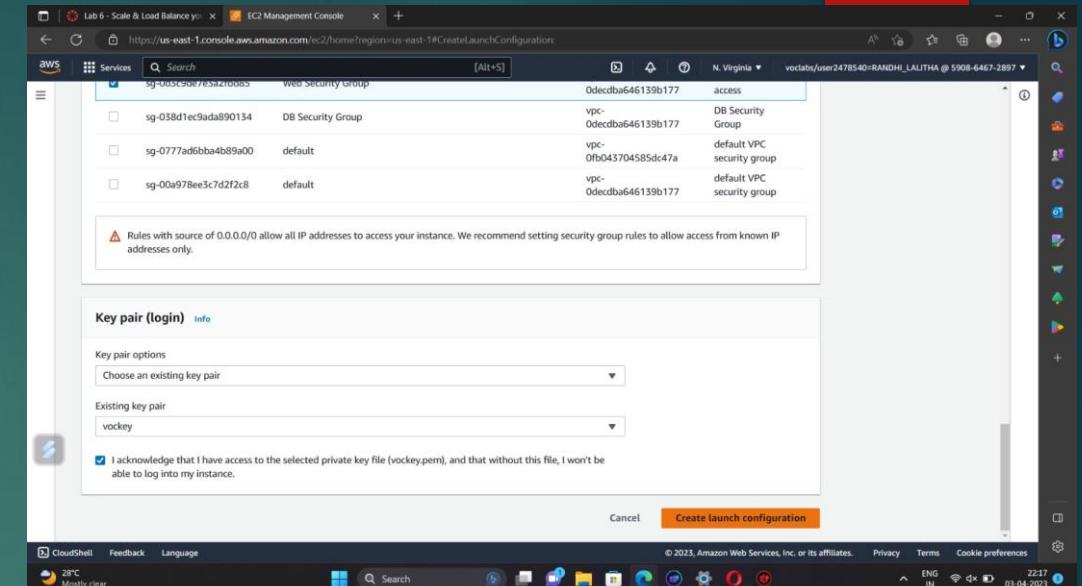
Create launch configuration

Select a launch configuration above

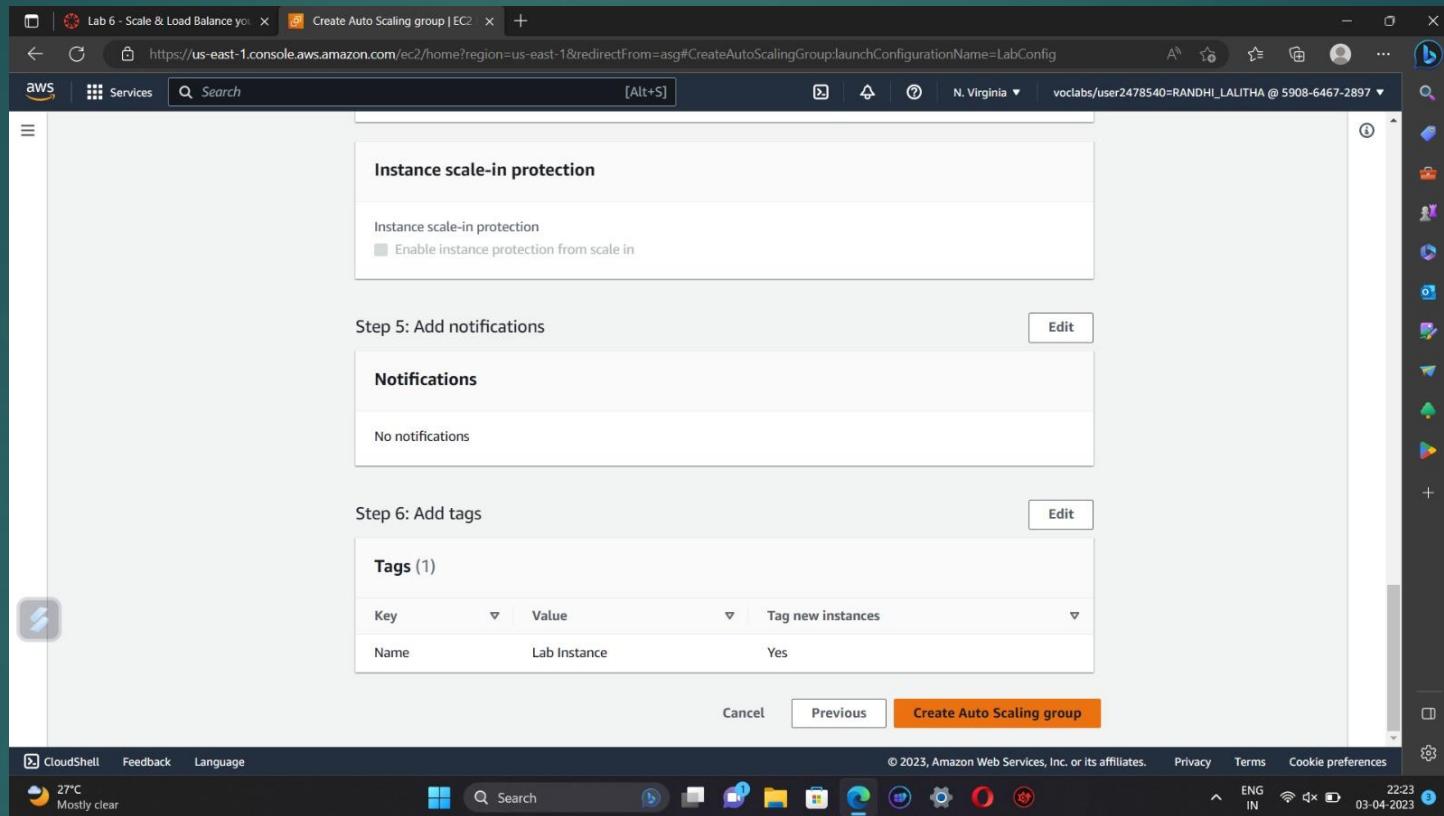
- ❖ Click create load balancer.

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**

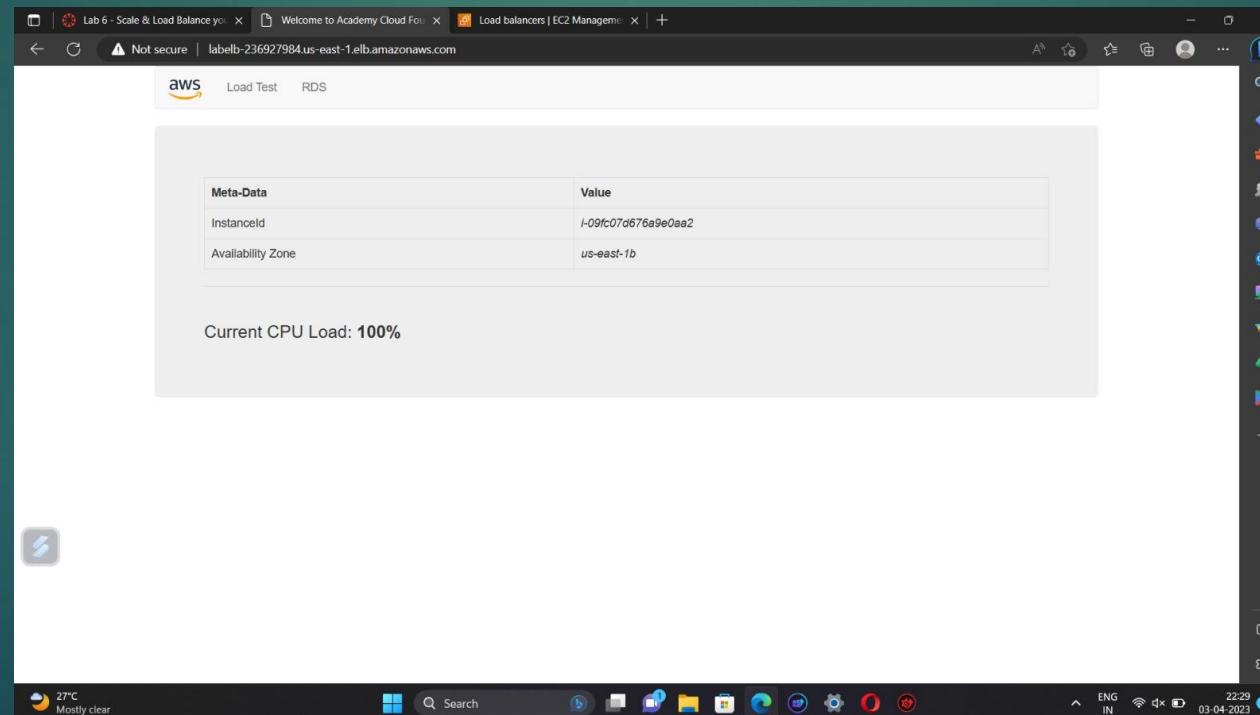


- ❖ Specify the values under Group size.
- ❖ Under **Scaling policies**, choose *Target tracking scaling policy* and name the policy. Specify metric type and target value. Then add a tag and click create auto scaling group.



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.

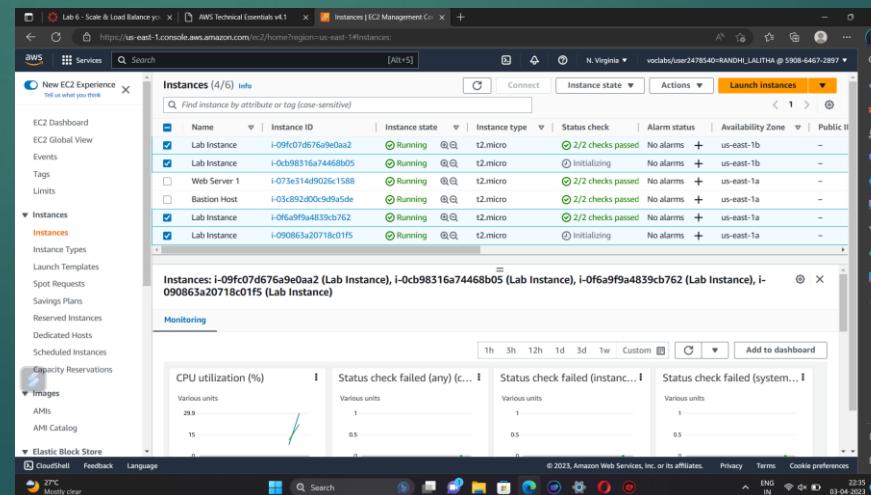


Task 5: Test Auto Scaling

- ❖ 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.

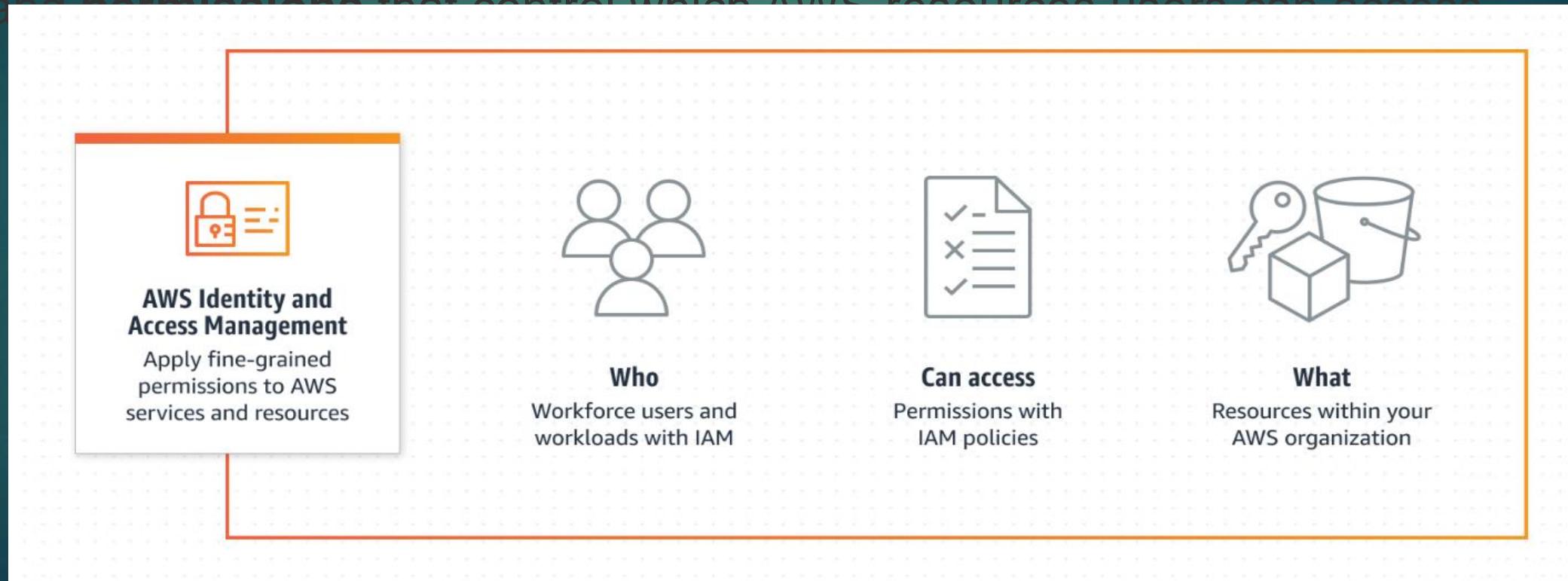
Click **Load Test** beside the AWS logo.This will cause the application to generate high loads.

- ❖ 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 services like IAM, Resource Access Manager, and Serverless Application Repository. The main content area displays the 'Security, Identity, & Compliance' section under the IAM category, listing various services such as Resource Access Manager, Cognito, Secrets Manager, GuardDuty, Amazon Inspector, Amazon Macie, IAM Identity Center, Certificate Manager, Key Management Service, CloudHSM, Directory Service, WAF & Shield, AWS Firewall Manager, AWS Artifact, Security Hub, Detective, AWS Signer, AWS Private Certificate Authority, AWS Audit Manager, Security Lake, and Amazon Verified Permissions.

The screenshot shows the IAM Management Console. The left sidebar has 'Identity and Access Management (IAM)' selected. Under the 'Users' section, it shows a list of 202 users. The right side of the screen displays a table with columns for User name, Groups, Last activity, MFA, Password age, and Active key age. At the bottom right of the user list, there is a blue 'Add users' button.

User name	Groups	Last activity	MFA	Password age	Active key age
20A31A0157	Admin	3 hours ago	None	7 days ago	7 days ago
20A31A0159	Admin	3 hours 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	7 days ago
20A31A0367	Admin	2 days ago	None	7 days ago	-
20A31A0394	Admin	15 hours ago	None	2 days ago	-
20A31a0401	Admin	2 days ago	None	2 days ago	-
20A31A0403	Admin	2 days ago	None	7 days ago	-
20A31A0406	Admin	2 minutes ago	None	7 days ago	-
20A31A0419	Admin	2 days ago	None	7 days ago	-
20A31A04E0	Admin, group1 and group2	2 days ago	None	6 days ago	7 days ago
20A31A04K2	Admin	2 hours ago	None	7 days ago	-
20A31A04N3	Admin	2 days ago	None	7 days ago	7 days ago
20A31A0513	Admin	2 days ago	None	7 days ago	-

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?

Specifying a user in Identity Center - Recommended

I want to create an IAM user

Console password

Autogenerated password

Custom password

Must be at least 8 characters long

Show 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

User details

User name
EmergencyAccess

Provide user access to the AWS Management Console - optional

Are you providing console access to a person?

Specifying a user in Identity Center - Recommended

I want to create an IAM user

Console password

Autogenerated password

Custom password

Must be at least 8 characters long

Show 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

Cancel Next

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

Set permissions

Specify user details

Step 2 Set permissions

Step 3 Review and create

Step 4 Retrieve password

Permissions options

Add user to group

Copy permissions

Attach policies directly

User groups (132)

Group name	Users	Attached policies	Created
ec2-readonly	0	AmazonEC2ReadOnlyAccess	2023-03-27 (7 days ago)
20A31A0564group	1	AmazonEC2FullAccess	2023-03-27 (7 days ago)
20A31A0564readonly	1	AmazonEC2ReadOnlyAccess	2023-03-27 (7 days ago)
20A31A0580usergroup	0	AmazonEC2FullAccess	2023-03-27 (7 days ago)
20A31A05G1	1	AmazonEC2FullAccess	2023-03-27 (7 days ago)
20A31A05g8	1	AmazonEC2FullAccess	2023-03-27 (7 days ago)
20A31A05H2	0	AmazonEC2FullAccess	2023-03-27 (7 days ago)
20A31A05H2-ec2-user	0	AmazonEC2ReadOnlyAccess	2023-03-27 (7 days ago)
20A31A05H4	1	AmazonEC2FullAccess	2023-03-27 (7 days ago)
20A31A05I1	0	AmazonEC2FullAccess	2023-03-27 (7 days ago)

Create group

CloudShell Feedback Language

28°C Humid

Search

11:03 PM 34.23

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

Get started with IAM - AWS | IAM Management Console

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

Step 4 Retrieve password

Create user group

User group name

EmergencyAccessGroup

Permissions policies (1/830)

Policy name	Type	Used as	Description
AdministratorAccess	AWS man...	Permissio...	Provides full acces...
AdministratorAccess-Amplify	AWS man...	None	Grants account ad...
AdministratorAccess-AWSElasti...	AWS man...	None	Grants account ad...
AlexaForBusinessDeviceSetup	AWS man...	None	Provide device set...
AlexaForBusinessFullAccess	AWS man...	None	Grants full access t...
AlexaForBusinessGatewayExec...	AWS man...	None	Provide gateway e...
AlexaForBusinessLifecycleDeleg...	AWS man...	None	Provide access to L...
AlexaForBusinessPolicyDelegate...	AWS man...	None	Provide access to P...
AlexaForBusinessReadOnlyAcc...	AWS man...	None	Provide read only ...
AmazonAPIGatewayAdministra...	AWS man...	None	Provides full acces...
AmazonAPIGatewayInvokeFull...	AWS man...	None	Provides full acces...
AmazonAPIGatewayPushToCle...	AWS man...	None	Allows API Gatewa...
AmazonAppFlowFullAccess	AWS man...	None	Provides full acces...

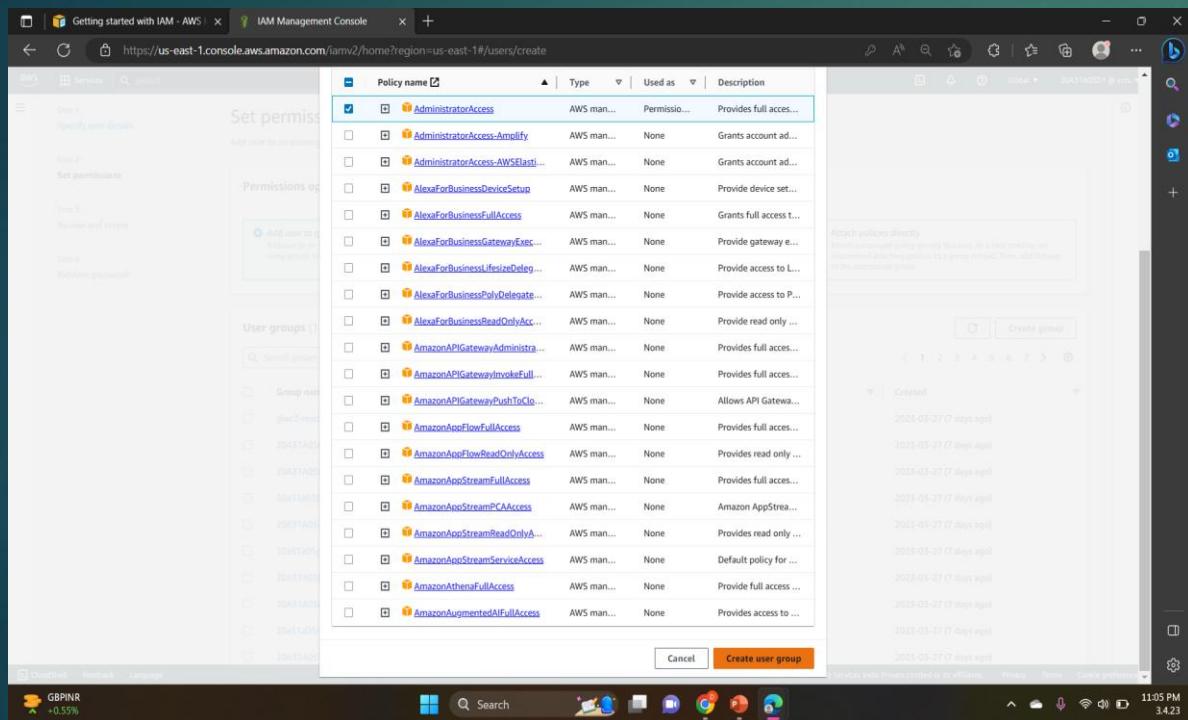
CloudShell Feedback Language

28°C Humid

Search

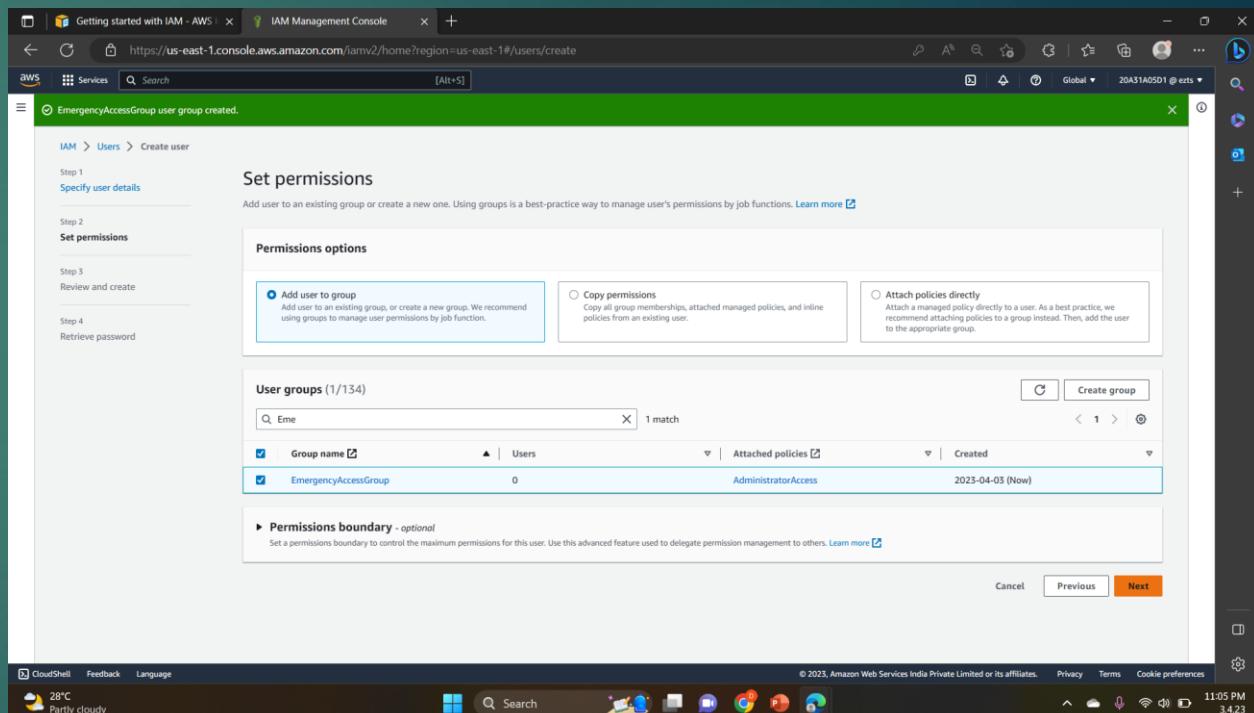
11:04 PM 34.23

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



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#/users/create>. The main page displays a list of existing user groups. A modal dialog is open, titled 'Set permissions', which lists various AWS managed policies. The 'AdministratorAccess' policy is selected and highlighted with a blue border. Other policies listed include 'AdministratorAccess-Amplify', 'AdministratorAccess-AWSElasti...', 'AlexaForBusinessDeviceSetup', 'AlexaForBusinessFullAccess', 'AlexaForBusinessGatewayExec...', 'AlexaForBusinessLambdaDeploy...', 'AlexaForBusinessPolicyDelete...', 'AlexaForBusinessReadOnlyAcc...', 'AmazonAPIGatewayAdministrator', 'AmazonAPIGatewayInvokeFull...', 'AmazonAPIGatewayPushToCloud...', 'AmazonAppFlowFullAccess', 'AmazonAppFlowReadOnlyAccess', 'AmazonAppStreamFullAccess', 'AmazonAppStreamPACcess', 'AmazonAppStreamReadOnlyAcc...', 'AmazonAppStreamServiceAccess', 'AmazonAthenaFullAccess', and 'AmazonAugmentedAIFullAccess'. At the bottom of the modal, there are 'Cancel' and 'Create user group' buttons.

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

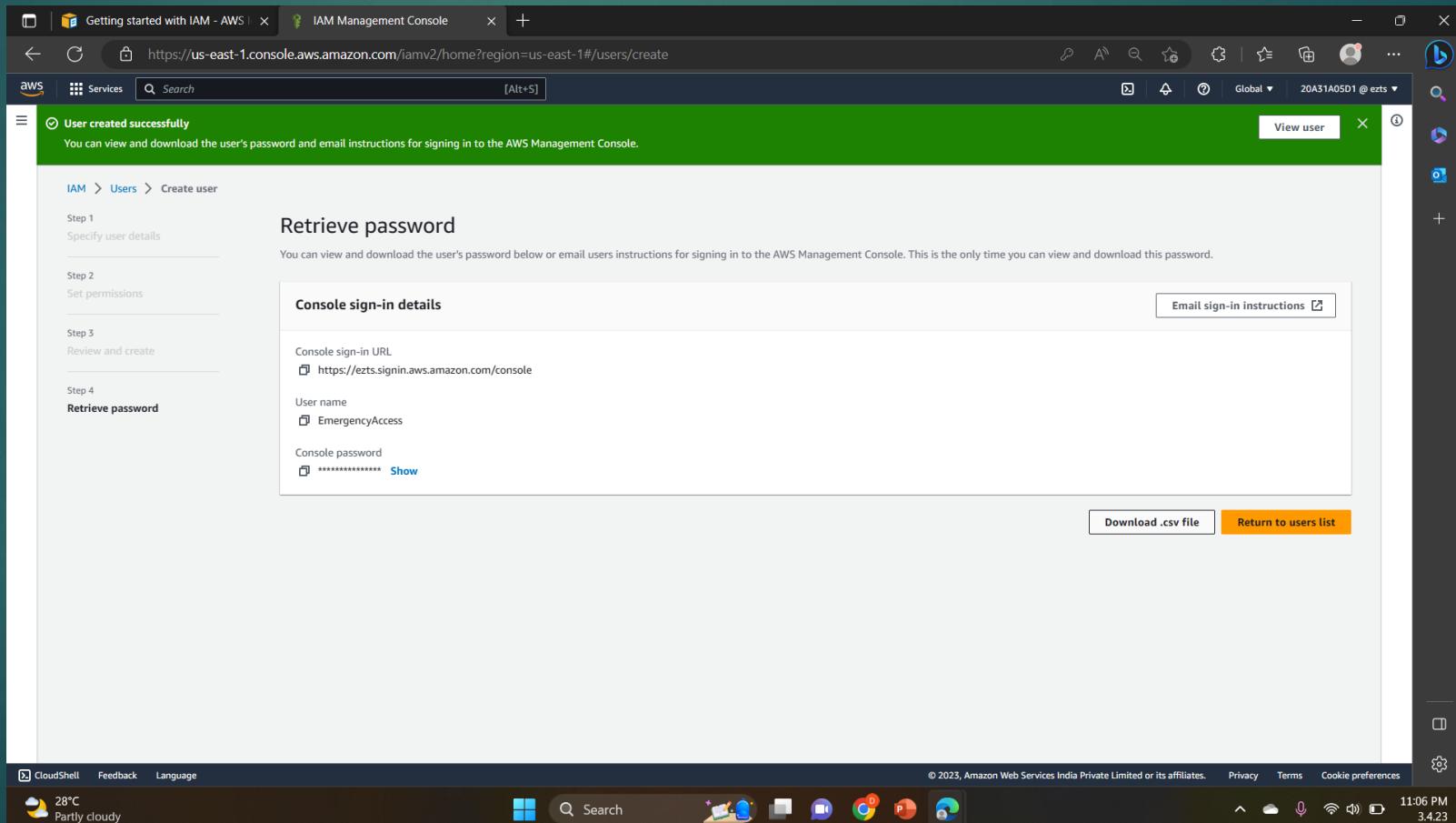


The screenshot shows the AWS IAM Management Console with the URL <https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/create>. The main page displays a confirmation message: 'EmergencyAccessGroup user group created.' Below this, the 'Set permissions' step is shown. The 'User groups' section lists 'EmergencyAccessGroup' under 'Group name'. The 'Permissions options' section includes 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. At the bottom, there are 'Previous' and 'Next' buttons, with 'Next' being highlighted.

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.



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) > User groups'. The page lists one user group: 'EmergencyAccessGroup'. The table columns are 'Group name', 'Users', 'Permissions', and 'Creation time'. The 'EmergencyAccessGroup' row shows 'Defined' under Permissions and '5 minutes ago' under Creation time. A search bar at the top filters results by 'EmergencyAccessGroup'. The bottom status bar shows the URL and system information like weather and battery level.

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 'Identity and Access Management (IAM) > User groups'. The title bar says 'Identity and Access Management (IAM) > User groups > EmergencyAccessGroup'. The page has a 'Summary' section with details like 'User group name: EmergencyAccessGroup', 'Creation time: April 03, 2023, 23:05 (UTC+05:30)', and 'ARN: arn:aws:iam:244575612640:group/EmergencyAccessGroup'. Below it is a 'Permissions' section with a table showing a single policy: 'AdministratorAccess'. The table columns are 'Policy name', 'Type', and 'Description'. The bottom status bar shows the URL and system information like weather and battery level.

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 open with 'User groups' selected. The main area displays a list of 'Other permission policies' under 'EmergencyAccessGroup'. One policy, 'AmazonEC2FullAccess', is selected and highlighted in blue. A 'Create policy' button is visible at the top right of the list.

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 open with 'User groups' selected. The main area shows the 'Permissions' tab for 'EmergencyAccessGroup'. It lists two policies: 'AmazonEC2FullAccess' and 'AdministratorAccess', both of which are AWS managed policies. A 'Delete' button is visible at the top right of the permissions section.

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' page. The left sidebar includes sections for 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 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...

At the bottom, there are CloudShell, Feedback, Language, and cookie preferences buttons.

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 'Custom' source. At the bottom, there are CloudShell, Feedback, Language, and cookie preferences buttons.

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. 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 at the top right of the table.

The screenshot shows the 'Create DB subnet group' configuration page. The left sidebar has 'Subnet groups' selected. The main area is titled 'Create DB subnet group'. It contains fields for 'Name' (set to 'DB-Subnet-Group'), 'Description' (set to 'DB Subnet Group'), and 'VPC' (set to 'Lab VPC (vpc-0a63c938af50af6dd)'). A note says: '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 is titled 'Amazon RDS' and 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: DB identifier, Role, Engine, Region & AZ, Size, Status, and Action. A search bar at the top of the table says 'Filter by databases'. 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. At the bottom of the page, there are links for CloudShell, Feedback, Language, and a footer with copyright information and cookie preferences.

This screenshot shows the 'Create database' wizard in the AWS RDS Management Console. The top navigation bar includes tabs for Services, Search, and a 'Create database - RDS Manager' tab. The main title is 'Create database'. Under 'Choose a database creation method', there are two options: 'Standard create' (selected) and 'Easy create'. The 'Standard create' option is described as setting all configuration options, including ones for availability, security, backups, and maintenance. The 'Easy create' option is described as using recommended best-practice configurations. On the right side, there is a 'MySQL' section with a detailed description: 'MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.' It also lists several bullet points: 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. Below this, there is a section for 'Engine options' with three choices: Aurora (MySQL Compatible), Aurora (PostgreSQL Compatible), and MySQL (selected). The MySQL icon features a hand holding a circular object. The bottom of the page has links for CloudShell, Feedback, Language, and a footer with copyright information and cookie preferences.

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.

Availability and durability

Deployment options [Info](#)

The deployment options below are limited to those supported by the engine you selected above.

Multi-AZ DB Cluster - [new](#)
Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.

Multi-AZ DB instance
Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.

Single DB instance
Creates a single DB instance with no standby DB instances.

Settings

DB instance identifier [Info](#)
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

database-1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

MySQL

MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.

- 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.
- Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.

Amazon RDS Optimized Writes - new [Info](#)

Show instance classes that support Amazon RDS Optimized Writes

DB instance class [Info](#)

Standard classes (includes m classes)
 Memory optimized classes (includes r and x classes)
 Burstable classes (includes t classes)

db.t3.micro
2 vCPUs 1 GiB RAM Network: 2,085 Mbps

Include previous generation classes

Storage

Storage type [Info](#)
Provisioned IOPS SSD (io1)
Flexibility in provisioning I/O

Allocated storage [Info](#)

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 highlighted. Below the table, there are tabs for Monitoring, Logs & events, Configuration, Maintenance & backups, and Tags.

At the bottom of the page, there are links for CloudShell, Feedback, Language, and a footer with copyright information and navigation icons.

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.

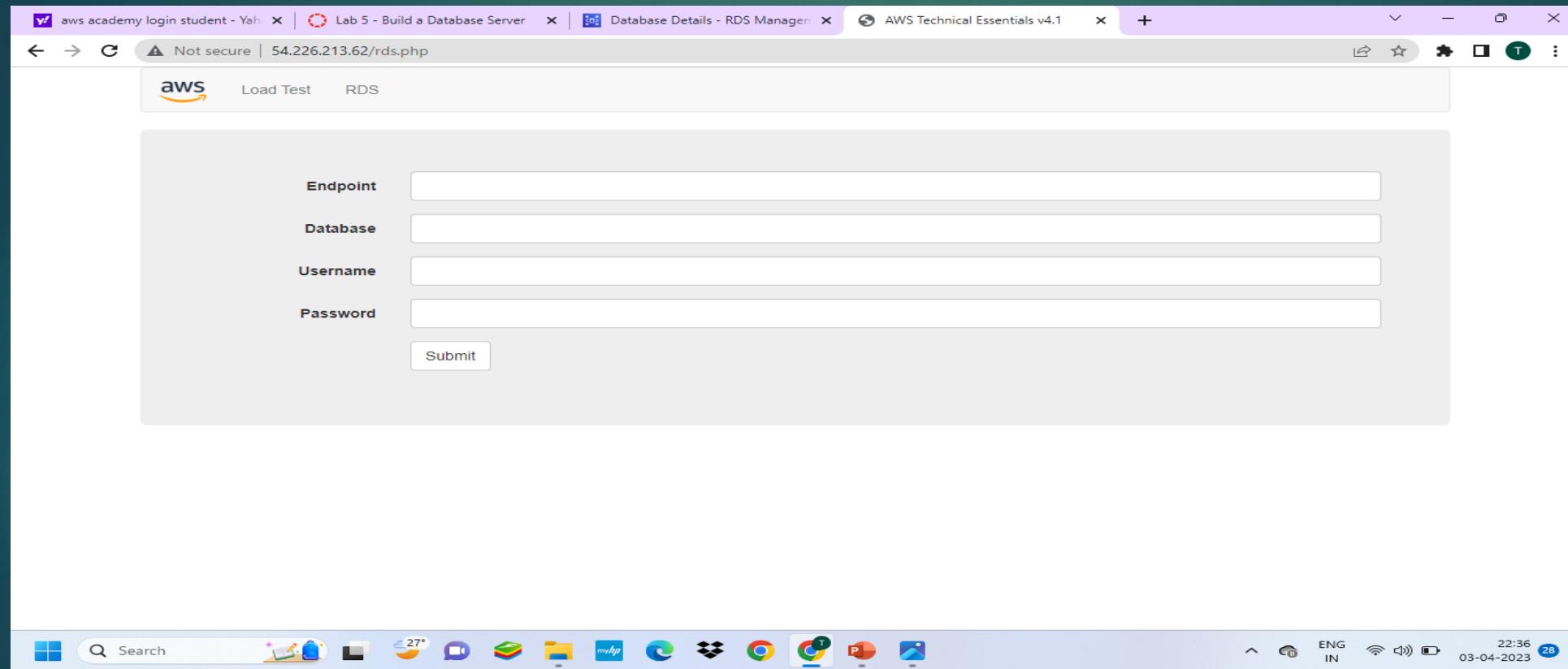
The screenshot shows the AWS Academy interface. On the left, there's a sidebar with icons for Account, Dashboard, Courses (with 10 notifications), Calendar, Inbox, History, and Help. The main area shows a course navigation path: ACFv2EN... > Modules > Module 8 ... > Lab 5 - Build a Database Server. The central part displays 'Database Details - RDS Manager' for a database named 'Lab 5 - Build a Database Server'. It shows various connection details and a table with the following data:

	Value
SecretKey	qwLdR6kIWlE9YvExDZWvazVmlAmzLhhN2GW4EWRX
WebServer	54.226.213.62
BastionHost	44.195.42.104
Region	us-east-1
AccessKey	AKIA276PEWVVAXXXS4H

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, there are 'Previous' and 'Next' buttons.

The screenshot shows a web browser window with the URL <https://54.226.213.62/load.php>. The page title is "AWS Technical Essentials v4.1" and it includes "Load Test" and "RDS" tabs. The content area displays a message: "Under High CPU Load! (auto refresh in 5 seconds)". Below it, it says "Current CPU Load: 100%". The browser taskbar at the bottom shows various open tabs and system status indicators.

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



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.

aws academy login student - Yah | Database Details - RDS Manager | Lab 5 - Build a Database Server | AWS Technical Essentials v4.1 | +

Not secure | 54.226.213.62/rds.php

aws Load Test RDS

Address Book

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

Add Contact

22:38 03-04-2023 28

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 Consoles

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

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

New EC2 Experience Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances 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

EC2 Global view

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.

Launch instance Migrate a server

Service health AWS Health Dashboard

Region US East (N. Virginia)

Status This service is operating normally

Save up to 90% on EC2 with Spot Instances Optimizes price-performance by combining EC2's purchase options and a choice of ASCI, Linux or Windows AMIs.

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

CloudShell Feedback Language

30°C Mostly clear

Lab 4 - Working with EBS

Instances | EC2 Management Consoles

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

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

New EC2 Experience Tell us what you think

Instances (2) info

Find instance by attribute or tag (case-sensitive)

Connect Instance state Actions Launch Instances

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

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

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

CloudShell Feedback Language

30°C Mostly clear

Lab 4 - Working with EBS

Create volume | EC2 Management Consoles

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

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

New EC2 Experience Tell us what you think

EC2 > Volumes > Create volume

Create volume Info

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

Lab 4 - Working with EBS

Volumes | EC2 Management Consoles

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

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

New EC2 Experience Tell us what you think

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

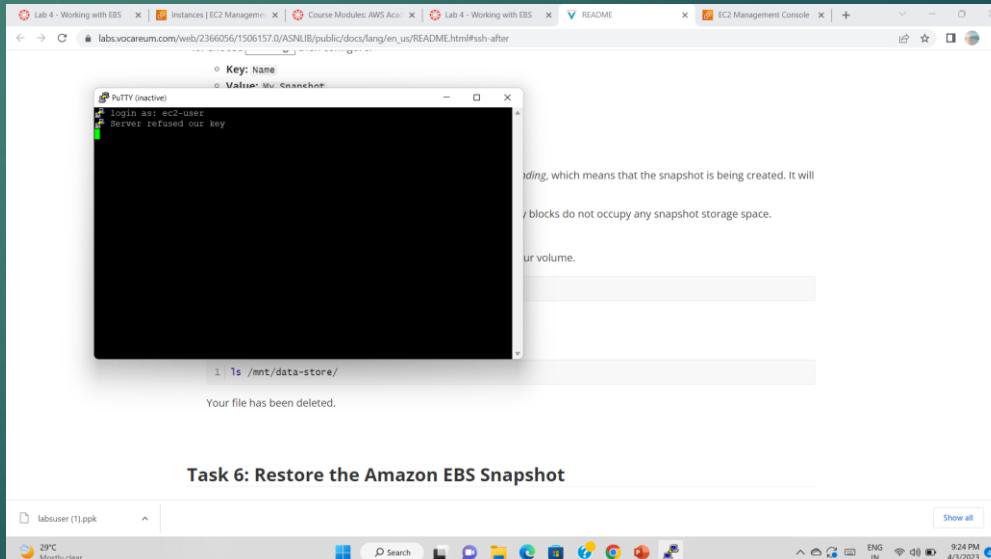
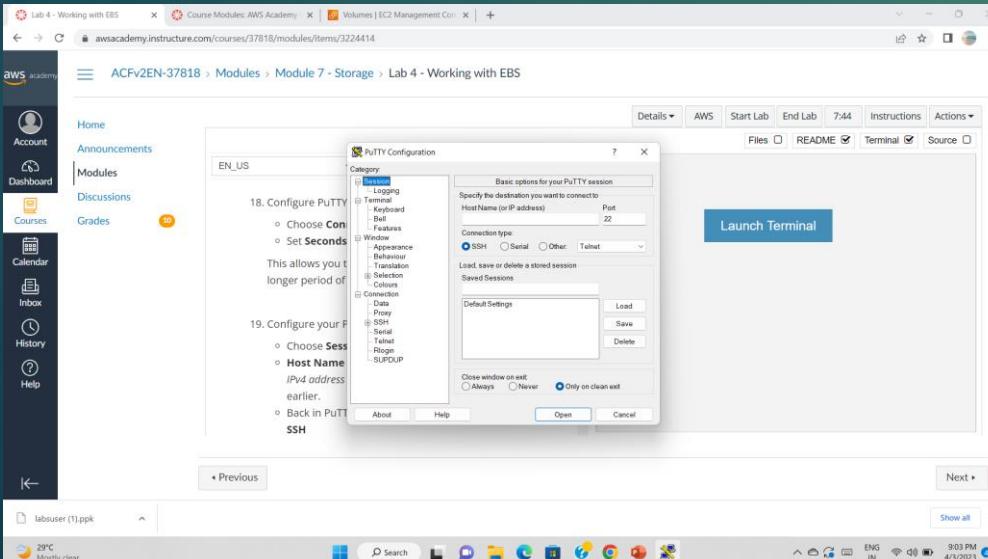
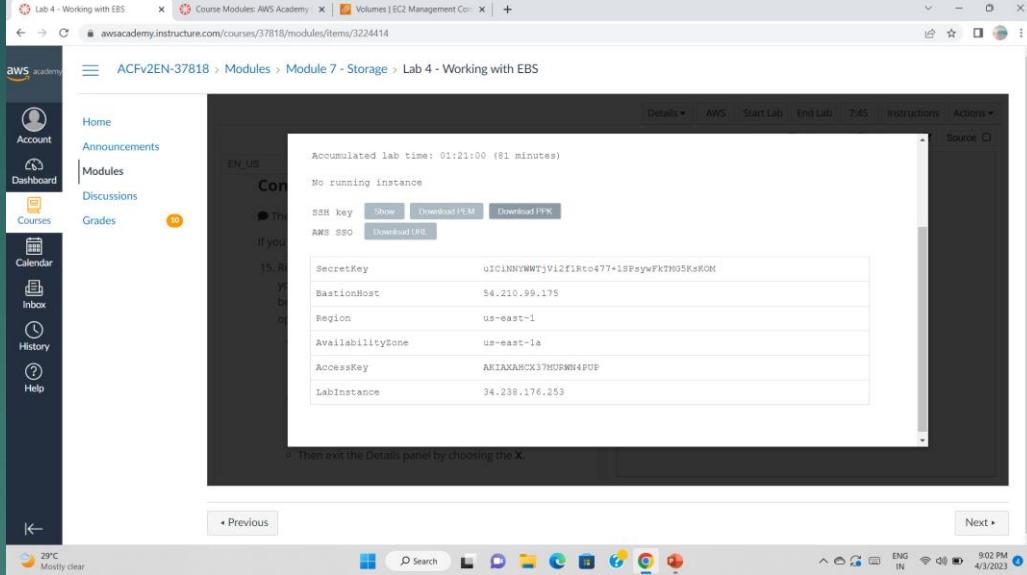
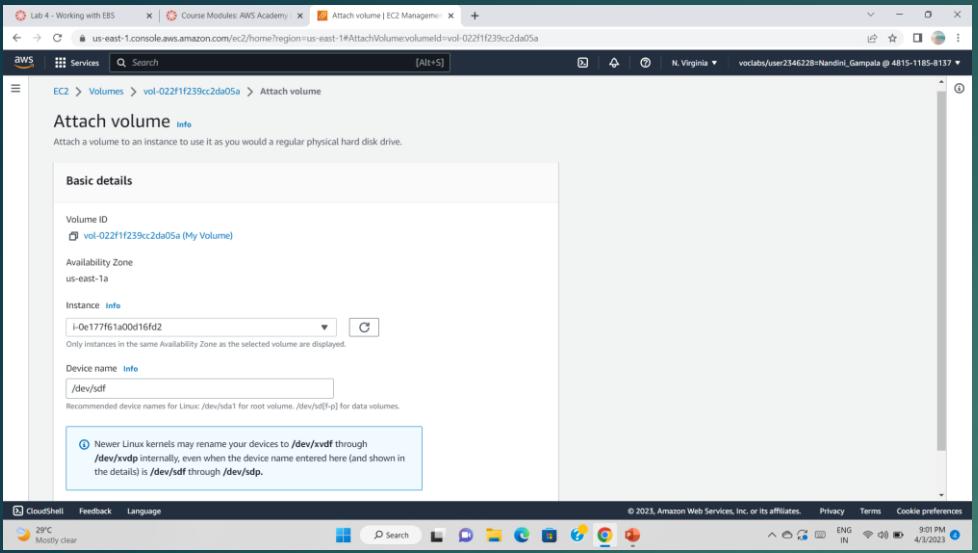
Name	Volume ID	Type	Size	IOPS	Throughput
My Volume	vol-022f1f239cc2da05a	gp2	1 GiB	100	-
	vol-088b8ff07838675838	gp3	8 GiB	3000	125

Volume ID: vol-022f1f239cc2da05a (My Volume)

Details Status checks Monitoring Tags

CloudShell Feedback Language

29°C Mostly clear



Screenshot of the AWS CloudShell interface showing the creation of an EBS volume. The terminal window displays the command:

```
aws ec2 create-volume --size 1 --volume-type gp2 --snapshot-id snap-013c8ef099b54ee35
```

Screenshot of the AWS CloudShell interface showing the creation of an EBS snapshot. The terminal window displays the command:

```
aws ec2 create-snapshot --volume-id vol-0d10d525f2f83a0c5
```

Screenshot of the AWS CloudShell interface showing the configuration of a new EBS volume from a snapshot. The terminal window displays the command:

```
aws ec2 create-volume --size 1 --volume-type gp2 --snapshot-id snap-013c8ef099b54ee35
```

Screenshot of the AWS CloudShell interface showing the attachment of the newly created EBS volume to an EC2 instance. The terminal window displays the command:

```
aws ec2 attach-volume --volume-id vol-032d6ef213670b26 --instance-id i-0229dbc7ee6522a7b --device /dev/sdg
```

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-458cae0 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

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-level ACLs.

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

CloudShell Feedback Language

27°C Mostly clear

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

Step 2

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.

Amazon S3

Buckets

Batch operations

Access analyzer for S3

Block public access (account settings)

Feature spotlight

Search for buckets

All access types

2 Buckets 1 Regions

Bucket name Access Region Date created

organization03 Error US East (N. Virginia) Dec 16, 2018 9:42:03 PM GMT-0500

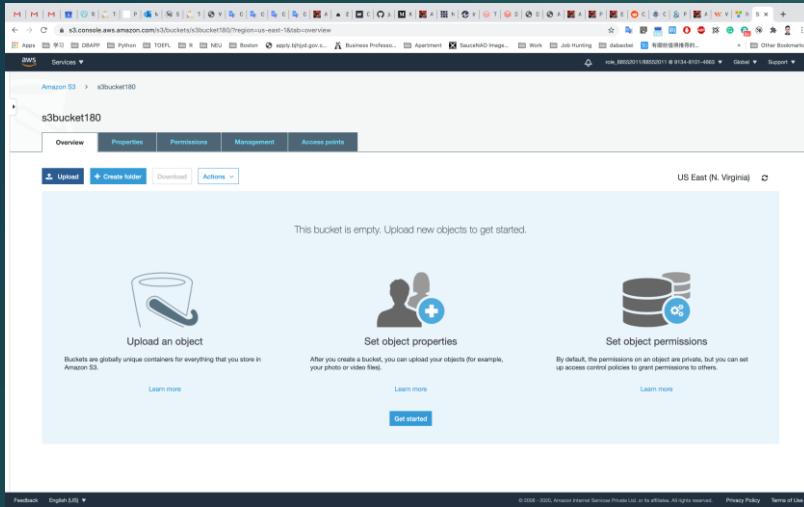
s3bucket180 Error US East (N. Virginia) Oct 8, 2020 4:22:24 PM GMT-0700

Discover the console

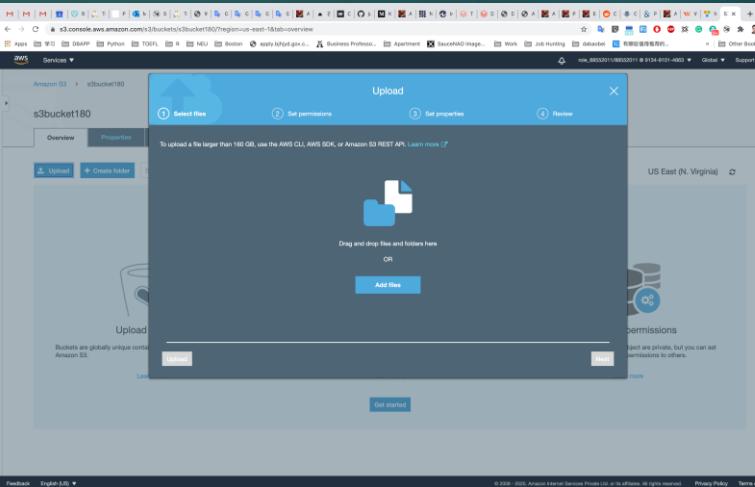
© 2006-2023, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Step 2

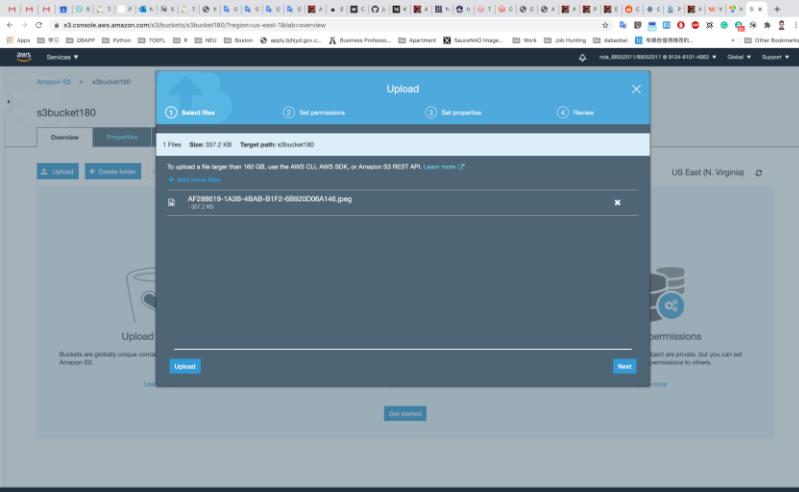
Step 3



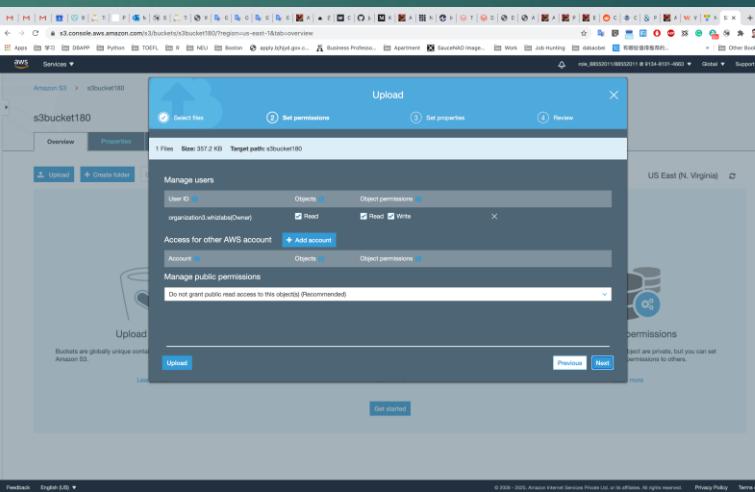
Step 4



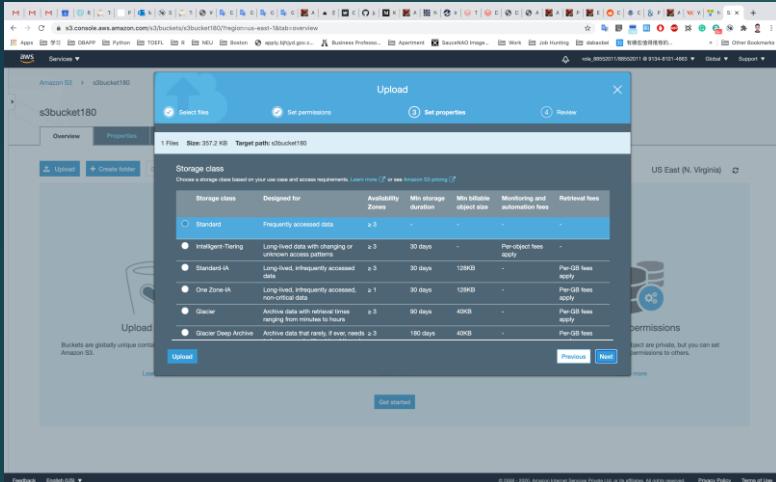
Step 5



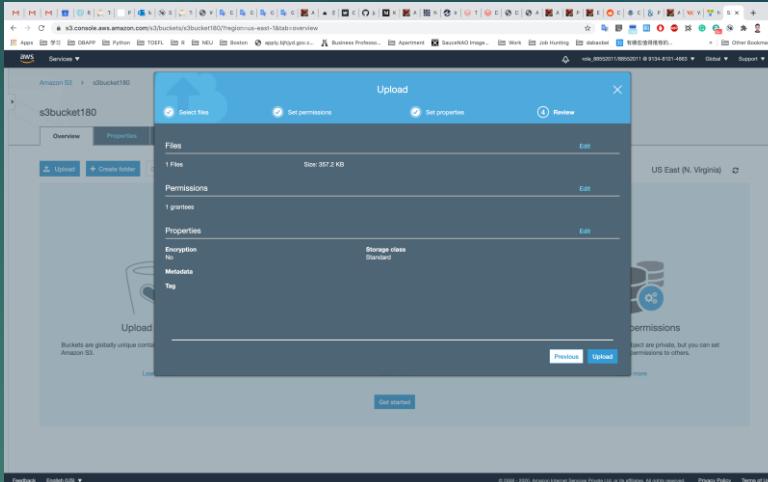
Step 6



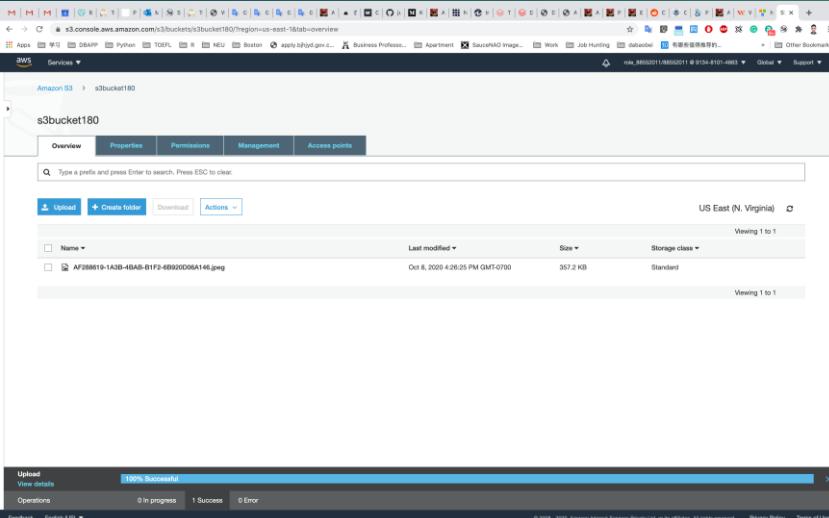
Step 7



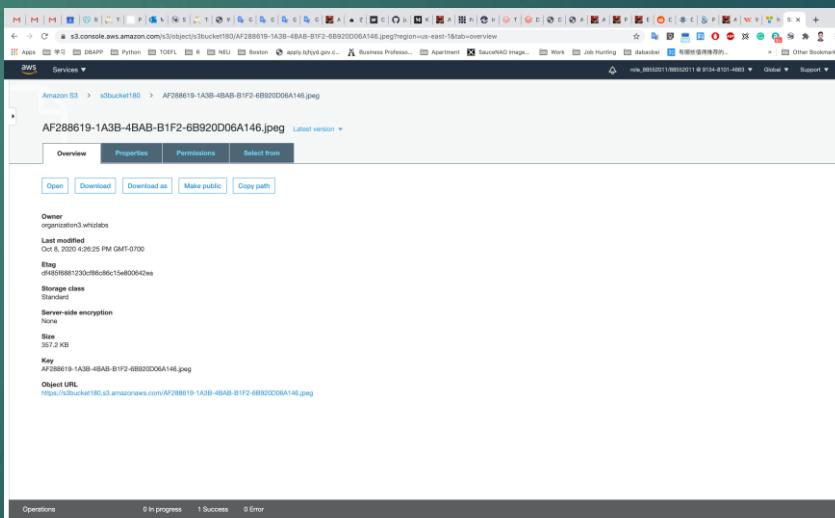
Step 8



Step 9



Step 10



Step 11

The screenshot shows the AWS S3 console with the permissions tab selected for an object named AF288619-1A3B-4BAB-B1F2-6B920D06A146.jpeg. It displays three sections: Access for object owner, Access for other AWS accounts, and Public access. Under Access for object owner, there is a single entry for the canonical ID of the account owner. Under Access for other AWS accounts, there is a section for adding accounts, but none are listed. Under Public access, there is a section for groups, but none are listed.

Step 12

This screenshot shows the same AWS S3 console page as Step 12, but with a second entry in the Access for object owner section. The new entry is for a different canonical ID, indicating that another user has been granted permissions to the object.

Step 13

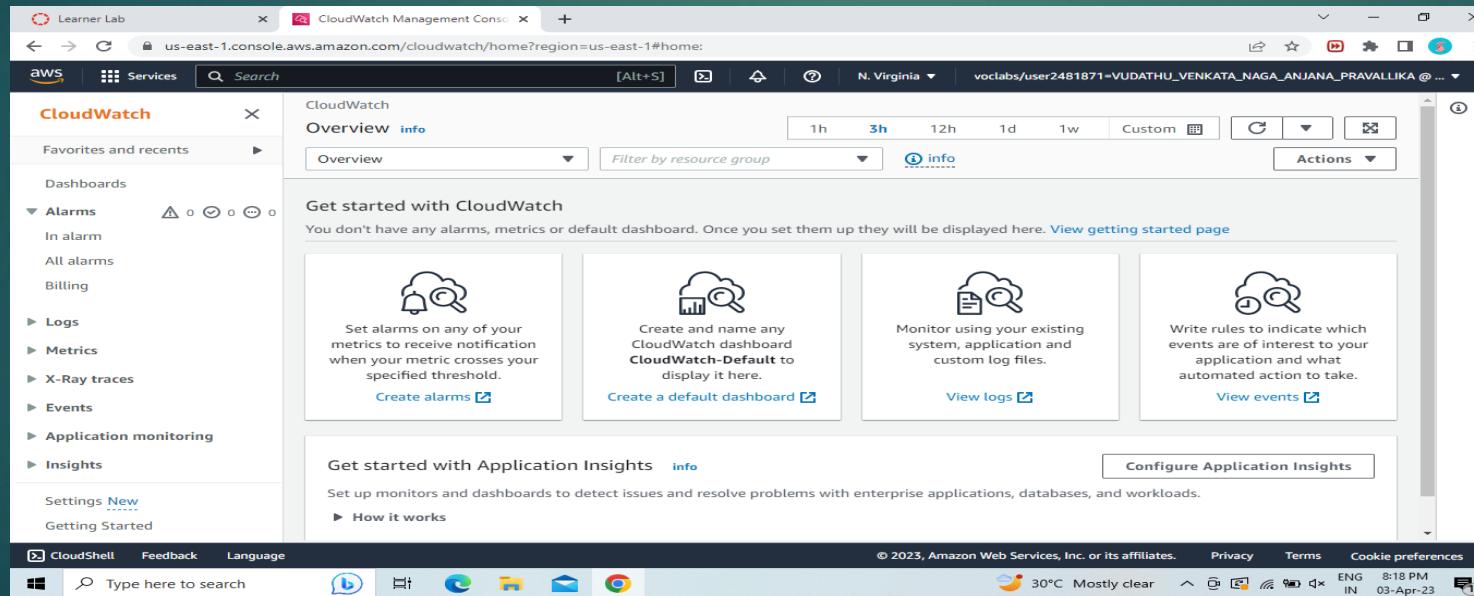


Step 14

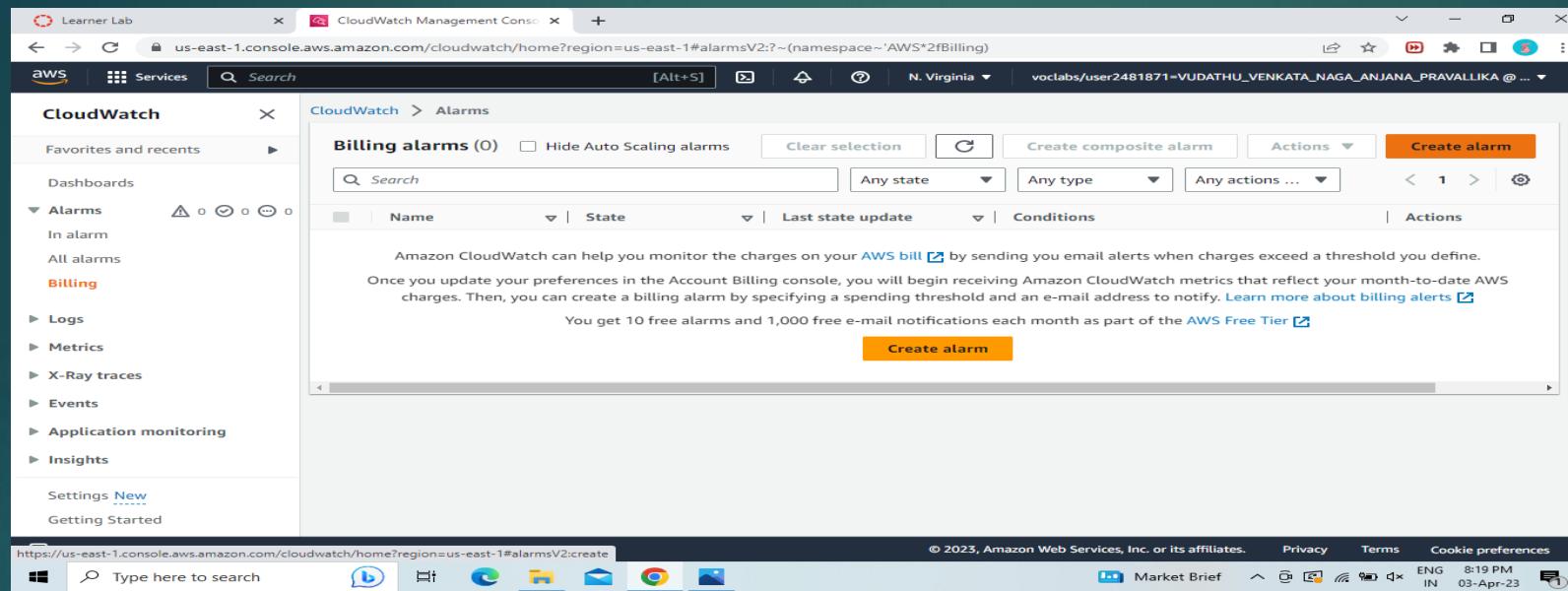
AWS CLOUDWATCH

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.

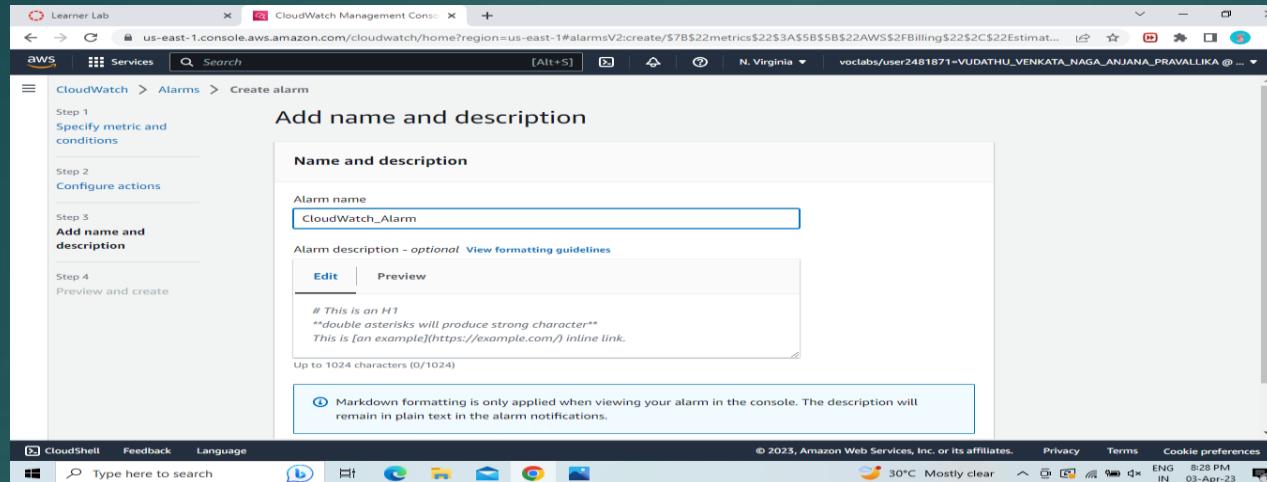
4.Click on Next.

The screenshots show the AWS CloudWatch Management Console interface for creating a new alarm. The left window displays the 'Specify metric and conditions' step, featuring a graph of 'EstimatedCharges' over time (from 03/28 to 04/02). The right window shows the 'Conditions' configuration step, where a static threshold of 100 Rupee is set for 'EstimatedCharges'.

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. It is configuring an SNS topic for notifications. The 'Create a new topic...' section has 'CloudWatch_Alarms' entered as the topic name. The 'Email endpoints that will receive the notification...' section contains the email address 'pravallikavudathu2003@gmail.com'. The 'Create topic' button is highlighted in blue.

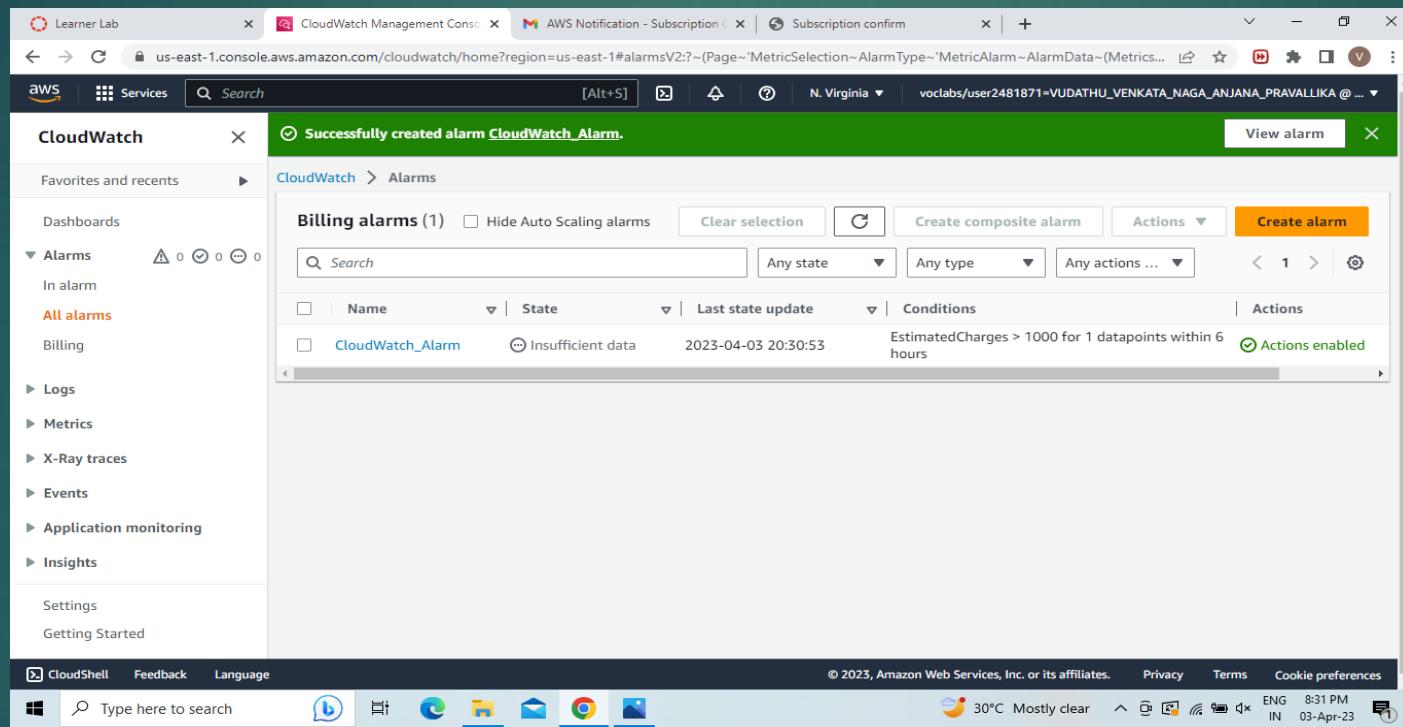
6.Give a name to your Alarm and Click on next.



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 image contains two screenshots. The left screenshot shows an email in the Gmail inbox titled 'AWS Notification - Subscription Confirmation' from 'AWS Notifications <no-reply@amazonaws.com>' with the subject 'AWS Notifications'. The email body contains instructions to confirm subscription by clicking a link. The right screenshot shows a browser window for 'AWS Notification - Subscription confirmation' with the URL https://sns.us-east-1.amazonaws.com/confirmation.html?TopicArn=arn:aws:sns:us-east-1:265498189509:CloudWatch_Alarms&Token=2336412f7fb68775d51e5e0425.... The page displays a green box with the text 'Subscription confirmed! You have successfully subscribed. Your subscription's ID is: arn:aws:sns:us-east-1:265498189509:Cloudwatch_Alarms:tbe0ea541-e7d9-4bc5-ed93-dc947a2772de If it was not your intention to subscribe, click here to unsubscribe.' Below this is the 'Simple Notification Service' logo.

- 8.Preview the details you have entered .
- 9.Click on Create alarm.This will Create your Alarm.



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))
```

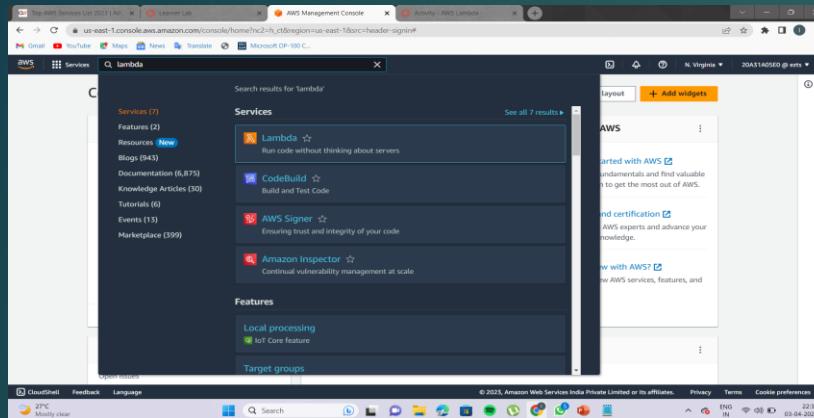
9) Replace the <REPLACE_WITH_REGION> placeholder with the actual Region that you are using. To do this:

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.



A screenshot of a code editor window titled 'lambda_function.py'. The code is written in Python and uses the boto3 library to stop EC2 instances. The code is as follows:

```
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))
```

