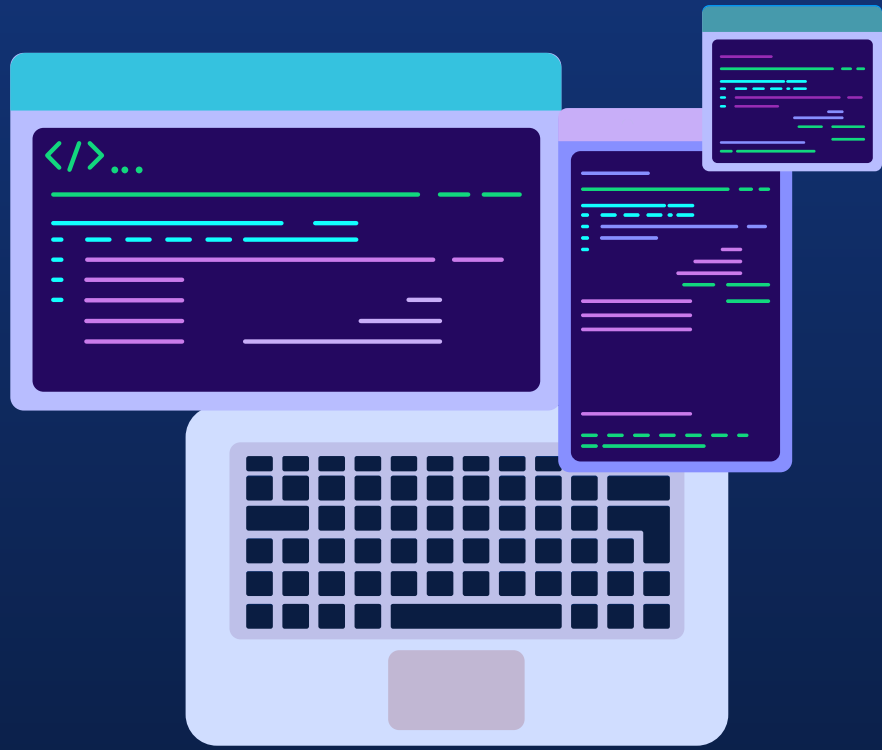
AWS
Lab Procedures

- V.Sampath(20A31A0562)

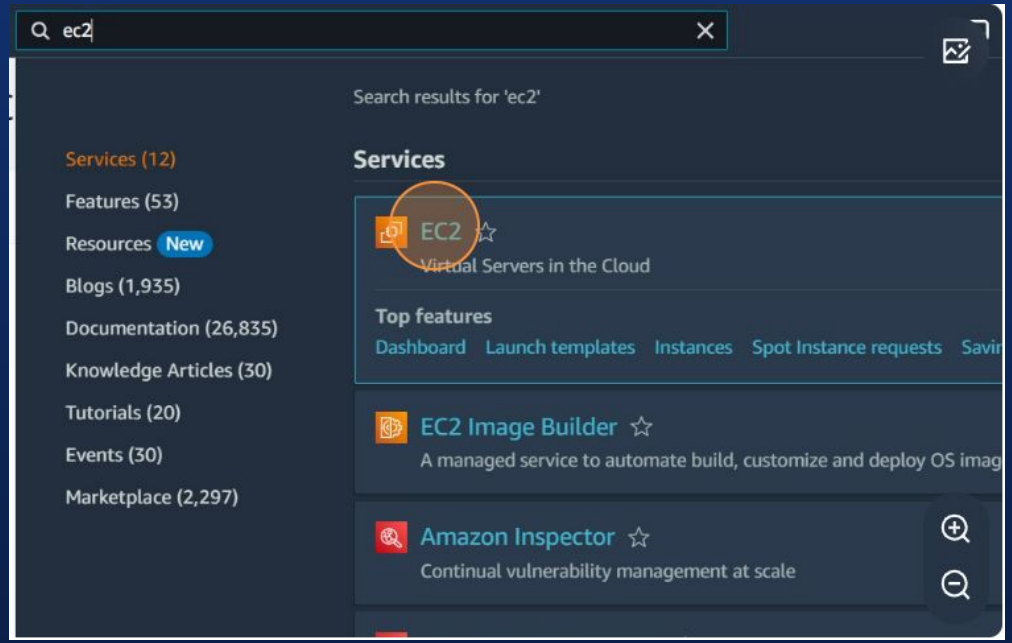


01

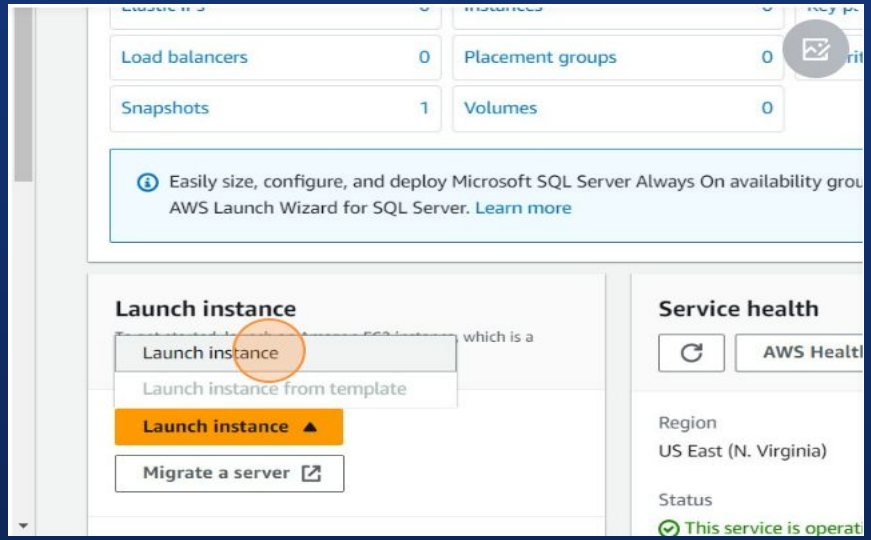
Amazon EC2 Instance

Step-1: Login to your AWS Management Console

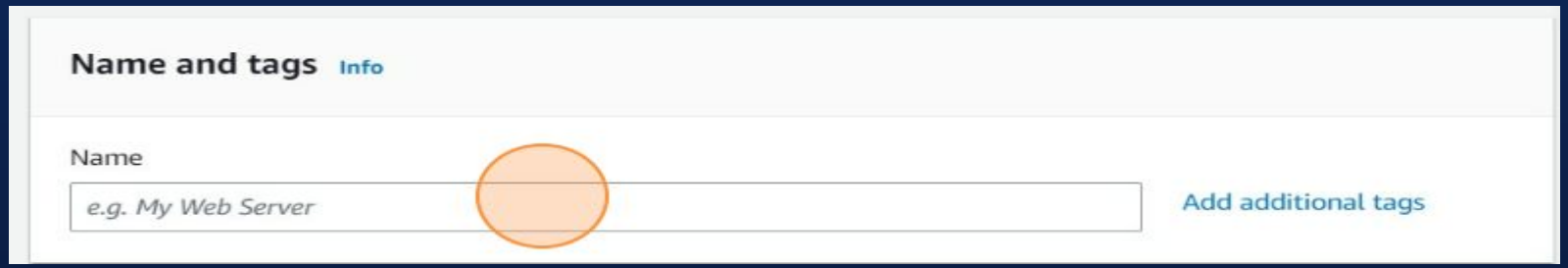
Step-2: Click on the search field and enter EC2. Select the EC2 service



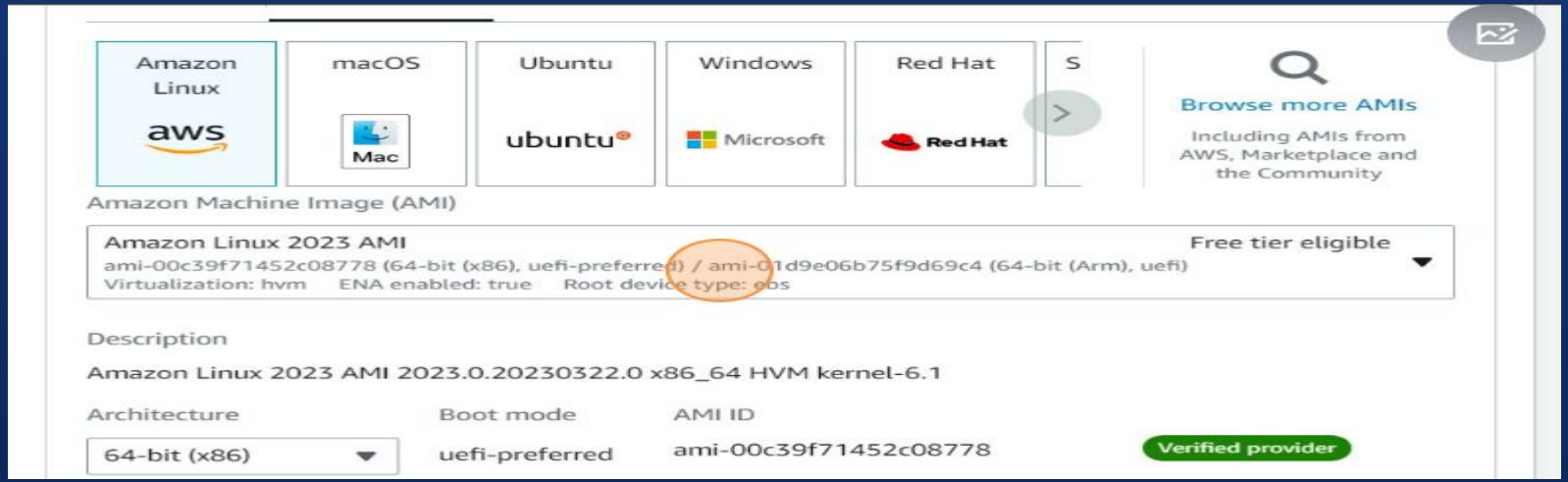
Step-3: Select Launch Instance and Click Launch instance



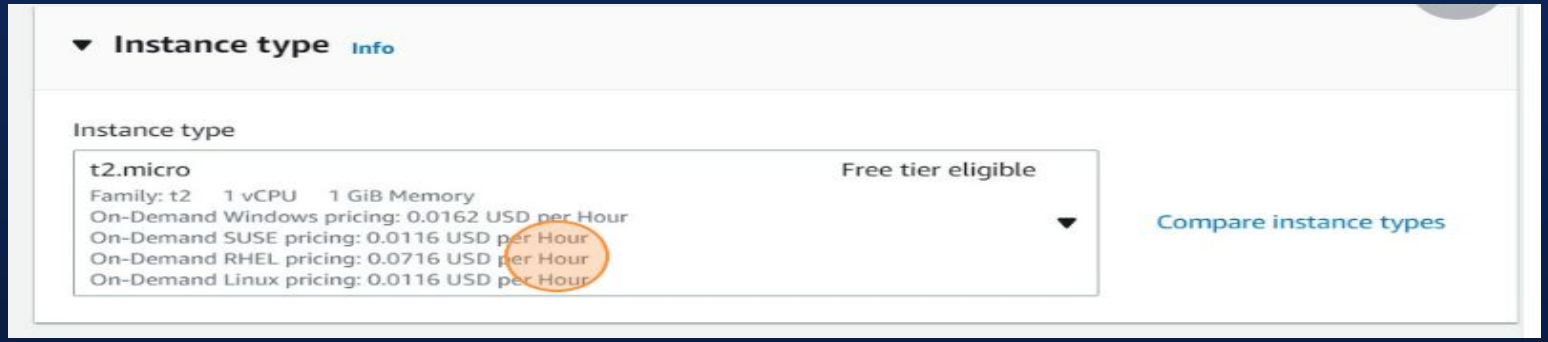
Step-4: Click on the Name field and enter your instance name(my-instance)



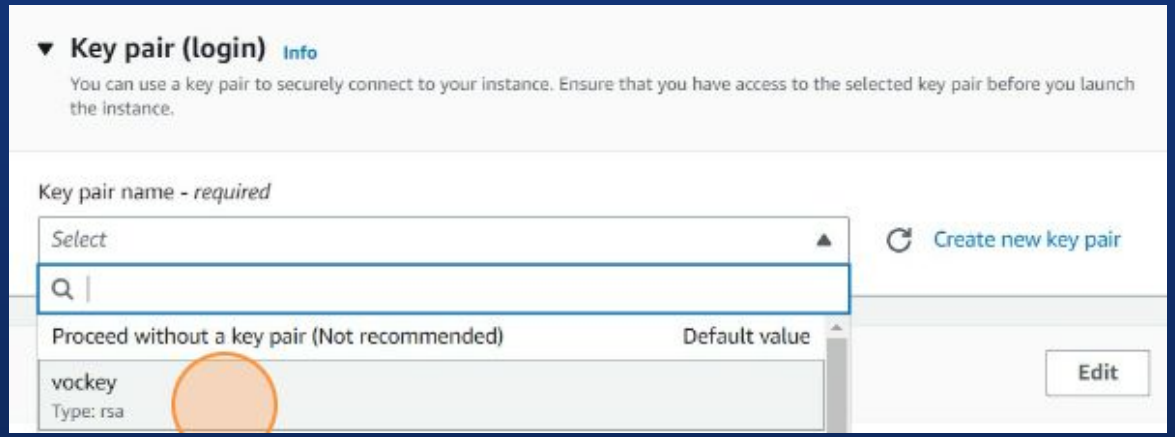
Step-5: Choose the required Operating System for the instance (Amazon Linux 2023 AMI)



Step-6: Select the instance type based on your requirements (t2.micro)

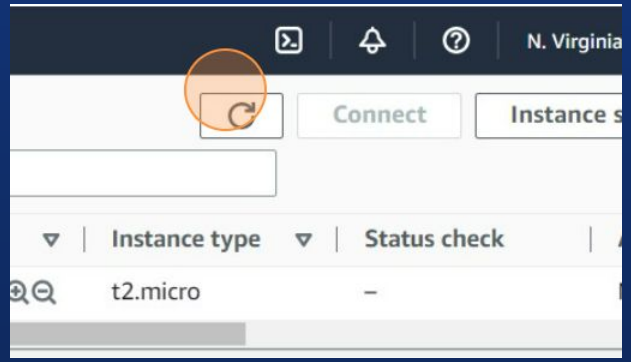


Step-7: Select the key-pair (you can go with the default one)

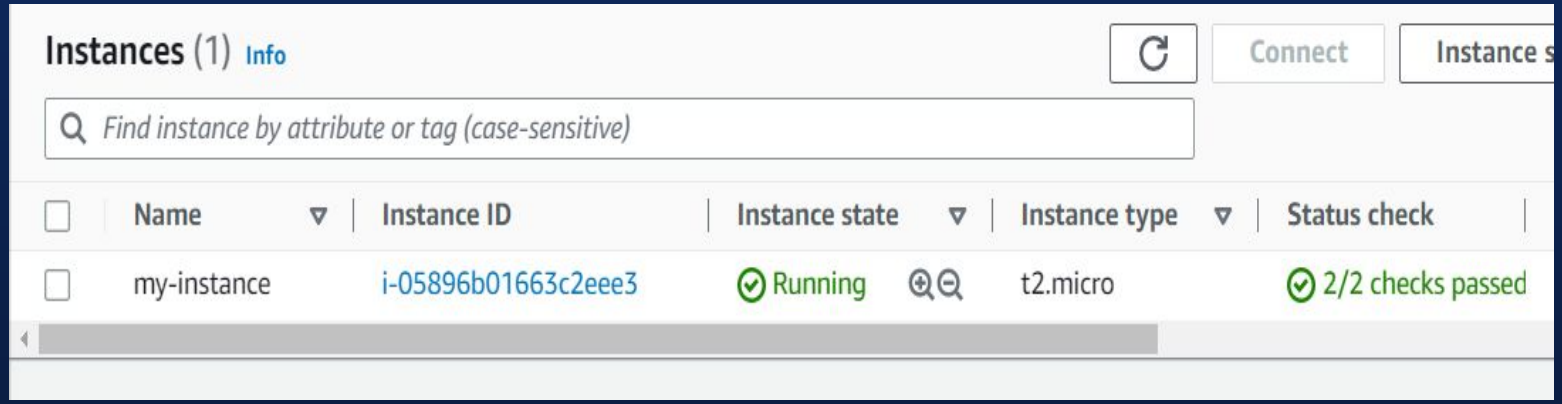


Step-8: Click on Launch instance in the summary panel to launch the instance(here the instance is launched without any custom security groups)

Step-9: Now go back to the instances page and wait till the instance you created enters into running state. Occasionally click the refresh icon to refresh the changes



Step-10: Your instance is successfully created.

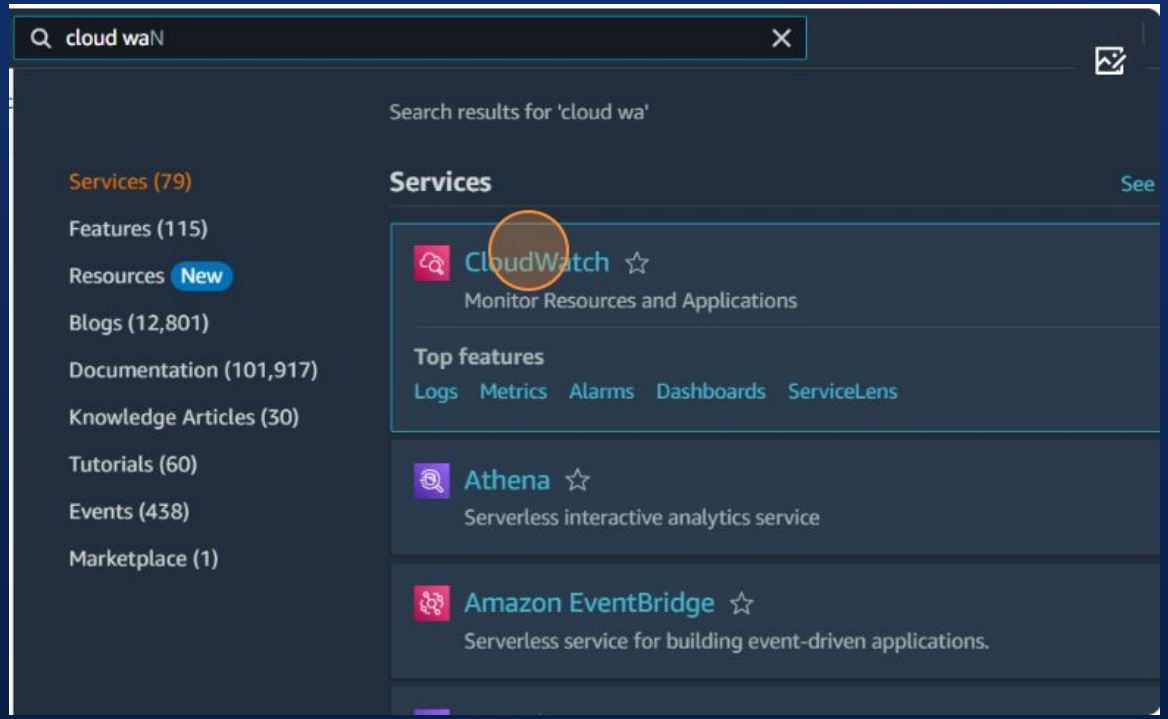


02

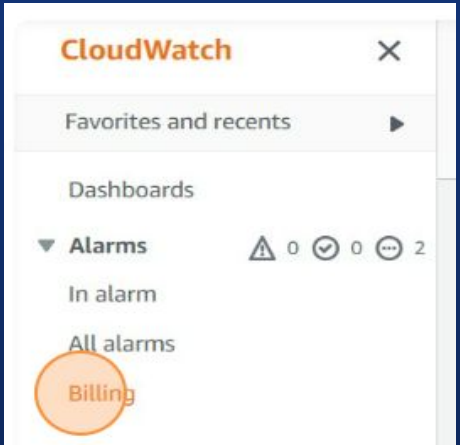
Amazon Cloud Watch

Step-1: Login to your AWS Management Console

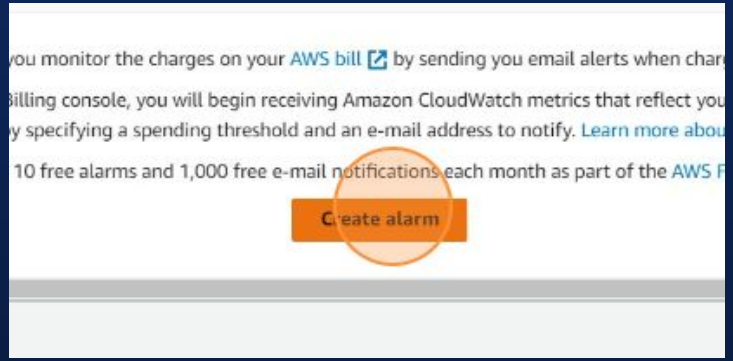
Step-2: Click on the search field and enter Cloud Watch. Select the Cloud Watch Service



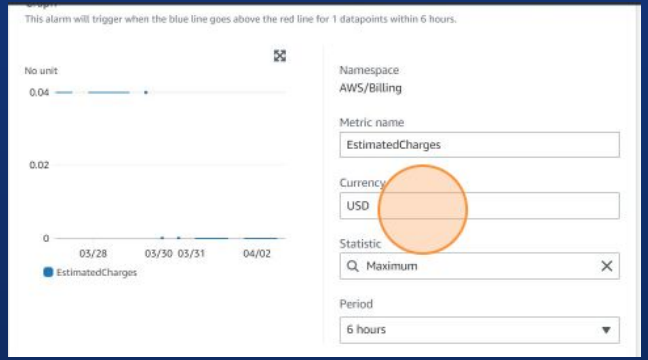
Step-3: Select the Billing Option in the left pane



Step-4: Click on the Create Alarm button

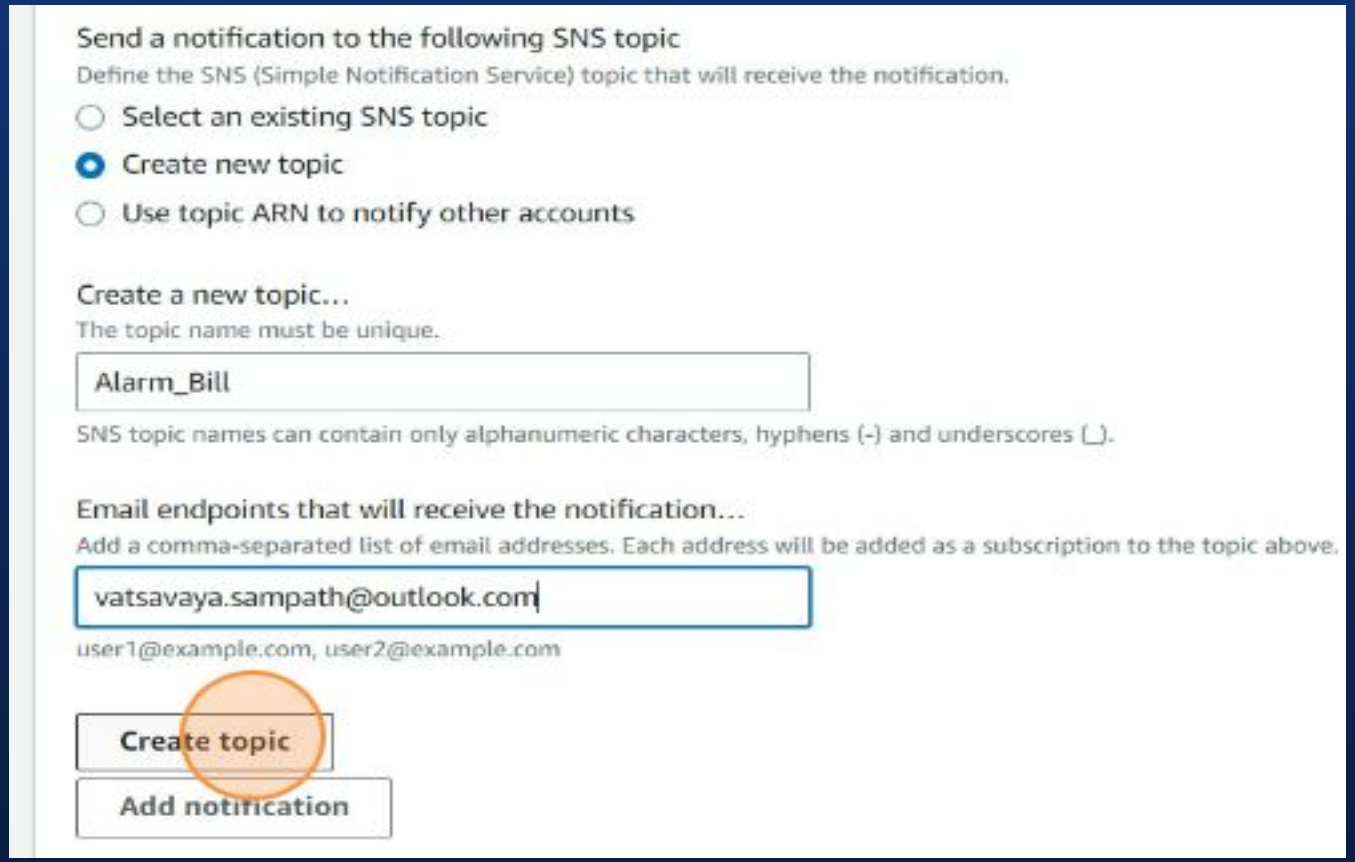


Step-5: Change the metrics to match our desired conditions

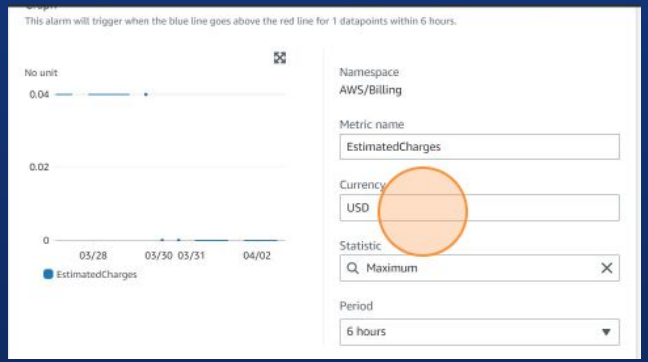


Step-6: Adjust the conditions and click NEXT.

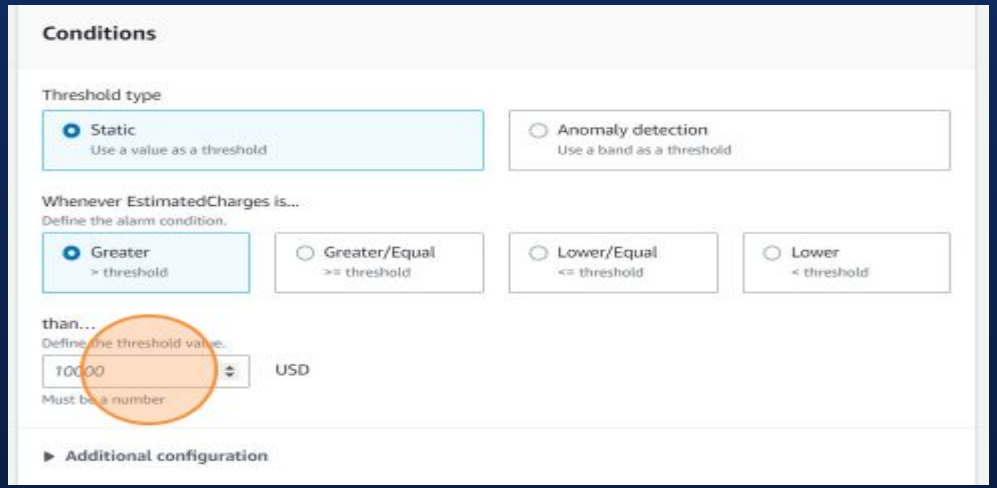
Step-7: Create a new topic for the SNS service with the Topic name and email endpoints that will receive the notification



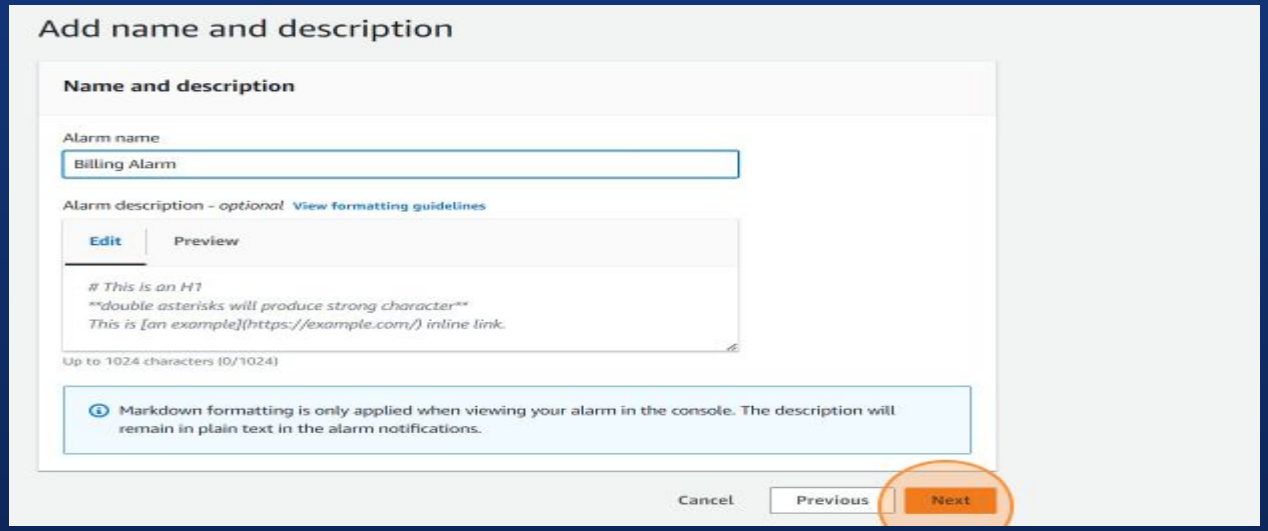
Step-8: Change the metrics to match our desired conditions



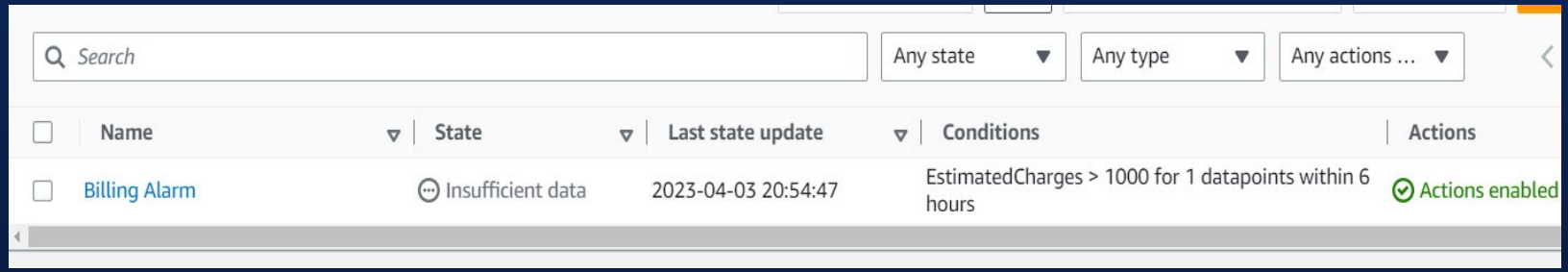
Step-9: Adjust the conditions and click NEXT.



Step-10: Give a name to the Alarm and click Next and click Create Alarm.



Step-11: The Alarm is successfully created.

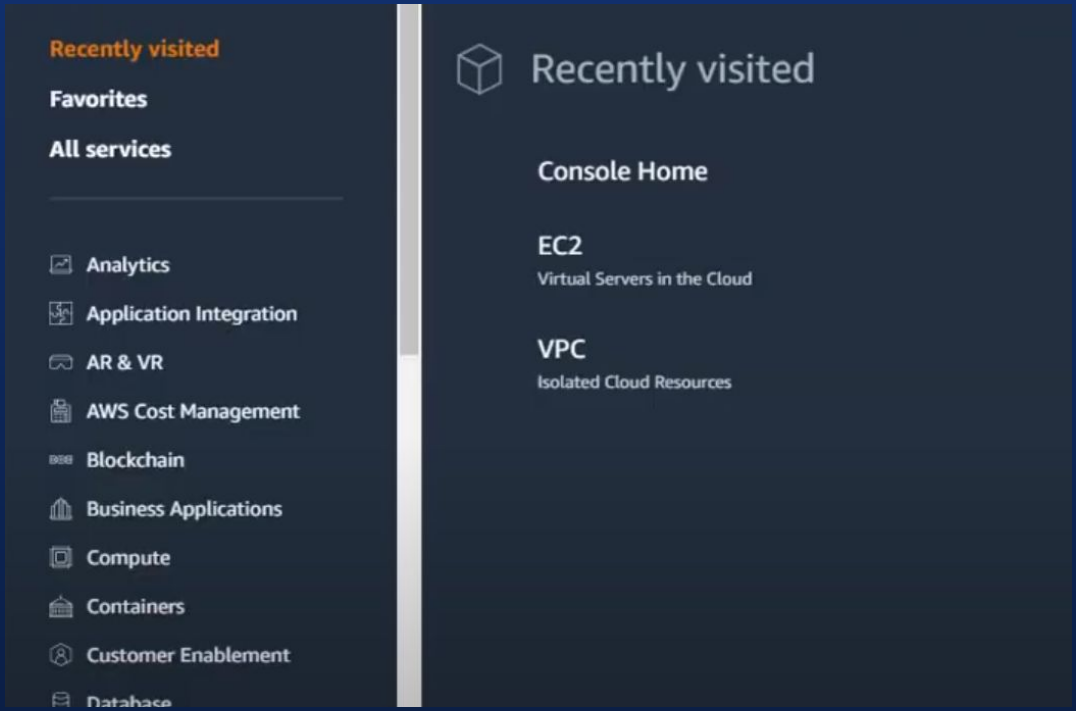


03

Amazon
Virtual Private Cloud

Step-1: Login to your AWS Management Console

Step-2: Click on the search field and enter VPC. Select the VPC service



Step-3: Choose Create VPC

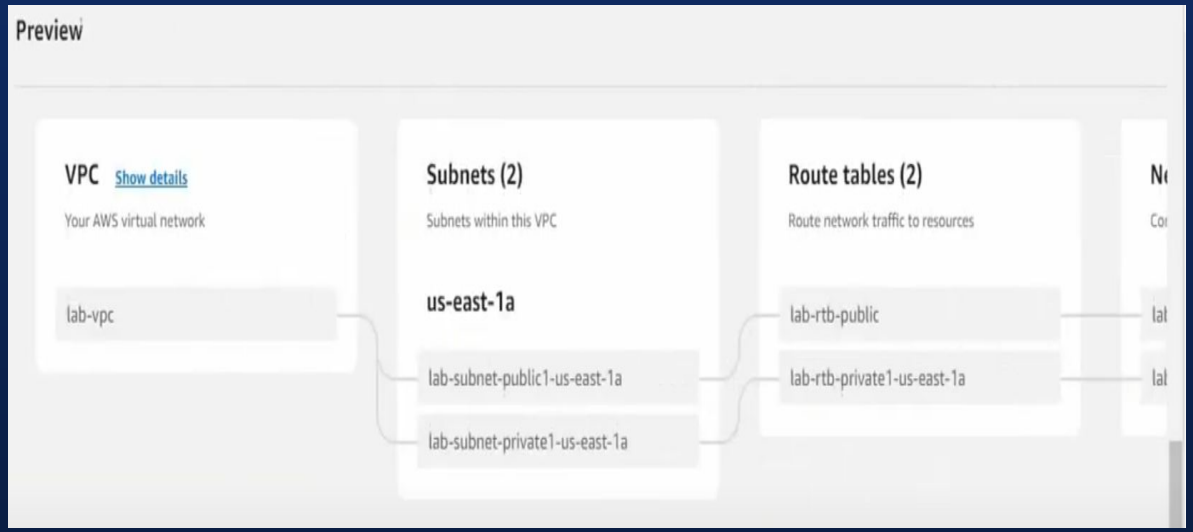
- Choose VPC and more.
- Under Name tag auto-generation, keep Auto-generate selected, however change the value from project to lab.
- Keep the IPv4 CIDR block set to 10.0.0.0/16
- For Number of Availability Zones, choose 1.
- For Number of public subnets, keep the 1 setting.
- For Number of private subnets, keep the 1 setting.
- Expand the Customize subnets CIDR blocks section
- Change Public subnet CIDR block in us-east-1a to 10.0.0.0/24
- Change Private subnet CIDR block in us-east-1a to 10.0.1.0/24
- Set NAT gateways to In 1 AZ.
- Set VPC endpoints to None.

Keep both DNS hostnames and DNS resolution enabled.

Step-4: In the Preview panel on the right, confirm the settings you have configured and then Click Create VPC

VPC: lab-vpc
Subnets:
us-east-1a
Public subnet name: lab-subnet-public1-us-east-1a
Private subnet name: lab-subnet-private1-us-east-1a

Route tables:
lab-rtb-public
lab-rtb-private1-us-east-1a
Network connections:
lab-igw
lab-nat-public1-us-east-1a



Step-5: In the left pane select create subnets options and create two subnets with the following properties:

VPC ID: lab-vpc (select from the menu).

Subnet name: lab-subnet-public2

Availability Zone: Select the second Availability Zone (for example, us-east-1b)

IPv4 CIDR block: 10.0.2.0/24

VPC ID: lab-vpc

Subnet name: lab-subnet-private2

Availability Zone: Select the second Availability Zone (for example, us-east-1b)

IPv4 CIDR block: 10.0.3.0/24

Step-6: In the left pane select create security groups.

Security group name: Web Security Group

Description: Enable HTTP access

VPC: choose the X to remove the currently selected VPC, then from the drop down list choose lab-vpc

In the Inbound rules pane, choose Add

Configure the following settings:

Type: HTTP

Source: Anywhere-IPv4

Description: Permit web requests

Step-7: Create a Amazon Linux 2023 AMI selected,t2.micro ec2 instance named Web Server1

Configure the Network settings:

Next to Network settings, choose Edit, then configure:

Network: lab-vpc
Subnet: lab-subnet-public2 (not Private!)
Auto-assign public IP: Enable
Next, you will configure the instance to use the Web Security Group that you created earlier.

Under Firewall (security groups), choose Select existing security group.

For Common security groups, select Web Security Group.

This security group will permit HTTP access to the instance.

At the bottom of the Summary panel on the right side of the screen choose Launch instance

Step-8: Check the architecture we built

- Wait until Web Server 1 shows 2/2 checks passed in the Status check column.
- This may take a few minutes. Choose the refresh icon at the top of the page every 30 seconds or so to more quickly become aware of the latest status of the instance.
- You will now connect to the web server running on the EC2 instance.
- Select Web Server 1.
- Copy the Public IPv4 DNS value shown in the Details tab at the bottom of the page.
- Open a new web browser tab, paste the Public DNS value and press Enter.

Meta-Data	Value
InstanceId	i-0a895b97f0c25e4d2
Availability Zone	us-east-1b

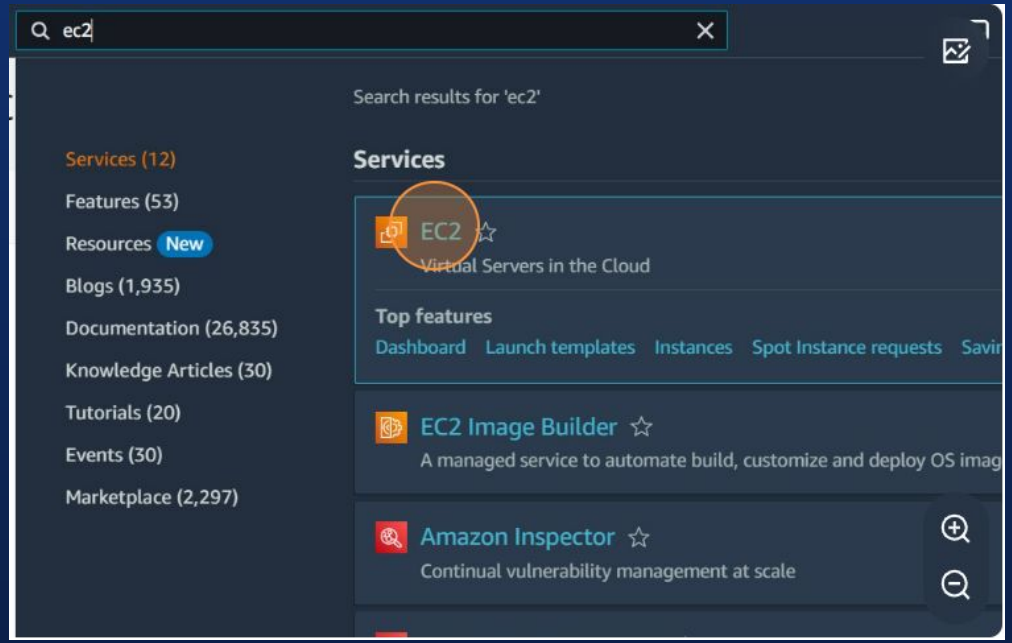
Current CPU Load: **0%**

04

AWS
Elastic Load Balancer

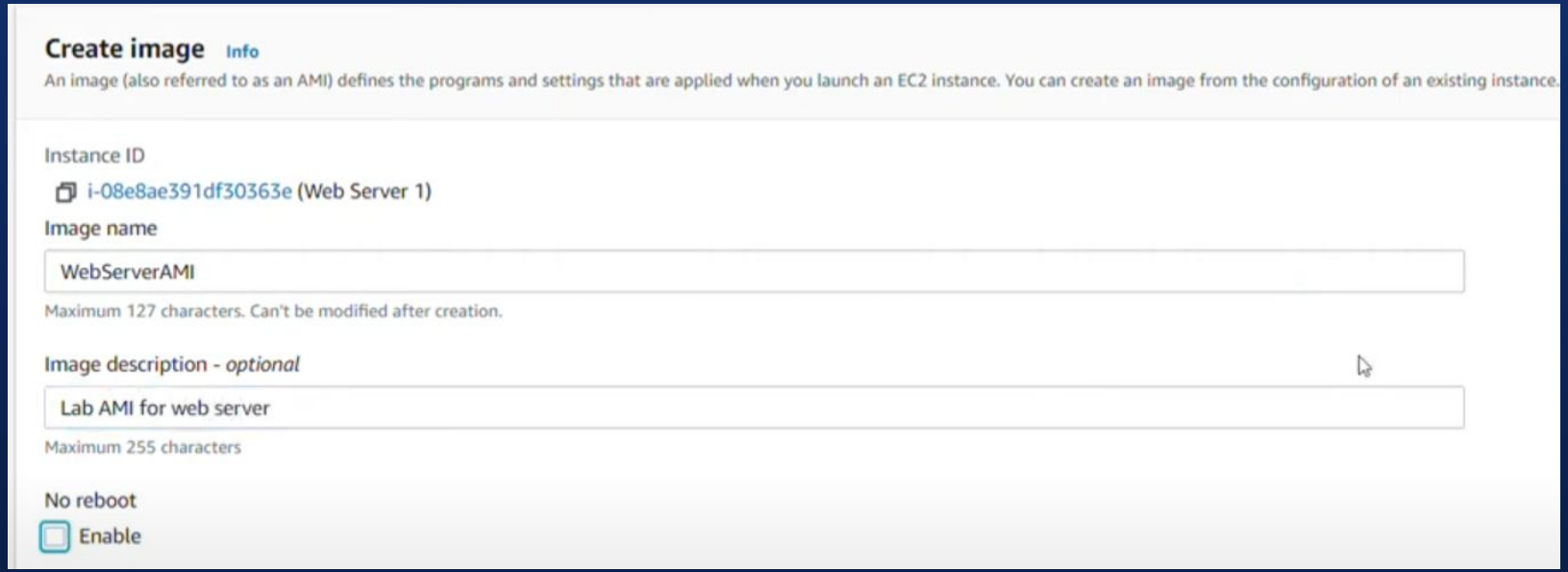
Step-1: Login to your AWS Management Console

Step-2: Click on the search field and enter EC2. Select the EC2 service



Step-3: Select Web Server 1 Instance and In the Actions menu, click Image and templates > Create image, then configure:

Image name: WebServerAMI
Image description: Lab AMI for Web Server
Click Create image



Step-4: In the left navigation pane ,select target groups

- Choose Create target group
- Choose a target type: Instances
- Target group name, enter: LabGroup
- Select Lab VPC from the VPC drop-down menu.
- Click Next and Click Create target group

Step-5: In the left navigation pane, click Load Balancers and choose Create Load Balancer.

- Under Application Load Balancer, choose Create
- Under Load balancer name, enter: LabELB
- Scroll down to the Network mapping section, then:
- For VPC, select: Lab VPC
- select Public Subnet 1 , select Public Subnet 2 from the Subnet drop down menu
- You should now have two subnets selected: Public Subnet 1 and Public Subnet 2.
- In the Security groups section:
- Choose the Security groups drop down menu and select Web Security Group
- Below the drop down menu, choose the X next to the default security group to remove it.
- The Web Security Group security group should now be the only one that appears.
- For the Listener HTTP:80 row, set the Default action to forward to LabGroup.
- Scroll to the bottom and choose Create load balancer

The load balancer is successfully created.

Load Balancer Creation Status

Successfully created load balancer

Load balancer LabELB was successfully created.

Note: It might take a few minutes for your load balancer to be fully set up and ready to route traffic, and for the targets to complete the registration process and pass the initial health checks.

Suggested next steps

- Discover other services that you can integrate with your load balancer. Visit the **Integrated services** tab within LabELB
- Consider using AWS Global Accelerator to further improve the availability and performance of your applications. AWS Global Accelerator console

Close

Step-6: In the left navigation pane ,select Launch Configurations and create a Launch Configuration with the following properties

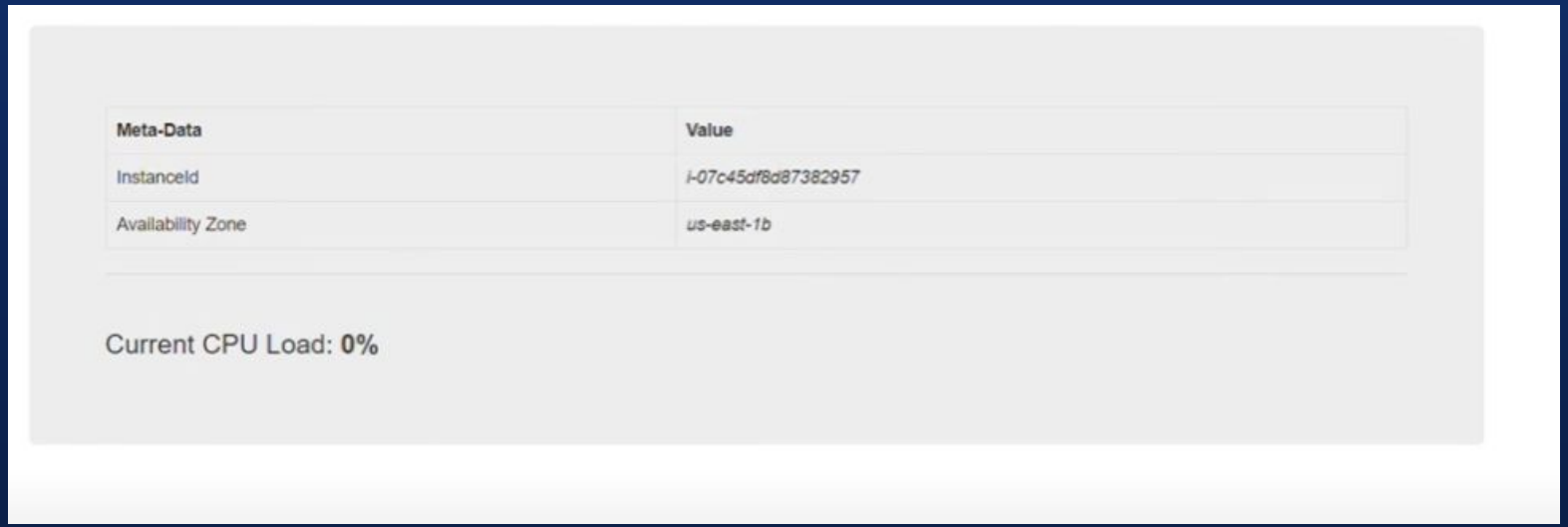
Launch configuration name: LabConfig
Amazon Machine Image (AMI) Choose Web Server AMI
Instance type: Select t3.micro

Choose Select an existing security group and Select Web Security Group
Under Key pair configure: choose vockey

From the Actions menu, choose Create Auto Scaling group
Enter Auto Scaling group name:
Name: Lab Auto Scaling Group
Choose Next

Step-7: Verify that the Load Balancing is working

- In the left navigation pane, click Instances.
- confirm that the new instances have passed their Health Check.
- In the left navigation pane, click Load Balancers.
- In the lower pane, copy the DNS name of the load balancer, making sure to omit "(A Record)".
- Open a new web browser tab, paste the DNS Name you just copied, and press Enter.



Meta-Data	Value
InstanceId	i-07c45df8d87382957
Availability Zone	us-east-1b

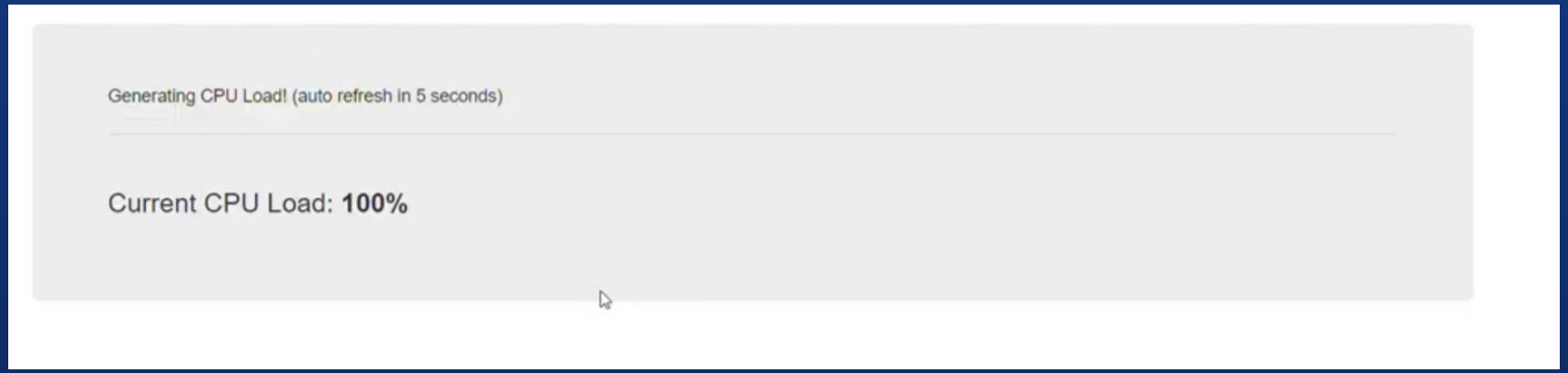
Current CPU Load: **0%**

Step-8: Update the auto scaling group

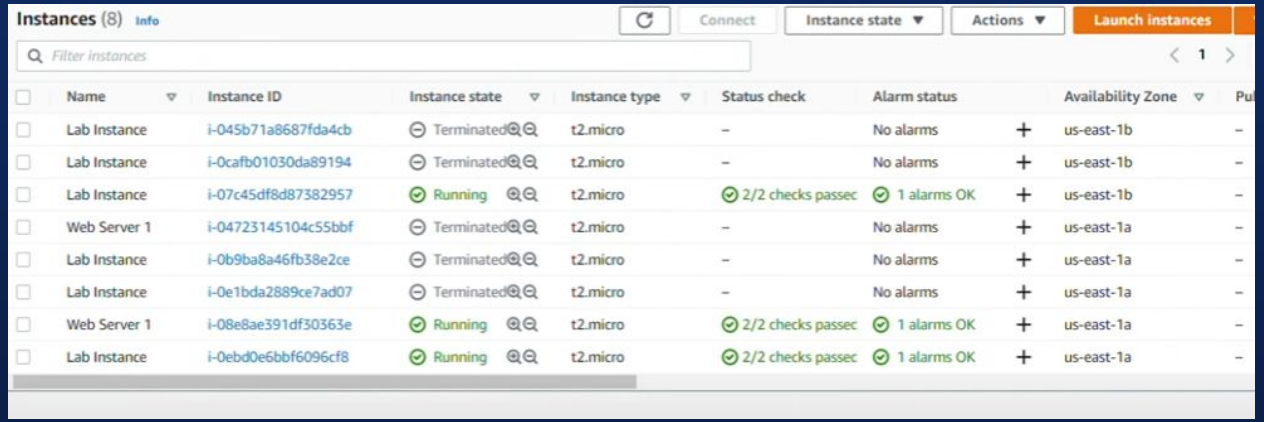
- In the left navigation pane, choose Auto Scaling Groups.
- Select Lab Auto Scaling Group.
- In the bottom half of the page, choose the Automatic Scaling tab.
- Select LabScalingPolicy.
- Click Actions and Edit.
- Change the Target Value to 50.
- Click Update

Step-9: Test the alarm trigger for auto scaling

- Return to the browser tab with the web application.
- Click Load Test beside the AWS logo.
- Return to browser tab with the CloudWatch console.
- In less than 5 minutes, the AlarmLow alarm should change to OK and the AlarmHigh alarm status should change to In alarm.
- On the Services menu, click EC2.
- In the left navigation pane, click Instances.
- More than two instances labeled Lab Instance should now be running. The new instance(s) were created by Auto Scaling in response to the Alarm.



Step-10: Terminate the instances



Instances (8) Info

Connect | Instance state | Actions | Launch instances

Filter instances

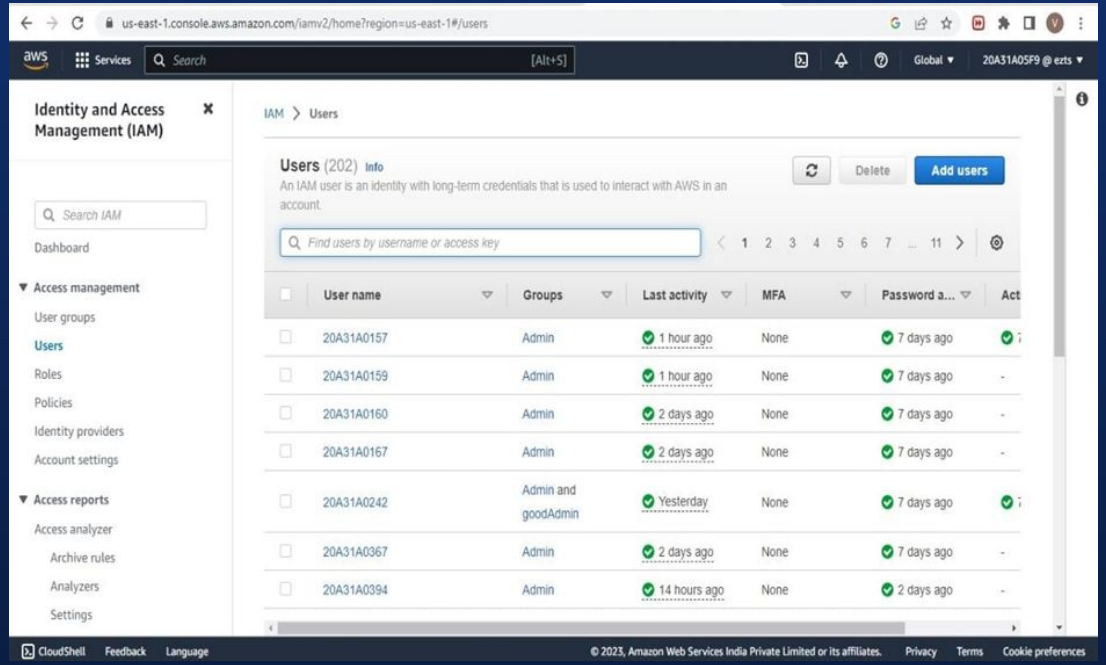
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Lab Instance	i-045b71a8687fda4cb	Terminated	t2.micro	–	No alarms	us-east-1b
Lab Instance	i-0cafb01030da89194	Terminated	t2.micro	–	No alarms	us-east-1b
Lab Instance	i-07c45df8d87382957	Running	t2.micro	2/2 checks passed	1 alarms OK	us-east-1b
Web Server 1	i-04723145104c55bbf	Terminated	t2.micro	–	No alarms	us-east-1a
Lab Instance	i-0b9ba8a46fb38e2ce	Terminated	t2.micro	–	No alarms	us-east-1a
Lab Instance	i-0e1bda2889ce7ad07	Terminated	t2.micro	–	No alarms	us-east-1a
Web Server 1	i-08e8ae391df30363e	Running	t2.micro	2/2 checks passed	1 alarms OK	us-east-1a
Lab Instance	i-0ebd0e6bbf6096cf8	Running	t2.micro	2/2 checks passed	1 alarms OK	us-east-1a

05

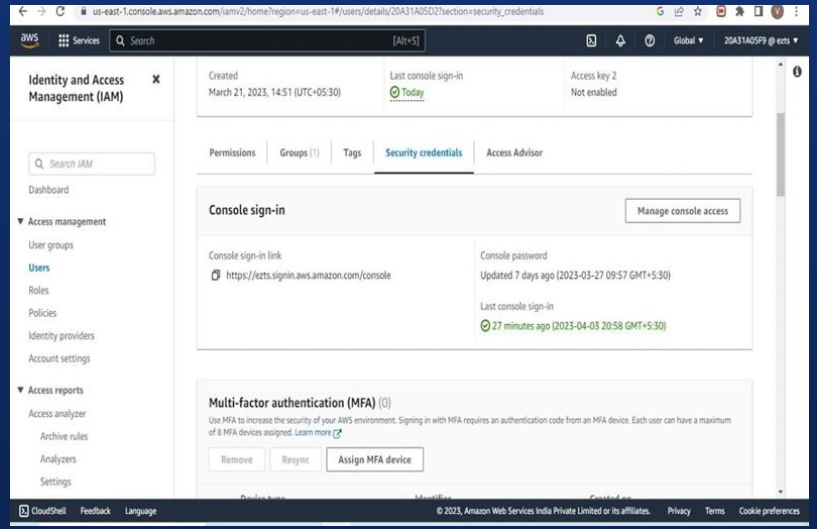
AWS Command Line Interface

AWS COMMAND LINE INTERFACE

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



Step 4 - In the users select the name of the user whose access keys you want to create.
Step 5 – Click on the Security Credentials tab.



Step 6 - In the access Keys section , choose Create access key.

Step 6 – Now you can use this access key to configure CLI

Step 7 - 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

06

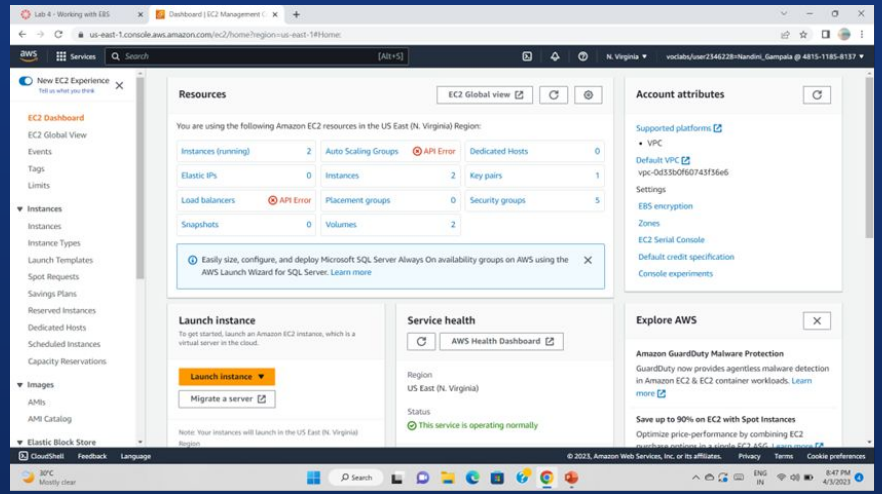
AWS
Elastic Block Storage

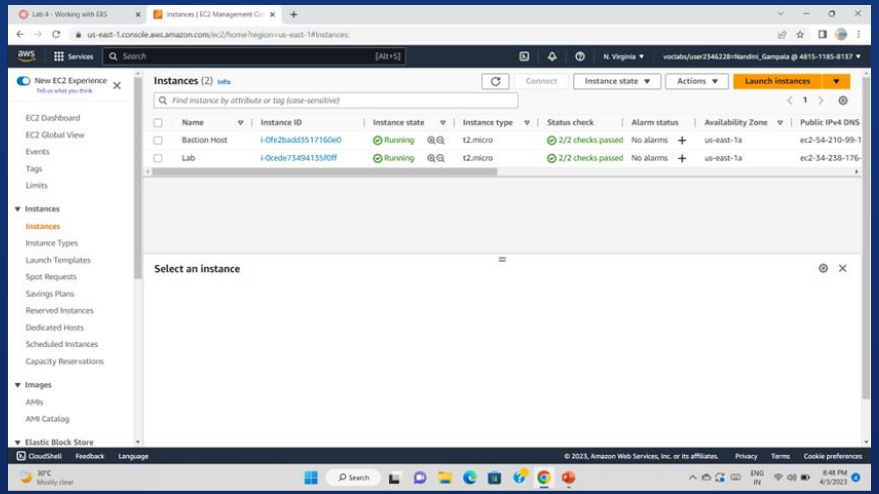
CREATING A EBS VOLUME

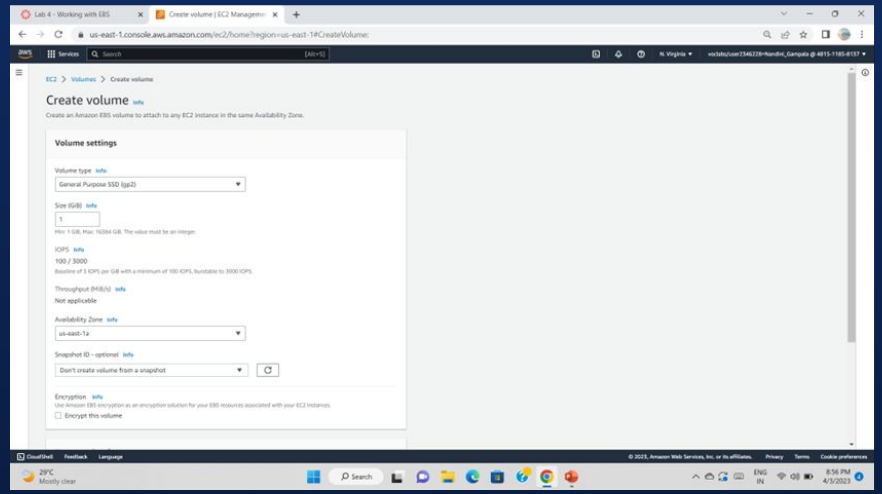
1. Open Management Console, on the services menu, open Ec2
2. In the left navigation pane choose instances and create an instance with a name
3. Next, In the left navigation pane choose Volumes
4. Click on Create Volume
5. Select volume type, size(Gib), and Availability Zone, and in Add tag section add key and value names.
6. Then click on create volume
7. Click on volumes on the left navigation pane select the created volume and attach a previously created instance to it.
8. Download the ppk file
9. Then, go to the “Details” drop-down, choose “show”
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 look like: df –h

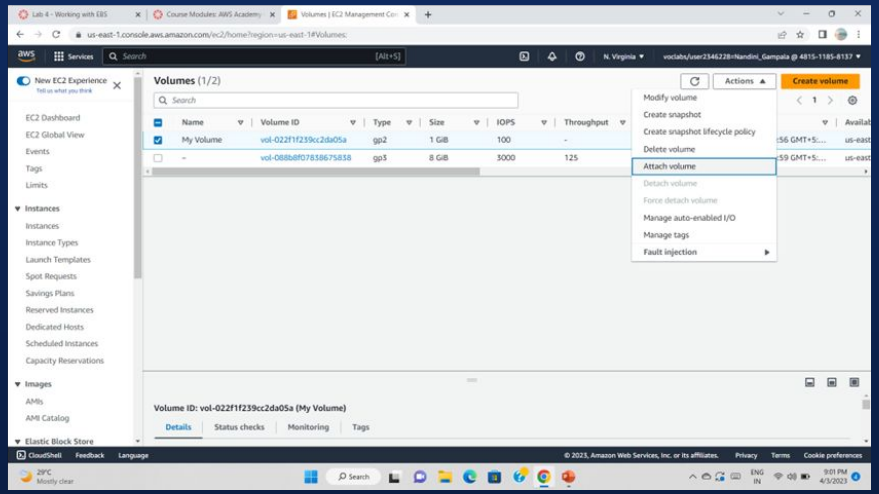
sudo mkfs –t ext3/dev/sdf etc.,

14. Create an EBS snapshot by giving the necessary fields.
15. Create a volume using a snapshot.
16. Attach the volume to the created EC2 instance


Lab 4 - Working with EBS
Dashboard | EC2 Management C
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Home:
Services
Search
[Alt+S]
N. Virginia
voclabs/user2346228=Nandini_Gampala @ 4815-1185-8137
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
AMI Catalog
Elastic Block Store
Resources
EC2 Global view
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 API Error
Placement groups 0
Security groups 5
Snapshots 0
Volumes 2
Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more
Account attributes
Supported platforms
VPC
Default VPC
vpc-0d33b0f60743f36e6
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
Note: Your instances will launch in the US East (N. Virginia) Region
Service health
AWS Health Dashboard
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
Optimize price-performance by combining EC2
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Lab 4 - Working with EBS
Instances | EC2 Management Co
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:
Services
Search
[Alt+S]
N. Virginia
voclabs/user2346228=Nandini_Gampala @ 4815-1185-8137
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
AMI Catalog
Elastic Block Store
Instances (2) Info
Connect
Instance state
Actions
Launch instances
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-0fe2badd5517160e0
Running
t2.micro
2/2 checks passed
No alarms
us-east-1a
ec2-54-210-99-1
Lab
i-0cede75494135f0ff
Running
t2.micro
2/2 checks passed
No alarms
us-east-1a
ec2-34-238-176-
Select an instance
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Lab 4 - Working with EBS
Create volume | EC2 Managemen
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateVolume:
Services
Search
[Alt+S]
N. Virginia
voclabs/user2346228=Nandini_Gampala @ 4815-1185-8137
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 Info
General Purpose SSD (gp2)
Size (GiB) Info
1
Min: 1 GiB, Max: 16384 GiB. The value must be an integer.
IOPS Info
100 / 3000
Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.
Throughput (MiB/s) Info
Not applicable
Availability Zone Info
us-east-1a
Snapshot ID - optional Info
Don't create volume from a snapshot
Encryption Info
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.
Encrypt this volume
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

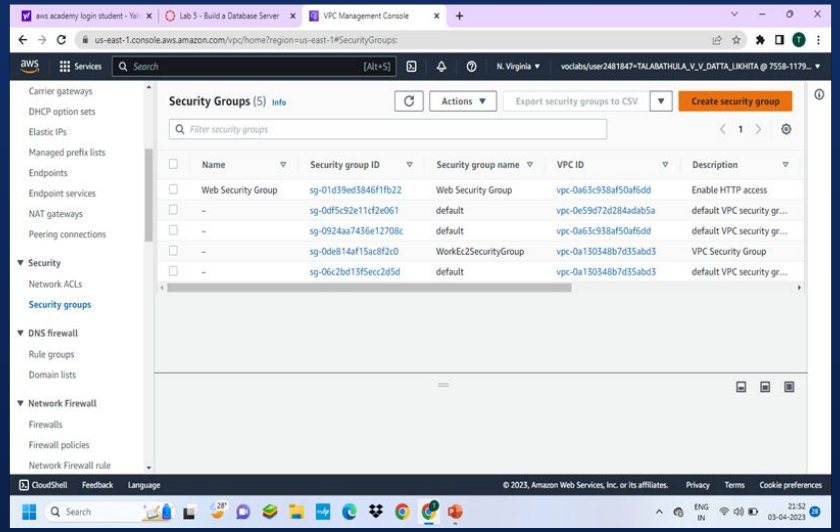

Lab 4 - Working with EBS
Course Modules: AWS Academy
Volumes | EC2 Management Co
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Volumes:
Services
Search
[Alt+S]
N. Virginia
voclabs/user2346228=Nandini_Gampala @ 4815-1185-8137
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes (1/2)
Actions
Create volume
Search
Name
Volume ID
Type
Size
IOPS
Throughput
My Volume
vol-022f1f239cc2da05a
gp2
1 GiB
100
-
vol-088b8f07858675858
gp3
8 GiB
3000
125
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
Volume ID: vol-022f1f239cc2da05a (My Volume)
Details
Status checks
Monitoring
Tags
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

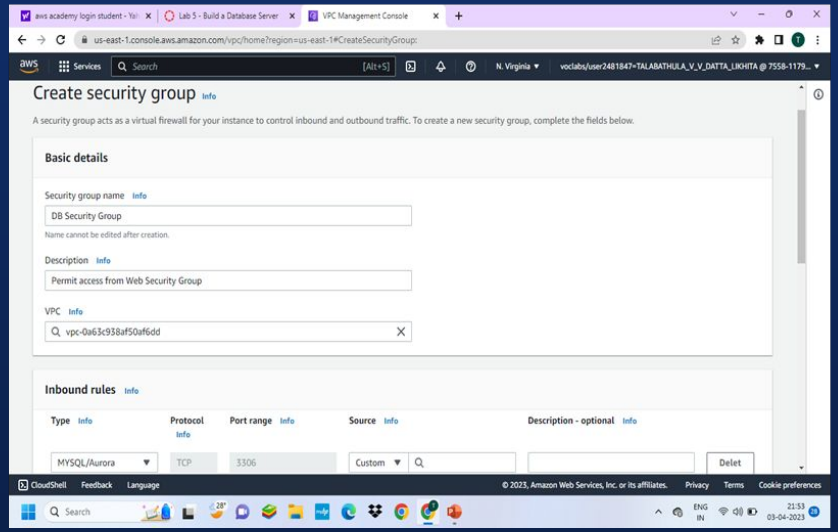
07

AWS RDS

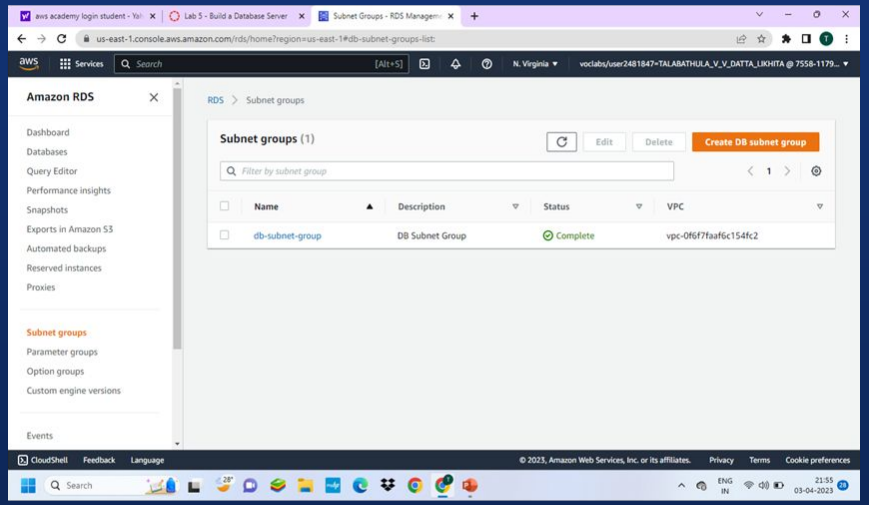
AWS RDS

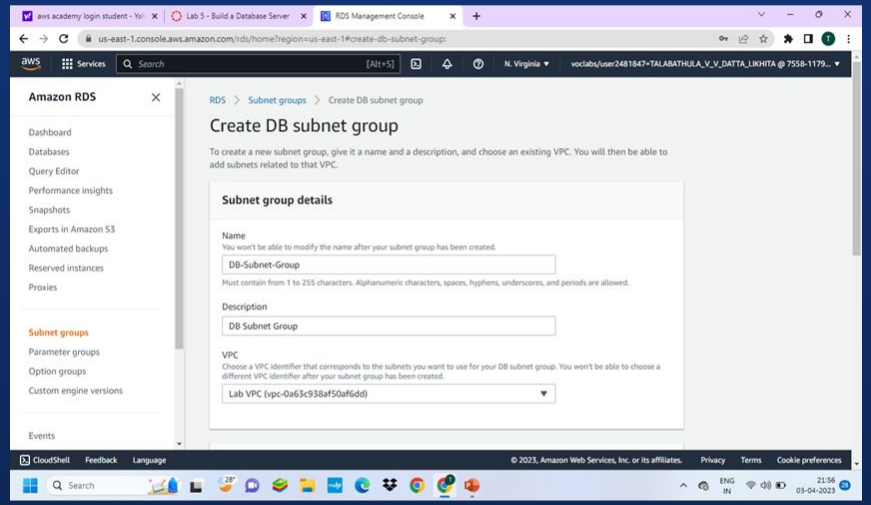
Step 1: Create a Security Group for the RDS DB Instance.
AWS management console → vpc → security groups → choose to create security group → and add an inbound rule → to create a security group.



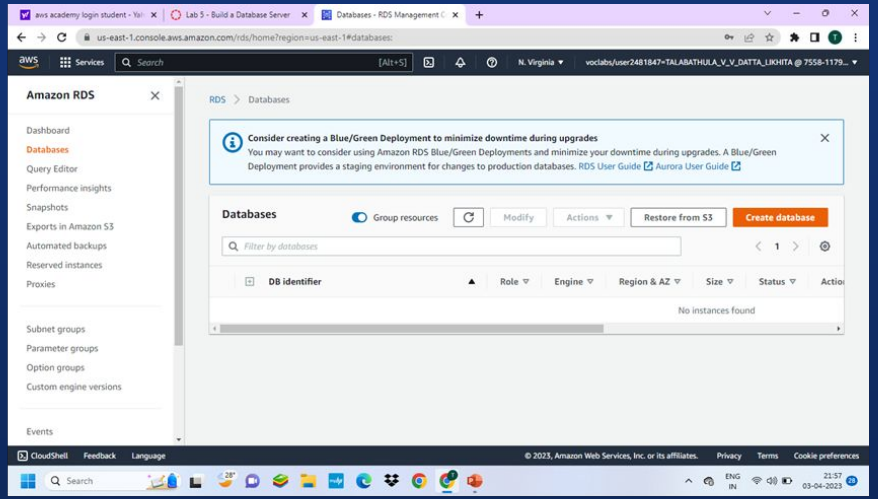


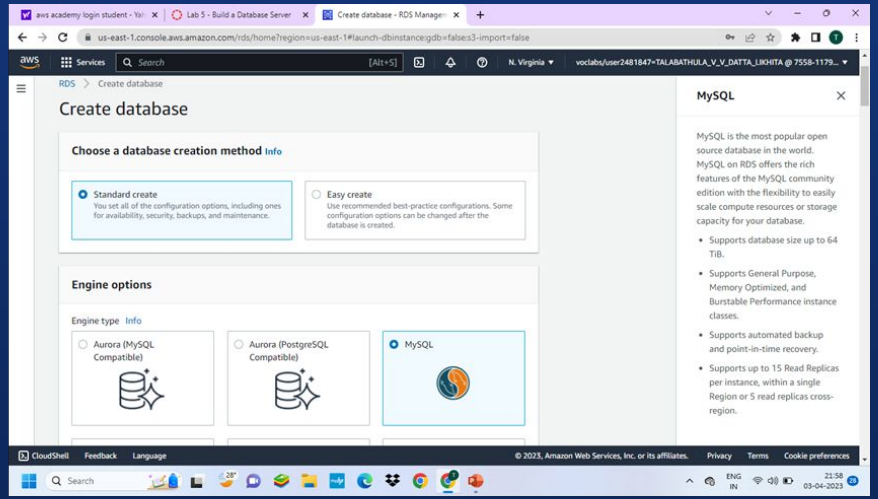
Step 2 : Create a DB Subnet Group.Rds → subnet groups → choose create DB subnet group → add subnets → create DB subnet group.



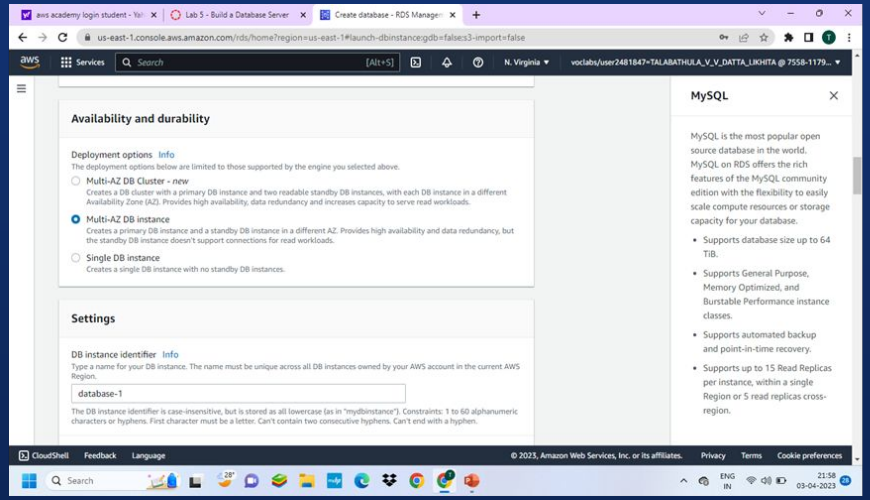


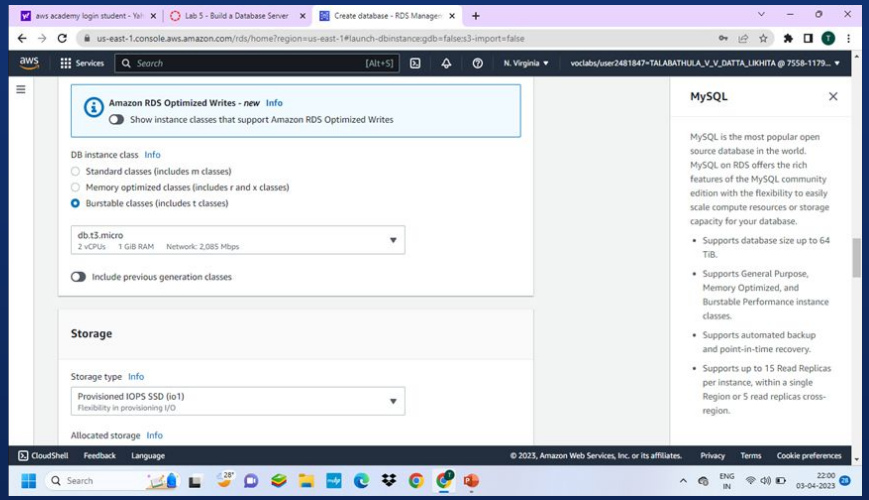
Step 3: In the left navigation pane, choose **Databases** → choose create database → MYSQL



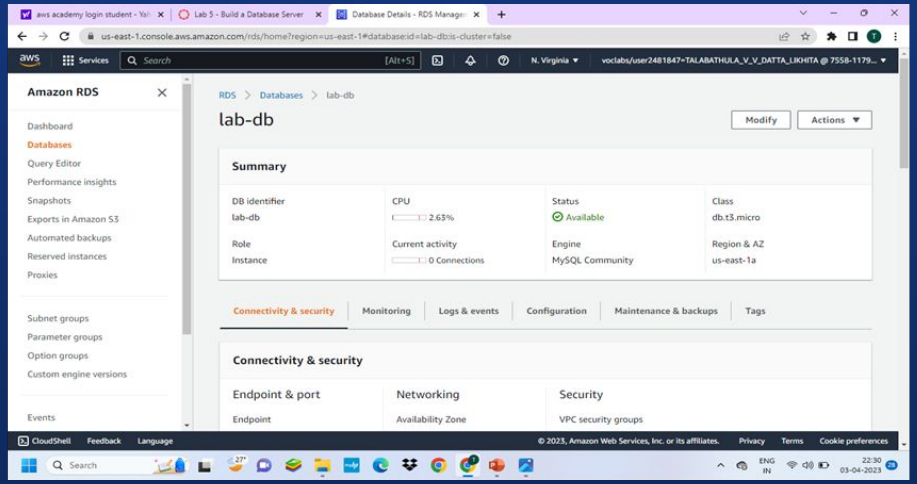


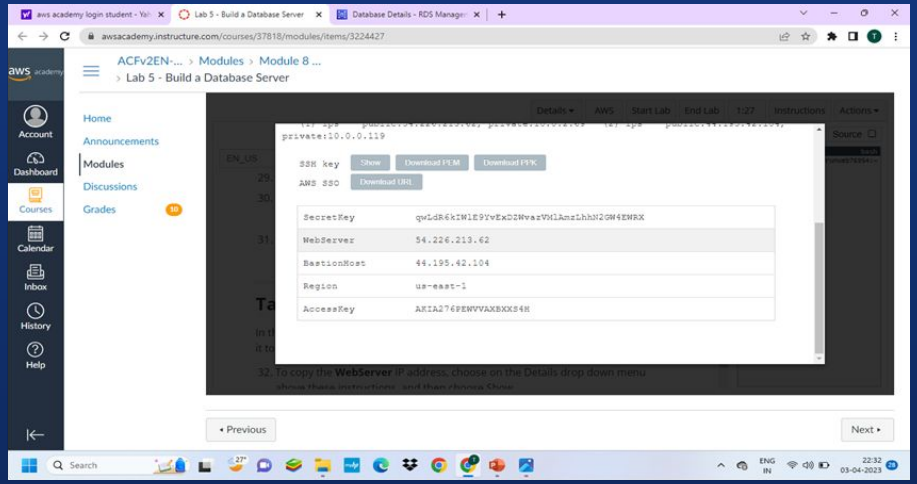
Step 4: In Availability and durability, choose Multi–AZ DB instance then configure settings, DB instance class, Storage, connectivity, choose existing vpc security group, and set up additional configuration.



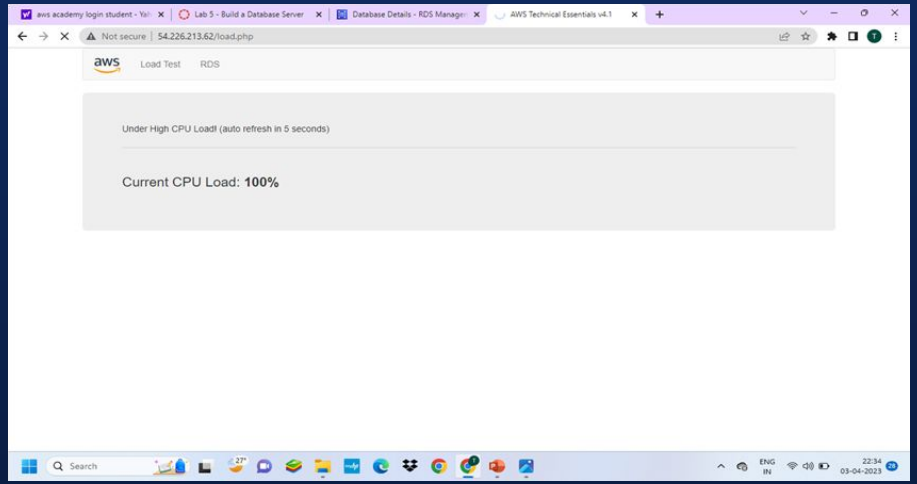


Step 5: Wait until Info changes to Modifying or Available.
Scroll down to the Connectivity & security section and copy the **Endpoint** field.

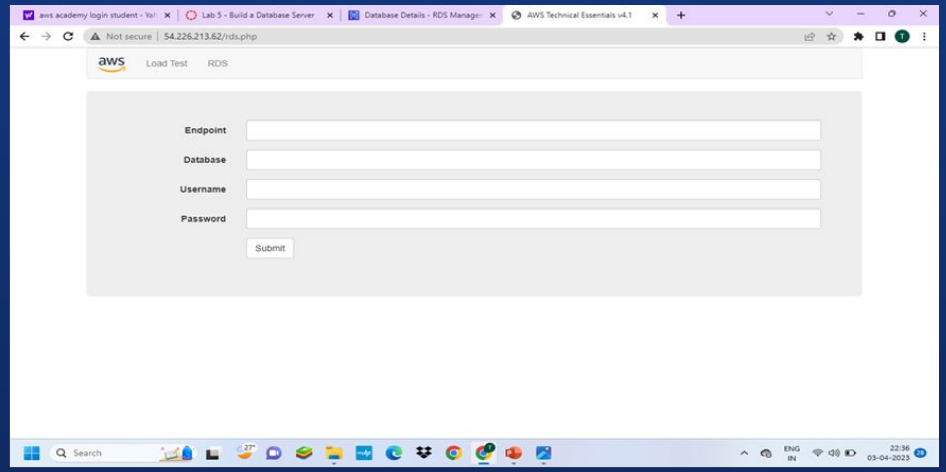




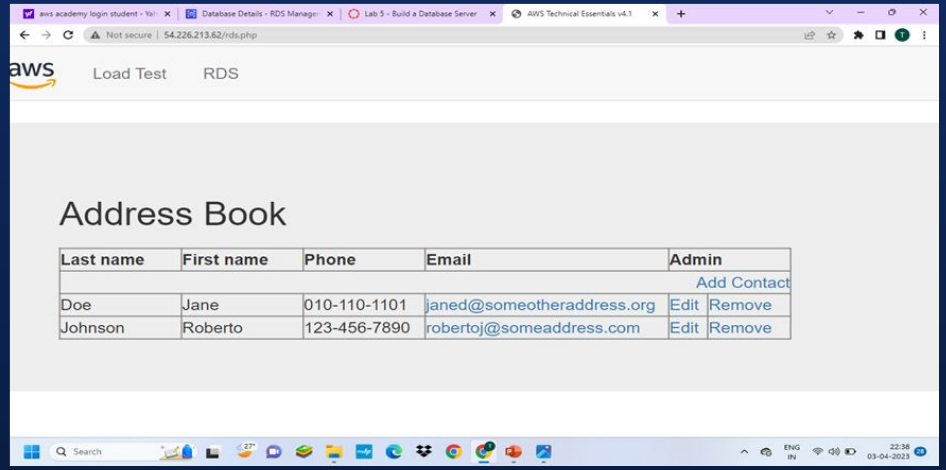
Step 6 : Interact with Your Database.
On Details , copy the **WebServer** IP address.
Open a new web browser tab, paste the WebServer IP address and press Enter.
The web application will be displayed, showing information about the EC2 instance.



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.



THANK YOU

05

OPERATING PLAN

05

OPERATING PLAN