Practical Implementation of AWS Services

Name - K.Naga Sri Lakshmi
Roll No - 20A31A4214

LAB 1 - EC2

LAB 1 - Introduction to Amazon EC2

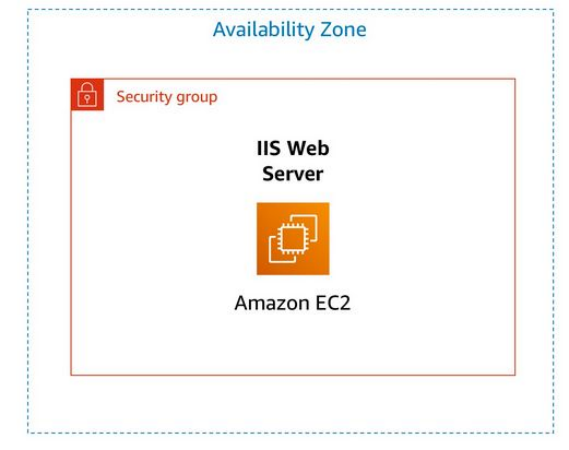
Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.

Setting up an EC2 Instance-

This lab provides us with a basic overview of launching, resizing, managing, and monitoring an Amazon EC2 instance.

We do the following in this lab

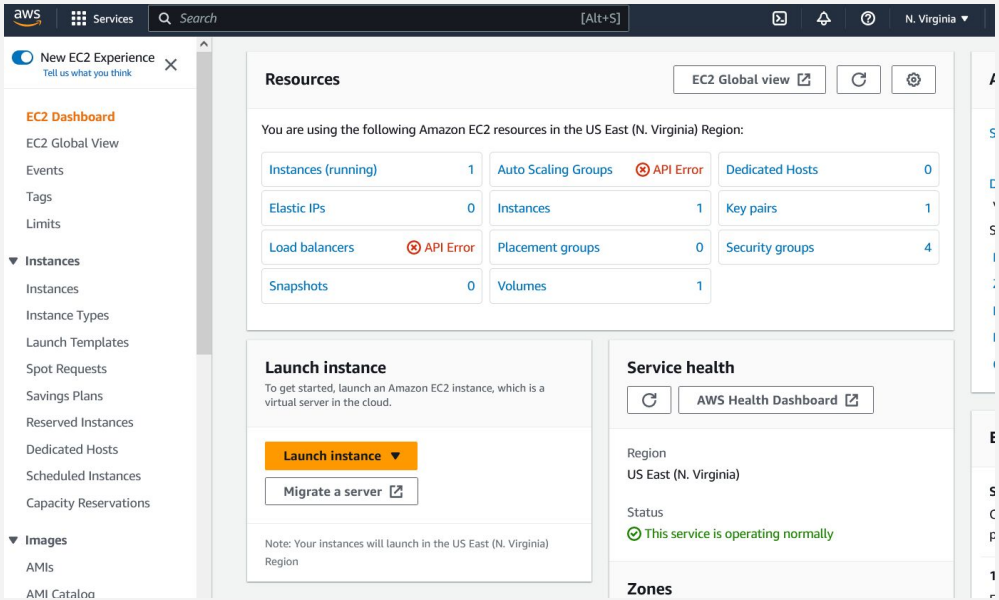
- Launch a web server with termination protection enabled
- Monitor Your EC2 instance
- Modify the security group that your web server is using to allow HTTP access
- Resize your Amazon EC2 instance to scale
- Explore EC2 limits
- Test termination protection
- Terminate your EC2 instance

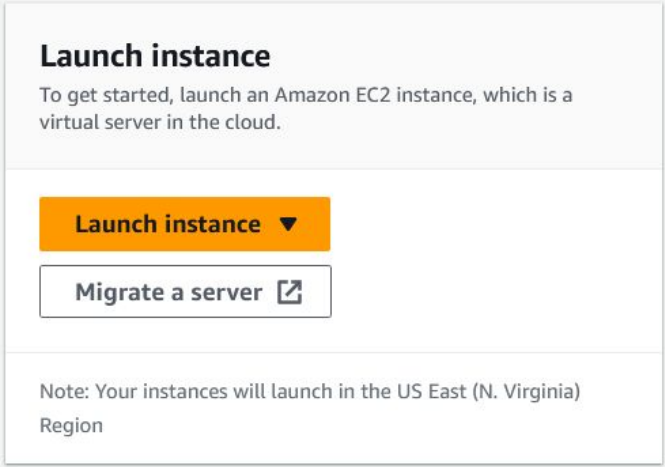


Task 1: Launch Your Amazon EC2 Instance

In the **AWS Management Console** choose **Services**, choose **Compute** and then choose **EC2**.
Note: Verify that your EC2 console is currently managing resources in the **N. Virginia** (us-east-1) region. And Verify that you are the same region by looking at the drop down menu at the top of the screen, to the left of your username. If it does not already indicate N. Virginia, choose the N. Virginia region from the region menu before proceeding to the next step.

Choose the Launch instance menu and select **Launch instance**.





Step 1: Name and tags

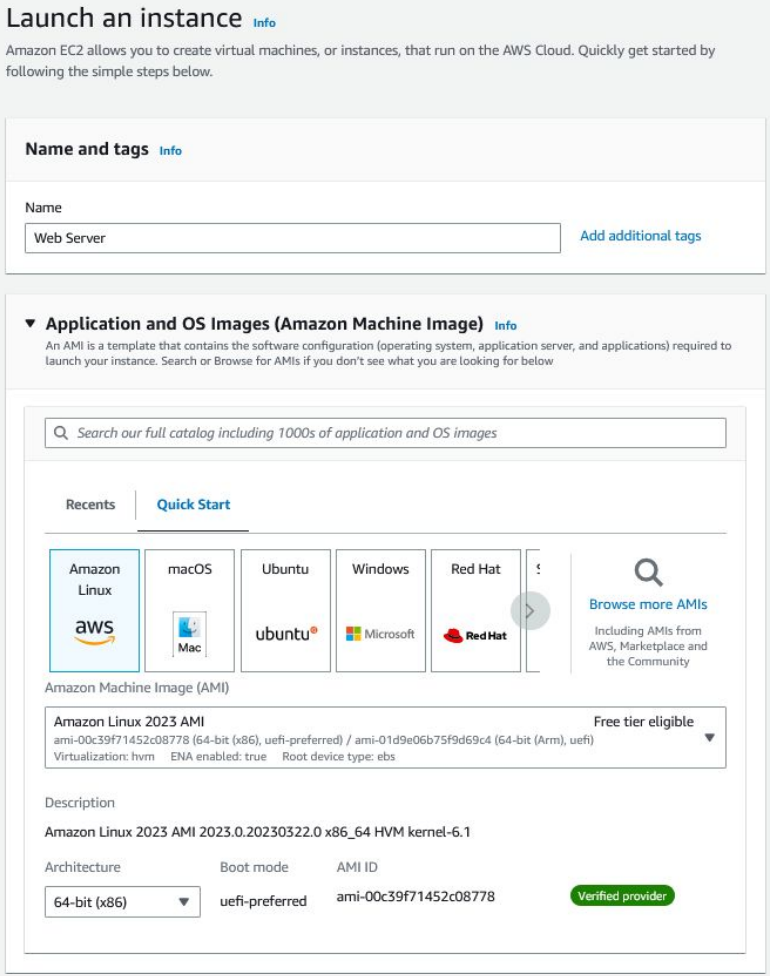
Give the instance the name `Web Server`.

- The Name you give this instance will be stored as a tag.
- Each tag consists of a Key and a Value, both of which you define. You can define multiple tags to associate with the instance if you want to.
- In this case, the tag that will be created will consist of a *key* called `Name` with a *value* of `Web Server`

Step 2: Application and OS Images (Amazon Machine Image)

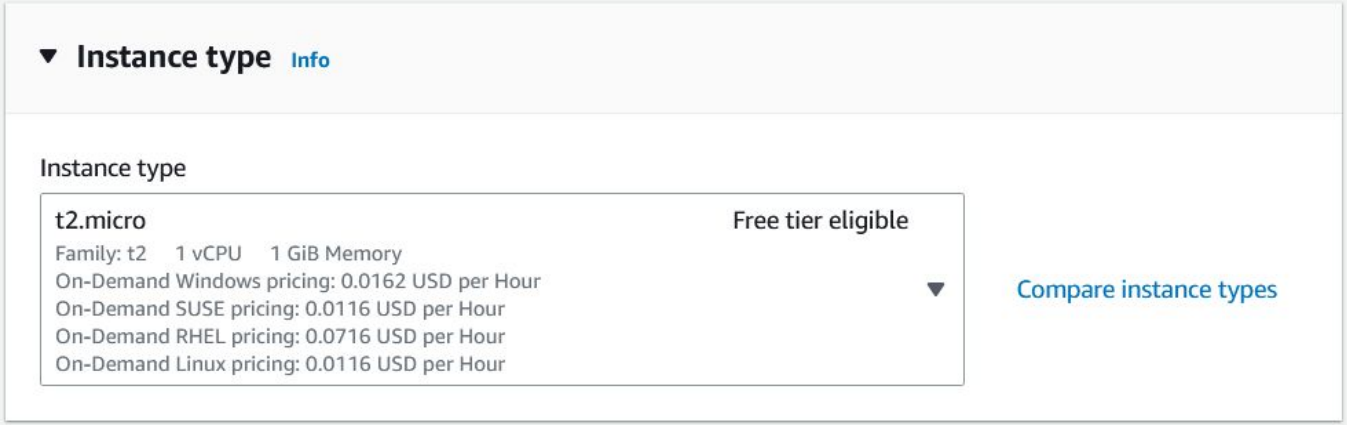
In the list of available *Quick Start* AMIs, keep the default

- **Amazon Linux** AMI selected.
  Also keep the default **Amazon Linux 2023 AMI** selected.
- An **Amazon Machine Image (AMI)** provides the information required to launch an instance, which is a virtual server in the cloud.



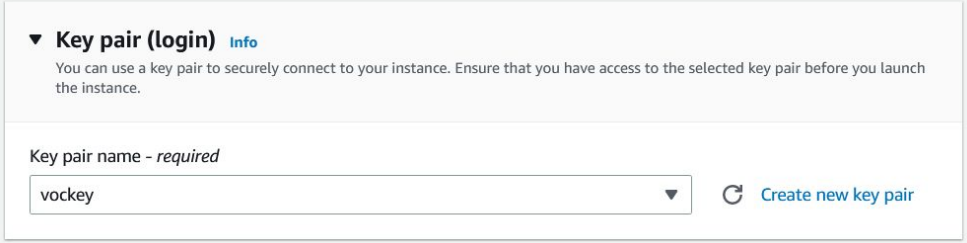
Step 3: Instance type

- In the *Instance type* panel, keep the default **t2.micro** selected.
- Amazon EC2 provides a wide selection of *instance types* optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications. Each instance type includes one or more *instance sizes*, allowing you to scale your resources to the requirements of your target workload.
- The t2.micro instance type has 1 virtual CPU and 1 GiB of memory.



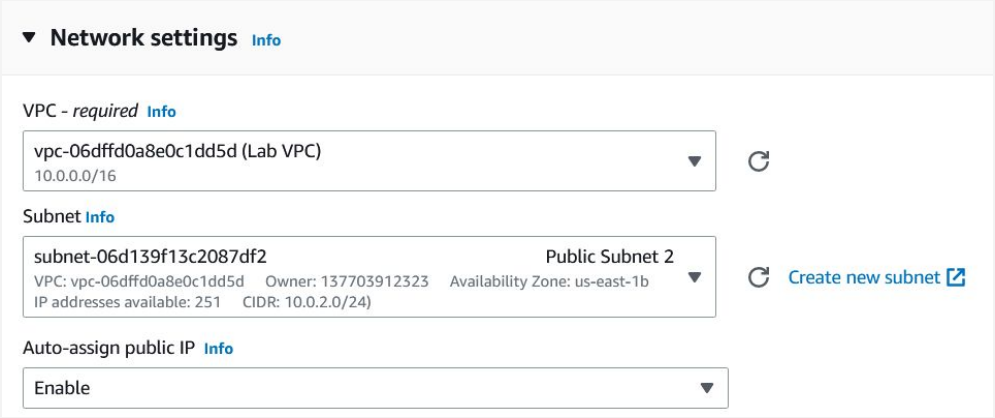
Step 4: Key pair (login)

For **Key pair name - *required***, choose **vockey**.
Amazon EC2 uses public–key cryptography to encrypt and decrypt login information.



Step 5: Network settings

- Next to Network settings, choose **Edit**.
- For **VPC**, select **Lab VPC**.
  The Lab VPC was created using an AWS CloudFormation template during the setup process of your lab. This VPC includes two public subnets in two different Availability Zones.
- Keep the default subnet. This is the subnet in which the instance will run. Notice also that by default, the instance will be assigned a public IP address.



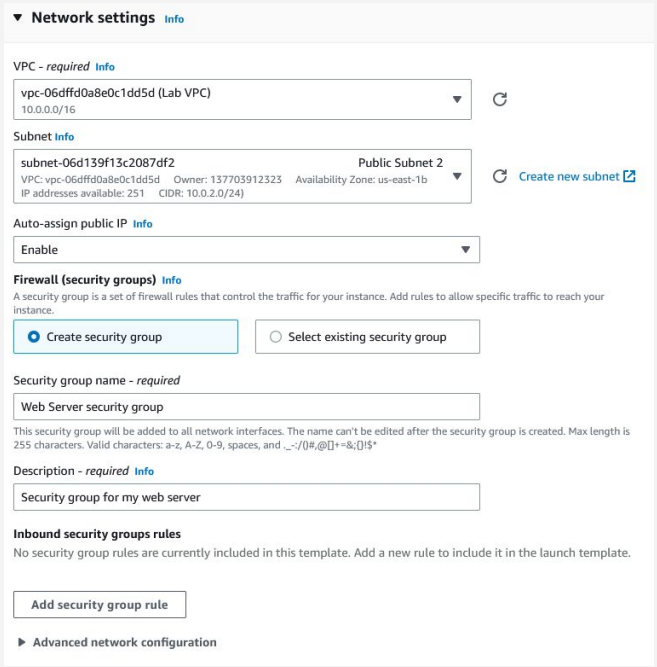
Under **Firewall (security groups)**, choose **Create security group** and configure:

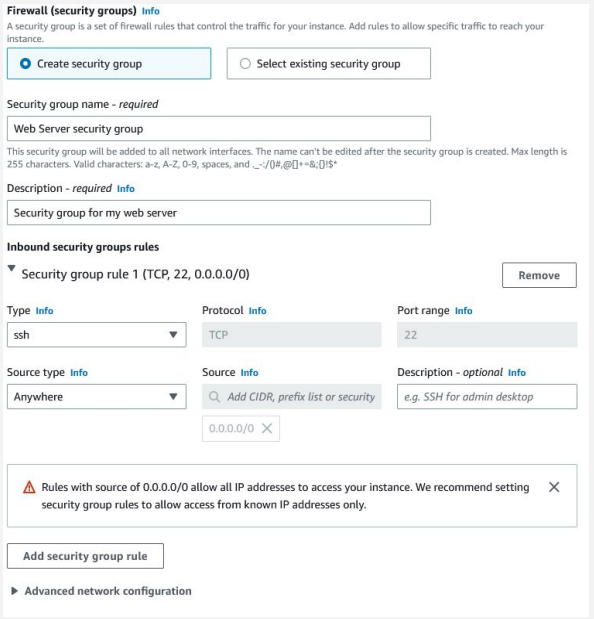
Security group name: `Web Server security group`

Description: `Security group for my web server`

A security group acts as a virtual firewall that controls the traffic for one or more instances.

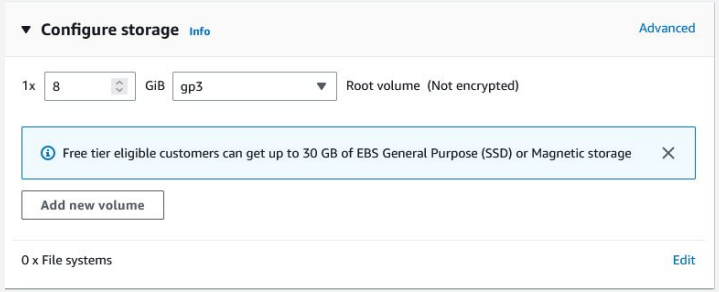
Under **Inbound security group rules**, notice that one rule exists. **Remove** this rule.





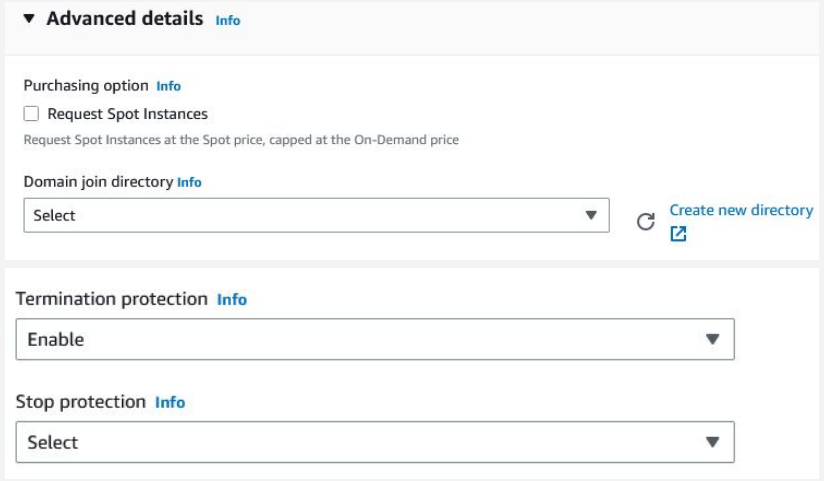
Step 6: Configure storage

In the Configure storage section, keep the default settings.
Amazon EC2 stores data on a network-attached virtual disk called Elastic Block Store.
You will launch the Amazon EC2 instance using a default 8 GiB disk volume. This will be your root volume (also known as a 'boot' volume).



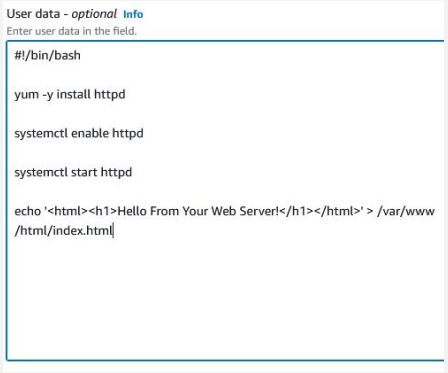
Step 7: Advanced details

Expand **Advanced details**.
For **Termination protection**, select **Enable**.
When an Amazon EC2 instance is no longer required, it can be *terminated*, which means that the instance is deleted and its resources are released.



- Scroll to the bottom of the page and then copy and paste the code shown below into the **User data** box:

  #!/bin/bash
  yum -y install httpd
  systemctl enable httpd
  systemctl start httpd
  echo '<html><h1>Hello From Your Web Server!</h1></html>' > /var/www/html/index.html



- When you launch an instance, you can pass *user data* to the instance that can be used

  to perform automated installation and configuration tasks after the instance starts. Your instance is running Amazon Linux 2. The *shell script* you have specified

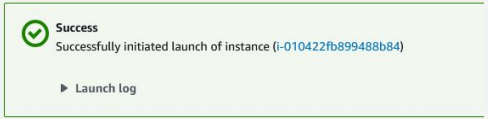
  will run as the *root* guest OS user when the instance starts.

The script will:

- ❏ Install an Apache web server (httpd)
- ❏ Configure the web server to automatically start on boot
- ❏ Run the Web server once it has finished installing
- ❏ Create a simple web page

Step 8: Launch the instance

At the bottom of the **Summary** panel on the right side of the screen choose Launch instance
You will see a Success message.

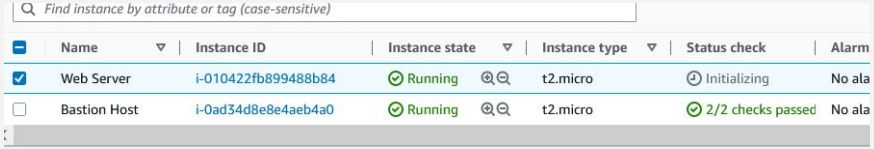


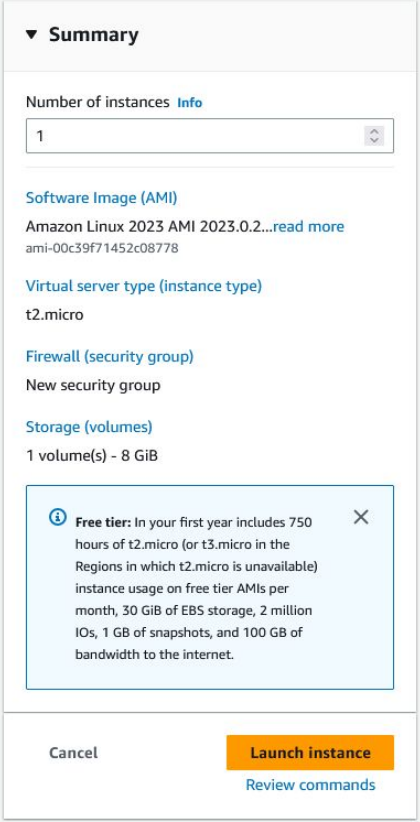
Choose View all instances

In the Instances list, select **Web Server**.

Review the information displayed in the **Details** tab.

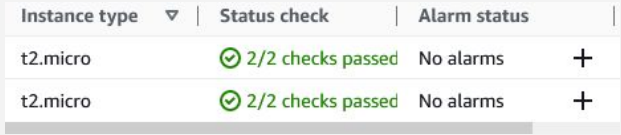
It includes information about the instance type,
security settings and network settings. The instance is assigned a *Public IPv4 DNS* that you can use to contact the instance from the Internet.
At first, the instance will appear in a *Pending* state, which means
it is being launched. It will then change to *Initializing*, and finally to *Running*..





Wait for your instance to display the following:

- **Instance State:** *Running*
- **Status Checks:** *2/2 checks passed*

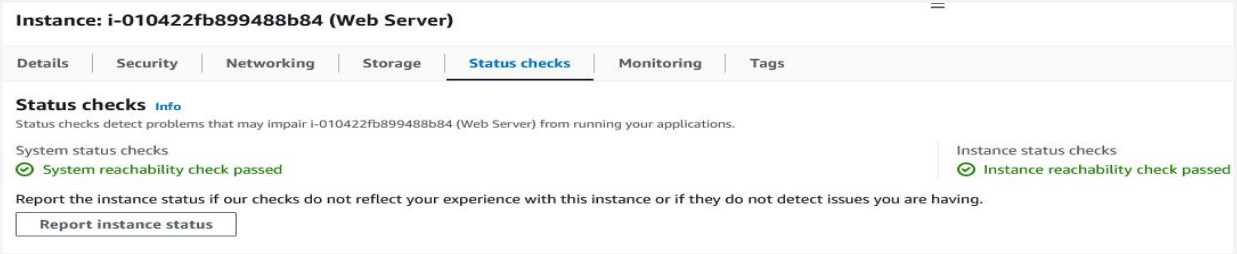


Congratulations! We have successfully launched your first Amazon EC2 instance.

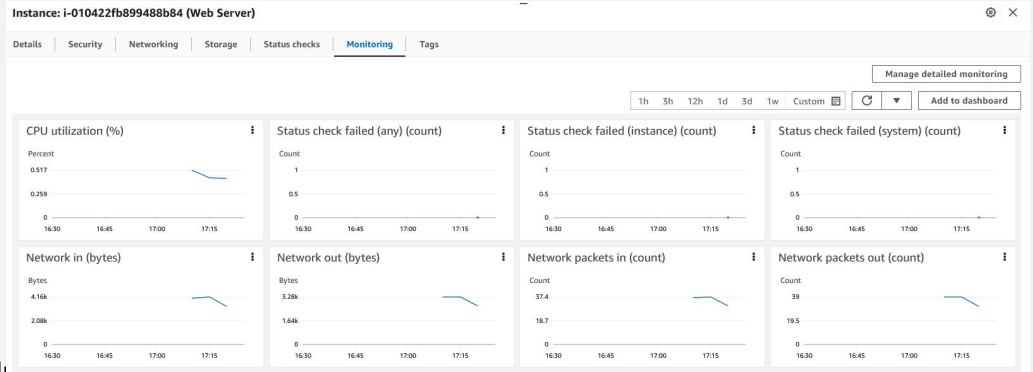
Task 2: Monitor Your Instance

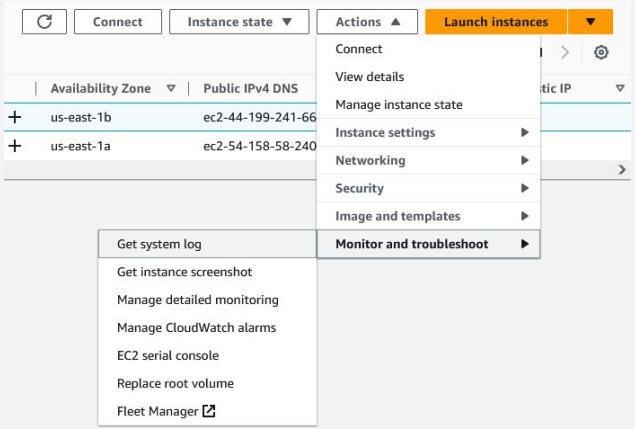
Monitoring is an important part of maintaining the reliability, availability, and performance of your Amazon Elastic Compute Cloud (Amazon EC2) instances and your AWS solutions.

Choose the **Status checks** tab.
With instance status monitoring, you can quickly determine whether Amazon EC2 has detected any problems that might prevent your instances from running applications. Amazon EC2 performs automated checks on every running EC2 instance to identify hardware and software issues.
Notice that both the **System reachability** and **Instance reachability** checks have passed.



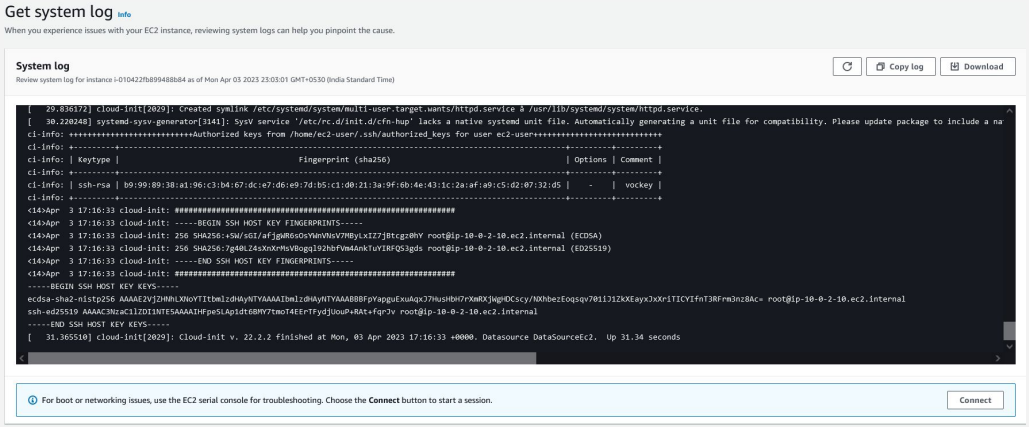
Choose the **Monitoring** tab.
This tab displays Amazon CloudWatch metrics for your instance. Currently, there are not many metrics to display because the instance was recently launched.
You can choose the three dots icon in any graph and select **Enlarge** to see an expanded view of the chosen metric.
Amazon EC2 sends metrics to Amazon CloudWatch for your EC2 instances. Basic (five-minute) monitoring is enabled by default. You can also enable detailed (one-minute) monitoring.





In the Actions menu towards the top of the console, select **Monitor and troubleshoot** > **Get system log**.
The System Log displays the console output of the instance, which is a valuable tool for problem diagnosis. It is especially useful for troubleshooting kernel problems and service configuration issues that could cause an instance to terminate or become unreachable before its SSH daemon can be started. If you do not see a system log, wait a few minutes and then try again.

Scroll through the output and note that the HTTP package was installed from the **user data** that you added when you created the instance.

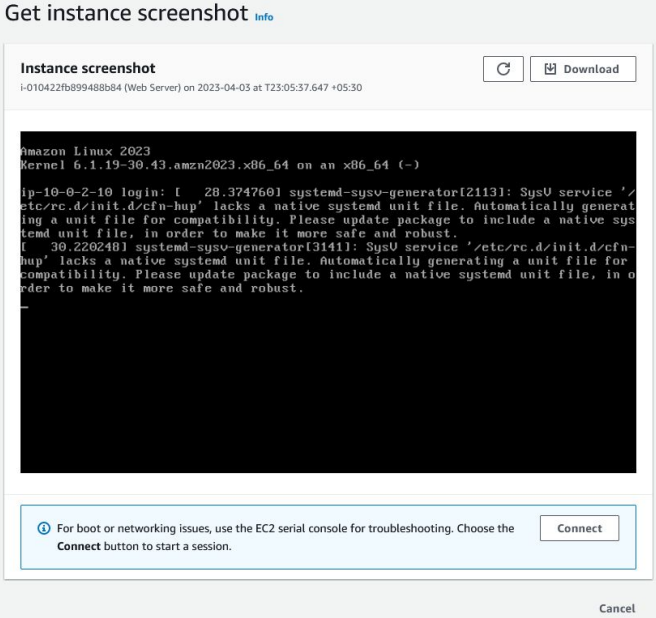


Choose **Cancel**.

Ensure **Web Server** is still selected. Then, in the Actions menu, select **Monitor and troubleshoot Get instance screenshot**.

This shows you what your Amazon EC2 instance console would look like if a screen were attached to it.

If you are unable to reach your instance via SSH or RDP, you can capture a screenshot of your instance and view it as an image. This provides visibility as to the status of the instance, and allows for quicker troubleshooting.

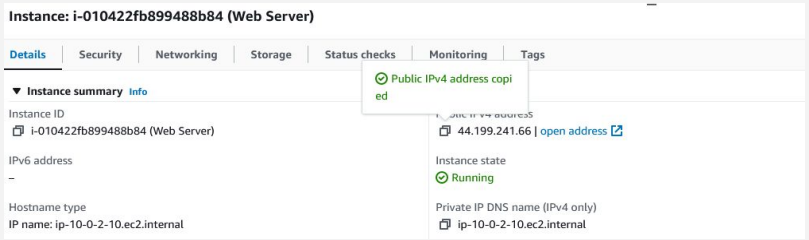


Choose **Cancel**.

Congratulations! We have explored several ways to monitor your instance.

Task 3: Update Your Security Group and Access the Web Server

When you launched the EC2 instance, we provided a script that installed a web server and created a simple web page. In this task, we will access content from the web server.



Ensure **Web Server** is still selected. Choose the **Details** tab.
Copy the **Public IPv4 address** of your instance to the clipboard.

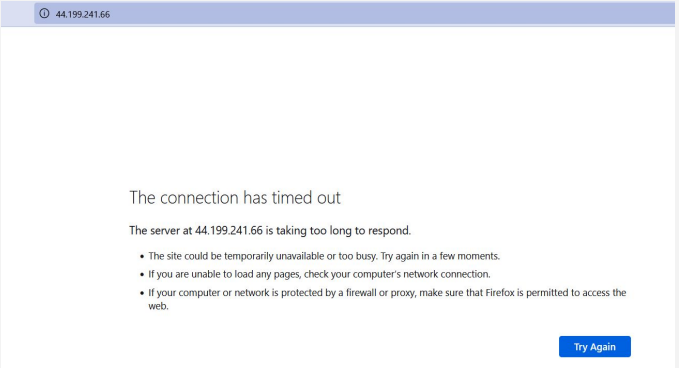
Open a new tab in your web browser, paste the IP address you just

copied, then press **Enter**.

We are **not** currently able to access your web server because the *security group* is not permitting inbound traffic on port 80, which is used for HTTP web requests. This is a demonstration of using a security group as a firewall to restrict the network traffic that is allowed in and out of an instance.

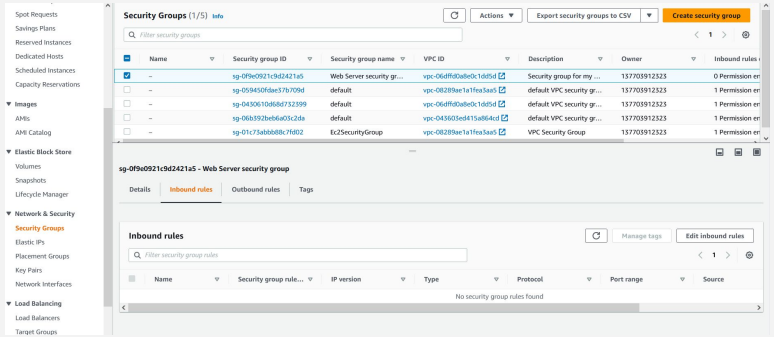
To correct this, you will now update the security group to

permit web traffic on port 80.

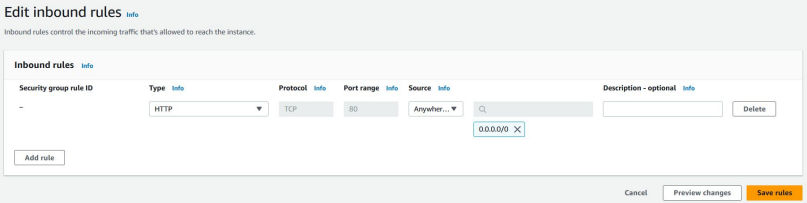


Keep the browser tab open, but return to the **EC2 Console** tab.
In the left navigation pane, choose **Security Groups**.
Select **Web Server security group**.
Choose the **Inbound rules** tab.
The security group currently has no inbound rules.
Choose Edit inbound rules, select Add rule and then configure:

- **Type:** *HTTP*
- **Source:** *Anywhere-IPv4*
- Choose Save rules



Return to the web server tab that you previously opened and refresh the page.
You should see the message *Hello From Your Web Server!*

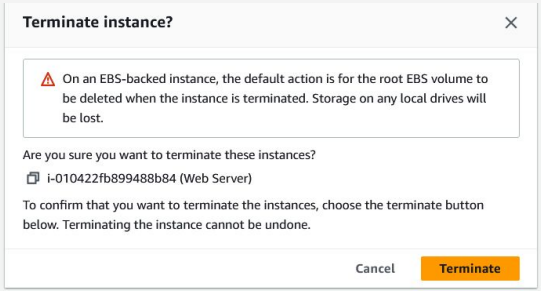


Congratulatio r security group to permit HTTP traffic into our Amazon EC2 Instance.

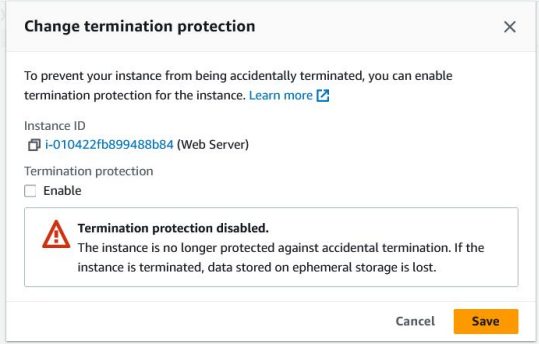
Task 6: Test Termination Protection

You can delete your instance when you no longer need it. This is referred to as *terminating* your instance. You cannot connect to or restart an instance after it has been terminated. In this task, you will learn how to use *termination protection*.

In left navigation pane, choose **Instances**.
Select the **Web Server** instance and in the Instance state menu, select **Terminate instance**.
Then choose Terminate
Note that there is a message that says: *Failed to terminate the instance i-1234567xxx. The instance 'i-1234567xxx' may not be terminated. Modify its 'disableApiTermination' instance attribute and try again.*



In the Actions menu, select **Instance settings Change termination protection**.
Remove the check next to **Enable**.
Choose Save
You can now terminate the instance.
Select the **Web Server** instance again and in the Instance state menu, select **Terminate instance**.
Choose Terminate



Congratulations! You have successfully tested termination protection and terminated your instance.

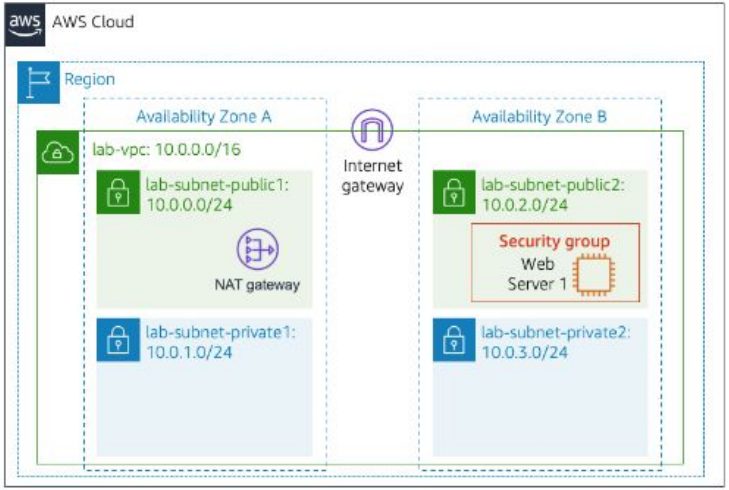
End the Lab

LAB 2 - VPC

Lab 2: Build your VPC and Launch a Web Server

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you defined. This virtual network closely resembles a traditional network that you would operate in your own data center, with the benefits of using the scalable infrastructure of AWS. You can create a VPC that spans multiple Availability Zones.

Scenario



Public Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	Internet gateway

Private Route Tables

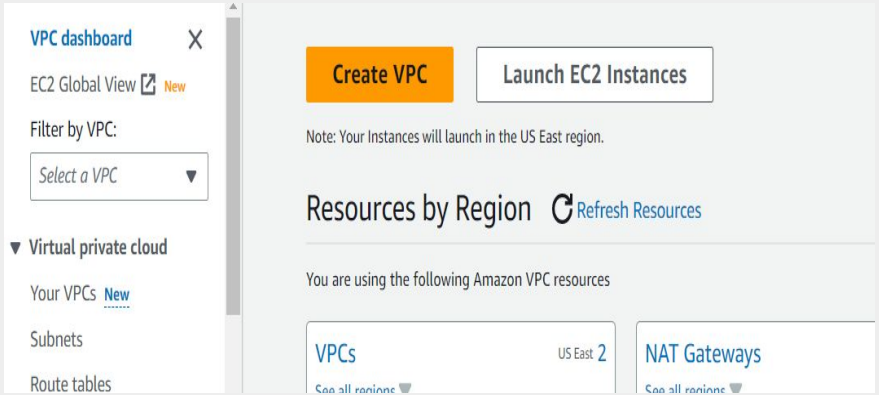
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	NAT gateway

Task 1: Create Your VPC

Begin creating a VPC.

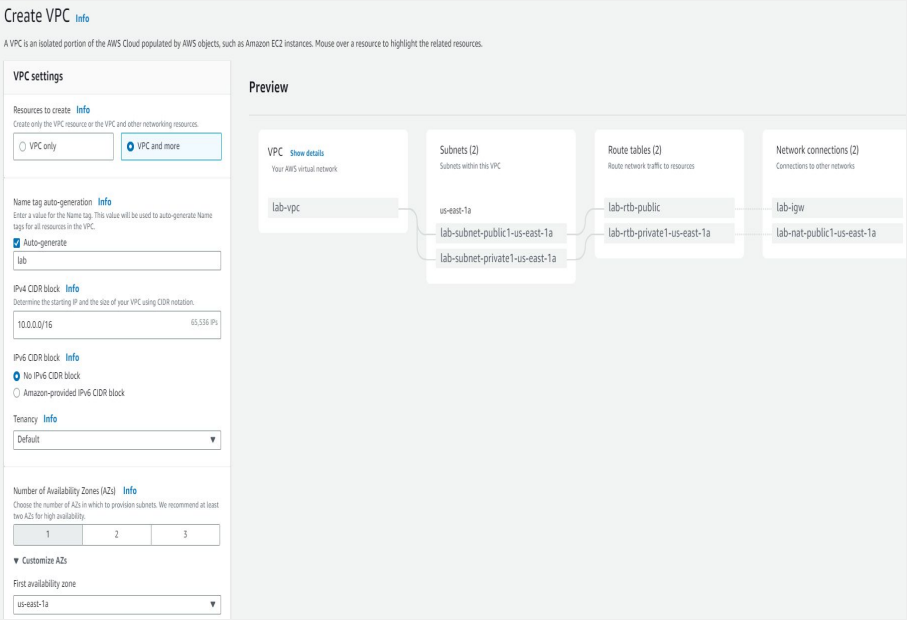
- In the top right of the screen, verify that N. Virginia (us-east-1) is the region.
- Choose the VPC dashboard link which is also towards the top left of the console.
- Next, choose Create VPC.

  Note: If you do not see a button with that name, choose the Launch VPC Wizard button instead.



Configure the VPC details in the *VPC settings* panel on the left:

- 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*. In the *Preview* panel on the right, confirm the settings you have configured.

VPC: lab-vpc

Subnets:

us-east-1a

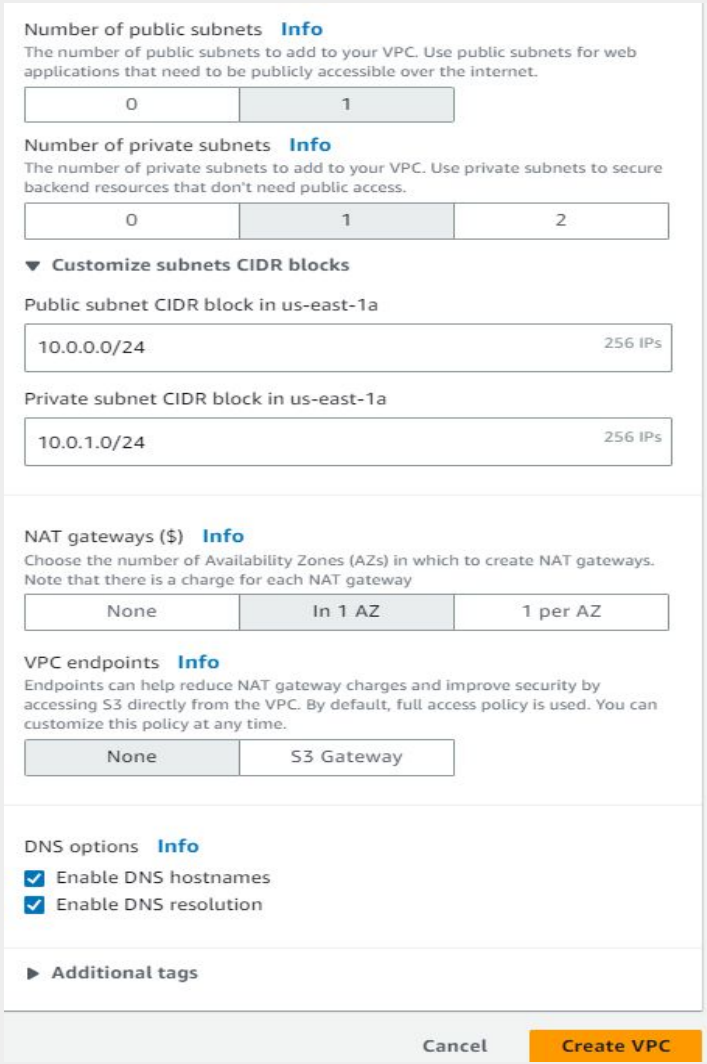
Public subnet name: lab-subnet-public1-us-east-1a

Private subnet name: lab-subnet-private1-us-east-1a

Route tableslab-rtb-public lab-rtb-private1-us-east-1a

Network connections lab-igw lab-nat-public1-us-east-1a

At the bottom of the screen, choose Create VPC choose View VPC



Task 2: Create Additional Subnets

In the left navigation pane, choose Subnets.

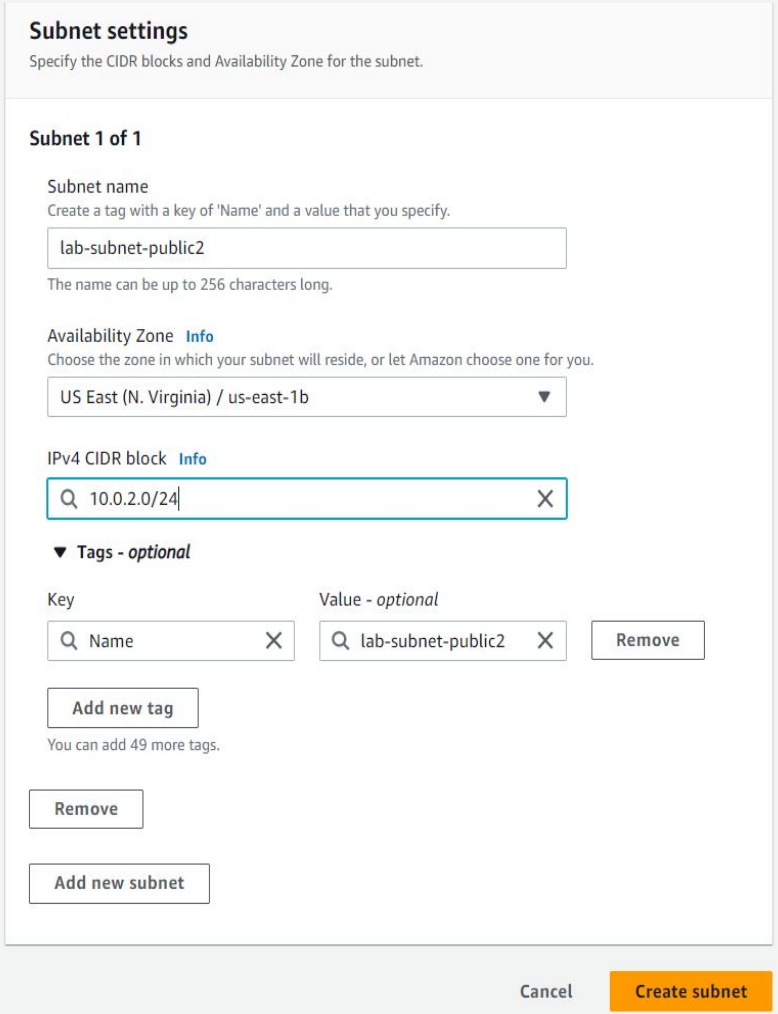
First, you will create a second *public* subnet.

Choose Create subnet then configure:

- 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

The subnet will have all IP addresses starting with 10.0.2.x.

Choose Create subnet

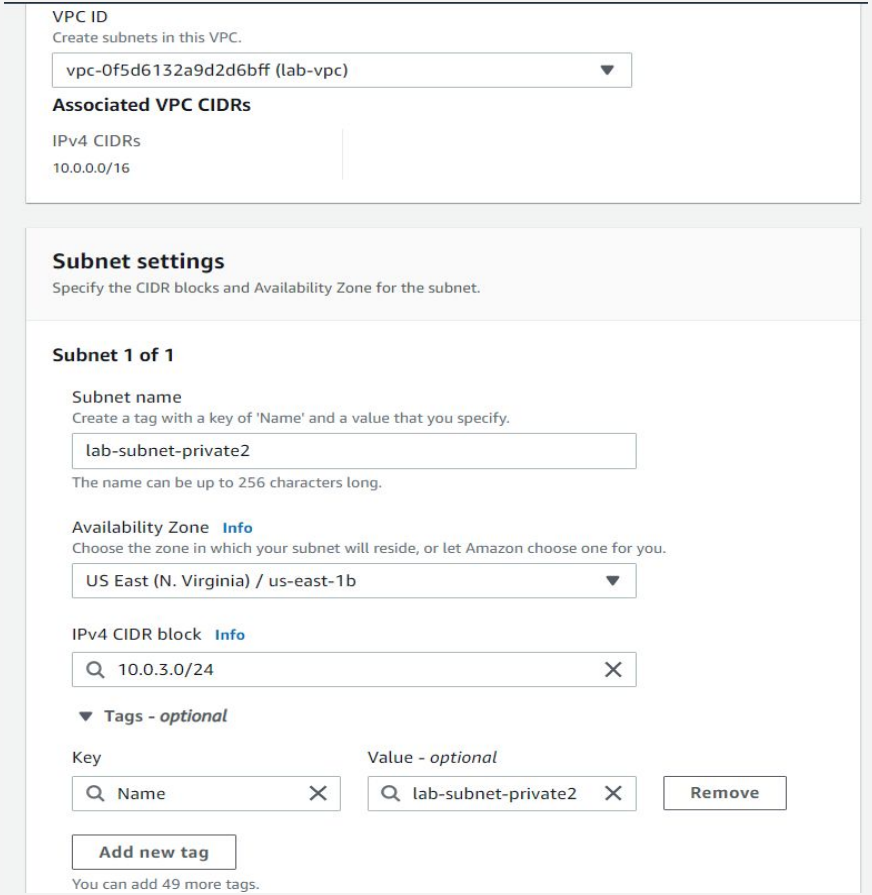


Choose Create subnet then configure:

- 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

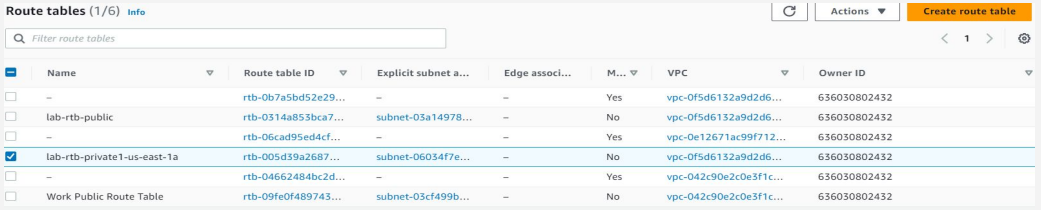
The subnet will have all IP addresses starting with 10.0.3.x.

Choose Create subnet



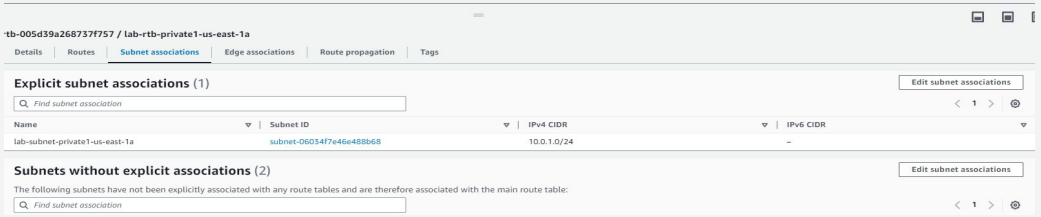
In the left navigation pane, choose Route tables.

Select the lab-rtb-private1-us-east-1a route table.



In the Explicit subnet associations panel,

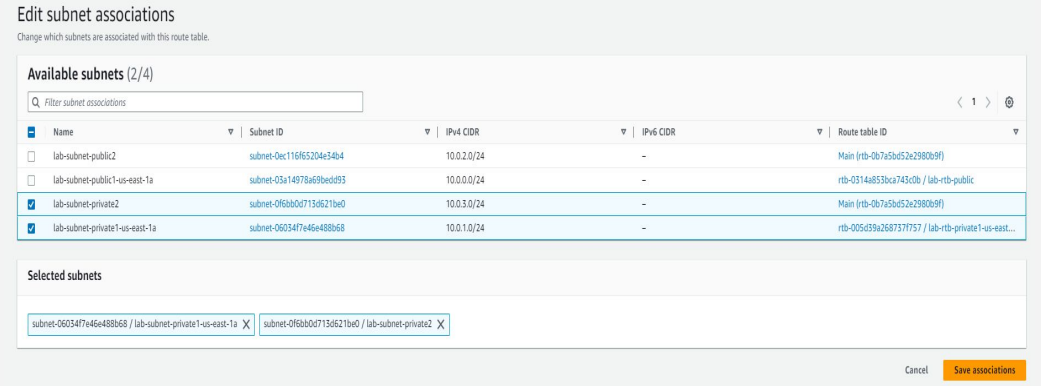
choose Edit subnet associations



Leave lab-subnet-private1-us-east-1a selected,

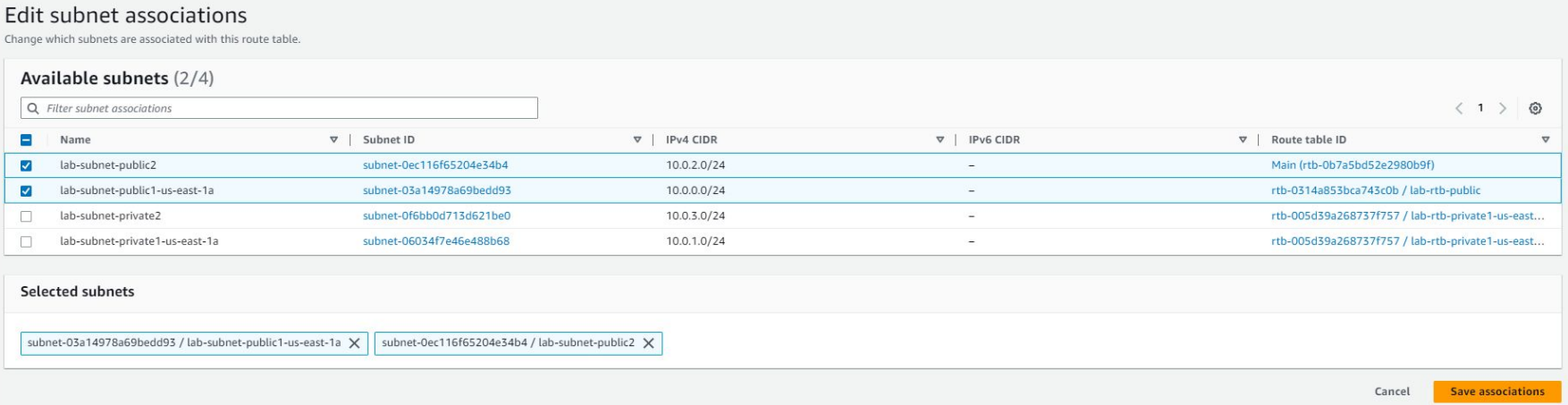
but also select lab-subnet-private2.

Choose Save associations



Select the lab-rtb-public route table

Choose the Subnet associations tab.
In the Explicit subnet associations area, choose Edit subnet associations
Leave lab-subnet-public1-us-east-1a selected, but also select lab-subnet-public2.
Choose Save associations



Task 3: Create a VPC Security Group

In the left navigation pane,

choose Security groups.

Choose Create security group and

then configure:

Security group name:

Web Security Group

Description: Enable HTTP access

choose lab-vpc

In the Inbound rules pane,

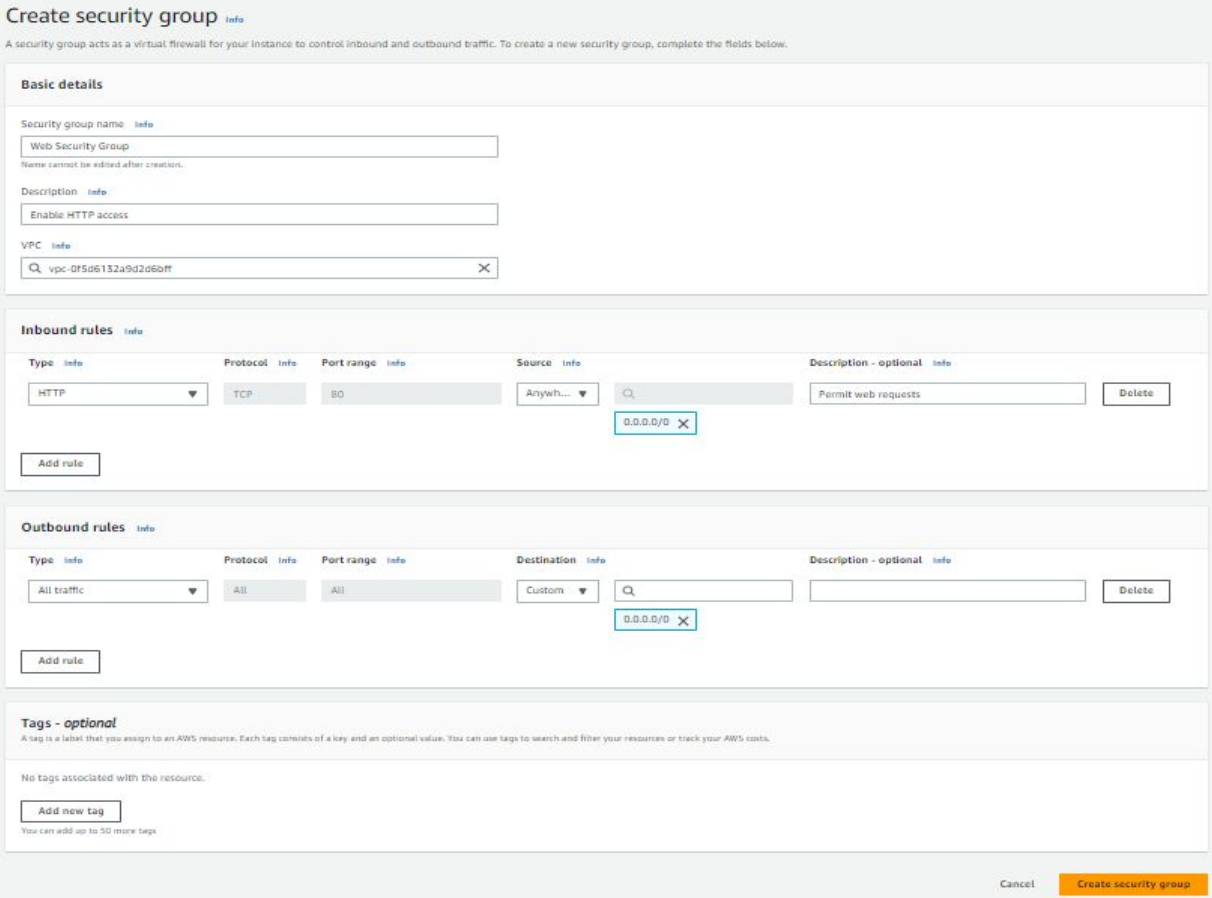
choose Add rule

Type: *HTTP*

Source: *Anywhere-IPv4*

Description: Permit web requests

choose Create security group



Task 4: Launch a Web Server Instance

.

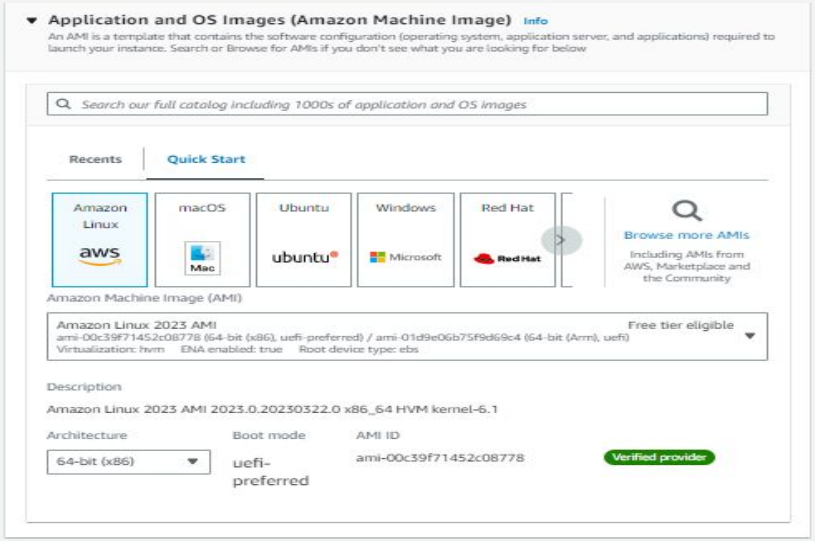
In the search box to the right of **Services**, search for and choose **EC2** to open the EC2 console.

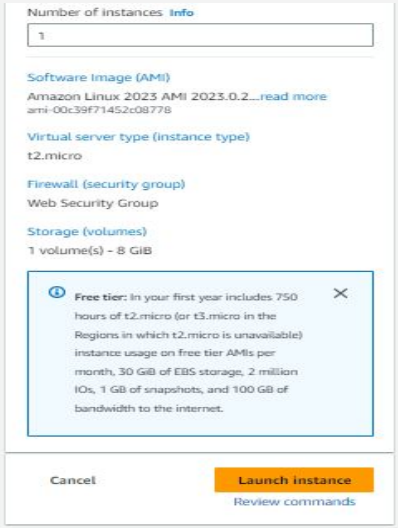
From the **Launch instance** menu choose **Launch instance**.

Name the instance:

Give it the name

`Web Server 1`





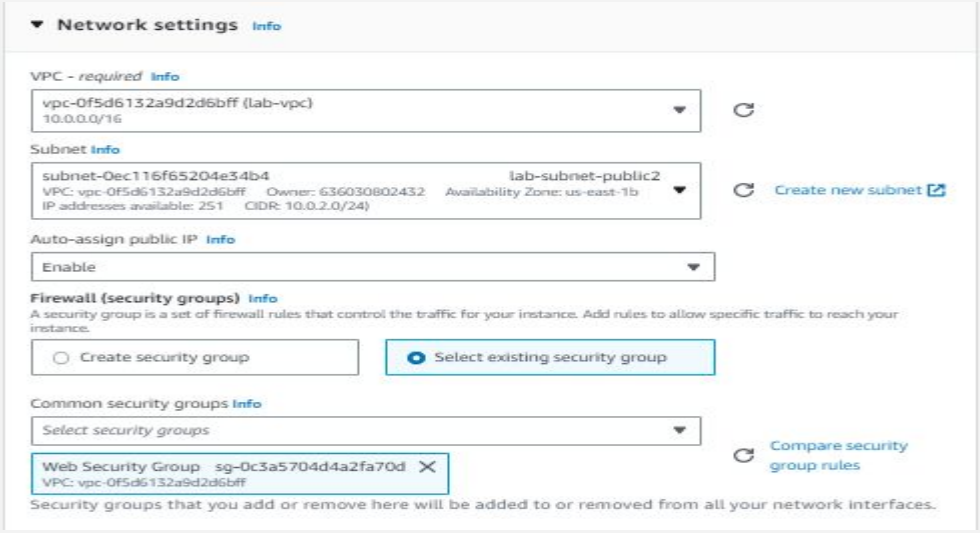
Choose an Instance type:
t2.micro

From the **Key pair name** menu, select **vockey**.

Configure the Network settings

Next to Network settings, choose **Edit**, then configu

- **Network:** *lab-vpc*
- **Subnet:** *lab-subnet-public2*
- **Auto-assign public IP:** *Enable*

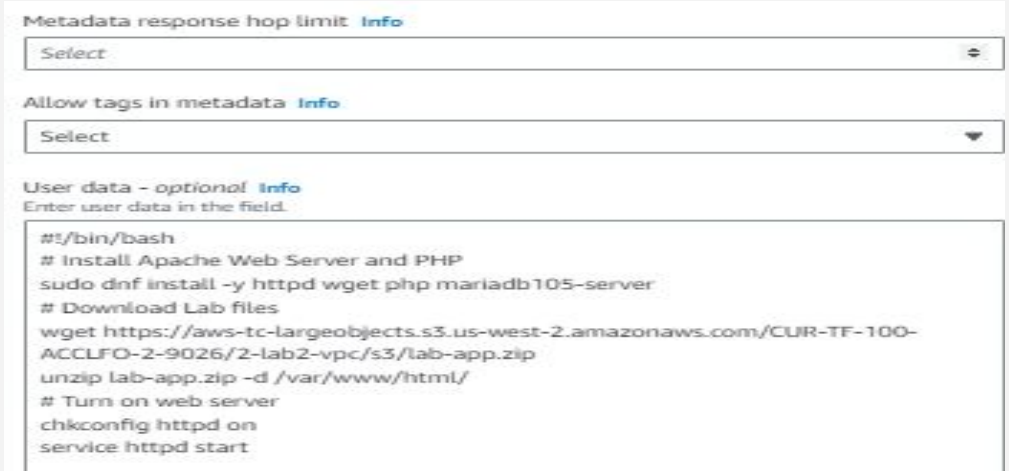


Common security groups, select **Web Security Group**.

Expand the **Advanced details** panel.
Launch instance

Wait until **Web Server 1** shows *2/2 checks*

passed in the **Status check** column.



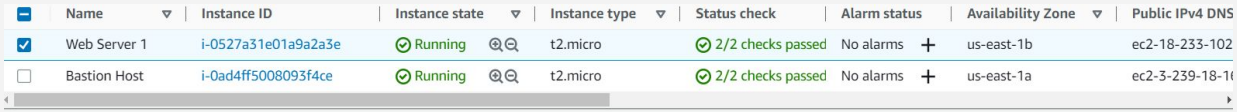
Select Web Server 1.

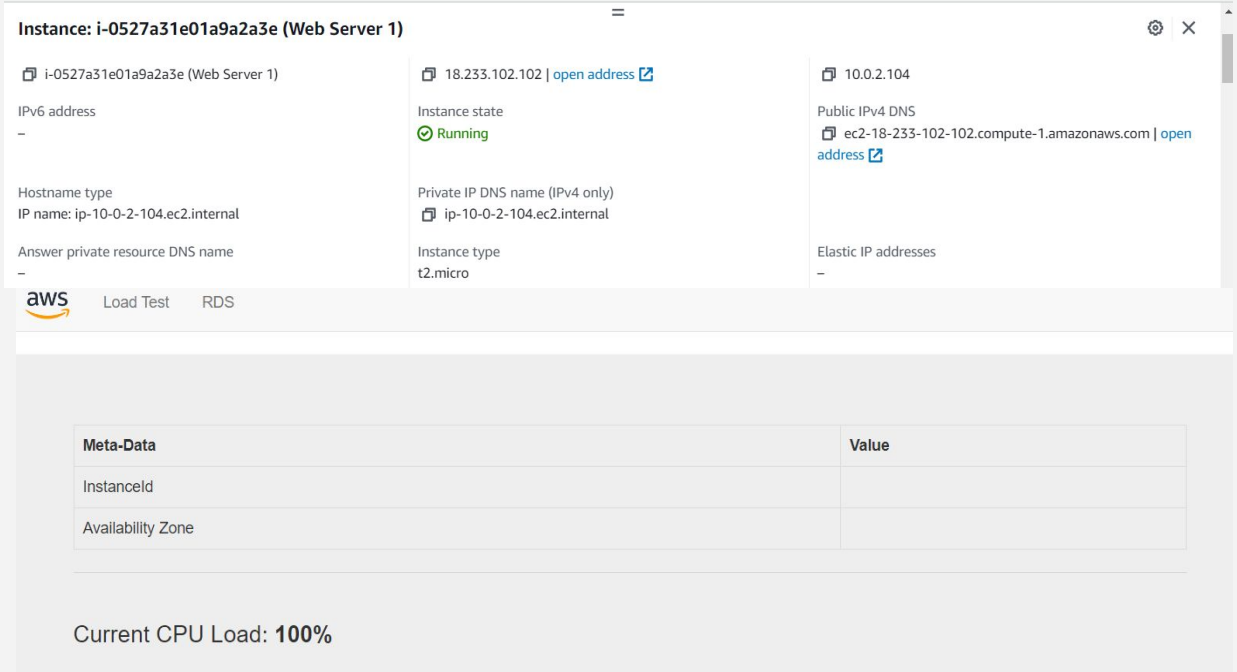
Copy the Public IPv4 DNS value shown in the Details tab at the bottom of the page.

Open a new web browser tab, paste the Public DNS value and press Enter.

You should see a web page displaying the AWS logo and instance meta-data values.

END the lab

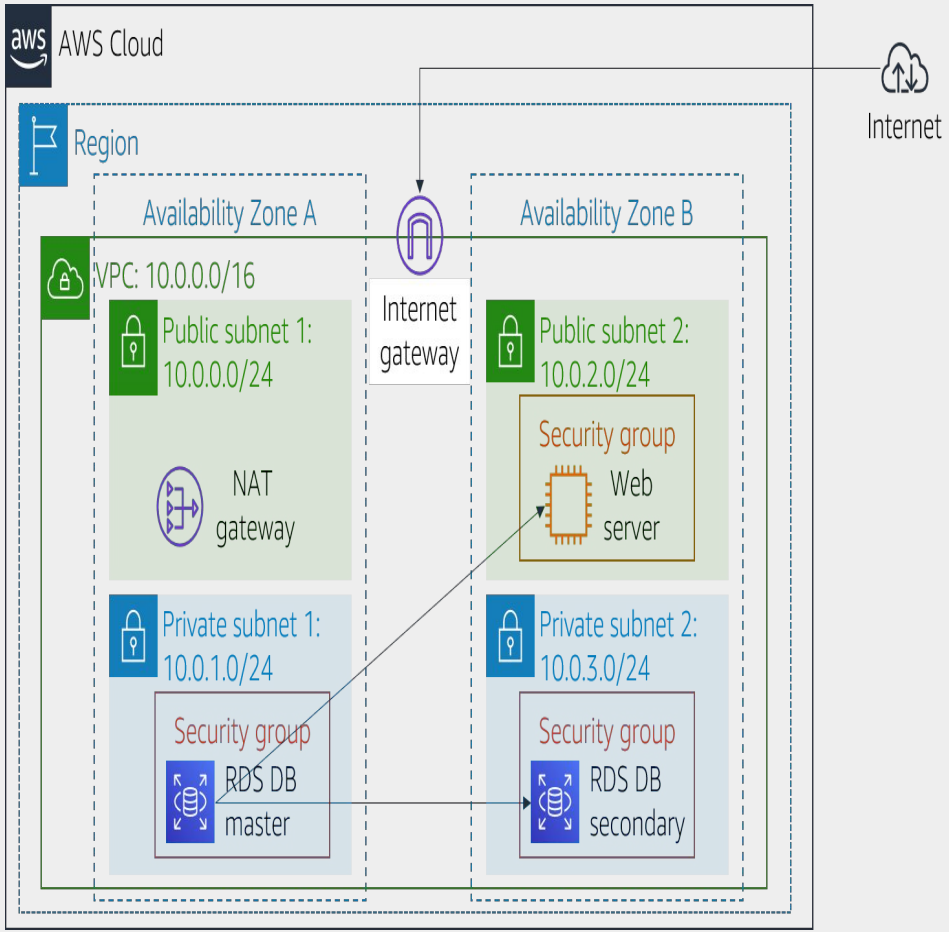




LAB 3 - DB Server

Lab 3: Build Your DB Server and Interact With Your DB Using an App

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while managing time-consuming database administration tasks, which allows you to focus on your applications and business. Amazon RDS provides you with six familiar database engines to choose from: Amazon Aurora, Oracle, Microsoft SQL Server,PostgreSQL, MySQL and MariaDB.

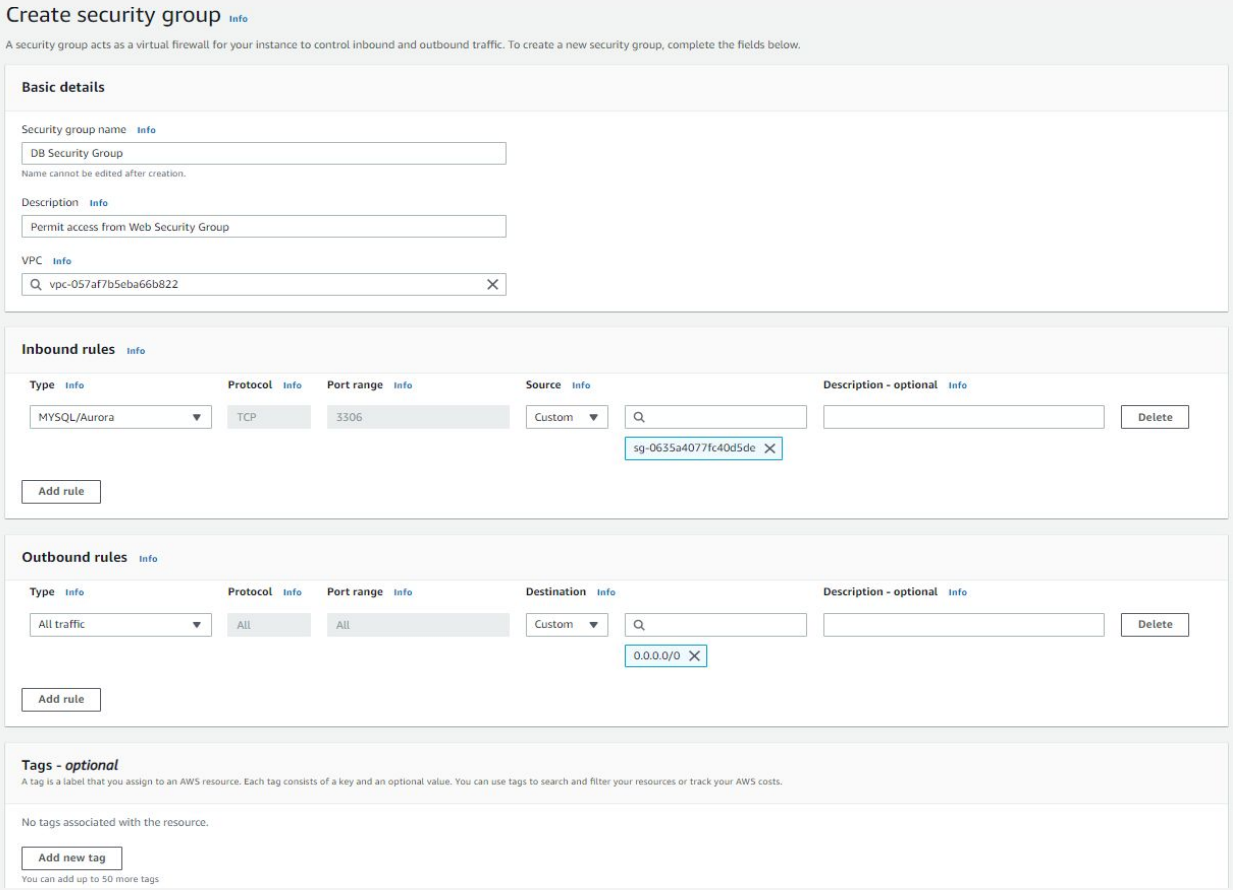


Task 1: Create a Security Group for the RDS DB Instance

- Security group name: DB Security Group
- Description: Permit access from Web Security Group
- VPC: *Lab VPC*

In the Inbound rules pane

- Type: *MySQL/Aurora (3306)*
- CIDR, IP, Security Group or Prefix List: Type sg and then select *Web Security Group*.



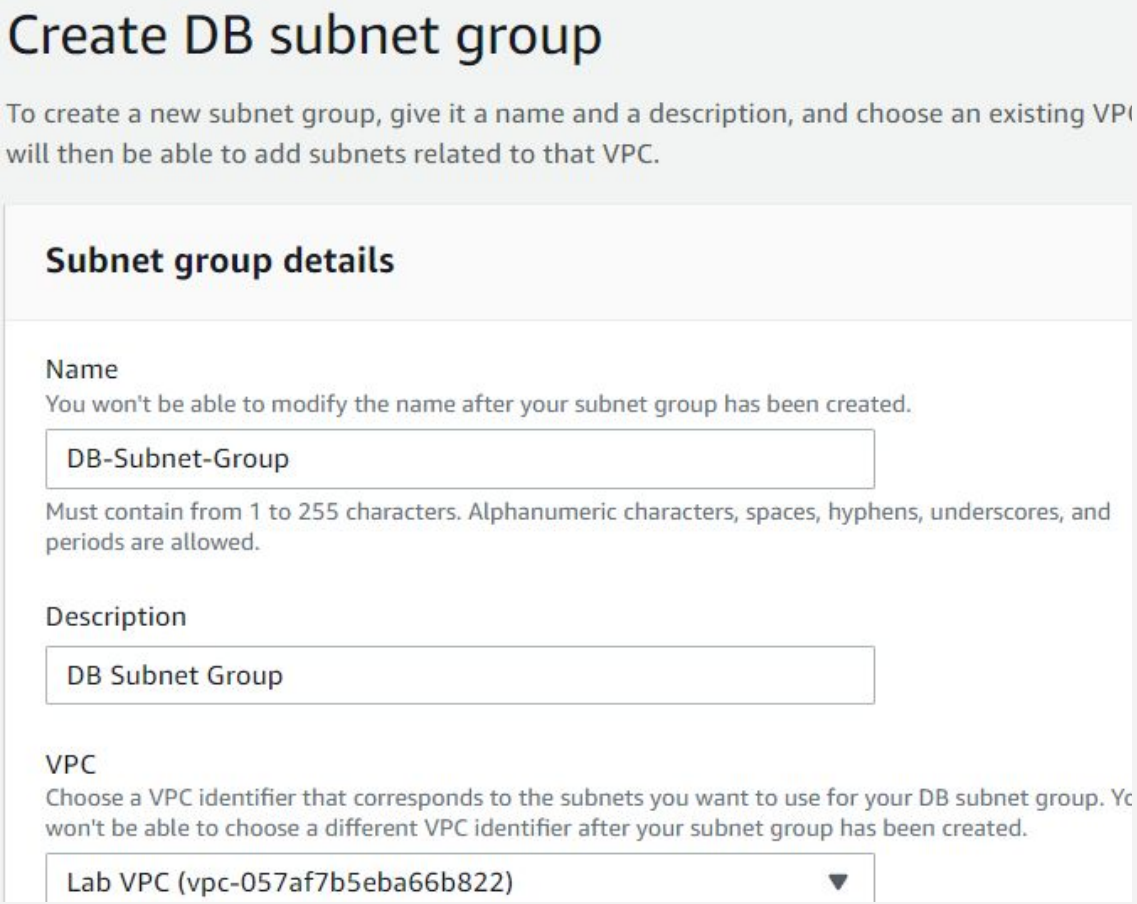
Task 2: Create a DB Subnet Group

Choose RDS

Choose Subnet groups.

Choose Create DB Subnet Group then configure:

- Name: DB-Subnet-Group
- Description: DB Subnet Group
- VPC: *Lab VPC*



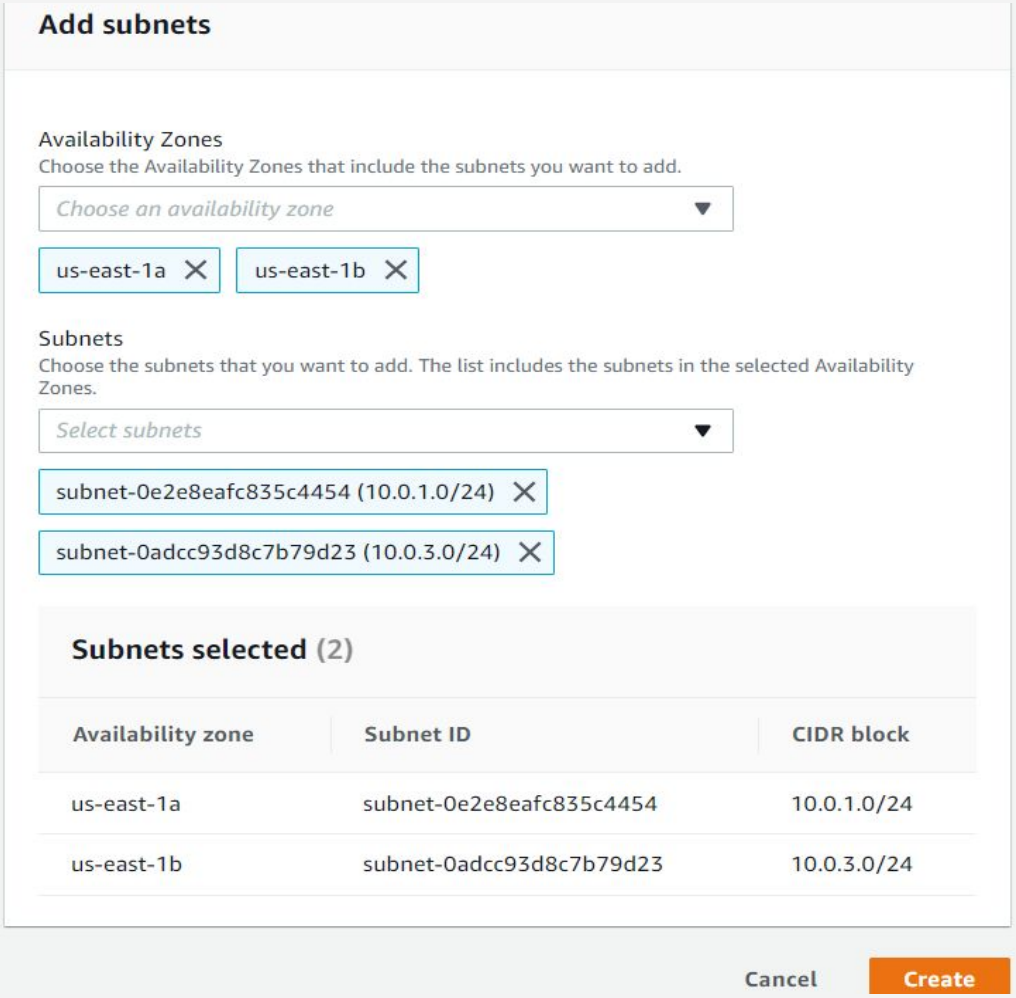
Scroll down to the Add Subnets section.

Expand the list of values under Availability Zones

and select the first two zones: us-east-1a and us-east-1b.

Expand the list of values under Subnets and select the subnets associated with the CIDR ranges 10.0.1.0/24 and 10.0.3.0/24.
These subnets should now be shown in the Subnets selected table.

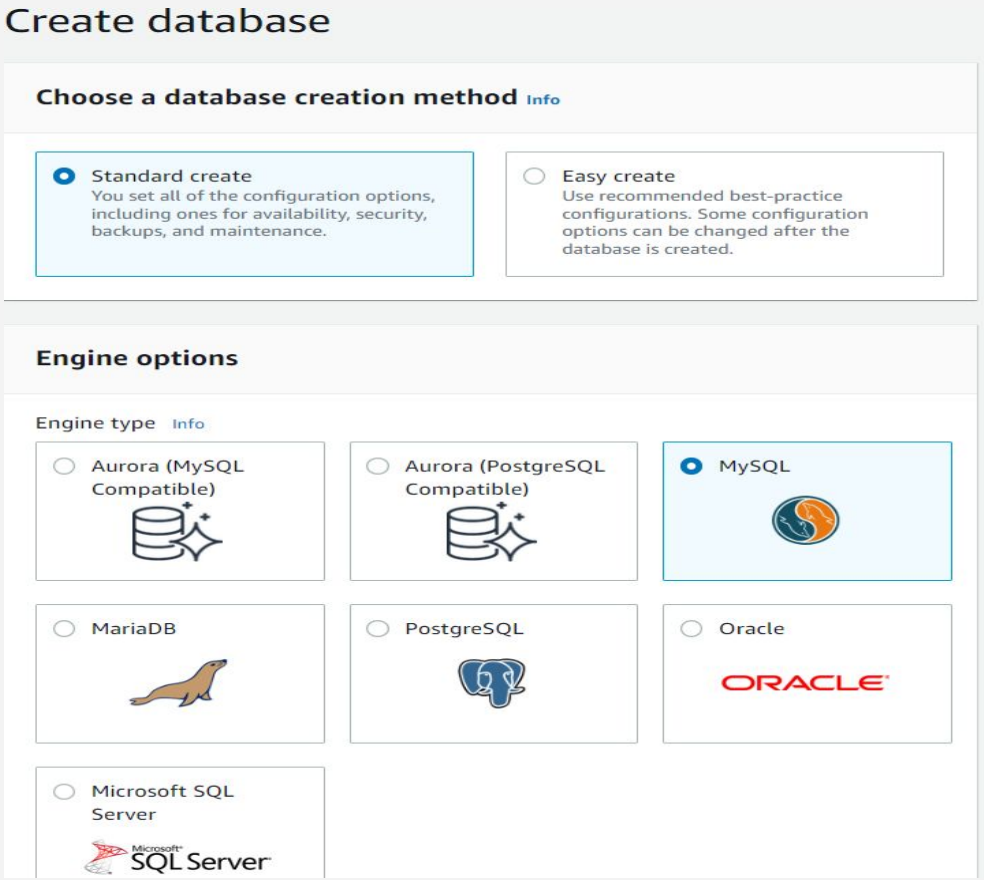
Choose Create

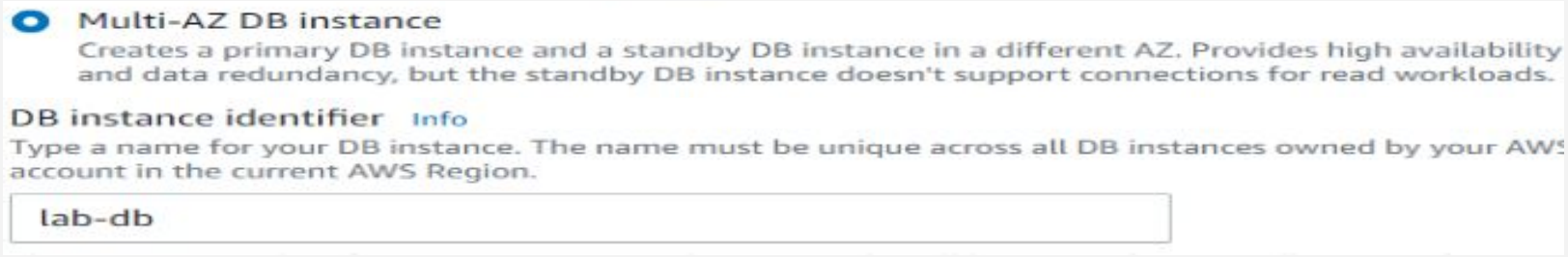


Task 3: Create an Amazon RDS DB Instance

Choose Databases.

Select MySQL.





DB instance identifier: lab-db

Master username: main

Master password: lab-password

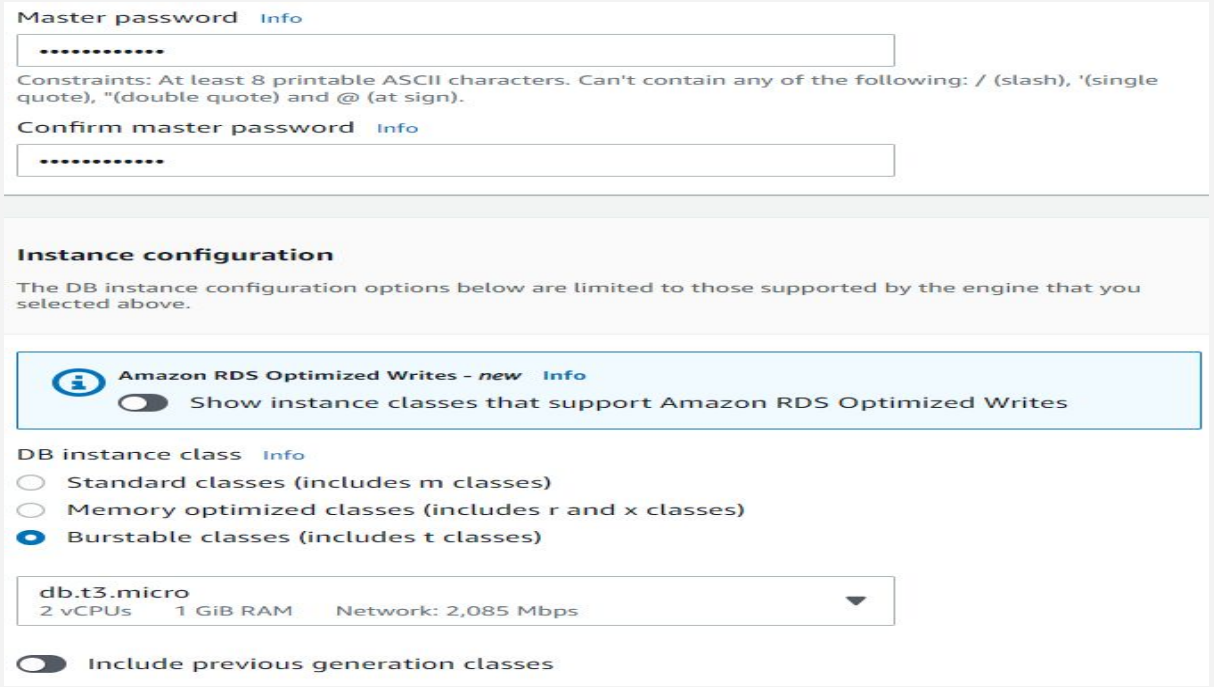
Confirm password: lab-password

Under DB instance class, configure:

Select Burstable classes

(includes t classes).

Select *db.t3.micro*



Storage

Storage type Info

General Purpose SSD (gp3)
Performance scales independently from storage

Virtual private cloud (VPC) Info
Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

Lab VPC (vpc-057af7b5eba66b822)

Only VPCs with a corresponding DB subnet group are listed.

VPC security group (firewall) Info
Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

- (•) Choose existing
  Choose existing VPC security groups
- ( ) Create new
  Create new VPC security group

Existing VPC security groups

Choose one or more options

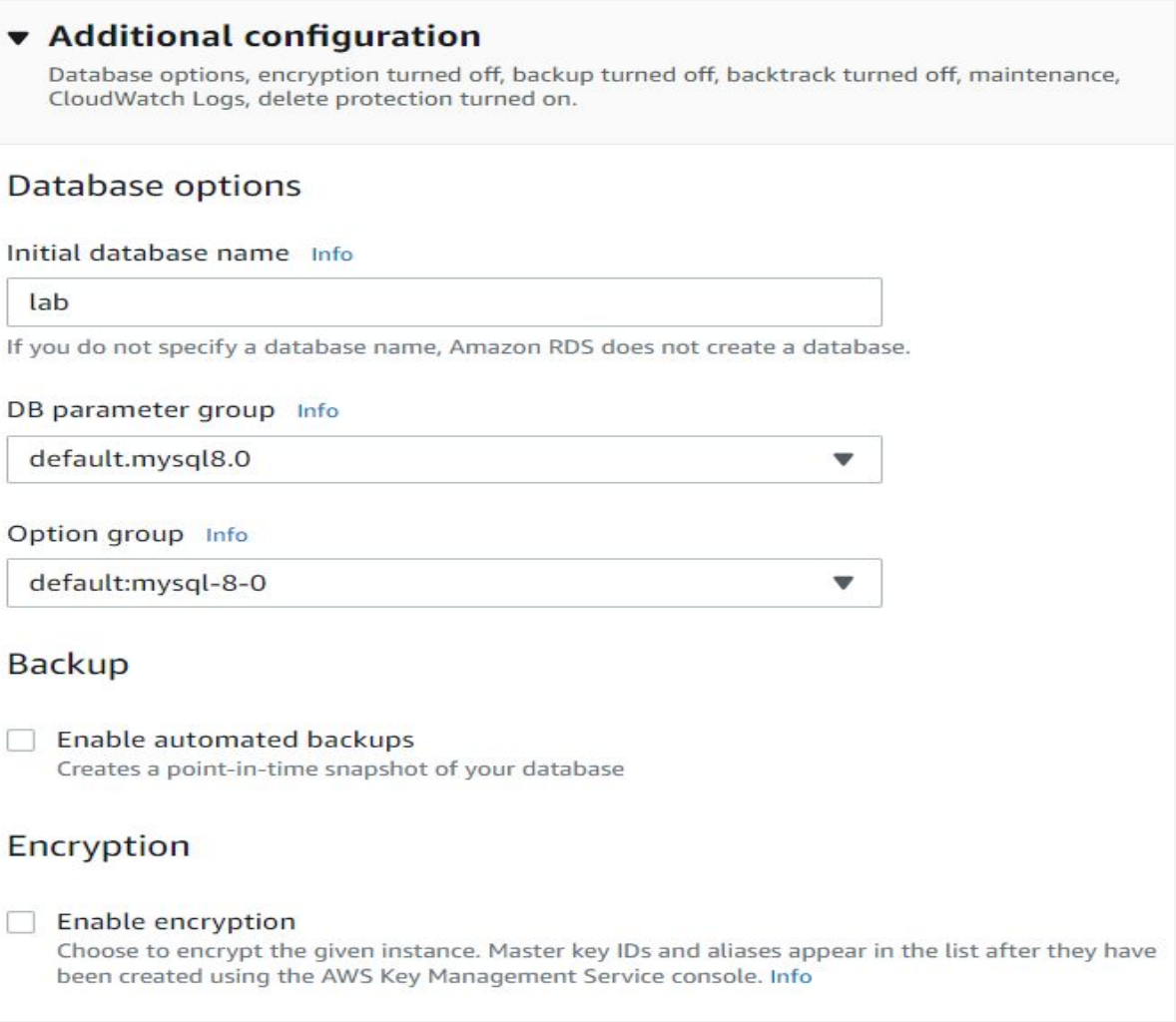
DB Security Group ×

Monitoring

Monitoring

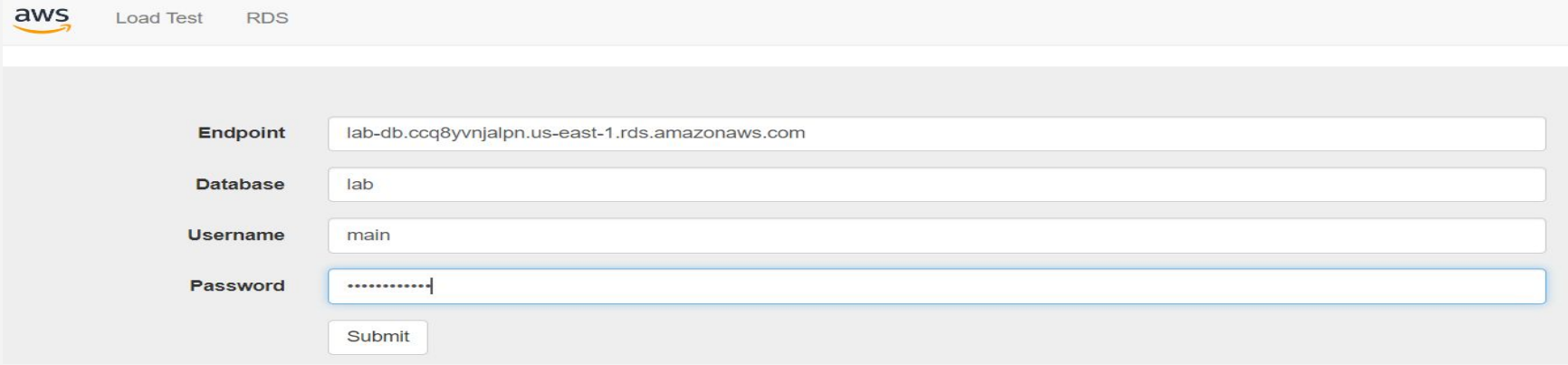
- [ ] Enable Enhanced monitoring
  Enabling Enhanced monitoring metrics are useful when you want to see how different processes or threads use the CPU.

Uncheck Enable automatic backups.
Uncheck Enable encryption
Uncheck Enable Enhanced monitoring.



Task 4: Interact with Your Database

To copy the Web Server IP address, choose on the Details drop down menu above these instructions, and then choose Show.Open a new web browser tab, paste the *Web Server* IP address and press Enter.
The web application will be displayed, showing information about the EC2 instance.Choose the RDS link at the top of the page.
You will now configure the application to connect to your database.



Address Book

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

Address Book

Add Contact

Last Name: Mathur
First Name: Emy
Phone: 3458926731
Email: emymathur@gmail.com
Submit

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

Address Book

Last name	First name	Phone	Email	Admin	
				Add Contact	
Doe	Jane	010-110-1101	janed@someotheraddress.org	Edit	Remove
Johnson	Roberto	123-456-7890	robertoj@someaddress.com	Edit	Remove
Mathur	Emy	3458926731	emymathur@gmail.com	Edit	Remove

Address Book

Entry has been removed

Last name	First name	Phone	Email	Admin	
				Add Contact	
Johnson	Roberto	123-456-7890	robertoj@someaddress.com	Edit	Remove
Mathur	Emy	3458926731	emymathur@gmail.com	Edit	Remove

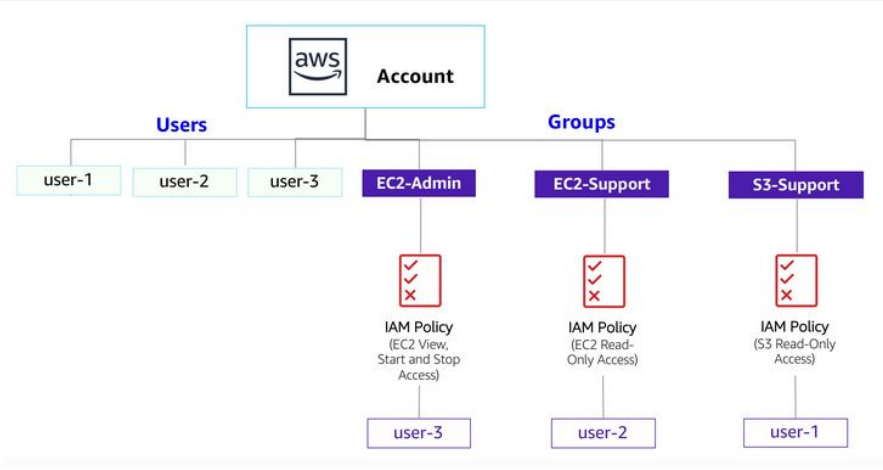
End the lab

LAB 4 - IAM

Lab 4: Introduction to AWS IAM

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.

- Exploring pre-created IAM Users and Groups
- Inspecting IAM policies as applied to the pre-created groups
- Following a real-world scenario, adding users to groups with specific capabilities enabled
- Locating and using the IAM sign-in URL
- Experimenting with the effects of policies on service access

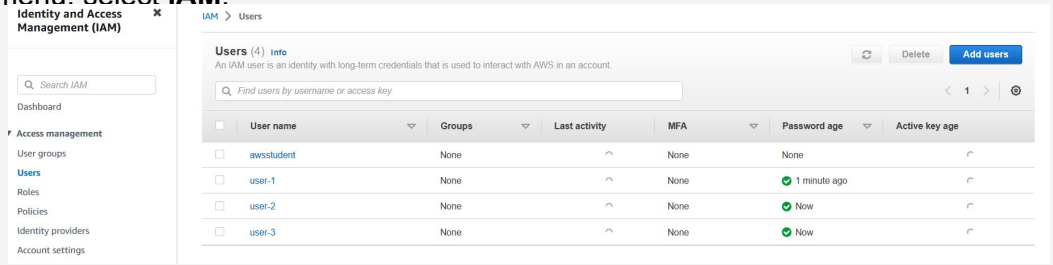


Task 1: Explore the Users and Groups

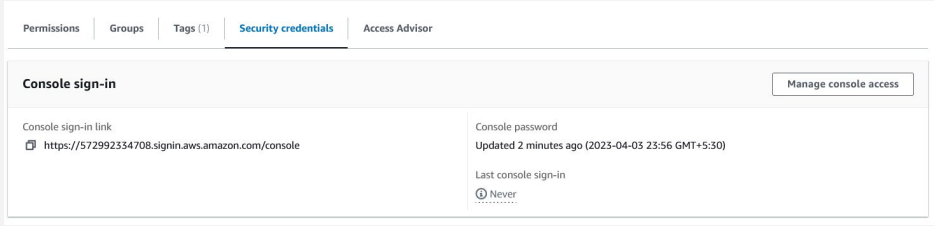
In this task, you will explore the Users and Groups that have already been created for you in IAM.

In the **AWS Management Console**, on the **Services** menu, select **IAM**.
In the navigation pane on the left, choose **Users**.
The following IAM Users have been created for you:

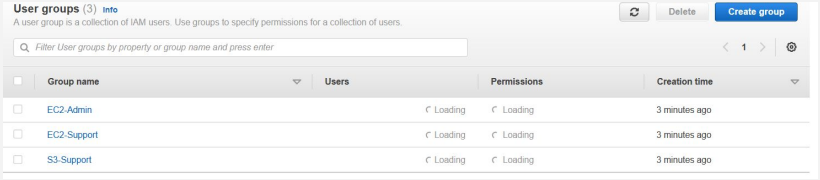
- user-1
- user-2
- user-3



Choose **user-1**.
This will bring to a summary page for user-1. The **Permissions** tab will be displayed.
Notice that user-1 does not have any permissions.
Choose the **Groups** tab.
user-1 also is not a member of any groups.
Choose the **Security credentials** tab.
user-1 is assigned a **Console password**



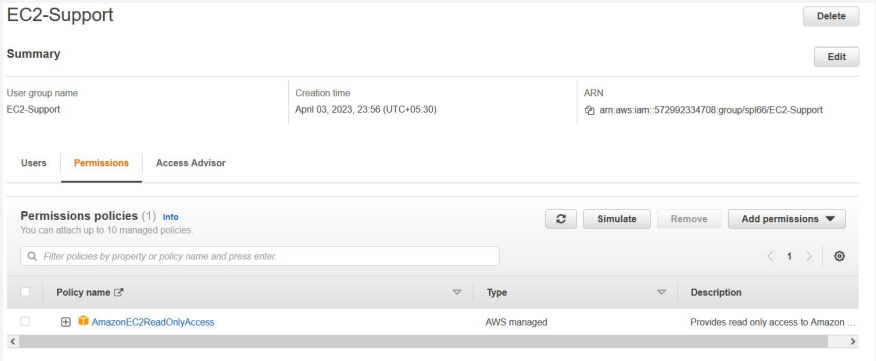
In the navigation pane on the left, choose **User groups**.
The following groups have already been created for you:



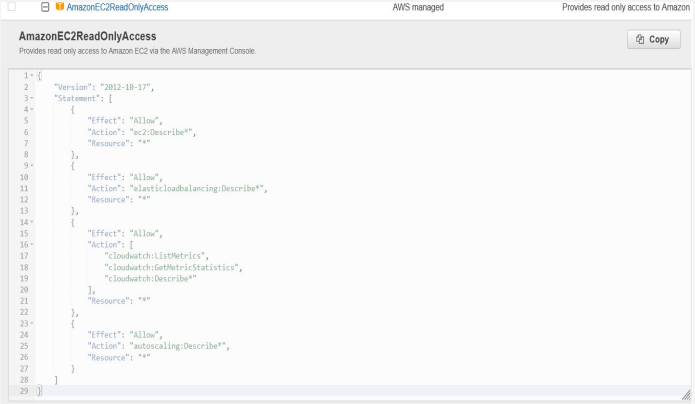
- EC2-Admin
- EC2-Support
- S3-Support

Choose the **EC2-Support** group.
This will bring you to the summary page for the **EC2-Support** group.

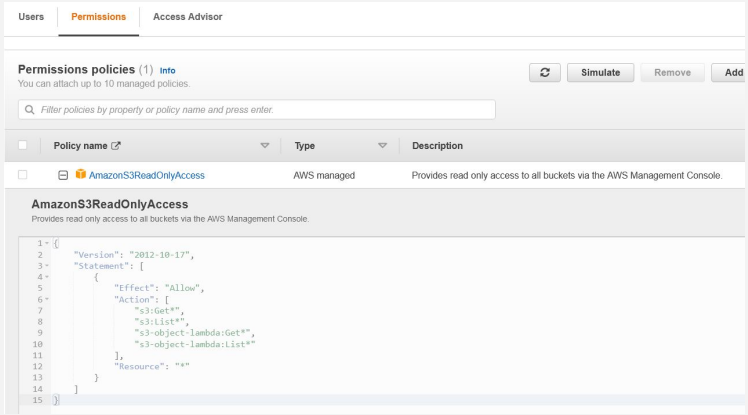
Choose the **Permissions** tab.
This group has a Managed Policy associated with it, called **AmazonEC2ReadOnlyAccess**. Managed Policies are pre-built policies (built either by AWS or by your administrators) that can be attached to IAM Users and Groups. When the policy is updated, the changes to the policy are immediately apply against all Users and Groups that are attached to the policy.



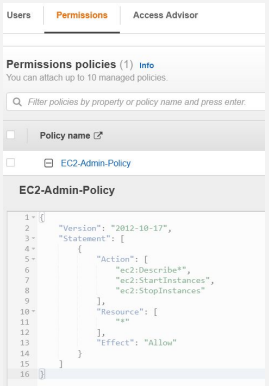
Choose the plus (**+**) icon next to the AmazonEC2ReadOnlyAccess policy to view the policy details.
Note: A policy defines what actions are allowed or denied for specific AWS resources.
This policy is granting permission to List and Describe information about EC2, Elastic Load Balancing, CloudWatch and Auto Scaling.
Choose the minus icon (**-**) to hide the policy details.



In the navigation pane on the left, choose **User groups**.
Choose the **S3-Support** group and then choose the **Permissions** tab.
The S3-Support group has the **AmazonS3ReadOnlyAccess** policy attached.
Choose the plus (**+**) icon to view the policy details.
This policy grants permissions to Get and List resources in Amazon S3.
Choose the minus icon (**-**) to hide the policy details.



In the navigation pane on the left, choose **User groups**.
Choose the **EC2-Admin** group and then choose the **Permissions** tab.
This Group is slightly different from the other two. Instead of a *Managed Policy*, it has an **Inline Policy**, which is a policy assigned to just one User or Group. Inline Policies are typically used to apply permissions for one-off situations.
Choose the plus (**+**) icon to view the policy details.



Task 2: Add Users to Groups

Add user-1 to the S3-Support Group

In the left navigation pane, choose **User groups**.
Choose the **S3-Support** group.
Choose the **Users** tab.
In the **Users** tab, choose **Add users**.

In the **Add Users to S3-Support** window, configure the following:

- Select **user-1**.
- At the bottom of the screen, choose **Add Users**.

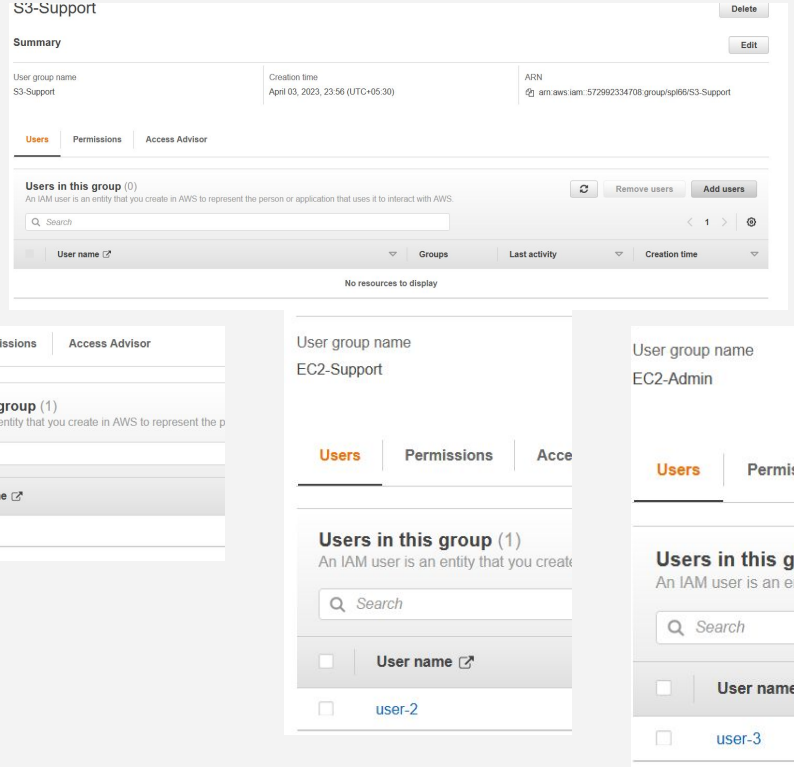
In the **Users** tab you will see that user-1 has been added to the group.

Add user-2 to the EC2-Support Group

Using similar steps to the ones above, add **user-2** to the **EC2-Support** group.
user-2 should now be part of the **EC2-Support** group.

Add user-3 to the EC2-Admin Group

Using similar steps to the ones above, add **user-3** to the **EC2-Admin** group.
user-3 should now be part of the **EC2-Admin** group.



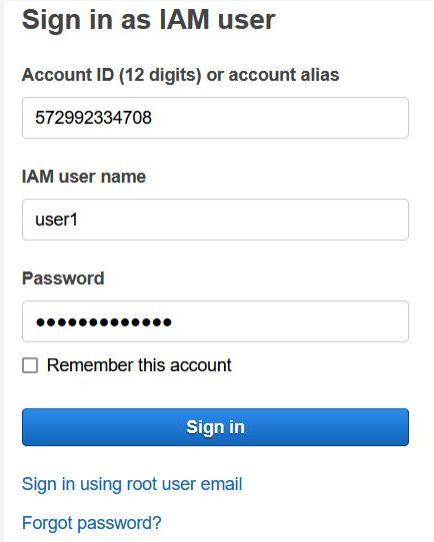
In the navigation pane on the left, choose **User groups**.
Each Group should now have a **1** in the Users column for the number of Users in each Group.
If you do not have a **1** beside each group, revisit the above instructions above to ensure that each user is assigned to a User group, as shown in the table in the Business Scenario section.

Group name	Users	Permissions
EC2-Admin	1	Defined
EC2-Support	1	Defined
S3-Support	1	Defined

Task 3: Sign-In and Test Users

In this task, you will test the permissions of each IAM User.

In the navigation pane on the left, choose **Dashboard**.
An **IAM users sign-in link** is displayed on the right. It will look similar to: *https://123456789012.signin*
This link can be used to sign-in to the AWS Account you are currently using.
Copy the **Sign-in URL for IAM users in this account** to a text editor.



Open a private (Incognito) window.
Mozilla Firefox
- Choose the menu bars at the top-right of the screen
- Select **New private window**

Google Chrome
- Choose the ellipsis at the top-right of the screen
- Select **New Incognito Window**

Microsoft Edge
- Choose the ellipsis at the top-right of the screen
- Choose **New InPrivate window**

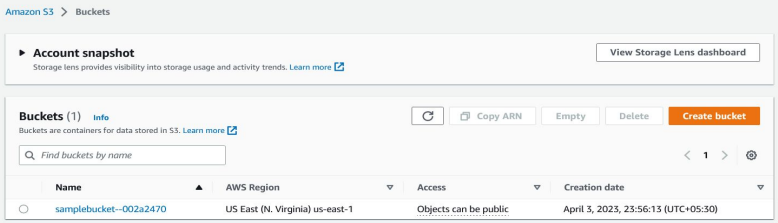
Microsoft Internet Explorer
- Choose the **Tools** menu option
- Choose **InPrivate Browsing**

Paste the **IAM users sign-in** link into the address bar of your private browser session and press **Enter**. Next, you will sign-in as **user-1**, who has been hired as your Amazon S3 storage support staff.

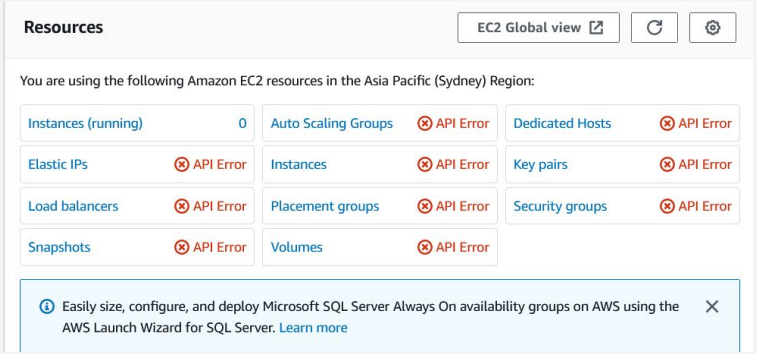
Sign-in with:

IAM user name: `user-1` & **Password:** `Lab-Password1`

In the **Services** menu, choose **S3**.
Choose the name of the bucket that exists in the account and browse the contents.
Since your user is part of the **S3-Support** Group in IAM, they have permission to view a list of Amazon S3 buckets and the contents.
Note: The bucket does not contain any objects.

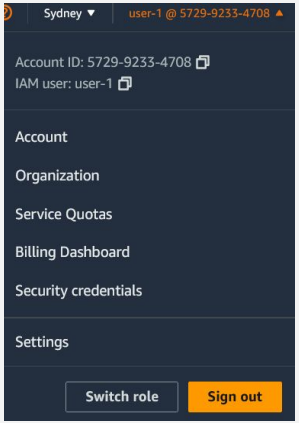


Now, test whether they have access to Amazon EC2.
In the **Services** menu, choose **EC2**.
In the left navigation pane, choose **Instances**.
You cannot see any instances. Instead, you see a message that states *You are not authorized to perform this operation*. This is because this user has not been granted any permissions to access Amazon EC2.



You will now sign-in as **user-2**, who has been hired as your Amazon EC2 support person.
Sign user-1 out of the **AWS Management Console** by completing the following actions:

- At the top of the screen, choose **user-1**
- Choose **Sign Out**



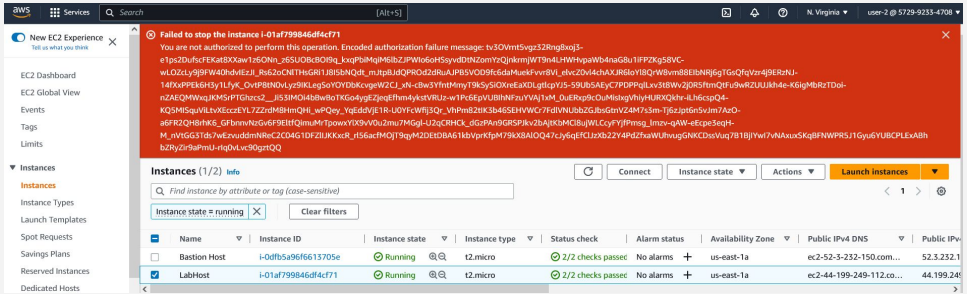
Paste the **IAM users sign-in** link into your private browser tab's address bar and press **Enter**.
Note: This link should be in your text editor.
Sign-in with:

- **IAM user name:** `user-2`
- **Password:** `Lab-Password2`

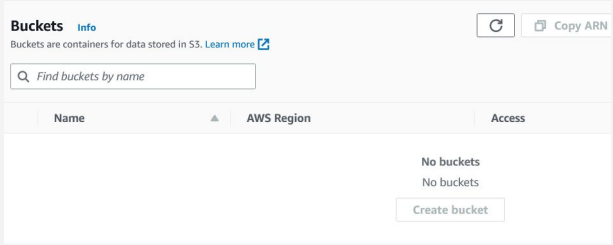
In the **Services** menu, choose **EC2**.
In the navigation pane on the left, choose **Instances**.
You are now able to see an Amazon EC2 instance because you have Read Only permissions. However, you will not be able to make any changes to Amazon EC2 resources.
If you cannot see an Amazon EC2 instance, then your Region may be incorrect. In the top-right of the screen, pull-down the Region menu and select the region that you noted at the start of the lab (for example, **N. Virginia**).

- Select the instance named *LabHost*.

In the **Instance state** menu above, select **Stop instance**.
In the **Stop Instance** window, select **Stop**.
You will receive an error stating *You are not authorized to perform this operation*. This demonstrates that the policy only allows you to view information, without making changes.



Choose the X to close the *Failed to stop the instance* message.
Next, check if user-2 can access Amazon S3.



In the **Services**, choose **S3**.
You will see the message **You don't have permissions to list buckets** because user-2 does not have permission to access Amazon S3.
You will now sign-in as **user-3**, who has been hired as your Amazon EC2 administrator.

Sign user-2 out of the **AWS Management Console** by completing the following actions:

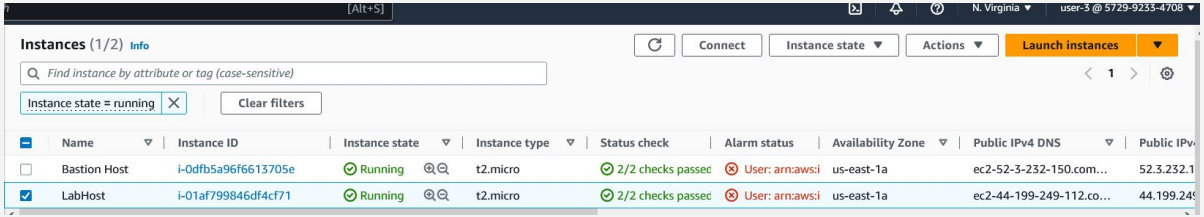
- At the top of the screen, choose **user-2**
- Choose **Sign Out**

Paste the **IAM users sign-in** link into your private window and press **Enter**.
Paste the sign-in link into the address bar of your private web browser tab again. If it is not in your clipboard, retrieve it from the text editor where you stored it earlier.

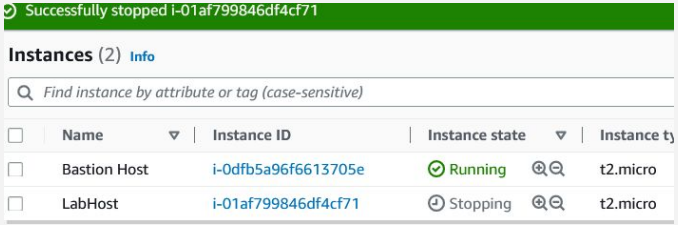
Sign-in with:

- **IAM user name:** user-3
- **Password:** Lab-Password3

In the **Services** menu, choose **EC2**.
In the navigation pane on the left, choose **Instances**.
As an EC2 Administrator, you should now have permissions to Stop the Amazon EC2 instance.
Select the instance named *LabHost* .



If you cannot see an Amazon EC2 instance, then your Region may be incorrect. In the top-right of the screen, pull-down the Region menu and select the region that you noted at the start of the lab (for example, **N. Virginia**).
In the **Instance state** menu, choose **Stop instance**.
In the **Stop instance** window, choose **Stop**.
The instance will enter the *stopping* state and will shutdown.



Close your private browser window.

Congratulations! You have completed the lab.

End Lab

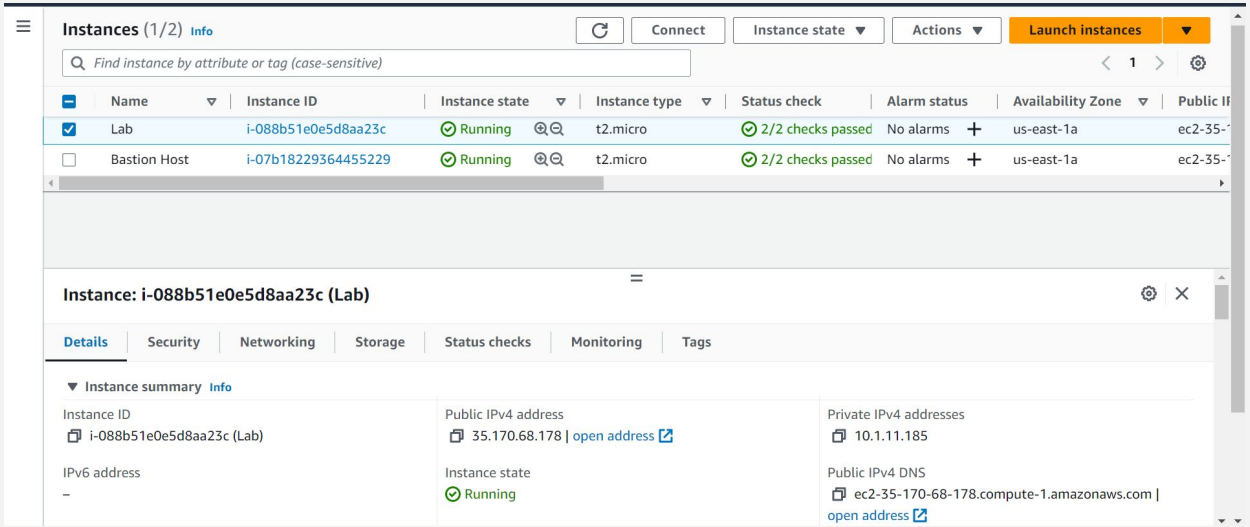
LAB 5: EBS

Task 1: Create a New EBS Volume

In the **AWS Management Console**, on the **Services** menu, click **EC2**.

In the left navigation pane, choose **Instances**.

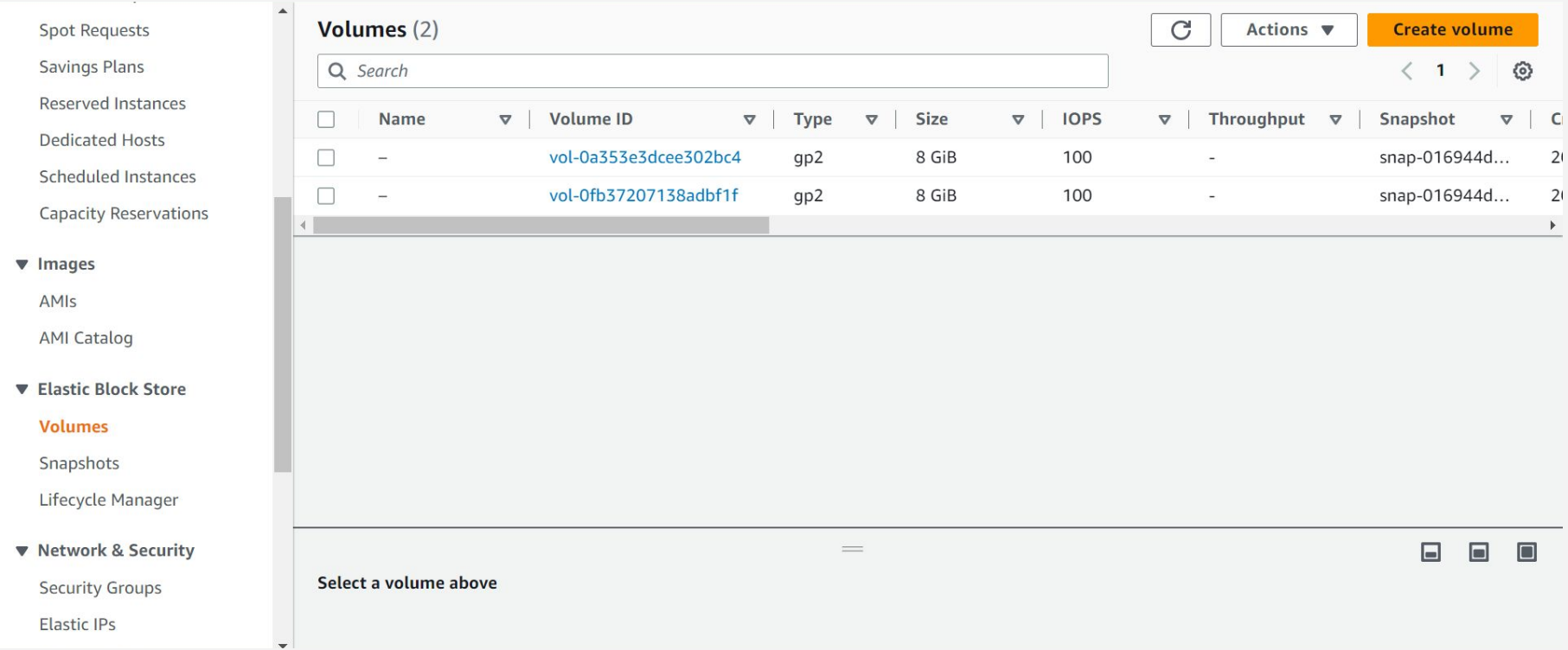
An Amazon EC2 instance named **Lab** has already been launched for your lab.



5. In the left navigation pane, choose **Volumes**.
   You will see an existing volume that is being used by the Amazon EC2 instance. This volume has a size of 8 GiB, which makes it easy to distinguish from the volume you will create next, which will be 1 GiB in size.

6. Choose **Create volume** then configure:
   - **Volume Type:** *General Purpose SSD (gp2)*
   - **Size (GiB):** 1. **NOTE**: You may be restricted from creating large volumes.
   - **Availability Zone:** Select the same availability zone as your EC2 instance.
   - Choose **Add Tag**
   - In the Tag Editor, enter:
     - **Key:** `Name`
     - **Value:** `My Volume`

7. Choose **Create Volume**
   Your new volume will appear in the list, and will move from the *Creating* state to the *Available* state. You may need to choose **refresh** to see your new volume.


Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Volumes (2)
Actions
Create volume
Search
1
Name
Volume ID
Type
Size
IOPS
Throughput
Snapshot
–
vol-0a353e3dcee302bc4
gp2
8 GiB
100
-
snap-016944d...
–
vol-0fb37207138adbf1f
gp2
8 GiB
100
-
snap-016944d...
Select a volume above

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

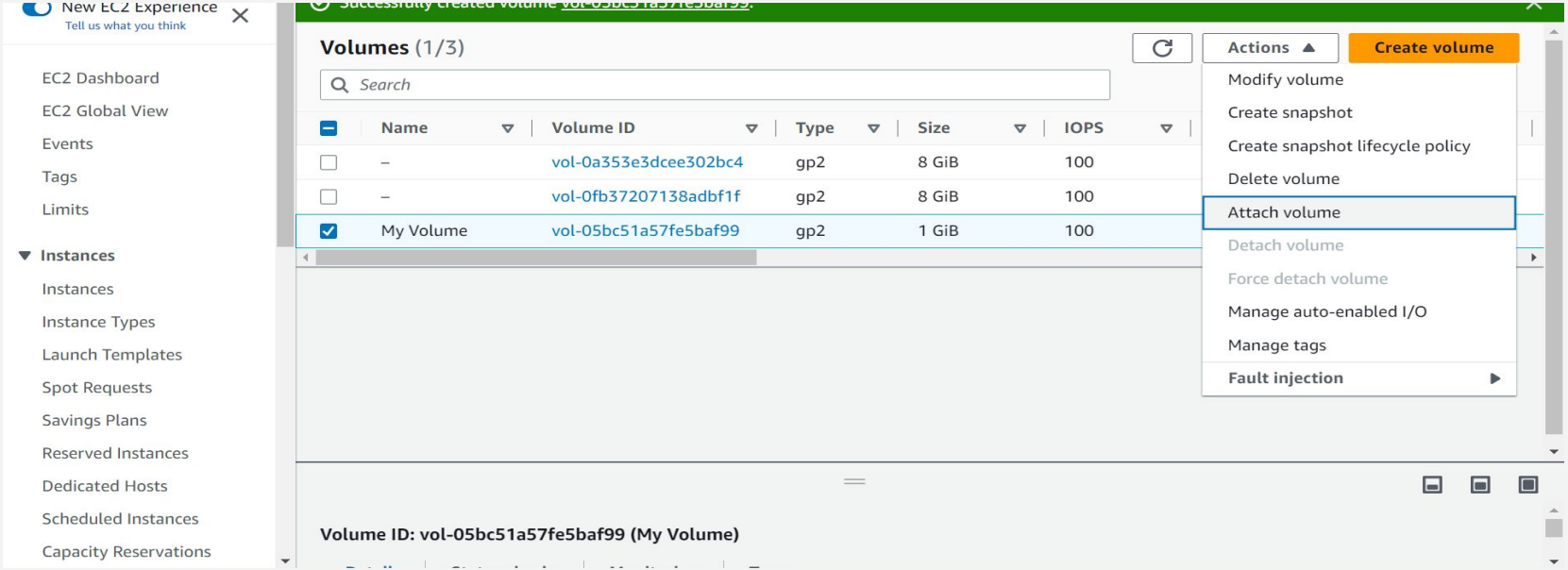
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.

Encrypt this volume

Task 2: Attach the Volume to an Instance

Select **My Volume**.

In the **Actions** menu, choose **Attach volume**.



Task 3: Connect to Your Amazon EC2 Instance

Windows Users: Using SSH to Connect

- Choose the Details drop down menu above these instructions you are currently reading, and then choose Show. A Credentials window will open.
- Choose the **Download PPK** button and save the **labsuser.ppk** file. Typically your browser will save it to the Downloads directory.
- Then exit the Details panel by choosing the **X**.

Download needed software Putty

- You will use **PuTTY** to SSH to Amazon EC2 instances.

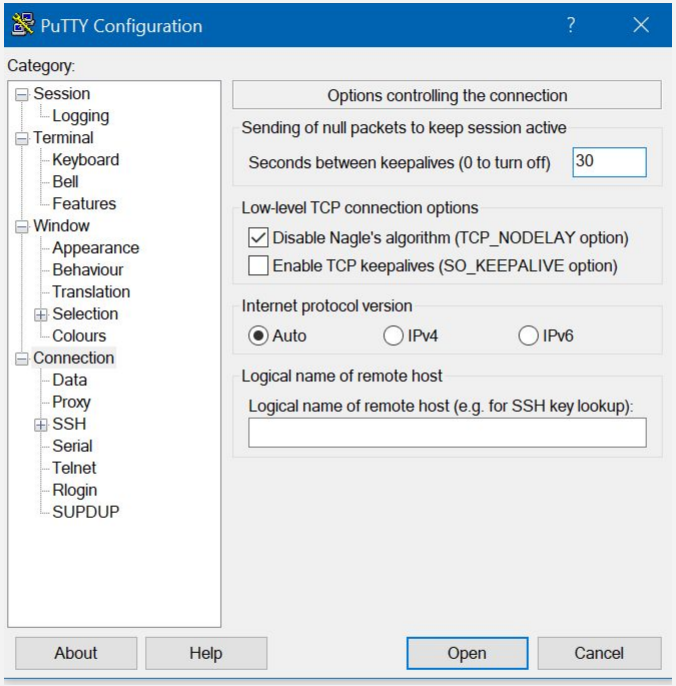
Open **putty.exe**


Details
AWS
Start Lab
End Lab
7:31
Instructions
Credentials
Cloud Access
AWS CLI:
Show
Cloud Labs
Remaining session time: 07:30:57(451 minutes)
Session started at: 2023-04-03T07:34:02-0700
Session to end at: 2023-04-03T15:34:02-0700
Accumulated lab time: 16:34:00 (994 minutes)
(1) ips -- public:35.170.68.178, private:10.1.11.185 (2) ips -- public:35.170.60.206, private:10.0.0.42
SSH key
Show
Download PEM
Download PPK
AWS SSO
Download URL

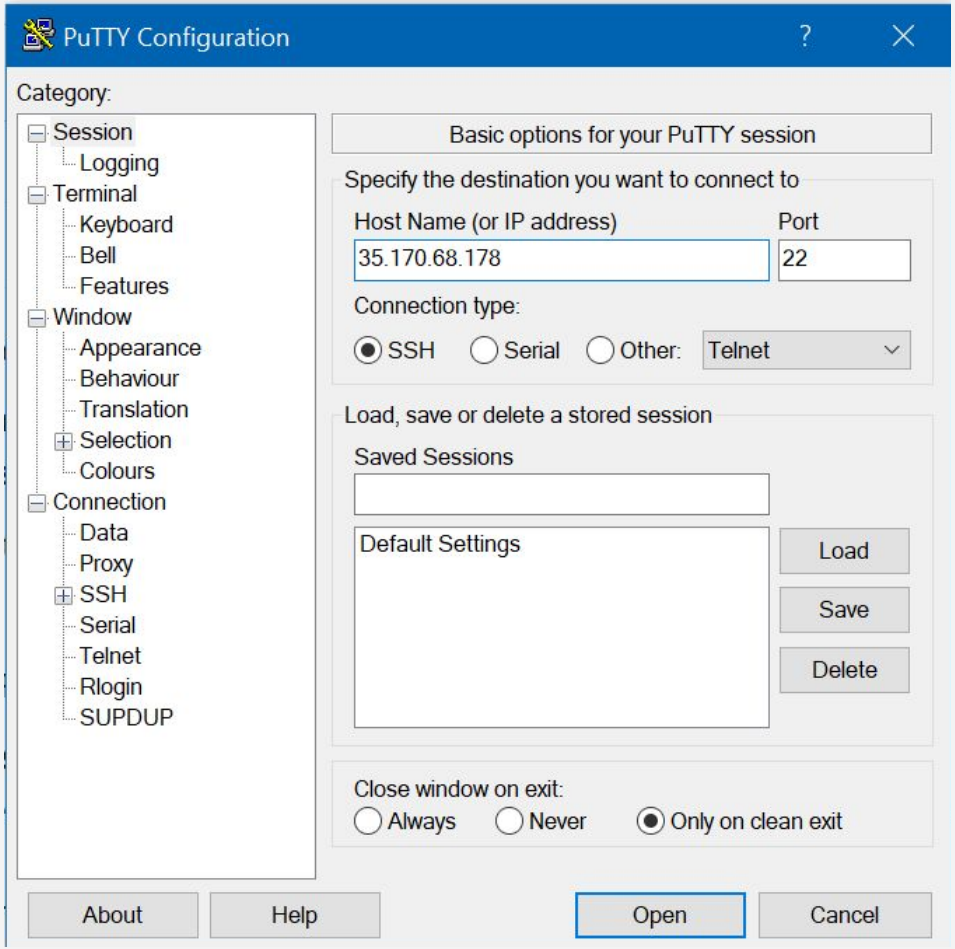
Configure PuTTY to not timeout:

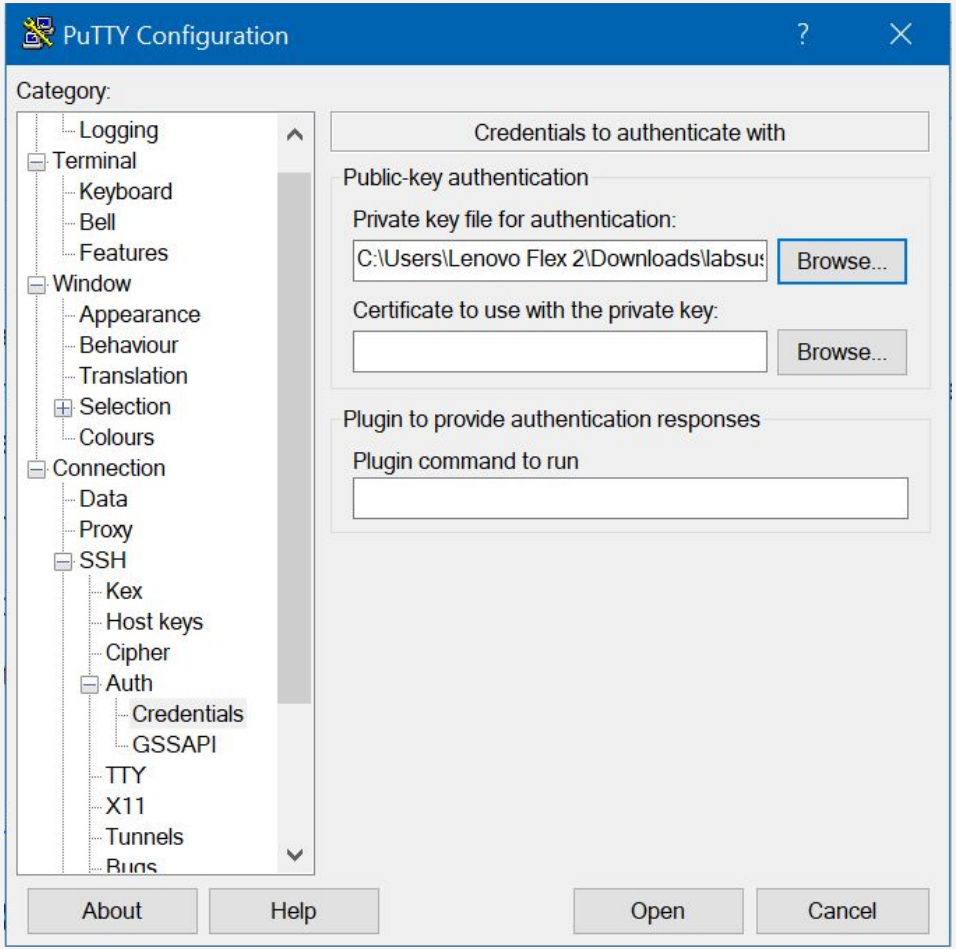
- Choose **Connection**
- Set **Seconds between keepalives** to `30`

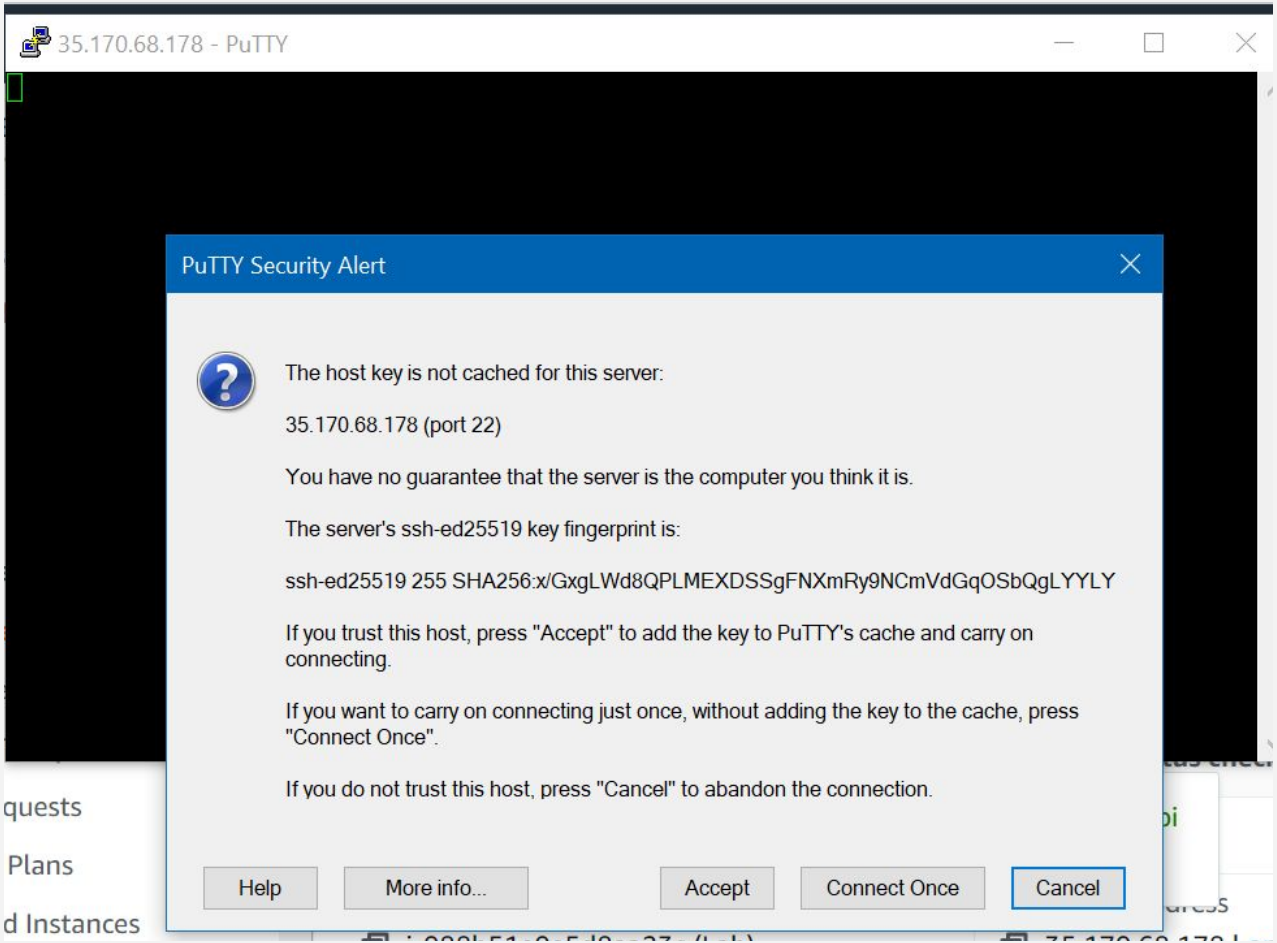
This allows you to keep the PuTTY session open for a longer period of time.



15. Configure your PuTTY session:
    - Choose **Session**
    - **Host Name (or IP address):** Paste the *Public DNS or IPv4 address* of the Lab instance that you noted earlier.
    - Back in PuTTY, in the **Connection** list, expand **SSH**
    - Choose **Auth** and expand **Credentials**
    - Under **Private key file for authentication:** Choose **Browse**
    - Browse to the *labsuser.ppk* file that you downloaded, select it, and choose **Open**
    - Choose **Open** again
20. To trust and connect to the host, choose **Accept**.
21. When prompted **login as**, enter: `ec2-user`
    This will connect you to the EC2 instance.


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
35.170.68.178
22
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel


PuTTY Configuration
Category:
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Kex
Host keys
Cipher
Auth
Credentials
GSSAPI
TTY
X11
Tunnels
Bugs
Credentials to authenticate with
Public-key authentication
Private key file for authentication:
C:\Users\Lenovo Flex 2\Downloads\labsu
Browse...
Certificate to use with the private key:
Browse...
Plugin to provide authentication responses
Plugin command to run
About
Help
Open
Cancel

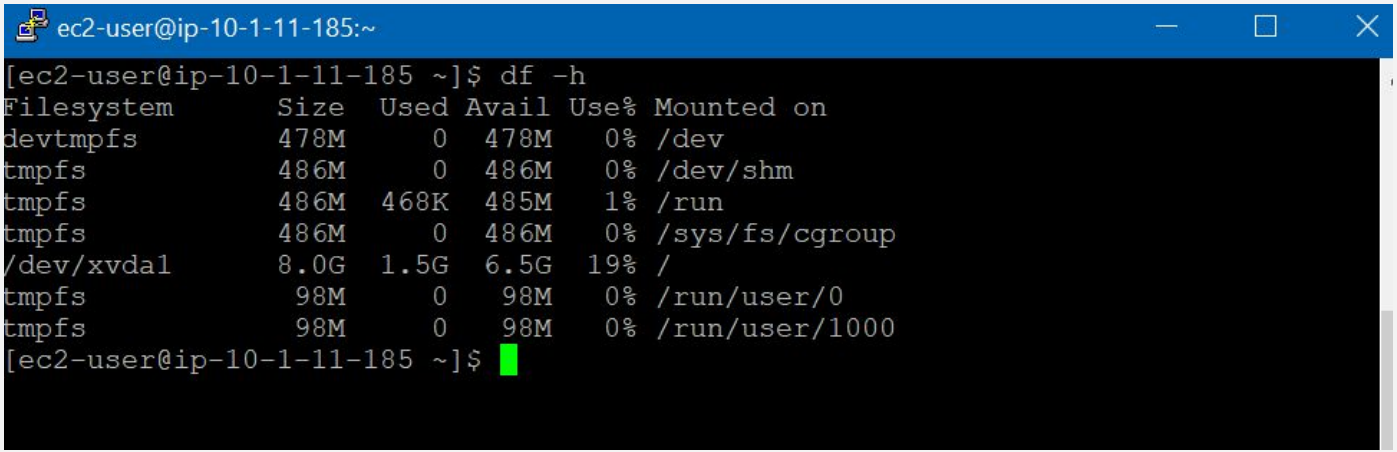

35.170.68.178 - PuTTY
PuTTY Security Alert
The host key is not cached for this server:
35.170.68.178 (port 22)
You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 SHA256:x/GxgLWd8QPLMEXDSSgFNXmRy9NCmVdGqOSbQgLYYLY
If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".
If you do not trust this host, press "Cancel" to abandon the connection.
Help
More info...
Accept
Connect Once
Cancel
quests
Plans
d Instances

Task 4: Create and Configure Your File System

In this task, you will add the new volume to a Linux instance as an ext3 file system under the /mnt/data-store mount point.

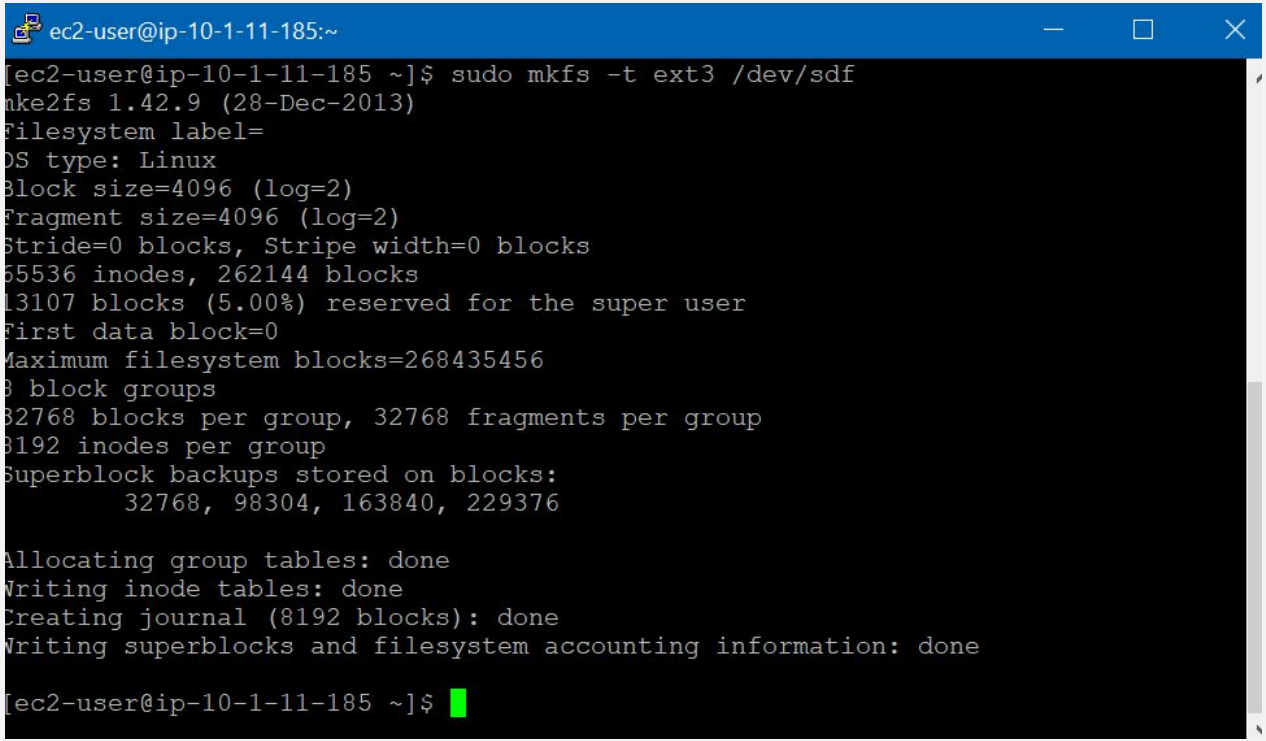
View the storage available on your instance:

```
df -h
```



Create an ext3 file system on the new volume:

```
sudo mkfs -t ext3 /dev/sdf
```



Create a directory for mounting the new storage volume:

```
sudo mkdir /mnt/data-store
```

Mount the new volume:

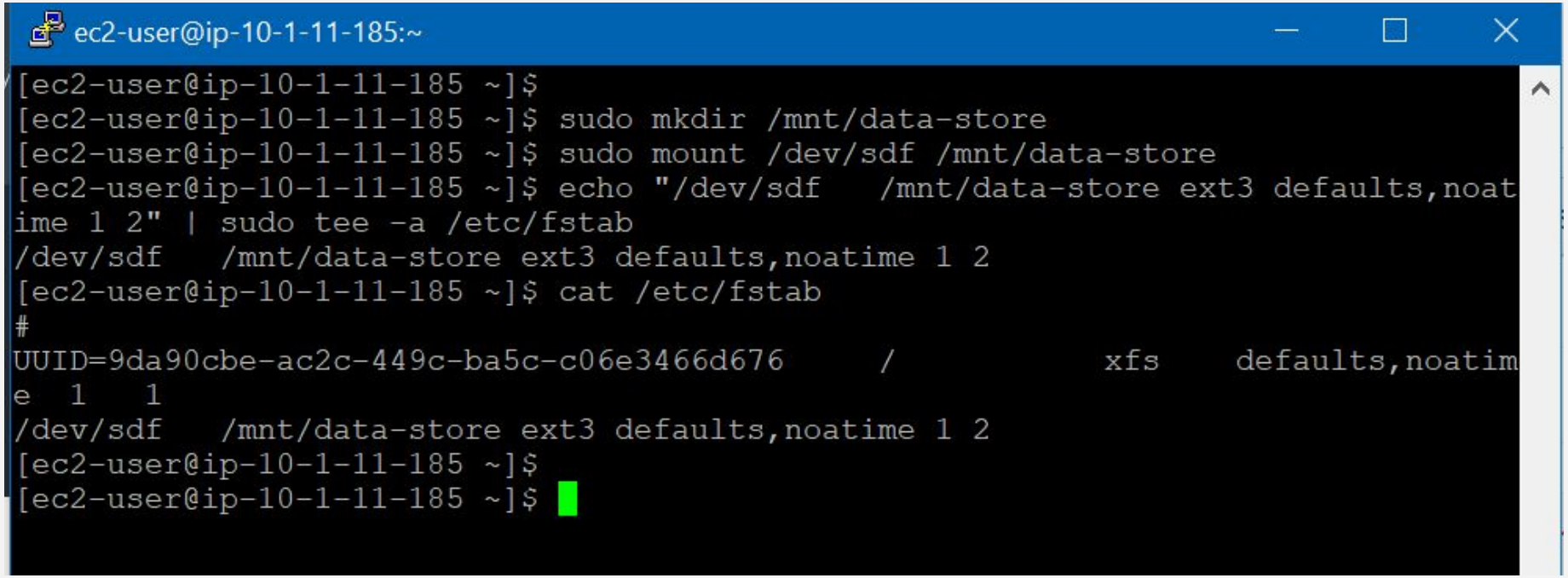
```
sudo mount /dev/sdf /mnt/data-store
```

To configure the Linux instance to mount this volume whenever the instance is started, you will need to add a line to */etc/fstab*.

```
echo "/dev/sdf   /mnt/data-store ext3 defaults,noatime 1 2" | sudo tee -a /etc/fstab
```

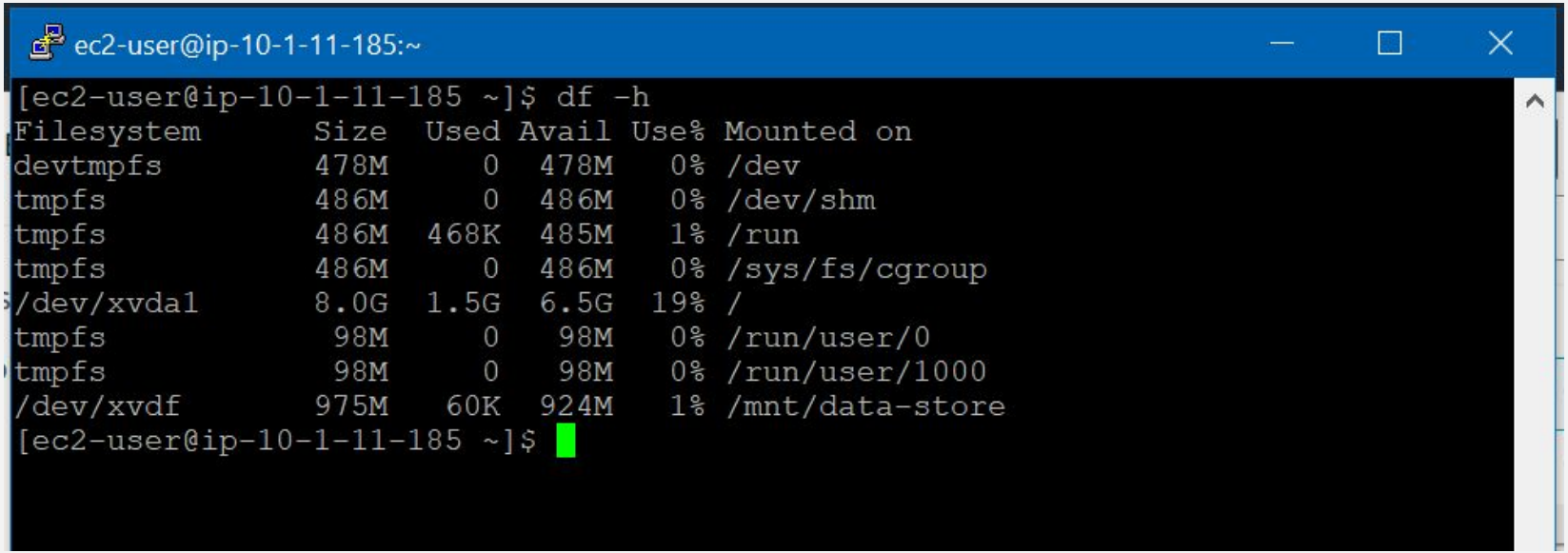
View the configuration file to see the setting on the last line:

```
cat /etc/fstab
```


ec2-user@ip-10-1-11-185:~
[ec2-user@ip-10-1-11-185 ~]$
[ec2-user@ip-10-1-11-185 ~]$ sudo mkdir /mnt/data-store
[ec2-user@ip-10-1-11-185 ~]$ sudo mount /dev/sdf /mnt/data-store
[ec2-user@ip-10-1-11-185 ~]$ echo "/dev/sdf /mnt/data-store ext3 defaults,noat
ime 1 2" | sudo tee -a /etc/fstab
/dev/sdf /mnt/data-store ext3 defaults,noatime 1 2
[ec2-user@ip-10-1-11-185 ~]$ cat /etc/fstab
#
UUID=9da90cbe-ac2c-449c-ba5c-c06e3466d676 / xfs defaults,noatim
e 1 1
/dev/sdf /mnt/data-store ext3 defaults,noatime 1 2
[ec2-user@ip-10-1-11-185 ~]$
[ec2-user@ip-10-1-11-185 ~]$

View the available storage again:

```
df -h
```

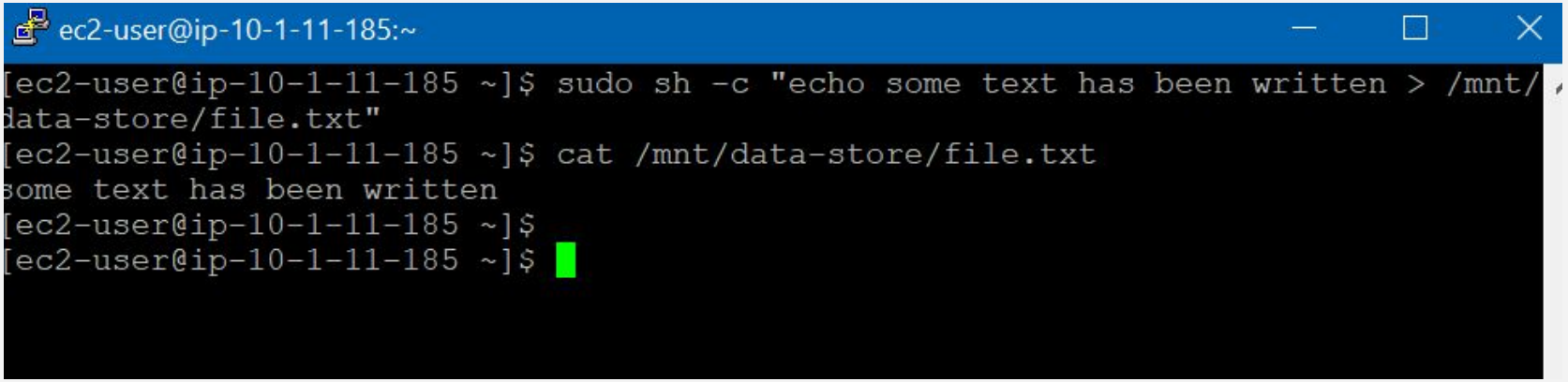


On your mounted volume, create a file and add some text to it.

```
sudo sh -c "echo some text has been written > /mnt/data-store/file.txt"
```

Verify that the text has been written to your volume.

```
cat /mnt/data-store/file.txt
```



Task 5: Create an Amazon EBS Snapshot

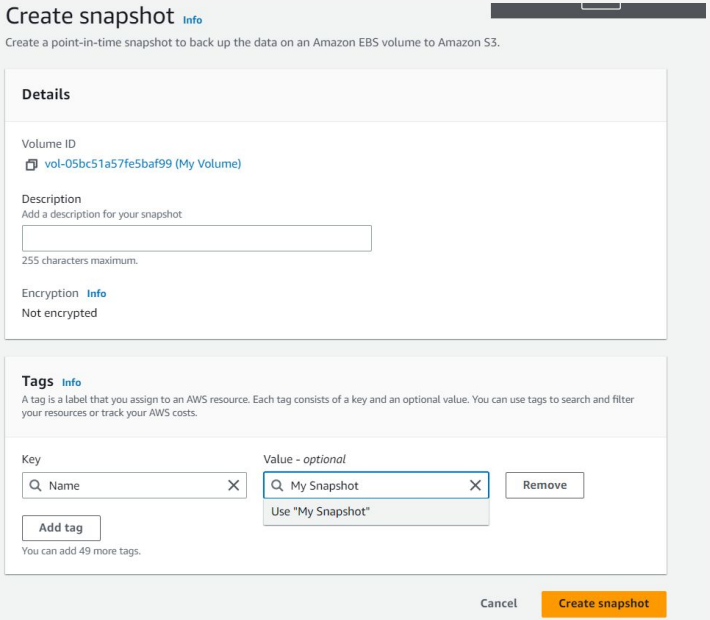
In the **AWS Management Console**, choose **Volumes** and select **My Volume**.

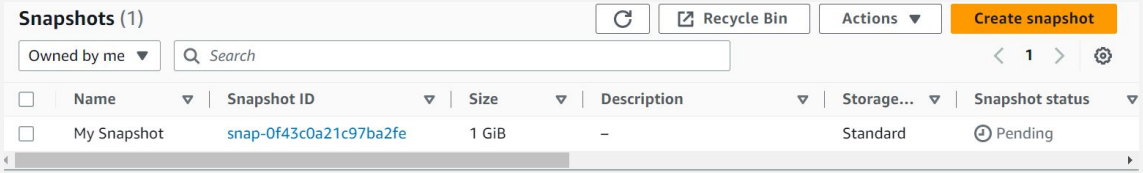
In the **Actions** menu, select **Create snapshot**.

Choose **Add tag** then configure:

- **Key:** `Name`
- **Value:** `My Snapshot`
- Choose **Create snapshot**

In the left navigation pane, choose **Snapshots**.


Create snapshot Info
Create a point-in-time snapshot to back up the data on an Amazon EBS volume to Amazon S3.
Details
Volume ID
vol-05bc51a57fe5baf99 (My Volume)
Description
Add a description for your snapshot
255 characters maximum.
Encryption Info
Not encrypted
Tags Info
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Name
Value - optional
My Snapshot
Use "My Snapshot"
Remove
Add tag
You can add 49 more tags.
Cancel
Create snapshot


Snapshots (1)
Recycle Bin
Actions
Create snapshot
Owned by me
Search
1
Name
Snapshot ID
Size
Description
Storage...
Snapshot status
My Snapshot
snap-0f43c0a21c97ba2fe
1 GiB
–
Standard
Pending

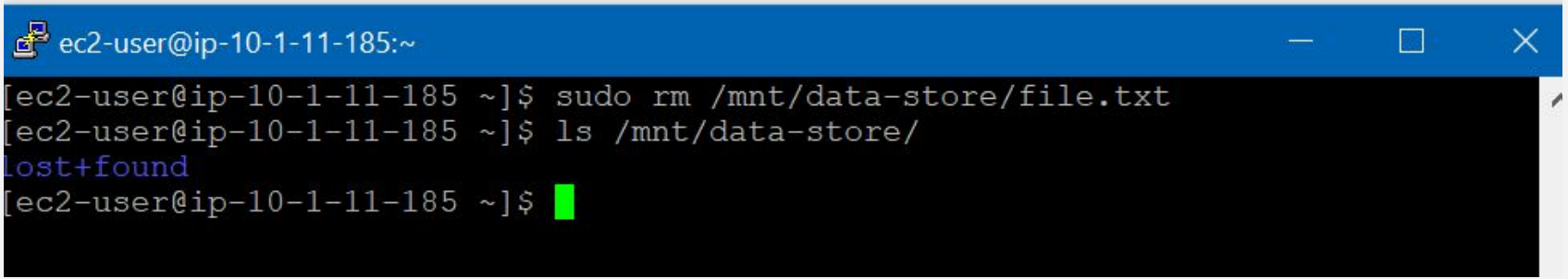
In your remote SSH session, delete the file that you created on your volume.

```
sudo rm /mnt/data-store/file.txt
```

Verify that the file has been deleted.

```
ls /mnt/data-store/
```

Your file has been deleted.



Task 6: Restore the Amazon EBS Snapshot

Create a Volume Using Your Snapshot

44. In the **AWS Management Console**, select **My Snapshot**.

45. In the **Actions** menu, select **Create volume from snapshot**.

46. For **Availability Zone** Select the same availability zone that you used earlier.

47. Choose **Add tag** then configure:
    - **Key:** `Name`
    - **Value:** `Restored Volume`
    - Choose **Create volume**

EC2 > Snapshots > snap-0f43c0a21c97ba2fe > Create volume

Create volume Info

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

Volume settings

Snapshot ID

snap-0f43c0a21c97ba2fe (My Snapshot)

Volume type Info

General Purpose SSD (gp2)

Size (GiB)

1

Min: 1 GiB, Max: 16384 GiB. The value must be an integer.

IOPS

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

Fast snapshot restore Info

Not enabled for selected snapshot

Encryption Info

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

Encrypt this volume

Tags - *optional* Info

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

Key	Value - *optional*	
Name	Restored Volume	Remove

Add tag

You can add 49 more tags.

Cancel Create volume

Attach the Restored Volume to Your EC2 Instance

48. In the left navigation pane, choose **Volumes**.

49. Select **Restored Volume**.

50. In the **Actions** menu, select **Attach volume**.

51. Choose the **Instance** field, then select the (Lab) instance that appears.
    Note that the **Device** field is set to */dev/sdg*. You will use this device identifier in a later task.

52. Choose **Attach volume**
    The volume state is now *in-use*.

EC2 > Volumes > vol-0639dfc5bc1b9143e > Attach volume

Attach volume Info

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

Basic details

Volume ID

vol-0639dfc5bc1b9143e (Restored Volume)

Availability Zone

us-east-1a

Instance Info

i-088b51e0e5d8aa23c

Only instances in the same Availability Zone as the selected volume are displayed.

Device name Info

/dev/sdg

Recommended device names for Linux: /dev/sda1 for root volume. /dev/sd[f-p] for data volumes.

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

Cancel Attach volume

Mount the Restored Volume

Create a directory for mounting the new storage volume:

```
sudo mkdir /mnt/data-store2
```

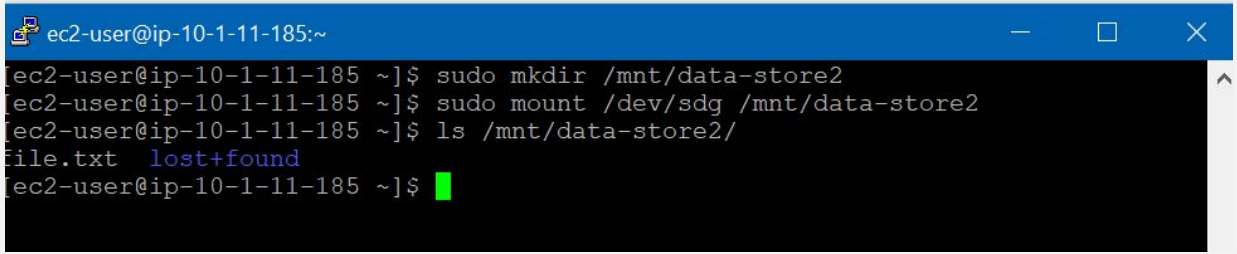
Mount the new volume:

```
sudo mount /dev/sdg /mnt/data-store2
```

Verify that volume you mounted has the file that you created earlier.

```
ls /mnt/data-store2/
```

You should see file.txt.



LAB 6: Scale and Load Balance Your Architecture

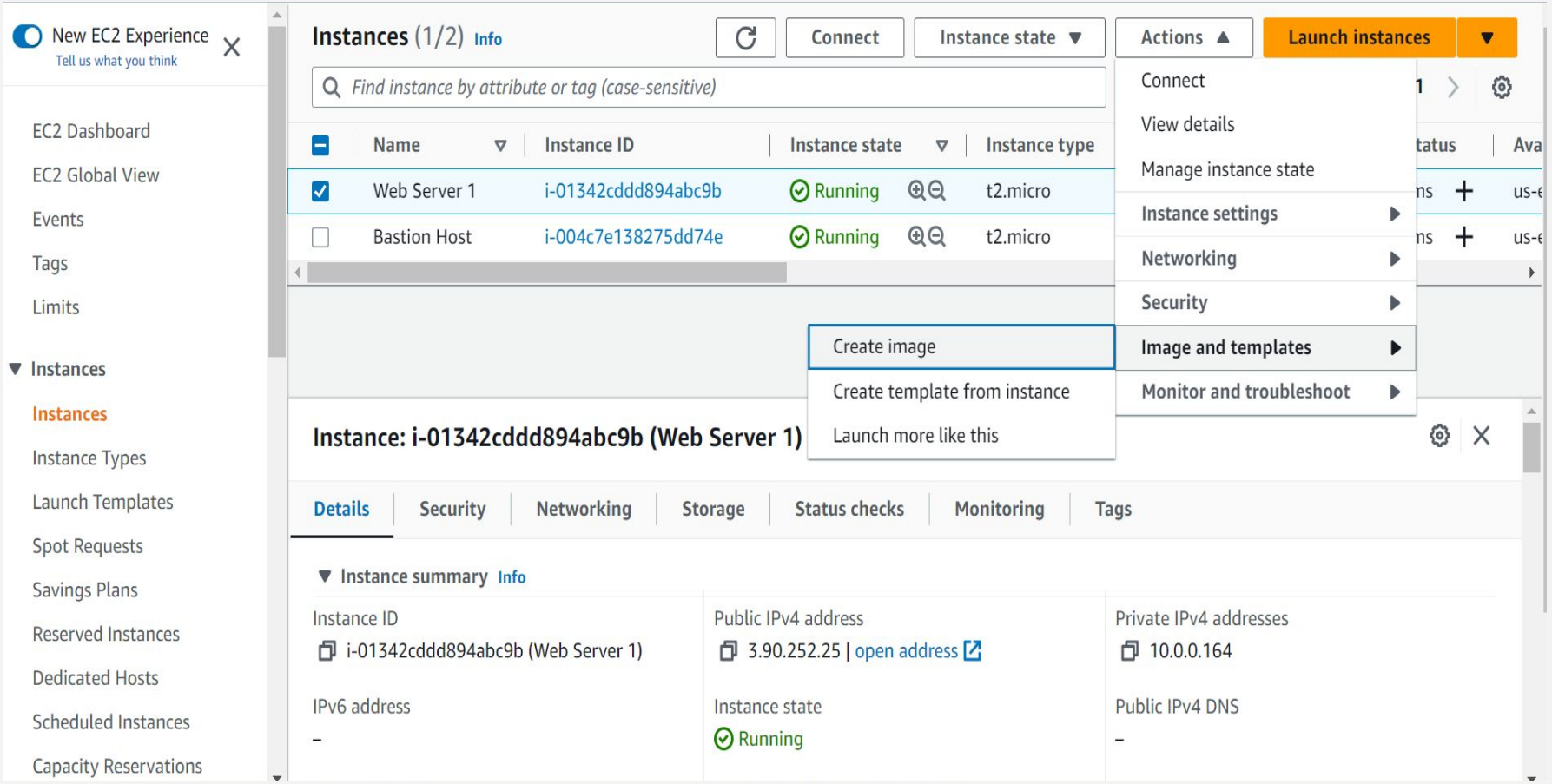
Task 1: Create an AMI for Auto Scaling

5. In the **AWS Management Console**, on the **Services** menu, click **EC2**.
6. In the left navigation pane, click **Instances**.

   First, you will confirm that the instance is running.
7. Wait until the **Status Checks** for **Web Server 1** displays *2/2 checks passed*. Click refresh to update.

   You will now create an AMI based upon this instance.
8. Select **Web Server 1**.
9. In the **Actions** menu, click **Image and templates** > **Create image**, then configure:
   - **Image name:** `WebServerAMI`
   - **Image description:** `Lab AMI for Web Server`
10. Click **Create image**

A confirmation banner displays the **AMI ID** for your new AMI.


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
Instances (1/2) Info
Connect
Instance state
Actions
Launch instances
Find instance by attribute or tag (case-sensitive)
Name
Instance ID
Instance state
Instance type
Web Server 1
i-01342cddd894abc9b
Running
t2.micro
Bastion Host
i-004c7e138275dd74e
Running
t2.micro
Connect
View details
Manage instance state
Instance settings
Networking
Security
Image and templates
Monitor and troubleshoot
Create image
Create template from instance
Launch more like this
Instance: i-01342cddd894abc9b (Web Server 1)
Details
Security
Networking
Storage
Status checks
Monitoring
Tags
Instance summary Info
Instance ID
i-01342cddd894abc9b (Web Server 1)
Public IPv4 address
3.90.252.25 | open address
Private IPv4 addresses
10.0.0.164
IPv6 address
–
Instance state
Running
Public IPv4 DNS
–

EC2 > Instances > i-01342cddd894abc9b > Create image

Create image Info

An image (also referred to as an AMI) defines the programs and settings that are applied when you launch an EC2 instance. You can create an image from the configuration of an existing instance.

Instance ID

i-01342cddd894abc9b (Web Server 1)

Image name

WebServerAMI

Maximum 127 characters. Can't be modified after creation.

Image description - *optional*

Lab AMI for Web Server

Maximum 255 characters

No reboot

☐ Enable

Instance volumes

Storage type	Device	Snapshot	Size	Volume type	IOPS	Throughput	Delete on termination	Encrypted
EBS	/dev/...	Create new snapshot fr...	8	EBS General Purpose S...	100		☑ Enable	☐ Enable

Add volume

During the image creation process, Amazon EC2 creates a snapshot of each of the above volumes.

Tags - *optional*

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

◉ Tag image and snapshots together
Tag the image and the snapshots with the same tag.

○ Tag image and snapshots separately
Tag the image and the snapshots with different tags.

No tags associated with the resource.

Add new tag

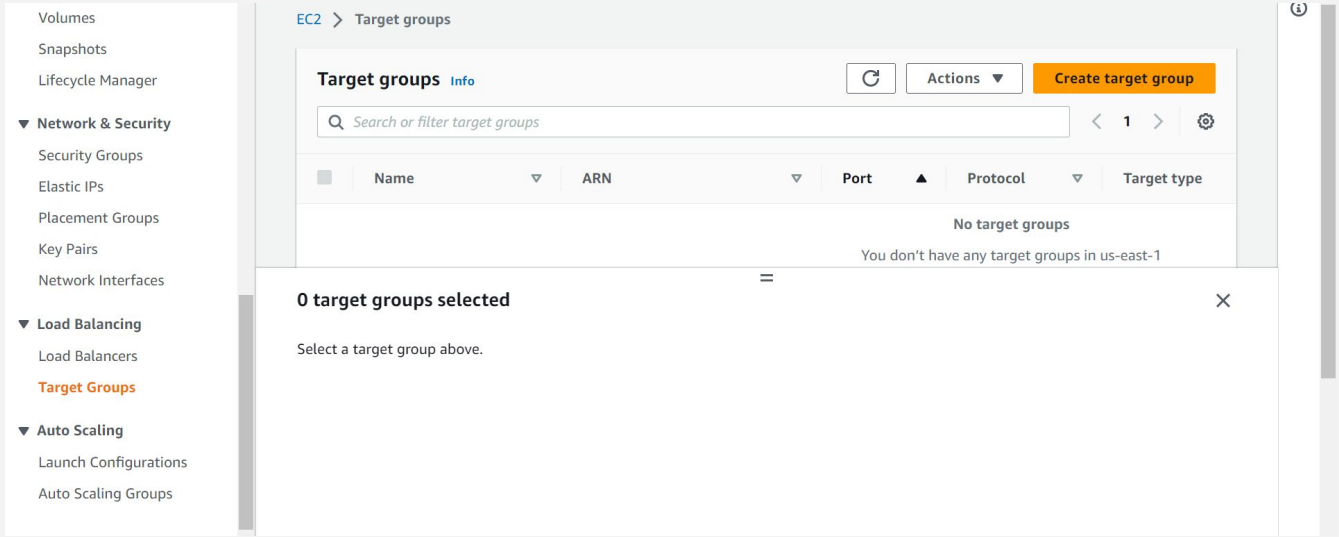
You can add up to 50 more tags.

Cancel | Create image

Task 2: Create a Load Balancer

In the left navigation pane, choose **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.



EC2 > Target groups > Create target group

Step 1
Specify group details

Step 2
Register targets

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Settings in this section cannot be changed after the target group is created.

Choose a target type

- (•) **Instances**
  - Supports load balancing to instances within a specific VPC.
  - Facilitates the use of Amazon EC2 Auto Scaling to manage and scale your EC2 capacity.
- ( ) **IP addresses**
  - Supports load balancing to VPC and on-premises resources.
  - Facilitates routing to multiple IP addresses and network interfaces on the same instance.
  - Offers flexibility with microservice based architectures, simplifying inter-application communication.
  - Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.
- ( ) **Lambda function**
  - Facilitates routing to a single Lambda function.
  - Accessible to Application Load Balancers only.
- ( ) **Application Load Balancer**
  - Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
  - Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

LabGroup

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol: HTTP : Port: 80

VPC

Select the VPC with the instances that you want to include in the target group.

Lab VPC
vpc-0b780fdec4a0f57a0
IPv4: 10.0.0.0/16

Protocol version

- (•) **HTTP1**
  Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.
- ( ) **HTTP2**
  Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.
- ( ) **gRPC**
  Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Health checks

The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol: HTTP

Health check path

Use the default path of "/" to ping the root, or specify a custom path if preferred.

/

Up to 1024 characters allowed.

▸ Advanced health check settings

Attributes

ⓘ Certain default attributes will be applied to your target group. You can view and edit them after creating the target group.

▸ **Tags - *optional***
Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.

Cancel | Next

Choose **Next**. The **Register targets** screen appears.

Review the settings and choose **Create target group**

In the left navigation pane, click **Load Balancers**.

At the top of the screen, choose **Create Load Balancer**.

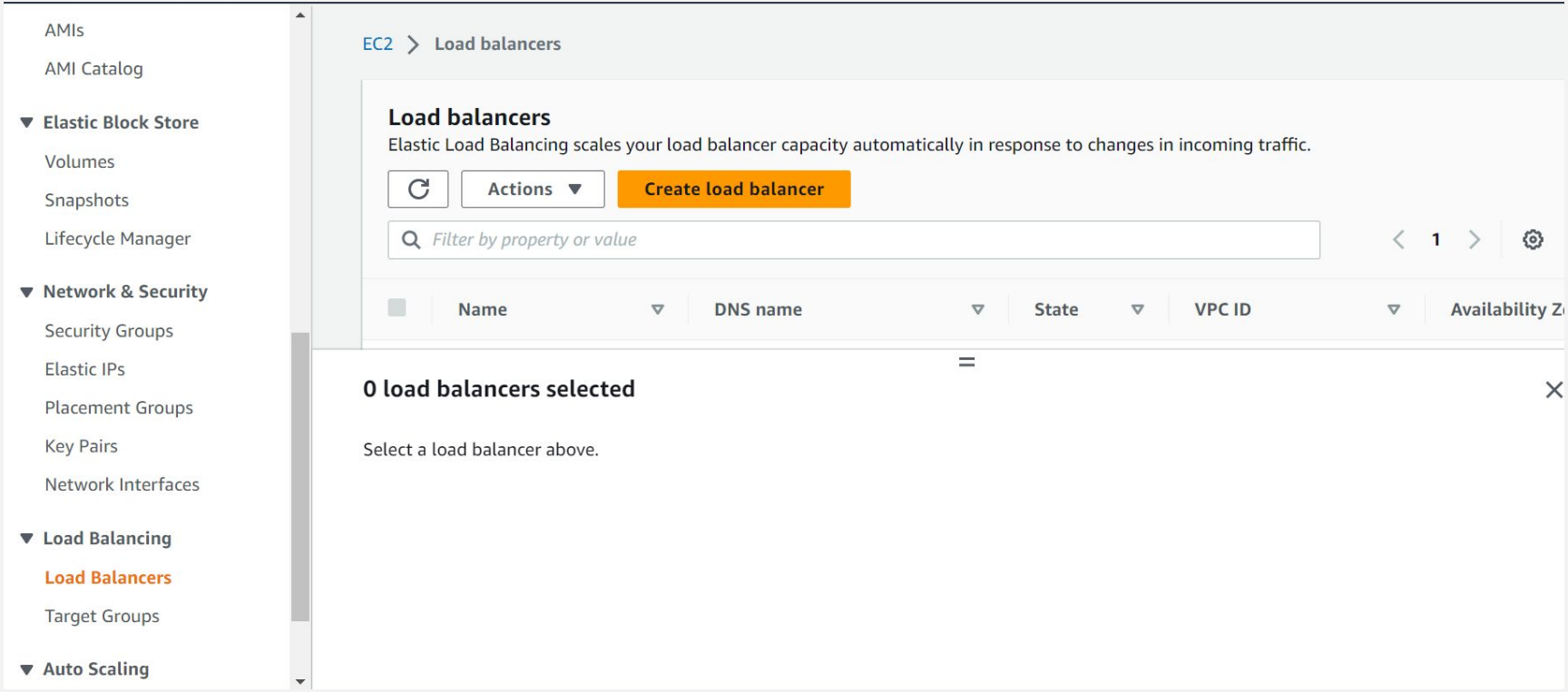
Under **Application Load Balancer**, choose **Create**

Under **Load balancer name**, enter: `LabELB`

Scroll down to the **Network mapping** section, then:

- For **VPC**, select: **Lab VPC**

- Choose the **first** displayed Availability Zone, then select **Public Subnet 1** from the Subnet drop down menu that displays beneath it.
- Choose the **second** displayed Availability Zone, then select **Public Subnet 2** from the Subnet drop down menu that displays beneath it.

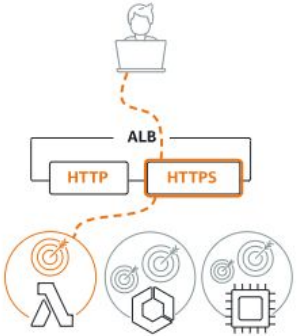

AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Load Balancing
Load Balancers
Target Groups
Auto Scaling
EC2
Load balancers
Load balancers
Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.
Actions
Create load balancer
Filter by property or value
1
Name
DNS name
State
VPC ID
Availability Z
0 load balancers selected
Select a load balancer above.

Select load balancer type

A complete feature-by-feature comparison along with detailed highlights is also available. Learn more

Load balancer types

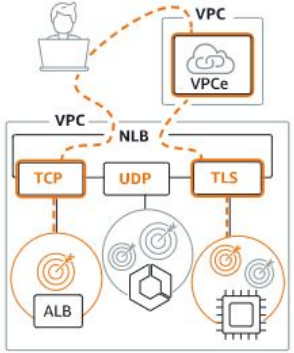
Application Load Balancer Info



Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

Create

Network Load Balancer Info



Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Create

Gateway Load Balancer Info

Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

Create

▶ Classic Load Balancer - *previous generation*

Close

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.

- Choose **View load balancer**

EC2 > Load balancers > Create Application Load Balancer

Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, n
on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to detern
applicable, it selects a target from the target group for the rule action.

▶ **How Elastic Load balancing works**

Basic configuration

Load balancer name

Name must be unique within your AWS account and cannot be changed after the load balancer is created.

LabELB

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme Info

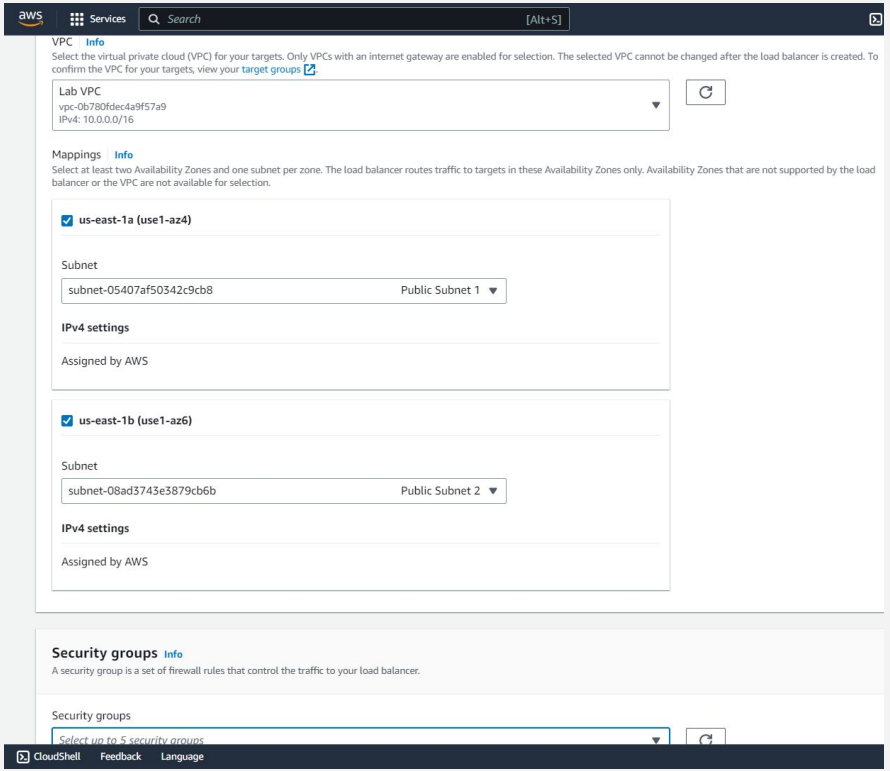
Scheme cannot be changed after the load balancer is created.

- (•) Internet-facing
  An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. Learn more
- ( ) Internal
  An internal load balancer routes requests from clients to targets using private IP addresses.

IP address type Info

Select the type of IP addresses that your subnets use.

- (•) IPv4
  Recommended for internal load balancers.
- ( ) Dualstack
  Includes IPv4 and IPv6 addresses.



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

22. In the left navigation pane, click **Launch Configurations**.
23. Click **Create launch configuration**
24. Configure these settings:
    - **Launch configuration name:** `LabConfig`
    - **Amazon Machine Image (AMI)** Choose *Web Server AMI*
    - **Instance type:**
        - Choose **Choose instance type**
        - Select *t3.micro*
        - Choose **Choose**

Additional configuration

- **Monitoring:** Select *Enable EC2 instance detailed monitoring within CloudWatch*

Under **Security groups**, you will configure the launch configuration to use the *Web Security Group* that has already been created for you.

- Choose **Select an existing security group**
- Select **Web Security Group**

Under **Key pair** configure:

- **Key pair options:** *Choose an existing key pair*
- **Existing key pair:** vockey
- Select **I acknowledge...**
- Click **Create launch configuration**

EC2 > Launch configurations > Create launch configuration

Create launch configuration Info

Instead of using launch configurations to create your EC2 Auto Scaling groups, we recommend that you use launch templates and make use of the Auto Scaling guidance option. For more information on migrating launch configurations and using launch templates, see the documentation

Create launch template

Launch configuration name

Name

LabConfig

Amazon machine image (AMI) Info

AMI

WebServerAMI

Instance type Info

Instance type

t3.micro (2 vCPUs, 1 GiB, EBS Only)

Choose instance type

Monitoring Info

Enable EC2 instance detailed monitoring within CloudWatch

EBS-optimized instance

Launch as EBS-optimized instance

Advanced details

Later, if you want to use a different launch configuration, you can create a new one and apply it to any Auto Scaling group. Existing launch configurations cannot be edited.

Storage (volumes) Info

EBS volumes

Remove

Volume type	Devices	Snapshot	Size (GiB)	Volume type
Root	/dev/xvda	snap-0a637fc35344ccf81	8	General purpose SSD (

Add new volume

Free tier eligible customers can get up to 30 GB of EBS storage. Learn more about free usage tier eligibility and usage restrictions.

Security groups Info

Assign a security group

Create a new security group

22. Select the checkbox for the *LabConfig* Launch Configuration.
23. From the **Actions** menu, choose *Create Auto Scaling group*
24. Enter Auto Scaling group name:
    - **Name:** `Lab Auto Scaling Group`
25. Choose **Next**
26. On the **Network** page configure
    - **Network:** *Lab VPC*
      You can ignore the message regarding "No public IP address"
    - **Subnet:** Select *Private Subnet 1 (10.0.1.0/24)* **and** *Private Subnet 2 (10.0.3.0/24)*
27. This will launch EC2 instances in private subnets across both Availability Zones.
28. Choose **Next**
29. In the **Load balancing - *optional*** pane, choose **Attach to an existing load balancer**
30. In the **Attach to an existing load balancer** pane, use the dropdown list to select *LabGroup*.
31. In the **Additional settings - *optional*** pane, select **Enable group metrics collection within CloudWatch**
    This will capture metrics at 1-minute intervals, which allows Auto Scaling to react quickly to changing usage patterns.
32. Choose **Next**
33. Under **Group size**, configure:
    - **Desired capacity:** 2
    - **Minimum capacity:** 2
    - **Maximum capacity:** 6
34. This will allow Auto Scaling to automatically add/remove instances, always keeping between 2 and 6 instances running.
35. Under **Scaling policies**, choose *Target tracking scaling policy* and configure:
    - **Lab policy name:** `LabScalingPolicy`
    - **Metric type:** *Average CPU Utilization*
    - **Target value:** `60`
36. This tells Auto Scaling to maintain an *average* CPU utilization *across all instances* at 60%. Auto Scaling will automatically add or remove capacity as required to keep the metric at, or close to, the specified target value. It adjusts to fluctuations in the metric due to a fluctuating load pattern.
37. Choose **Next**
    Auto Scaling can send a notification when a scaling event takes place. You will use the default settings.
38. Choose **Next**
    Tags applied to the Auto Scaling group will be automatically propagated to the instances that are launched.
39. Choose **Add tag** and Configure the following:
    - **Key:** `Name`
    - **Value:** `Lab Instance`
40. Click **Next**
41. Review the details of your Auto Scaling group, then click **Create Auto Scaling group**. If you encounter an error **Failed to create Auto Scaling group**, then click **Retry Failed Tasks**.
    Your Auto Scaling group will initially show an instance count of zero, but new instances will be launched to reach the **Desired** count of 2 instances.

Step 1
Choose launch template or configuration

Step 2
Choose instance launch options

Step 3 - *optional*
Configure advanced options

Step 4 - *optional*
Configure group size and scaling policies

Step 5 - *optional*
Add notifications

Step 6 - *optional*
Add tags

Choose launch template or configuration Info

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group. If you currently use launch configurations, you might consider migrating to launch templates.

Name

Auto Scaling group name
Enter a name to identify the group.

Lab Auto Scaling Group

Must be unique to this account in the current Region and no more than 255 characters.

Launch configuration Info

Switch to launch template

⚠ Instead of using launch configurations to create your EC2 Auto Scaling groups, we recommend that you use launch templates and make use of the Auto Scaling guidance option. For more information on migrating launch configurations and using launch templates, see the documentation

Security groups Info

Assign a security group

- ○ Create a new security group
- ◉ Select an existing security group

Security groups

Copy to new | View rules

web

1

Security group ID	Name	VPC ID	Description
sg-0cc91ba448c114269	Web Security Group	vpc-0b780fdec4a9f57a9	Enable HTTP access

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Key pair (login) Info

Key pair options

Choose an existing key pair

Existing key pair

vockey

☑ I acknowledge that I have access to the selected private key file (vockey.pem), and that without this file, I won't be able to log into my instance.

Cancel | Create launch configuration