

# 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**.

The screenshot shows the AWS Management Console with the EC2 service selected. The main dashboard displays various EC2 resources: 1 running instance, 0 Auto Scaling Groups, 0 Dedicated Hosts, 0 Elastic IPs, 1 instance, 1 key pair, 0 load balancers, 0 placement groups, 0 security groups, 0 snapshots, and 1 volume. On the left sidebar, the 'Instances' section is expanded, showing options like Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, and Images. In the bottom left corner of the main dashboard, there is a 'Launch instance' button, which is highlighted with a yellow box. To the right of the main dashboard, there is a large callout box with the title 'Launch instance'. It contains the text 'To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.' Below this is a large orange 'Launch instance' button with a downward arrow, also highlighted with a yellow box. Further down, there is a 'Migrate a server' button. At the bottom of the callout box, a note states 'Note: Your instances will launch in the US East (N. Virginia) Region'.

## 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.

### Launch an instance Info

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

The screenshot shows the AWS Launch an instance wizard. It starts with the 'Name and tags' step, where the instance is named 'Web Server'. Then it moves to the 'Application and OS Images (Amazon Machine Image)' step, where the 'Amazon Linux' AMI is selected. The 'Amazon Linux 2023 AMI' details are shown, including its ID, architecture (64-bit x86), boot mode (uefi-preferred), and AMI ID.

**Name and tags Info**

Name  
Web Server Add additional tags

**Application and OS Images (Amazon Machine Image) Info**

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

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

Recents Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat ... !  Browse more AMIs  
Including AMIs from AWS, Marketplace and the Community

**Amazon Machine Image (AMI)**

**Amazon Linux 2023 AMI** Free tier eligible

ami-00c39f71452c08778 (64-bit (x86), uefi-preferred) / ami-01d9e06b75f9d69c4 (64-bit (Arm), uefi)  
Virtualization: hvm ENA enabled: true Root device type: ebs

Description  
Amazon Linux 2023 AMI 2023.0.20230322.0 x86\_64 HVM kernel-6.1

Architecture Boot mode AMI ID  
64-bit (x86) uefi-preferred ami-00c39f71452c08778 Verified provider

## 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.

The screenshot shows the 'Instance type' configuration section of the AWS Lambda setup. The 't2.micro' instance type is selected, indicated by a blue border around its row. The row contains the following information:

Instance type	Info
t2.micro	Free tier eligible
Family: t2	1 vCPU 1 GiB Memory
On-Demand Windows pricing:	0.0162 USD per Hour
On-Demand SUSE pricing:	0.0116 USD per Hour
On-Demand RHEL pricing:	0.0716 USD per Hour
On-Demand Linux pricing:	0.0116 USD per Hour

Below the table, there is a 'Compare instance types' link.

## Step 4: Key pair (login)

For **Key pair name - required**, choose **vockey**.

Amazon EC2 uses public–key cryptography to encrypt and decrypt login information.

▼ **Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

vockey

[Create new key pair](#)

## 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.

▼ **Network settings** [Info](#)

VPC - required [Info](#)

vpc-06dff0a8e0c1dd5d (Lab VPC)  
10.0.0.0/16

Subnet [Info](#)

subnet-06d139f13c2087df2 Public Subnet 2  
VPC: vpc-06dff0a8e0c1dd5d Owner: 137703912323 Availability Zone: us-east-1b  
IP addresses available: 251 CIDR: 10.0.2.0/24

[Create new subnet](#)

Auto-assign public IP [Info](#)

Enable

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.

▼ Network settings [Info](#)

VPC - required [Info](#)  
vpc-06dff0a8e0c1dd5d (Lab VPC)  
10.0.0.0/16

Subnet Info  
subnet-06d139f13c2087df2 Public Subnet 2  
VPC: vpc-06dff0a8e0c1dd5d Owner: 137703912323 Availability Zone: us-east-1b  
IP addresses available: 251 CIDR: 10.0.0.0/24

Create new subnet

Auto-assign public IP [Info](#)  
Enable

Firewall (security groups) [Info](#)  
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group  
 Select existing security group

Security group name - required  
Web Server security group

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_-./@#=;&|\$^

Description - required [Info](#)  
Security group for my web server

Inbound security groups rules  
No security group rules are currently included in this template. Add a new rule to include it in the launch template.

Add security group rule  
Advanced network configuration

Firewall (security groups) [Info](#)  
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group  
 Select existing security group

Security group name - required  
Web Server security group

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_-./@#=;&|\$^

Description - required [Info](#)  
Security group for my web server

Inbound security groups rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)  
Remove

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
ssh	TCP	22

Source type [Info](#)  
Anywhere

Source [Info](#)  
Add CIDR, prefix list or security  
e.g. SSH for admin desktop

0.0.0.0/0 X

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.

Add security group rule  
Advanced network configuration

## 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).

The screenshot shows the 'Configure storage' section with the following details:

- Volume count: 1x
- Volume size: 8 GiB
- Volume type: gp3
- Description: Root volume (Not encrypted)
- Info message: Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage
- Buttons: Add new volume, Edit
- File systems: 0 x File systems

## 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.

The screenshot shows the 'Advanced details' section with the following configuration:

- Purchasing option: Request Spot Instances (unchecked)
- Domain join directory: Select (dropdown menu)
- Termination protection: Enable
- Stop protection: Select (dropdown menu)

Buttons: Create new directory (with icons for copy and create)

- 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

User data - optional [Info](#)  
Enter user data in the field.

```
#!/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
```

## 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..*



▼ **Summary**

Number of instances [Info](#)  
 ▼

**Software Image (AMI)**  
Amazon Linux 2023 AMI 2023.0.2...[read more](#)  
ami-00c39f71452c08778

**Virtual server type (instance type)**  
t2.micro

**Firewall (security group)**  
New security group

**Storage (volumes)**  
1 volume(s) - 8 GiB

ⓘ **Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. X

ⓘ **Find instance by attribute or tag (case-sensitive)**

Name	Instance ID	Instance state	Instance type	Status check	Alarm
<input checked="" type="checkbox"/> Web Server	i-010422fb899488b84	<span style="color: green;">Running</span>	<span style="color: green;">Running</span>	t2.micro	<span style="color: green;">Initializing</span>
<input type="checkbox"/> Bastion Host	i-0ad34d8e8e4aeb4a0	<span style="color: green;">Running</span>	<span style="color: green;">Running</span>	t2.micro	<span style="color: green;">2/2 checks passed</span>

Cancel Launch instance [Review commands](#)

Wait for your instance to display the following:

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

Instance type	Status check	Alarm status	
t2.micro	✓ 2/2 checks passed	No alarms	+
t2.micro	✓ 2/2 checks passed	No alarms	+

**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.

Instance: i-010422fb899488b84 (Web Server)

Details | Security | Networking | Storage | **Status checks** | Monitoring | Tags

**Status checks** Info

Status checks detect problems that may impair i-010422fb899488b84 (Web Server) from running your applications.

System status checks

✓ System reachability check passed

Instance status checks

✓ Instance reachability check passed

Report the instance status if our checks do not reflect your experience with this instance or if they do not detect issues you are having.

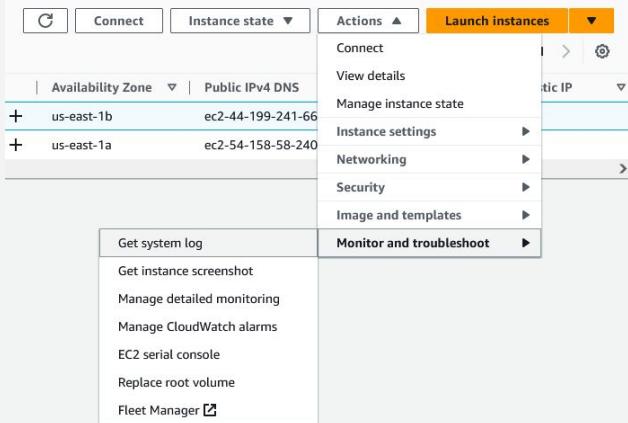
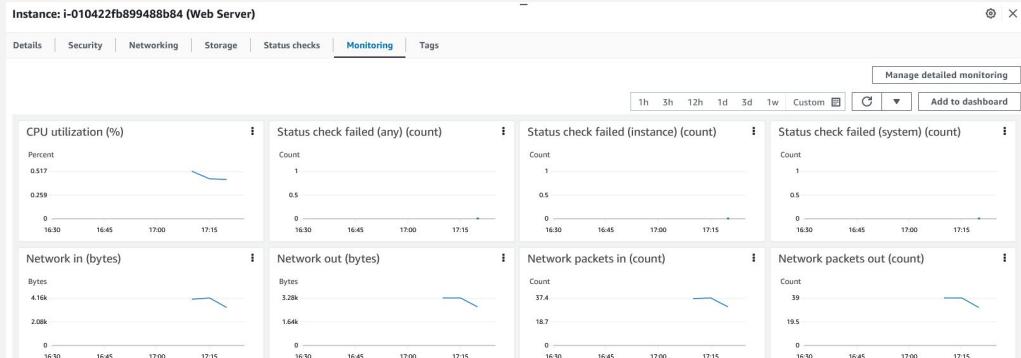
Report instance status

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.**

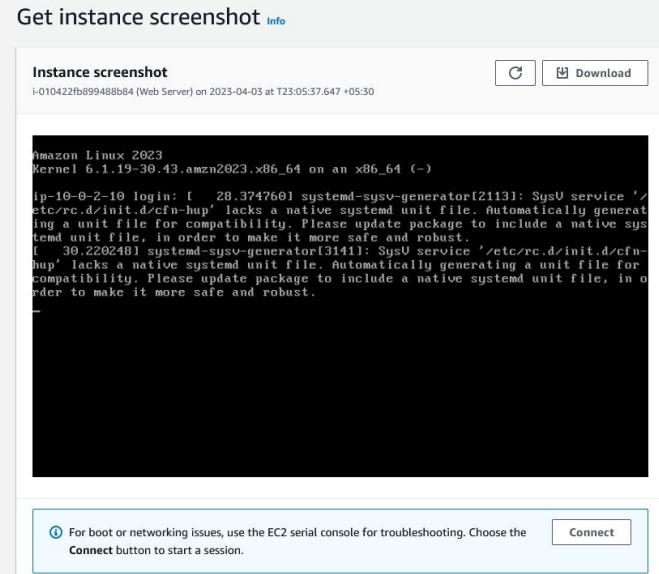
Ensure **Web Server** is still selected. Then, in the Actions menu, select **Monitor and troubleshoot Get instance screenshot**.

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.

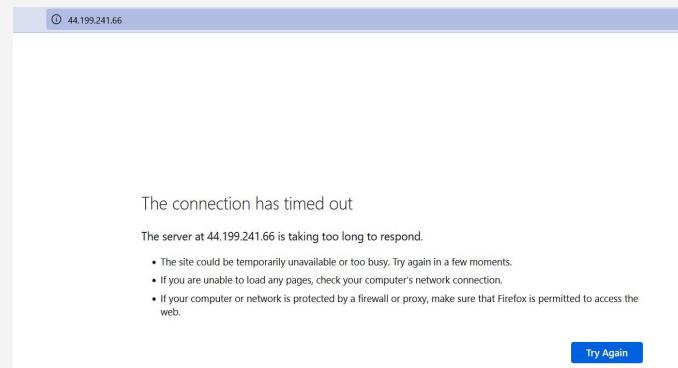
Open a new tab in your web browser, paste the IP address you just

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.

The image contains three screenshots of the AWS EC2 Security Groups console. The first screenshot shows the main list of security groups with one named "Web Server security group" selected. The second screenshot shows the "Inbound rules" tab for this specific group, which is currently empty. The third screenshot shows the "Edit inbound rules" dialog box, where a new rule is being added for "Type: HTTP", "Protocol: TCP", "Port range: 80", and "Source: Anywhere-IPv4".

# 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

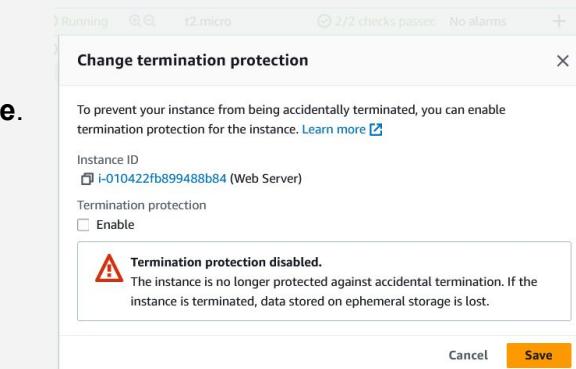
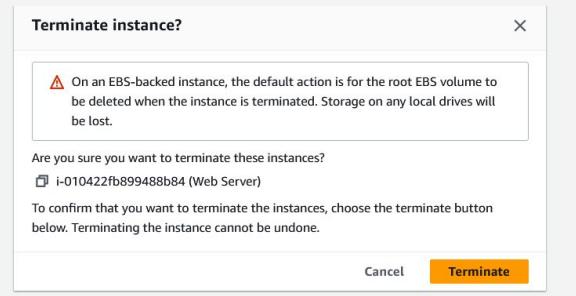
You can now terminate the instance.

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

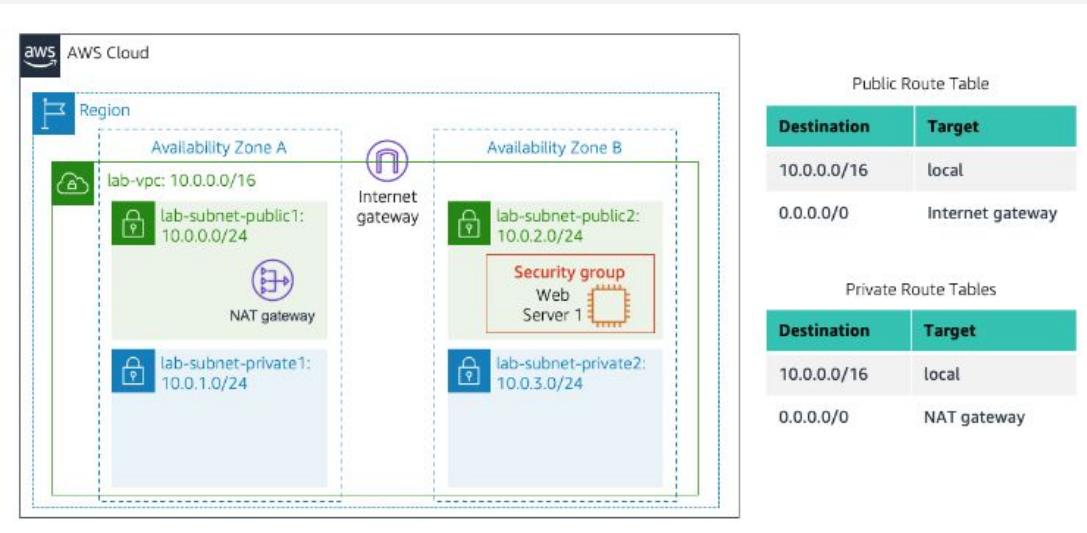


# LAB 2 - VPC

# 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



# 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.

The screenshot shows the AWS VPC Dashboard. At the top right, there are two prominent buttons: "Create VPC" (orange background) and "Launch EC2 Instances". Below these buttons, a note states: "Note: Your Instances will launch in the US East region." To the right of the note is a section titled "Resources by Region" with a "Refresh Resources" button. This section displays the following counts: 2 VPCs (US East), 2 NAT Gateways (US East). On the left side of the dashboard, there is a sidebar with a "Select a VPC" dropdown and links for "Virtual private cloud", "Your VPCs", "Subnets", and "Route tables". The main content area is titled "Create VPC" and contains several configuration panels: "VPC settings" (with tabs for "VPC only" and "VPC and more", and fields for "Name tag auto-generation" set to "Auto-generate" with value "lab"), "IPv4 CIDR block" (set to "10.0.0.0/16"), "IPv6 CIDR block" (set to "No IPv6 CIDR block"), "Tenancy" (set to "Default"), and "Number of Availability Zones (AZs)" (set to "1"). To the right of the configuration panels is a "Preview" section showing a network diagram with a VPC containing two subnets ("us-east-1a" and "us-east-1a") and two route tables ("lab-rtb-public" and "lab-rtb-private1-us-east-1a"). These components are connected to a NAT gateway ("lab-igw") and an internet gateway ("lab-nat-public1-us-east-1a").

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 tables lab-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**

#### Number of public subnets [Info](#)

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0	1
---	---

#### Number of private subnets [Info](#)

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0	1	2
---	---	---

#### ▼ Customize subnets CIDR blocks

##### Public subnet CIDR block in us-east-1a

10.0.0.0/24	256 IPs
-------------	---------

##### Private subnet CIDR block in us-east-1a

10.0.1.0/24	256 IPs
-------------	---------

#### NAT gateways (\$) [Info](#)

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None	In 1 AZ	1 per AZ
------	---------	----------

#### VPC endpoints [Info](#)

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None	S3 Gateway
------	------------

#### DNS options [Info](#)

- Enable DNS hostnames
- Enable DNS resolution

#### ► Additional tags

Cancel

Create 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**

**Subnet settings**  
Specify the CIDR blocks and Availability Zone for the subnet.

**Subnet 1 of 1**

**Subnet name**  
Create a tag with a key of 'Name' and a value that you specify.  
  
The name can be up to 256 characters long.

**Availability Zone** [Info](#)  
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

**IPv4 CIDR block** [Info](#)  
 X

**▼ Tags - optional**

Key	Value - optional	Remove
<input type="text" value="Name"/> X	<input type="text" value="lab-subnet-public2"/> X	Remove

Add new tag  
You can add 49 more tags.

Remove

Add new subnet

**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**

VPC ID  
Create subnets in this VPC.  
vpc-0f5d6132a9d2d6bff (lab-vpc) ▾

Associated VPC CIDRs  
IPv4 CIDRs  
10.0.0.0/16

**Subnet settings**  
Specify the CIDR blocks and Availability Zone for the subnet.

**Subnet 1 of 1**

Subnet name  
Create a tag with a key of 'Name' and a value that you specify.  
lab-subnet-private2  
The name can be up to 256 characters long.

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

IPv4 CIDR block [Info](#)  
10.0.3.0/24 X

▼ Tags - optional  
Key Value - optional  
Name lab-subnet-private2 X Remove  
Add new tag  
You can add 49 more tags.

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**

Route tables (1/6) <a href="#">Info</a>								
<input type="text"/> Filter route tables								
Name	Route table ID	Explicit subnet ass...	Edge associ...	M...	VPC	Owner ID		
-	rtb-0b7a5bd5e29...	-	-	Yes	vpc-0f5d6132a9d2d6...	636030802452		
lab-rtb-public	rtb-0314a853bc...	subnet-03a14978...	-	No	vpc-0f5d6132a9d2d6...	636030802452		
-	rtb-06cad95ed4cf...	-	-	Yes	vpc-0e12671ac99f712...	636030802452		
<input checked="" type="checkbox"/> lab-rtb-private1-us-east-1a	rtb-005d39a2687...	subnet-06034f7e...	-	No	vpc-0f5d6132a9d2d6...	636030802452		
-	rtb-04662484bc2d...	-	-	Yes	vpc-042c90e2c0e3f1c...	636030802452		
Work Public Route Table	rtb-09fe0f489743...	subnet-03cf499b...	-	No	vpc-042c90e2c0e3f1c...	636030802452		

tb-005d39a268737f757 / lab-rtb-private1-us-east-1a

Details | Routes | **Subnet associations** | Edge associations | Route propagation | Tags

Explicit subnet associations (1)

Edit subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
lab-subnet-private1-us-east-1a	subnet-06034f7e46e488b68	10.0.10.0/24	-

Subnets without explicit associations (2)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)

Filter subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
lab-subnet-public2	subnet-0ec116f65204e34b4	10.0.2.0/24	-	Main (rtb-0b7a5bd5e29809f)
lab-subnet-public1-us-east-1a	subnet-03a14978a695bed93	10.0.0.0/24	-	rtb-0314a853bc743cb / lab-rtb-public
<input checked="" type="checkbox"/> lab-subnet-private2	subnet-0f6bb0d7150621ba0	10.0.3.0/24	-	Main (rtb-0b7a5bd5e29809f)
<input checked="" type="checkbox"/> lab-subnet-private1-us-east-1a	subnet-06034f7e46e488b68	10.0.10.0/24	-	rtb-005d39a268737f757 / lab-rtb-private1-us-east-1a

Selected subnets

subnet-06034f7e46e488b68 / lab-subnet-private1-us-east-1a X  subnet-0f6bb0d7150621ba0 / lab-subnet-private2 X

Save associations

Cancel **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**

### Edit subnet associations

Change which subnets are associated with this route table.

**Available subnets (2/4)**

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/> lab-subnet-public2	subnet-0ec116f65204e34b4	10.0.2.0/24	-	Main (rtb-0b7a5bd52e2980b9f)
<input checked="" type="checkbox"/> lab-subnet-public1-us-east-1a	subnet-03a14978a69bedd93	10.0.0.0/24	-	rtb-0314a853bca743c0b / lab-rtb-public
<input type="checkbox"/> lab-subnet-private2	subnet-0f6bb0d713d621be0	10.0.3.0/24	-	rtb-005d39a268737f757 / lab-rtb-private1-us-east...
<input type="checkbox"/> lab-subnet-private1-us-east-1a	subnet-06034f7e46e488b68	10.0.1.0/24	-	rtb-005d39a268737f757 / lab-rtb-private1-us-east...

**Selected subnets**

subnet-03a14978a69bedd93 / lab-subnet-public1-us-east-1a X    subnet-0ec116f65204e34b4 / lab-subnet-public2 X

**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**

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

**Basic details**

Security group name Info  
 Name cannot be edited after creation.

Description Info

VPC Info

**Inbound rules** Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>	Delete
HTTP	TCP	80	Anywhere... <input type="button" value="X"/> 0.0.0.0/0 <input type="button" value="X"/>	Permit web requests	<input type="button" value="Delete"/>

**Outbound rules** Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Destination <small>Info</small>	Description - optional <small>Info</small>	Delete
All traffic	All	All	Custom <input type="button" value="X"/> 0.0.0.0/0 <input type="button" value="X"/>		<input type="button" value="Delete"/>

**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.

No tags associated with the resource.

You can add up to 50 more tags

# 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

The screenshot shows the AWS Lambda console interface for creating a new function. At the top, there's a search bar and a 'Recent' dropdown. Below that, a 'Quick Start' section features logos for Amazon Linux, macOS, Ubuntu, Windows, and Red Hat, along with a search icon and a 'Browse more AMIs' link. A specific AMI entry for 'Amazon Linux 2023 AMI' is highlighted, showing its ID, architecture (x86\_64), boot mode (UEFI preferred), and AMI ID. A 'Free tier eligible' badge is present. To the right, there's a detailed description of the AMI, including its version (2023.0.20230322.0), architecture (x86\_64), and kernel (HVM). Below this, the 'Instance type' section shows 't2.micro' selected, with details about its performance, memory, and pricing. The 'Key pair (login)' section asks for a key pair name, with 'vockey' entered. On the far right, there are 'Cancel', 'Launch instance', and 'Review commands' buttons. A large callout box highlights the 'Free tier' information, stating it includes 750 hours of t2.micro usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GiB of snapshots, and 100 GB of bandwidth.

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 configi

- 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.

**Network settings** [Info](#)

**VPC - required** [Info](#)  
vpc-0f5d6132a9d2d6bff (lab-vpc)  
10.0.0.0/16

**Subnet info**  
subnet-0ec116f65204e34b4 lab-subnet-public2  
VPC: vpc-0f5d6132a9d2d6bff Owner: 636030802432 Availability Zone: us-east-1b  
IP addresses available: 251 CIDR: 10.0.2.0/24

**Create new subnet**

**Auto-assign public IP** [Info](#)  
Enable

**Firewall (security groups)** [Info](#)  
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group  Select existing security group

**Common security groups** [Info](#)  
Select security groups

Web Security Group sg-0c3a5704d4a2fa70d X  
VPC: vpc-0f5d6132a9d2d6bff

**Compare security group rules**

Security groups that you add or remove here will be added to or removed from all your network interfaces.

**Metadata response hop limit** [Info](#)  
Select

**Allow tags in metadata** [Info](#)  
Select

**User data - optional** [Info](#)  
Enter user data in the field.

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

Select Web Server 1.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Web Server 1	i-0527a31e01a9a2a3e	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b	ec2-18-233-102
Bastion Host	i-0ad4ff5008093f4ce	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-3-239-18-16

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

Instance: i-0527a31e01a9a2a3e (Web Server 1)

i-0527a31e01a9a2a3e (Web Server 1)	18.233.102.102   <a href="#">open address</a>	10.0.2.104
IPv6 address	Instance state	Public IPv4 DNS
-	Running	<a href="#">ec2-18-233-102-102.compute-1.amazonaws.com</a>   <a href="#">open address</a>
Hostname type	Private IP DNS name (IPv4 only)	Elastic IP addresses
IP name: ip-10-0-2-104.ec2.internal	<a href="#">ip-10-0-2-104.ec2.internal</a>	-
Answer private resource DNS name	Instance type	
-	t2.micro	

aws Load Test RDS

Meta-Data

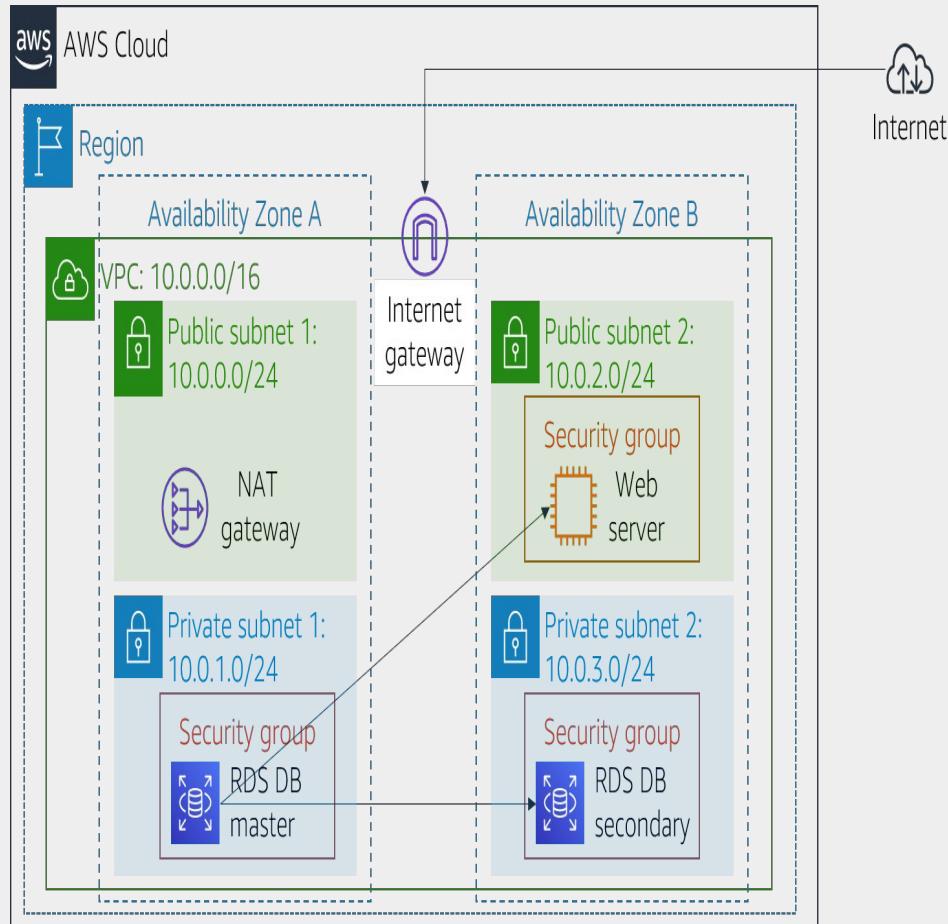
Value
InstanceId
Availability Zone

Current CPU Load: 100%

# 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.

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

**Basic details**

Security group name [Info](#)  
 Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)  
 [X](#)

**Inbound rules** [Info](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>	Delete
MySQL/Aurora	TCP	3306	Custom	<input type="text" value="sg-0635a4077fc40d5dc"/> <a href="#">X</a>	<a href="#">Delete</a>

[Add rule](#)

**Outbound rules** [Info](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Destination <a href="#">Info</a>	Description - optional <a href="#">Info</a>	Delete
All traffic	All	All	Custom	<input type="text" value="0.0.0.0"/> <a href="#">X</a>	<a href="#">Delete</a>

[Add rule](#)

**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.

No tags associated with the resource.

[Add new tag](#)  
You can add up to 50 more tags

# 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*

## Create DB subnet group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

### Subnet group details

#### Name

You won't be able to modify the name after your subnet group has been created.

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

#### Description

#### VPC

Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.



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

## Add subnets

### Availability Zones

Choose the Availability Zones that include the subnets you want to add.

Choose an availability zone

us-east-1a X

us-east-1b X

### Subnets

Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.

Select subnets

subnet-0e2e8eafc835c4454 (10.0.1.0/24) X

subnet-0adcc93d8c7b79d23 (10.0.3.0/24) X

### Subnets selected (2)

Availability zone	Subnet ID	CIDR block
us-east-1a	subnet-0e2e8eafc835c4454	10.0.1.0/24
us-east-1b	subnet-0adcc93d8c7b79d23	10.0.3.0/24

Cancel

Create

# Task 3: Create an Amazon RDS DB Instance

## Create database

### Choose a database creation method Info

#### Standard create

You set all of the configuration options, including ones for availability, security, backups, and maintenance.

#### Easy create

Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

### Engine options

#### Engine type Info

#### Aurora (MySQL Compatible)



#### Aurora (PostgreSQL Compatible)



#### MySQL



#### MariaDB



#### PostgreSQL



#### Oracle

ORACLE®

#### Microsoft SQL Server



Choose Databases.

Select MySQL.

## Multi-AZ DB instance

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

### DB instance identifier [Info](#)

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

lab-db

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

#### Master password [Info](#)

.....

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote), "(double quote) and @ (at sign).

#### Confirm master password [Info](#)

.....

#### Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.



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

Show instance classes that support Amazon RDS Optimized Writes

#### DB instance class [Info](#)

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

db.t3.micro

2 vCPUs 1 GiB RAM Network: 2,085 Mbps



Include previous generation classes

## Storage

### Storage type [Info](#)

**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 X

## 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.

## ▼ Additional configuration

Database options, encryption turned off, backup turned off, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned on.

### Database options

Initial database name [Info](#)

lab

If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group [Info](#)

default.mysql8.0



Option group [Info](#)

default:mysql-8-0



### Backup

**Enable automated backups**

Creates a point-in-time snapshot of your database

### Encryption

**Enable encryption**

Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. [Info](#)

# 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.

The screenshot shows a web-based configuration interface for connecting to an Amazon RDS database. At the top, there's a navigation bar with the AWS logo, 'Load Test', and 'RDS' tabs. Below the navigation, there are four input fields for database connection parameters:

Endpoint	lab-db.ccq8yvnjalpn.us-east-1.rds.amazonaws.com
Database	lab
Username	main
Password	.....

At the bottom of the form is a 'Submit' button.

# Address Book

Last name	First name	Phone	Email	Admin	
<a href="#">Add Contact</a>					
Doe	Jane	010-110-1101	<a href="#">janed@someotheraddress.org</a>	<a href="#">Edit</a>	<a href="#">Remove</a>
Johnson	Roberto	123-456-7890	<a href="#">robertoj@someaddress.com</a>	<a href="#">Edit</a>	<a href="#">Remove</a>

# Address Book

## Add Contact

Last Name:	Mathur
First Name:	Emy
Phone:	3458926731
Email:	<a href="mailto:emymathur@gmail.com">emymathur@gmail.com</a>
<input type="button" value="Submit"/>	

Last name	First name	Phone	Email	Admin	
<a href="#">Add Contact</a>					
Doe	Jane	010-110-1101	<a href="#">janed@someotheraddress.org</a>	<a href="#">Edit</a>	<a href="#">Remove</a>
Johnson	Roberto	123-456-7890	<a href="#">robertoj@someaddress.com</a>	<a href="#">Edit</a>	<a href="#">Remove</a>

# Address Book

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

# Address Book

Entry has been removed

Last name	First name	Phone	Email	Admin	
<a href="#">Add Contact</a>					
Johnson	Roberto	123-456-7890	robertoj@someaddress.com	<a href="#">Edit</a>	<a href="#">Remove</a>
Mathur	Emy	3458926731	emymathur@gmail.com	<a href="#">Edit</a>	<a href="#">Remove</a>

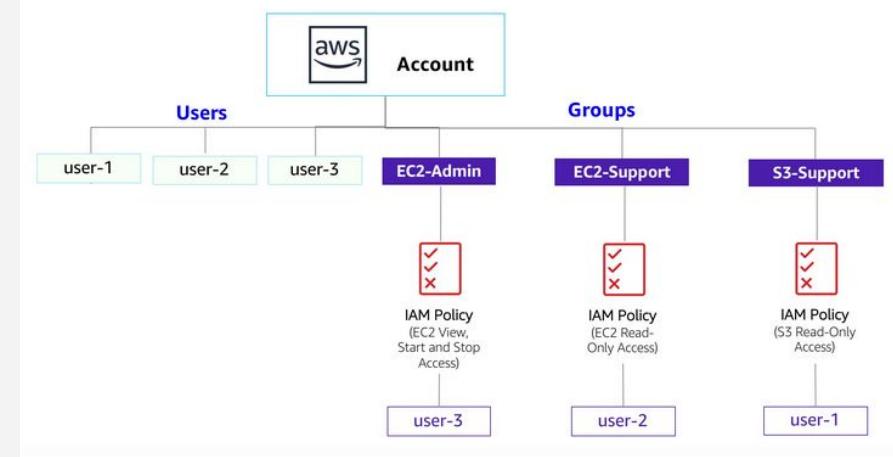
End the lab

# 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

User name	Groups	Last activity	MFA	Password age	Active key age
awsstudent	None	None	None	None	None
user-1	None	None	None	1 minute ago	Now
user-2	None	None	None	Now	Now
user-3	None	None	None	Now	Now

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**

Console sign-in	Manage console access
Console sign-in link <a href="https://572992334708.signin.aws.amazon.com/console">https://572992334708.signin.aws.amazon.com/console</a>	Console password Updated 2 minutes ago (2023-04-05 23:56 GMT+5:30) Last console sign-in Never

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

Group name	Users	Permissions	Creation time
EC2-Admin	>Loading	>Loading	3 minutes ago
EC2-Support	>Loading	>Loading	3 minutes ago
S3-Support	>Loading	>Loading	3 minutes ago

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.

EC2-Support		<a href="#">Delete</a>
Summary		
User group name	EC2-Support	Creation time
		April 03, 2023, 23:56 (UTC+05:30)
		ARN <a href="#">arn:aws:iam:572992334708:group/spl66/EC2-Support</a>
Users	Permissions	<a href="#">Edit</a>
Permissions policies (1) <a href="#">Info</a>		
You can attach up to 10 managed policies.		
<a href="#">Add permissions</a>		
<a href="#">Filter policies by property or policy name and press enter.</a>		
Policy name	Type	Description
AmazonEC2ReadOnlyAccess	AWS managed	Provides read only access to Amazon ...

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.

A screenshot of the AWS Management Console showing the inline policy 'AmazonEC2ReadOnlyAccess' for the 'EC2-Admin' user group. The policy details are displayed in a code editor-like interface. The policy grants read-only access to various AWS services including EC2, ELB, CloudWatch Metrics, and Auto Scaling. The JSON code is as follows:

```
1- [ {  
2-     "Version": "2012-10-17",  
3-     "Statement": [  
4-         {  
5-             "Effect": "Allow",  
6-             "Action": "ec2:Describe*",  
7-             "Resource": "*"  
8-         },  
9-         {  
10-            "Effect": "Allow",  
11-            "Action": "elasticloadbalancing:Describe*",  
12-            "Resource": "*"  
13-        },  
14-        {  
15-            "Effect": "Allow",  
16-            "Action": [  
17-                "cloudwatch:ListMetrics",  
18-                "cloudwatch:GetMetricStatistics",  
19-                "cloudwatch:Describe"  
20-            ],  
21-            "Resource": "*"  
22-        },  
23-        {  
24-            "Effect": "Allow",  
25-            "Action": "autoscaling:Describe*",  
26-            "Resource": "*"  
27-        }  
28-    ]  
29-}
```

A screenshot of the AWS Management Console showing the inline policy 'AmazonS3ReadOnlyAccess' for the 'S3-Support' user group. The policy details are displayed in a code editor-like interface. The policy grants read-only access to all buckets in Amazon S3. The JSON code is as follows:

```
1- [ {  
2-     "Version": "2012-10-17",  
3-     "Statement": [  
4-         {  
5-             "Effect": "Allow",  
6-             "Action": [  
7-                 "s3:Get*",  
8-                 "s3:List*",  
9-                 "s3:ObjectLambda:Get*",  
10-                 "s3:ObjectLambda:List"  
11-             ],  
12-             "Resource": "*"  
13-         }  
14-     ]  
15-}
```

## 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.

<input type="checkbox"/>	Group name	Users	Permissions
<input type="checkbox"/>	EC2-Admin	1	<span>Defined</span>
<input type="checkbox"/>	EC2-Support	1	<span>Defined</span>
<input type="checkbox"/>	S3-Support	1	<span>Defined</span>

S3-Support

Summary

User group name: S3-Support

Creation time: April 03, 2023, 23:56 (UTC+05:30)

ARN: arn:aws:iam:572992334708:group/spl66/S3-Support

Users Permissions Access Advisor

Users in this group (0)  
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search User name Groups Last activity Creation time

No resources to display

EC2-Support

User group name: EC2-Support

EC2-Admin

User group name: EC2-Admin

Users Permissions Access Advisor

Users in this group (1)  
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search User name Groups Last activity Creation time

No resources to display

Users in this group (1)  
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search User name Groups Last activity Creation time

No resources to display

Users in this group (1)  
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search User name Groups Last activity Creation time

No resources to display

### 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](https://123456789012signin)

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.

The screenshot shows the AWS S3 Buckets page. At the top, there's an 'Account snapshot' section with a 'Storage lens provides visibility into storage usage and activity trends' link. Below it is a search bar labeled 'Find buckets by name'. A table lists one bucket:

Name	AWS Region	Access	Creation date
samplebucket--002a2470	US East (N. Virginia) us-east-1	Objects can be public	April 3, 2023, 23:56:13 (UTC+05:30)

Actions available include 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'.

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**

The screenshot shows the AWS Management Console navigation bar with 'Sydney' selected and 'user-1 @ 5729-9233-4708' signed in. A message box says: 'Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more'.

The main content area displays a grid of EC2 resources with API error icons:

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

The screenshot shows the AWS Management Console navigation bar with 'Sydney' selected and 'user-1 @ 5729-9233-4708' signed in. The sidebar includes links for Account, Organization, Service Quotas, Billing Dashboard, Security credentials, and Settings. At the bottom are 'Switch role' and 'Sign out' buttons.

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.

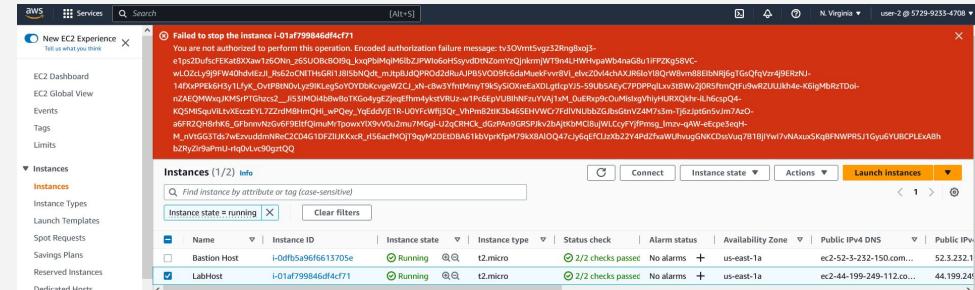
If you cannot see an Amazon EC2 instance, then your Region may be incorrect. In the top-right of the screen, pull-down the Region menu and select the region that you noted at the start of the lab (for example, **N. Virginia**).

- Select the instance named *LabHost*.

In the **Instance state** menu above, select **Stop instance**.

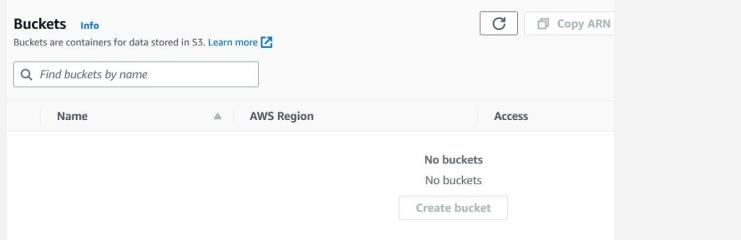
In the **Stop Instance** window, select **Stop**.

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.



The screenshot shows the AWS S3 Buckets page. At the top, there are buttons for 'Buckets' (selected), 'Info', and 'Copy ARN'. Below that, a note says 'Buckets are containers for data stored in S3. Learn more'. A search bar contains the placeholder 'Find buckets by name'. A table header includes columns for 'Name', 'AWS Region', and 'Access'. The main content area displays a message: 'No buckets' and 'No buckets'. At the bottom right is a 'Create bucket' button.

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* .

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
Bastion Host	i-0dfb5a96f6613705e	Running	t2.micro	2/2 checks passed	User: arnaws!	us-east-1a	ec2-52-3-232-150.com...	52.3.232.1
<input checked="" type="checkbox"/> LabHost	i-01af799846df4cf71	Running	t2.micro	2/2 checks passed	User: arnaws!	us-east-1a	ec2-44-199-249-112.co...	44.199.249.112

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**

Name	Instance ID	Instance state	Instance type
Bastion Host	i-0dfb5a96f6613705e	Running	t2.micro
<input type="checkbox"/> LabHost	i-01af799846df4cf71	Stopping	t2.micro

# 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.

The screenshot shows the AWS Management Console interface for the EC2 service. The top navigation bar includes links for 'Instances (1/2)', 'Info', 'Connect', 'Instance state', 'Actions', and a prominent orange 'Launch instances' button. Below the navigation is a search bar labeled 'Find instance by attribute or tag (case-sensitive)'. The main content area displays a table of running instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input checked="" type="checkbox"/> Lab	i-088b51e0e5d8aa23c	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	No alarms	+ us-east-1a	ec2-35-
<input type="checkbox"/> Bastion Host	i-07b18229364455229	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	No alarms	+ us-east-1a	ec2-35-

Below the table, a modal window is open for the instance 'Lab'. The title bar says 'Instance: i-088b51e0e5d8aa23c (Lab)'. The 'Details' tab is selected, showing the following information:

Instance summary		
Instance ID i-088b51e0e5d8aa23c (Lab)	Public IPv4 address 35.170.68.178   <a href="#">open address</a>	Private IPv4 addresses 10.1.11.185
IPv6 address -	Instance state <span>Running</span>	Public IPv4 DNS ec2-35-170-68-178.compute-1.amazonaws.com   <a href="#">open address</a>

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:

- o **Volume Type:** General Purpose SSD (*gp2*)
- o **Size (GiB):** 1. **NOTE:** You may be restricted from creating large volumes.
- o **Availability Zone:** Select the same availability zone as your EC2 instance.
- o Choose **Add Tag**
- o 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

&lt; 1 &gt;



Search

<input type="checkbox"/>	Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot		C
<input type="checkbox"/>	-	vol-0a353e3dcee302bc4	gp2	8 GiB	100	-	snap-016944d...	2023-07-10 10:45:00	
<input type="checkbox"/>	-	vol-0fb37207138adbf1f	gp2	8 GiB	100	-	snap-016944d...	2023-07-10 10:45:00	



## 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**.

The screenshot shows the AWS EC2 Volumes page. On the left, there's a sidebar with various EC2-related options like EC2 Dashboard, Global View, Events, Tags, Limits, Instances, and several instance-specific sections. The 'Instances' section is expanded, showing sub-options like Instances, Instance Types, Launch Templates, etc. In the main content area, a table lists three volumes. The third volume, named 'My Volume' with Volume ID 'vol-05bc51a57fe5baf99', has a blue checkmark next to it. To the right of the table is an 'Actions' menu with several options: Modify volume, Create snapshot, Create snapshot lifecycle policy, Delete volume, **Attach volume** (which is highlighted with a blue box), Detach volume, Force detach volume, Manage auto-enabled I/O, Manage tags, and Fault injection.

Name	Volume ID	Type	Size	IOPS
-	vol-0a353e3dcee302bc4	gp2	8 GiB	100
-	vol-0fb37207138adb1f	gp2	8 GiB	100
<input checked="" type="checkbox"/> My Volume	vol-05bc51a57fe5baf99	gp2	1 GiB	100

Volume ID: vol-05bc51a57fe5baf99 (My 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**

## 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

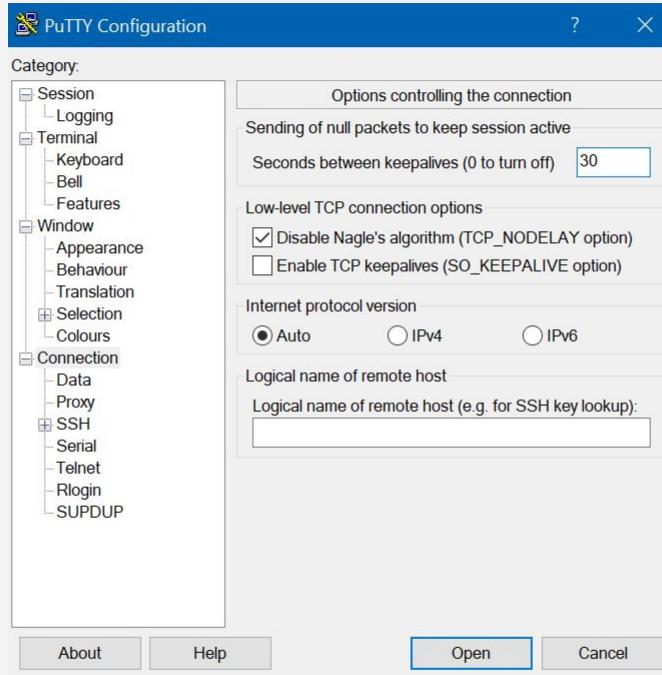
AWS SSO

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:
  - o Choose **Session**
  - o **Host Name (or IP address):** Paste the *Public DNS or IPv4 address* of the Lab instance that you noted earlier.
  - o Back in PuTTY, in the **Connection** list, expand **SSH**
  - o Choose **Auth** and expand **Credentials**
  - o Under **Private key file for authentication:** Choose **Browse**
  - o Browse to the *labsuser.ppk* file that you downloaded, select it, and choose **Open**
  - o 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

?

X

### 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)

35.170.68.178

Port

22

Connection type:

SSH

Serial

Other:

Telnet



Load, save or delete a stored session

Saved Sessions

Load

Save

Delete

Default Settings

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
    - Runas

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

### 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

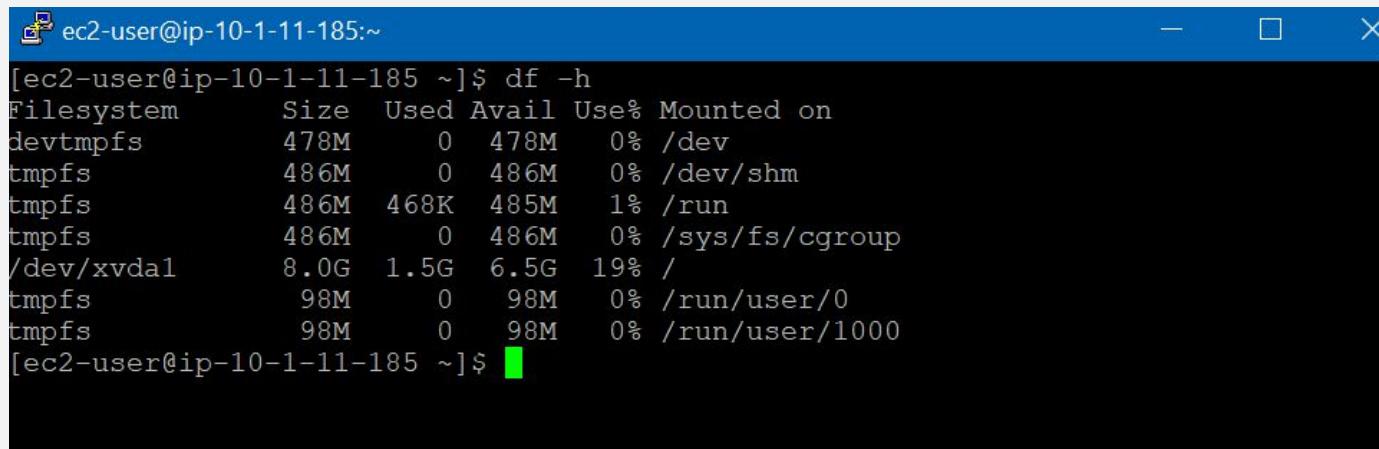
Cancel

# 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`

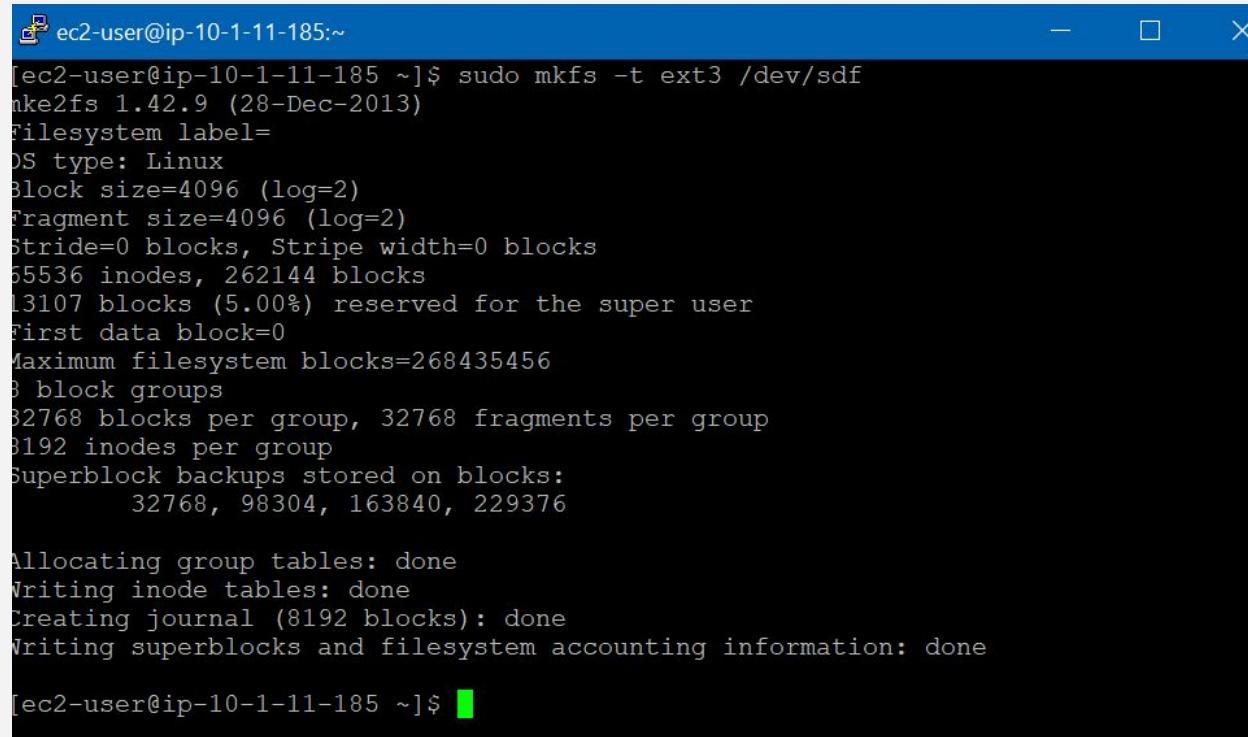


The screenshot shows a terminal window with a blue header bar containing a cloud icon, the text "ec2-user@ip-10-1-11-185:~", and standard window control buttons (minimize, maximize, close). The main area of the terminal displays the output of the "df -h" command, which lists the current disk usage across various file systems. The output is as follows:

```
[ec2-user@ip-10-1-11-185 ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        478M    0  478M   0% /dev
tmpfs          486M    0  486M   0% /dev/shm
tmpfs          486M  468K  485M   1% /run
tmpfs          486M    0  486M   0% /sys/fs/cgroup
/dev/xvda1     8.0G  1.5G  6.5G  19% /
tmpfs          98M    0   98M   0% /run/user/0
tmpfs          98M    0   98M   0% /run/user/1000
[ec2-user@ip-10-1-11-185 ~]$ █
```

Create an ext3 file system on the new volume:

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



```
[ec2-user@ip-10-1-11-185 ~]$ sudo mkfs -t ext3 /dev/sdf
[ec2-user@ip-10-1-11-185 ~]$ mkfs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
65536 inodes, 262144 blocks
13107 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=268435456
3 block groups
32768 blocks per group, 32768 fragments per group
3192 inodes per group
Superblock backups stored on blocks:
      32768, 98304, 163840, 229376

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

[ec2-user@ip-10-1-11-185 ~]$
```

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
```



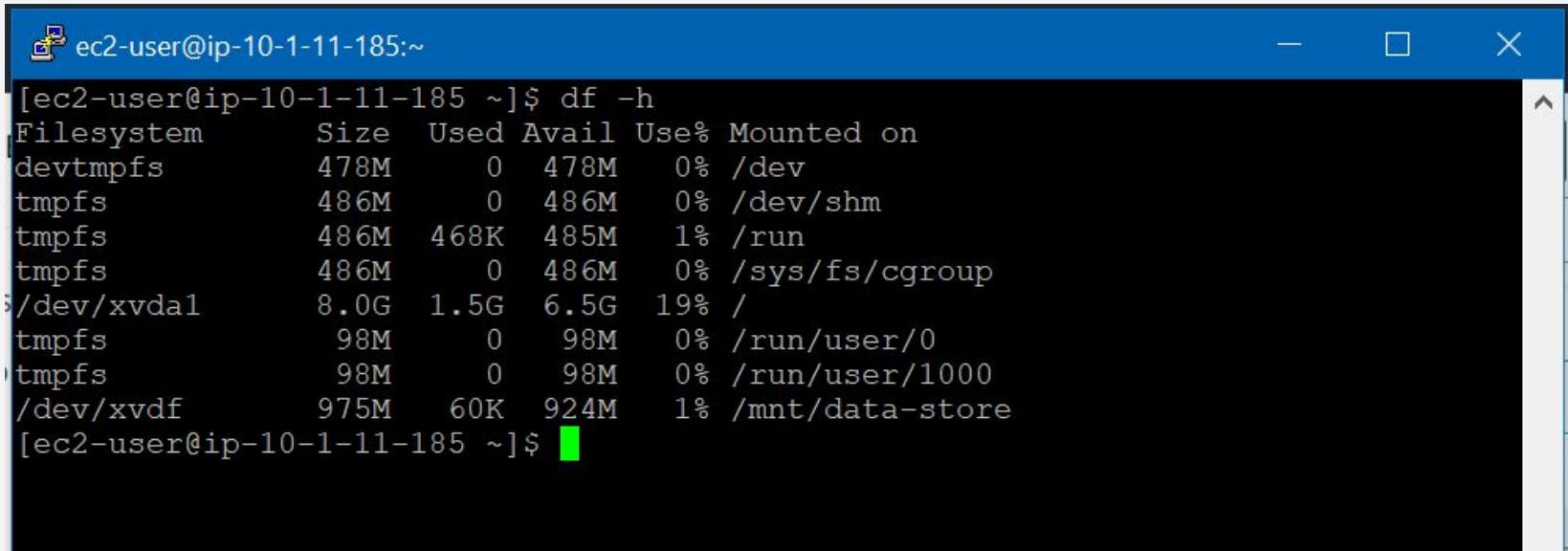
ec2-user@ip-10-1-11-185:~



```
[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,noatime 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
```



The screenshot shows a terminal window with a blue header bar. The title bar contains the text "ec2-user@ip-10-1-11-185:~". The main area of the terminal displays the output of the "df -h" command, which lists the file systems and their usage statistics. The output is as follows:

Filesystem	Size	Used	Avail	Use%	Mounted on
devtmpfs	478M	0	478M	0%	/dev
tmpfs	486M	0	486M	0%	/dev/shm
tmpfs	486M	468K	485M	1%	/run
tmpfs	486M	0	486M	0%	/sys/fs/cgroup
/dev/xvda1	8.0G	1.5G	6.5G	19%	/
tmpfs	98M	0	98M	0%	/run/user/0
tmpfs	98M	0	98M	0%	/run/user/1000
/dev/xvdf	975M	60K	924M	1%	/mnt/data-store

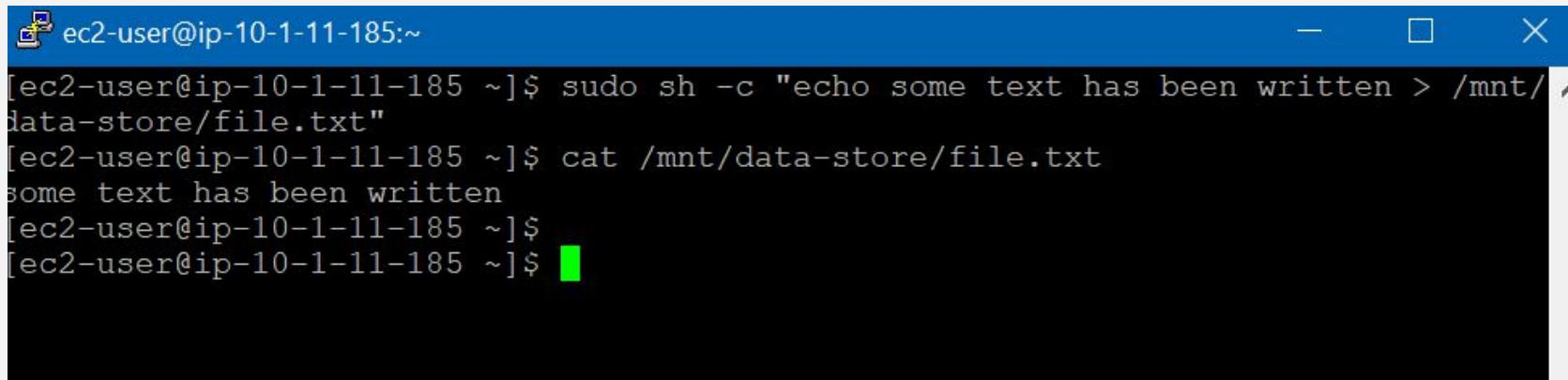
The terminal prompt "[ec2-user@ip-10-1-11-185 ~]\$ " is visible at the bottom of the window.

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
```



The screenshot shows a terminal window with a blue header bar. The header displays the user name 'ec2-user' and the IP address 'ip-10-1-11-185'. The main window contains a black background with white text. It shows the following sequence of commands and their output:

```
[ec2-user@ip-10-1-11-185 ~]$ sudo sh -c "echo some text has been written > /mnt/data-store/file.txt"
[ec2-user@ip-10-1-11-185 ~]$ cat /mnt/data-store/file.txt
some text has been written
[ec2-user@ip-10-1-11-185 ~]$
```

A green vertical bar is visible on the right side of the terminal window, indicating where the cursor is located.

# 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	Value - optional
<input type="text"/> Name	<input type="text"/> My Snapshot <a href="#">Use "My Snapshot"</a>

You can add 49 more tags.

[Cancel](#) [Create snapshot](#)

## Snapshots (1)

Owned by me ▾		Search			Recycle Bin	Actions ▾	<a href="#" style="background-color: orange; color: white; border-radius: 5px; padding: 2px 10px;">Create snapshot</a>	< 1 >			
<input type="checkbox"/>	Name		Snapshot ID		Size		Description		Storage...	Snapshot status	
<input type="checkbox"/>	My Snapshot		<a href="#">snap-0f43c0a21c97ba2fe</a>		1 GiB		-		Standard		Pending

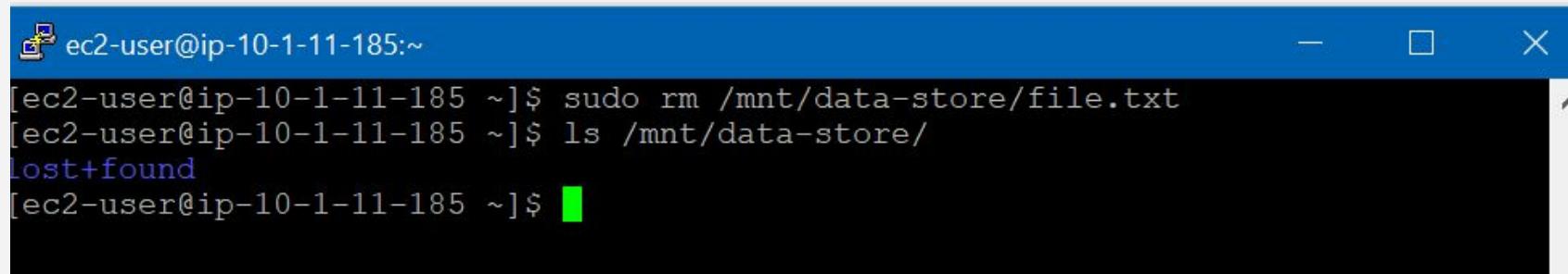
In your remote SSH session, delete the file that you created on your volume.

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

Verify that the file has been deleted.

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

Your file has been deleted.



The screenshot shows a terminal window with a blue header bar. The header bar contains a small icon, the text "ec2-user@ip-10-1-11-185:~" on the left, and standard window control buttons (minimize, maximize, close) on the right. The main window is black and displays the following text:

```
[ec2-user@ip-10-1-11-185 ~]$ sudo rm /mnt/data-store/file.txt
[ec2-user@ip-10-1-11-185 ~]$ ls /mnt/data-store/
lost+found
[ec2-user@ip-10-1-11-185 ~]$ █
```

# 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**

## 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

Name

#### Value - optional

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*.

## 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
```

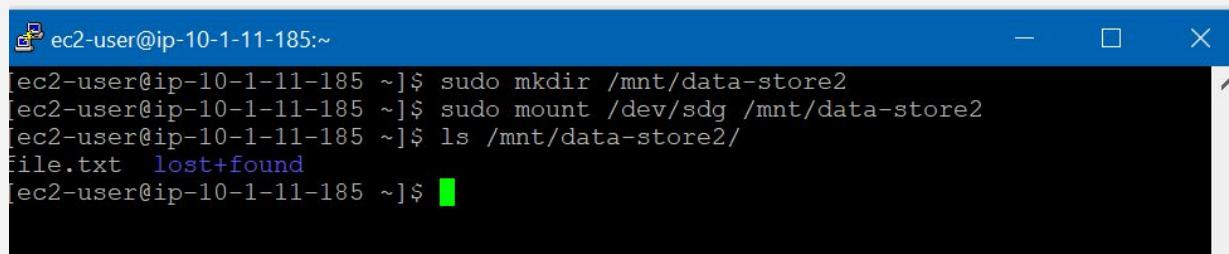
Mount the new volume:

```
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.



```
ec2-user@ip-10-1-11-185:~$ sudo mkdir /mnt/data-store2
ec2-user@ip-10-1-11-185:~$ sudo mount /dev/sdg /mnt/data-store2
ec2-user@ip-10-1-11-185:~$ ls /mnt/data-store2/
file.txt  lost+found
ec2-user@ip-10-1-11-185:~$
```

# **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 X

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	
<input checked="" type="checkbox"/>	Web Server 1	i-01342cddd894abc9b	Running	t2.micro	
<input type="checkbox"/>	Bastion Host	i-004c7e138275dd74e	Running	t2.micro	

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

-

### 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.

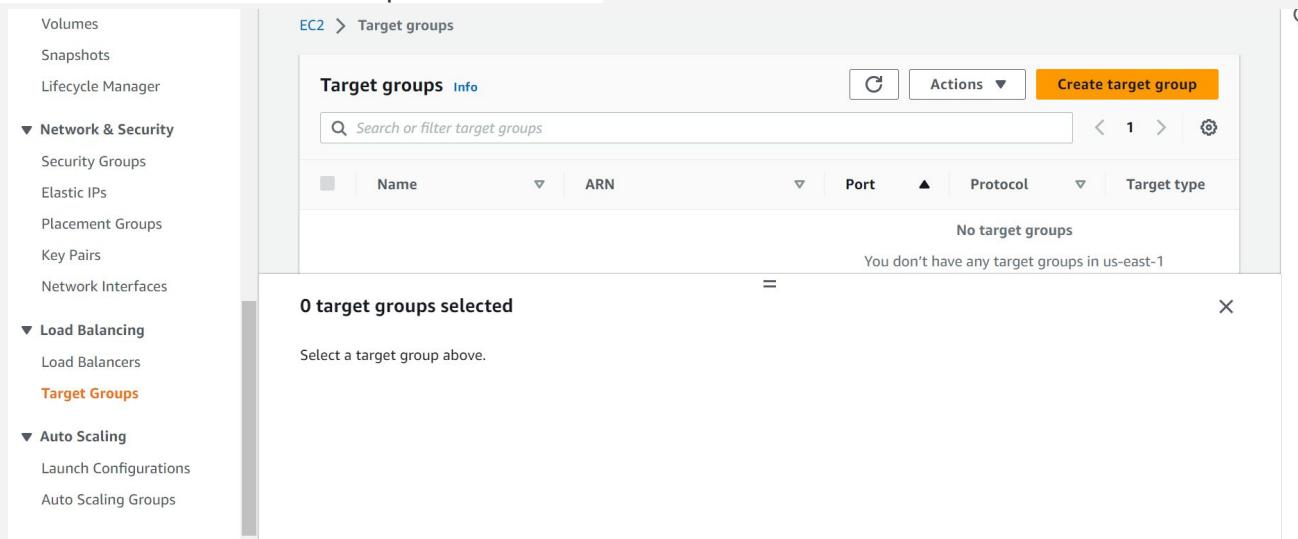
Cancel

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.



Step 1  
Specify group detailsStep 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 address/SGS

- 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 multi-interface-based architectures, simplifying inter-communication communications.
- Supports IPv4 endpoints, enabling end-to-end IPv6 communications, and (IPv4-to-IPv6 NAT).

 Lambda function

- Permits 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

## Port

HTTP

80

## VPC

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

Lab VPC

Subnet: subnet-000000000000000000

IP v4: 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. Note: 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.

/

100 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		
<p><b>Application Load Balancer</b> <a href="#">Info</a></p> <p>The Application Load Balancer (ALB) is designed for flexible feature sets for applications with HTTP and HTTPS traffic. It operates at the request level, providing advanced routing and visibility features for microservices and containers.</p> <p><a href="#">Create</a></p>	<p><b>Network Load Balancer</b> <a href="#">Info</a></p> <p>The Network Load Balancer (NLB) is ideal for ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses. It operates at the connection level, handling millions of requests per second securely.</p> <p><a href="#">Create</a></p>	<p><b>Gateway Load Balancer</b> <a href="#">Info</a></p> <p>The Gateway Load Balancer (GWLB) is for deploying and managing a fleet of third-party virtual appliances that support GENEVE. These appliances enable improved security, compliance, and policy controls.</p> <p><a href="#">Create</a></p>
<p>▶ <a href="#">Classic Load Balancer - previous generation</a></p>		

[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**

## Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine 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.

The screenshot shows the AWS Create Application Load Balancer configuration interface. At the top, there's a navigation bar with 'aws' logo, 'Services' dropdown, and a search bar. Below the navigation is a 'VPC' section with a 'Info' link and a note about selecting a VPC. A dropdown menu shows 'Lab VPC' with ID 'vpc-0b780fdec4a9f57a9' and IPv4 range '10.0.0.0/16'. The main configuration area has several sections:

- Mappings**: Shows two mappings: 'us-east-1a (use1-az4)' and 'us-east-1b (use1-az6)'. Each mapping includes a 'Subnet' dropdown (containing 'subnet-05407af50342c9cb8' and 'subnet-08ad3743e3879cb6b' respectively), an 'IPv4 settings' section ('Assigned by AWS'), and a 'Security groups' section ('Select up to 5 security groups').
- Security groups**: A note says 'A security group is a set of firewall rules that control the traffic to your load balancer.' Below is a 'Security groups' dropdown with the placeholder 'Select up to 5 security groups'.
- CloudShell**, **Feedback**, and **Language** buttons are at the bottom right.

# 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:
  - o **Launch configuration name:** `LabConfig`
  - o **Amazon Machine Image (AMI)** Choose *Web Server AMI*
  - o **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.

- o Choose **Select an existing security group**
- o 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**

## 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 [\[2\]](#)

[Create launch template](#)

### Launch configuration name

#### Name

### Amazon machine image (AMI) Info

#### AMI

### Instance type Info

#### Instance type

[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

<input type="checkbox"/> Volume type	Devices	Snapshot	Size (GiB)	Volume type
<input type="checkbox"/>	/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:  
o **Name:** Lab Auto Scaling Group
25. Choose **Next**
26. On the **Network** page configure  
o **Network:** Lab VPC  
You can ignore the message regarding "No public IP address"  
o **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:  
o **Desired capacity:** 2  
o **Minimum capacity:** 2  
o **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:  
o **Lab policy name:** LabScalingPolicy  
o **Metric type:** Average CPU Utilization  
o **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:  
o **Key:** Name  
o **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.

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](#)[X](#)< 1 >

<input checked="" type="checkbox"/> Security group ID	Name	VPC ID	Description
<input checked="" type="checkbox"/> 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



Existing key pair



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

[Cancel](#)[Create launch configuration](#)