



Amity School of Engineering and Technology (ASET)

Cloud Computing Practitioner [CSE314]

Practical Lab File

Name Dhruv Rastogi
Class 5CSE 10Y
Roll No A2372019006
Batch 2019 - 2023
Faculty Ms. Dolly Sharma

CONTENTS

S. No	Name of Experiment	Signature
01	Introduction to Amazon EC2	
02	Build your VPC and Launch a Web Server	
03	Working with EBS	
04	Build Your DB Server and Interact With Your DB Using an App	
05	Scale and Load Balance Your Architecture	
06	Introduction to AWS IAM	
07	Activity 1: AWS Lambda	
08	Activity 2: AWS Elastic Beanstalk	
09	Activity 3: Explore the sandbox environment	

Practical 1

AIM

Introduction to Amazon EC2

THEORY

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.

Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change.

Amazon EC2 changes the economics of computing by allowing you to pay only for capacity that you actually use. Amazon EC2 provides developers the tools to build failure resilient applications and isolate themselves from common failure scenarios.

By the end of this lab, you will be able to:

- 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

PROCEDURE

Task 1: Launch Your Amazon EC2 Instance

In this task, you will launch an Amazon EC2 instance with *termination protection*. Termination protection prevents you from accidentally terminating an EC2 instance. You will deploy your instance with a User Data script that will allow you to deploy a simple web server.

5. In the **AWS Management Console** on the **Services** menu, click **EC2**.
6. Choose **Launch Instance**, then select **Launch Instance**

Step 1: Choose an Amazon Machine Image (AMI)

An **Amazon Machine Image (AMI)** provides the information required to launch an instance, which is a virtual server in the cloud. An AMI includes:

- A template for the root volume for the instance (for example, an operating system or an application server with applications)

- Launch permissions that control which AWS accounts can use the AMI to launch instances
- A block device mapping that specifies the volumes to attach to the instance when it is launched

The **Quick Start** list contains the most commonly-used AMIs. You can also create your own AMI or select an AMI from the AWS Marketplace, an online store where you can sell or buy software that runs on AWS.

7. Click **Select** next to **Amazon Linux 2 AMI** (at the top of the list).

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Search for an AMI by entering a search term e.g. "Windows"

Quick Start

My AMIs	AWS Marketplace	Community AMIs	Free tier only
			<input type="checkbox"/> Free tier only ⓘ

Amazon Linux 2 AMI (HVM, SSD Volume Type) - ami-0c2b8ca1dad447f8a (64-bit x86) / ami-06cf15d6d096df5d2 (64-bit Arm)

Select

Amazon Linux Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

macOS Big Sur 11.4 - ami-059ff882c04ebcd21

The macOS Big Sur AMI is an EBS-backed, AWS-supported image. This AMI includes the AWS Command Line Interface, Command Line Tools for Xcode, Amazon SSM Agent, and Homebrew. The AWS Homebrew Tap includes the latest versions of multiple AWS packages included in the AMI.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

macOS Catalina 10.15.7 - ami-093900cc07f14a8f7

The macOS Catalina AMI is an EBS-backed, AWS-supported image. This AMI includes the AWS Command Line Interface, Command Line Tools for Xcode, Amazon SSM Agent, and Homebrew. The AWS Homebrew Tap includes the latest versions of multiple AWS packages included in the AMI.

Select

64-bit (Mac)

Step 2: Choose an Instance Type

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.

You will use a **t2.micro** instance which should be selected by default. This instance type has 1 virtual CPU and 1 GiB of memory. **NOTE:** You may be restricted from using other instance types in this lab.

8. Click **Next: Configure Instance Details**

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance families Current generation ShowHide Columns

Family	CPU Credits	RAM (GB)	EBS-Optimized Available	Network Performance	IPv6 Support		
t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

Step 3: Configure Instance Details

This page is used to configure the instance to suit your requirements. This includes networking and monitoring settings.

The **Network** indicates which Virtual Private Cloud (VPC) you wish to launch the instance into. You can have multiple networks, such as different ones for development, testing and production.

9. For Network, 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.

10. For Enable termination protection, select Protect against accidental termination.

When an Amazon EC2 instance is no longer required, it can be *terminated*, which means that the instance is stopped and its resources are released. A terminated instance cannot be started again. If you want to prevent the instance from being accidentally terminated, you can enable *termination protection* for the instance, which prevents it from being terminated.

11. Scroll down, then expand Advanced Details.

A field for **User data** will appear.

When you launch an instance, you can pass *user data* to the instance that can be used to perform common automated configuration tasks and even run scripts after the instance starts.

Your instance is running Amazon Linux, so you will provide a *shell script* that will run when the instance starts.

12. Copy the following commands and paste them into the User data field:

13. #!/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
```

14. The script will:

- Install an Apache web server (httpd)
- Configure the web server to automatically start on boot
- Activate the Web server
- Create a simple web page

13. Click **Next: Add Storage**

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	<input type="text" value="1"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-085206476ff6fee8b Lab VPC <input type="button" value="Create new VPC"/>	
Subnet	subnet-024be4c2f95dca2d4 Public Subnet 1 us-east-1 251 IP Addresses available	<input type="button" value="Create new subnet"/>
Auto-assign Public IP	<input type="button" value="Use subnet setting (Enable)"/>	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	<input type="button" value="Open"/>	
Domain join directory	<input type="button" value="No directory"/> <input type="button" value="Create new directory"/>	
IAM role	<input type="button" value="None"/> <input type="button" value="Create new IAM role"/>	
Shutdown behavior	<input type="button" value="Stop"/>	
Stop - Hibernate behavior	<input type="checkbox"/> Enable hibernation as an additional stop behavior	
Enable termination protection	<input checked="" type="checkbox"/> Protect against accidental termination	

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

Step 3: Configure Instance Details

Enable termination protection	<input checked="" type="checkbox"/> Protect against accidental termination
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring <small>Additional charges apply.</small>
Tenancy	Shared - Run a shared hardware instance <small>Additional charges will apply for dedicated tenancy.</small>
Elastic Inference	<input type="checkbox"/> Add an Elastic Inference accelerator <small>Additional charges apply.</small>
Credit specification	<input type="checkbox"/> Unlimited <small>Additional charges may apply</small>
File systems	<input type="button" value="Add file system"/> <input type="button" value="Create new file system"/>

▼ Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-024be4c2f95dca2d4	Auto-assign	Add IP	The selected subnet does not support IPv6 because it does not have an IPv6 CIDR.

[Add Device](#)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

Step 3: Configure Instance Details

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-024be4c2	Auto-assign	Add IP	The selected subnet does not support IPv6 because it does not have an IPv6 CIDR.

Advanced Details

Enclave: Enable

Metadata accessible: Enabled

Metadata version: V1 and V2 (token optional)

Metadata token response hop limit: 1

User data:

```
#!/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
```

Buttons: Cancel, Previous, Review and Launch, Next: Add Storage

Step 4: Add Storage

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).

14. Click **Next: Add Tags**

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-090e9376979c86d7b	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Note: Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Buttons: Cancel, Previous, Review and Launch, Next: Add Tags

Step 5: Add Tags

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you have assigned to it. Each tag consists of a Key and a Value, both of which you define.

15. Click **Add Tag** then configure:

- **Key:** Name
- **Value:** Web Server

16. Click **Next: Configure Security Group**

The screenshot shows the AWS Step 5: Add Tags configuration page. At the top, there's a navigation bar with the AWS logo, Services dropdown, search bar, user info (voclabs/user1542351=omeirf02@gmail.com @ 5842-7048-1537), region (N. Virginia), and Support link. Below the navigation, a breadcrumb trail shows steps 1 through 7. The current step, 5. Add Tags, is highlighted. The main content area is titled "Step 5: Add Tags". It contains instructions about what a tag is and how it can be applied. A table allows adding a tag with a key and value, and checkboxes for associating the tag with Instances, Volumes, and Network Interfaces. One tag is currently listed: "Name" with "Web Server" as the value, checked for all three categories. At the bottom, there are "Cancel", "Previous", "Review and Launch" (which is blue and underlined, indicating it's the next step), and "Next: Configure Security Group" buttons. The footer includes links for Feedback, English (US), Privacy Policy, Terms of Use, and Cookie preferences.

Step 6: Configure Security Group

A **security group** acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add *rules* to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group.

17. On **Step 6: Configure Security Group**, configure:

- **Security group name:** Web Server security group
- **Description:** Security group for my web server

18. In this lab, you will not log into your instance using SSH. Removing SSH access will improve the security of the instance.

19. Delete the existing SSH rule.

20. Click **Review and Launch**

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group:

Create a new security group
 Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
This security group has no rules				

Add Rule

Warning
You will not be able to connect to this instance as the AMI requires port(s) 22 to be open in order to have access. Your current security group doesn't have port(s) 22 open.

Cancel Previous **Review and Launch**

Step 7: Review Instance Launch

The Review page displays the configuration for the instance you are about to launch.

20. Click **Launch**

A **Select an existing key pair or create a new key pair** window will appear.

Amazon EC2 uses public–key cryptography to encrypt and decrypt login information. To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance.

In this lab you will not log into your instance, so you do not require a key pair.

21. Click the **Choose an existing key pair** drop-down and select *Proceed without a key pair*.

22. Select **I acknowledge that**

23. Click **Launch Instances**

Your instance will now be launched.

24. Click **View Instances**

The instance will appear in a *pending* state, which means it is being launched. It will then change to *running*, which indicates that the instance has started booting. There will be a short time before you can access the instance.

The instance receives a *public DNS name* that you can use to contact the instance from the Internet.

Your **Web Server** should be selected. The **Description** tab displays detailed information about your instance.

To view more information in the Description tab, drag the window divider upwards.

Review the information displayed in the **Description** tab. It includes information about the instance type, security settings and network settings.

25. Wait for your instance to display the following:

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

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

This screenshot shows the 'Step 7: Review Instance Launch' page. At the top, there are tabs for 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. The 7. Review tab is highlighted. Below the tabs, there's a section titled 'Step 7: Review Instance Launch' with the sub-instruction: 'Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.' There are three expandable sections: 'AMI Details', 'Instance Type', and 'Security Groups'. The 'AMI Details' section shows an 'Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0c2b8ca1dad447f8a' with a note that it's a 'Free tier eligible' item. The 'Instance Type' section lists an 'i2.micro' instance type with 1 vCPU, 1 GiB memory, EBS only storage, and low-to-moderate network performance. The 'Security Groups' section shows a single security group named 'Web Server security group' which is described as a 'Security group for my web server'. It lists rules for this group. At the bottom right, there are 'Cancel', 'Previous', and a large blue 'Launch' button.

This screenshot shows the same 'Step 7: Review Instance Launch' page, but with a modal dialog box open over the main content. The dialog is titled 'Select an existing key pair or create a new key pair'. It contains instructions about what a key pair is and notes that the selected key pair will be added to the set of keys authorized for the instance. It also mentions that for Windows AMIs, the private key file is required to obtain the password used to log into the instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Below this text, there's a dropdown menu set to 'Proceed without a key pair', a checkbox for acknowledging the connection via EC2 Instance Connect, and a note that EC2 Instance Connect is only supported on Amazon Linux 2 and Ubuntu. At the bottom of the dialog are 'Cancel' and 'Launch Instances' buttons. The background of the main page shows the same instance configuration details as the previous screenshot, including the security group and launch buttons.

Launch Status

 Your instances are now launching
The following instance launches have been initiated: i-03d25e8a53d79490b [View launch log](#)

 Get notified of estimated charges
[Create billing alerts](#) to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances
Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.
Click [View Instances](#) to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out](#) how to connect to your instances.

▼ Here are some helpful resources to get you started

- [How to connect to your Linux instance](#)
- [Amazon EC2: User Guide](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: Discussion Forum](#)

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes (Additional charges may apply)
- Manage security groups

[View Instances](#)

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.

26. Click 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.

https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Web Server	i-001add7f70ddc985	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b	ec2-3-238-164-1
Bastion Host	i-0f645e372f44c46b2	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-18-232-114-

Instance: i-001add7f70ddc985 (Web Server)

[Details](#) [Security](#) [Networking](#) [Storage](#) [Status checks](#) [Monitoring](#) [Tags](#)

Status checks [Info](#)
Status checks detect problems that may impair i-001add7f70ddc985 (Web Server) from running your applications.

System status checks  **System 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](#)

Instance status checks  **Instance reachability check passed**

27. Click 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 click on a graph to see an expanded view.

Amazon EC2 sends metrics to Amazon CloudWatch for your EC2 instances. Basic (five-minute) monitoring is enabled by default. You can enable detailed (one-minute) monitoring.

The screenshot shows the AWS CloudWatch Metrics interface. At the top, there's a search bar and a navigation bar with tabs for 'Instances (1/2)', 'Info', 'Actions', and 'Launch instances'. Below this is a table of instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Web Server	i-001add7f70ddc985	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b	ec2-3-238-164-1
Bastion Host	i-0f645e372f44c46b2	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-18-232-114-

Below the table, a specific instance is selected: 'Web Server' (i-001add7f70ddc985). A detailed monitoring tab is open, showing three metrics graphs: CPU utilization (%), Status check failed (any), and Status check failed (instance). The CPU utilization graph shows a single data series for the Web Server instance, with values around 1.22% at 10:15 and 0.611% at 10:20. The status check failed graphs show no data available for all three categories.

28. In the **Actions** menu, 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.

The screenshot shows the AWS Cloud Computing Practical File interface. On the left, the navigation pane includes 'New EC2 Experience', 'EC2 Dashboard', 'Events', 'Tags', 'Limits', 'Instances' (selected), 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', 'Scheduled Instances', 'Capacity Reservations', 'Images' (AMIs), and 'Elastic Block Store' (Volumes, Snapshots). The main content area shows 'Instances (1/2) Info' with two entries: 'Web Server' (i-001add7f70ddc985, Running, t2.micro, 2/2 checks passed, No alarm) and 'Bastion Host' (i-0f645e372f44c46b2, Running, t2.micro, 2/2 checks passed, No alarm). A context menu is open for the Web Server instance, listing 'Get system log', 'Get instance screenshot', 'Manage detailed monitoring', 'Manage CloudWatch alarms', 'EC2 Serial Console', and 'Replace root volume'. Below the instances are four small charts: 'CPU utilization (%)' (Percent: 1.22, 0.611), 'Status check failed (any) (co...' (1, 0.5), 'Status check failed (instanc...) (1, 0.5), and 'Status check failed (system...) (1, 0.5). The bottom of the screen shows the Windows taskbar with various pinned icons and the date/time as 06-08-2021 04:44 PM.

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

The screenshot shows the 'Get system log' page for instance i-001add7f70ddc985. The log output is as follows:

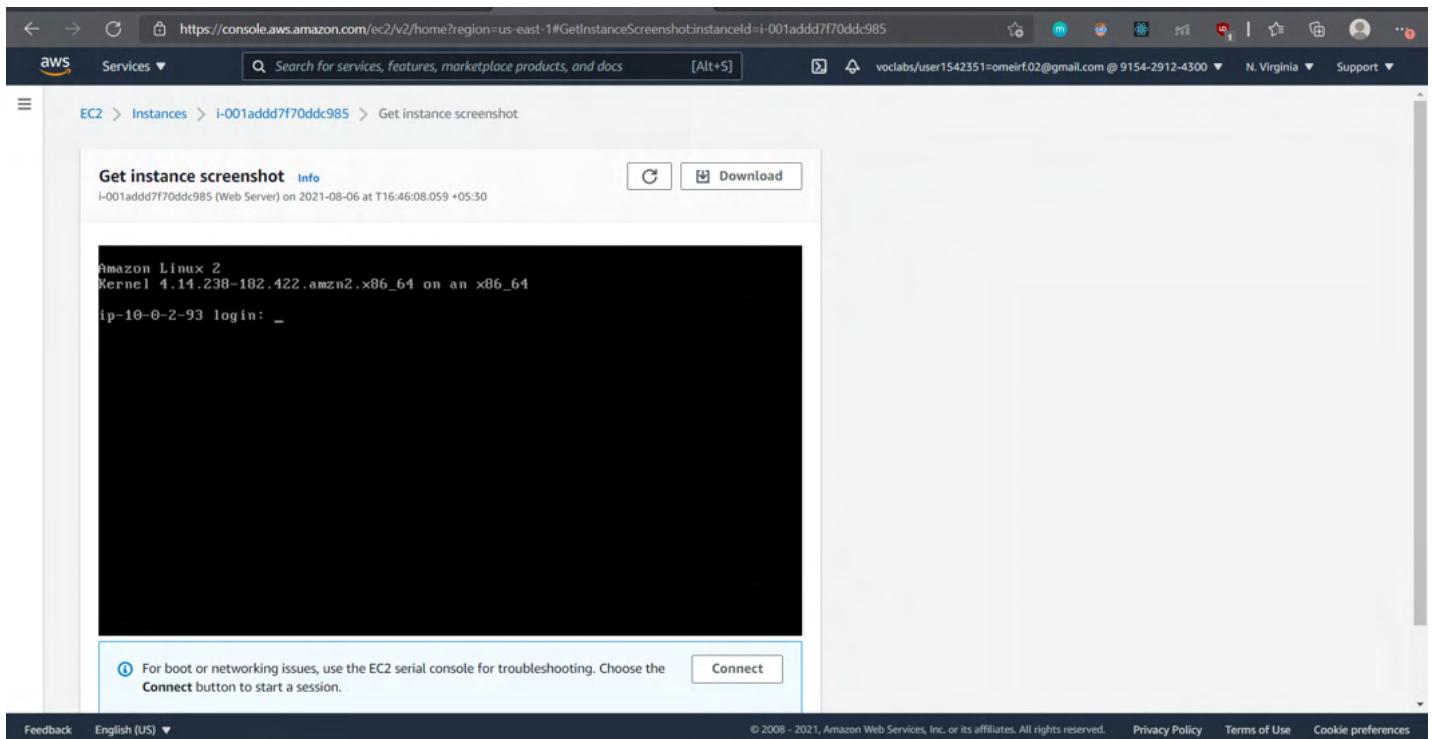
```
[ 25.086011] cloud-init[3162]: --> running transaction check
[ 25.083698] cloud-init[3162]: ---> Package apr-util-bdb.x86_64 0:1.6.1-5.amzn2.0.2 will be installed
[ 25.396679] cloud-init[3162]: --> Finished Dependency Resolution
[ 25.426272] cloud-init[3162]: Dependencies Resolved
[ 25.431972] cloud-init[3162]: =====
[ 25.439059] cloud-init[3162]: Package          Arch      Version       Repository      Size
[ 25.444242] cloud-init[3162]: =====
[ 25.449668] cloud-init[3162]: Installing:
[ 25.452678] cloud-init[3162]: httpd           x86_64    2.4.48-2.amzn2      amzn2-core   1.3 M
[ 25.458556] cloud-init[3162]: Installing for dependencies:
[ 25.462262] cloud-init[3162]: apr             x86_64    1.6.3-5.amzn2.0.2      amzn2-core   118 k
[ 25.467889] cloud-init[3162]: apr-util        x86_64    1.6.1-5.amzn2.0.2      amzn2-core   99 k
[ 25.473526] cloud-init[3162]: apr-util-bdb  x86_64    1.6.1-5.amzn2.0.2      amzn2-core   19 k
[ 25.479479] cloud-init[3162]: generic-logos-httdp noarch  18.0.0-4.amzn2      amzn2-core   19 k
[ 25.484979] cloud-init[3162]: httpd-filesystem noarch  2.4.48-2.amzn2      amzn2-core   24 k
[ 25.490621] cloud-init[3162]: httpd-tools     x86_64    2.4.48-2.amzn2      amzn2-core   87 k
[ 25.497914] cloud-init[3162]: mailcap        noarch  2.1.41-2.amzn2      amzn2-core   31 k
[ 25.503597] cloud-init[3162]: mod_http2      x86_64    1.15.19-1.amzn2.0.1      amzn2-core   149 k
[ 25.509662] cloud-init[3162]: Transaction Summary
[ 25.513172] cloud-init[3162]: =====
[ 25.519064] cloud-init[3162]: Install  1 Package (+8 Dependent packages)
[ 25.523701] cloud-init[3162]: Total download size: 1.9 M
```

A note at the bottom of the log page states: 'For boot or networking issues, use the EC2 serial console for troubleshooting. Choose the Connect button to start a session.' The bottom of the screen shows the Windows taskbar with various pinned icons and the date/time as 06-08-2021 04:44 PM.

30. Choose Cancel.

31. 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.

32. Choose **Cancel**.

Congratulations! You 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, you provided a script that installed a web server and created a simple web page. In this task, you will access content from the web server.

33. Click the **Details** tab.

34. Copy the **IPv4 Public IP** of your instance to your clipboard.

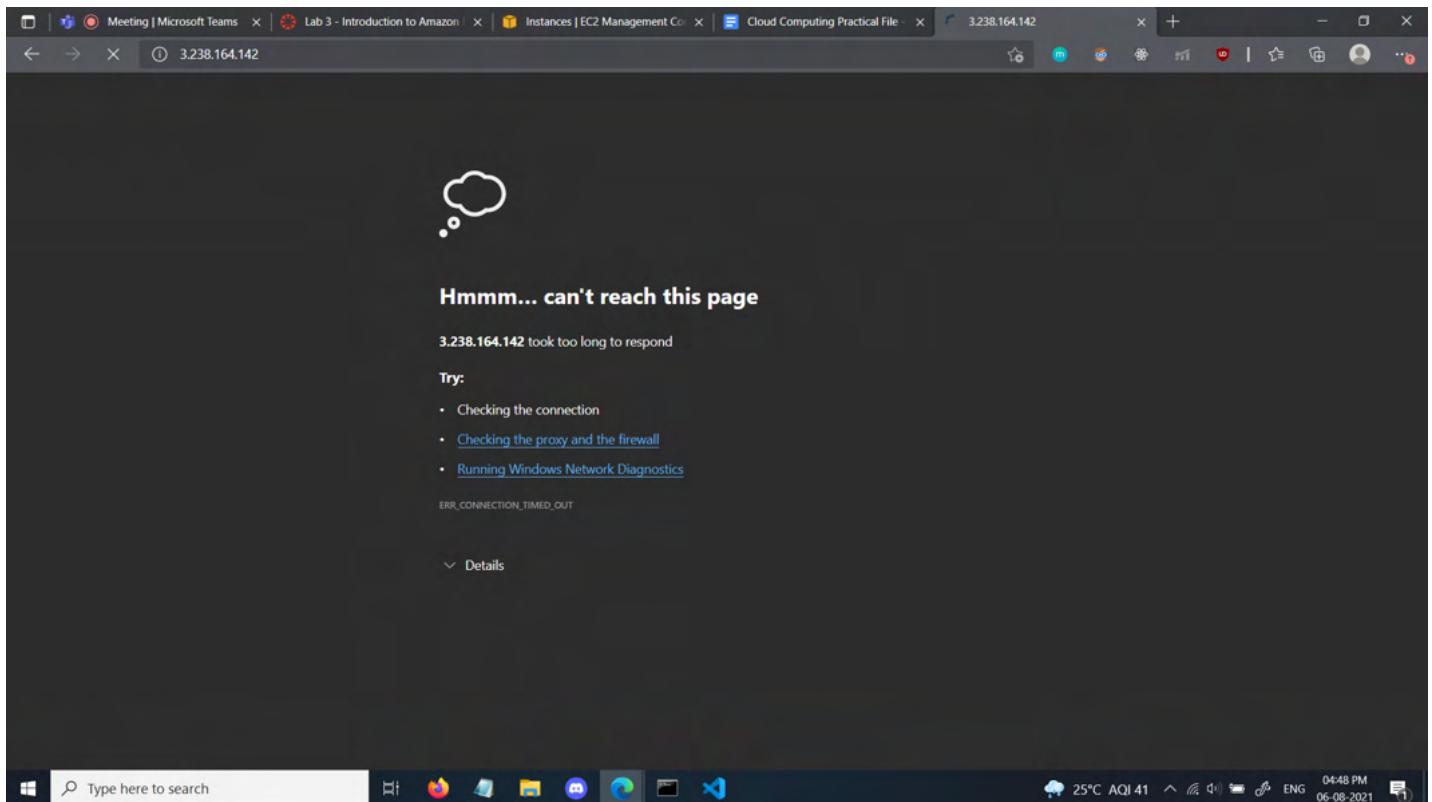
35. Open a new tab in your web browser, paste the IP address you just copied, then press **Enter**.

Question: Are you able to access your web server? Why not?

You 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.



36. Keep the browser tab open, but return to the **EC2 Management Console** tab.

37. In the left navigation pane, click **Security Groups**.

38. Select **Web Server security group**.

39. Click the **Inbound** tab.

The security group currently has no rules.

40. Click **Edit inbound rules** then configure:

- Type: HTTP**
- Source: Anywhere**
- Click Save rules**

The screenshot shows the AWS EC2 Management Console. On the left, there's a navigation sidebar with sections like 'Instances', 'Images', and 'Elastic Block Store'. The main content area is titled 'sg-0f68b61e656623570 - Web Server security group'. It shows 'Details' for the security group, including its name ('Web Server security group'), ID ('sg-0f68b61e656623570'), description ('Security group for my web server'), and VPC ID ('vpc-06676e7583a2c9fb9'). Below this, the 'Inbound rules' tab is selected, showing a table with columns: Name, Security group rule..., IP version, Type, Protocol, and Port range. A note at the bottom of this section says 'No security group rules found'. There's also a 'Run Reachability Analyzer' button. The bottom of the page includes standard AWS footer links like 'Feedback', 'English (US)', and 'Cookie preferences'.

The screenshot shows the AWS EC2 Management Console with the URL <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#ModifyInboundSecurityGroupRules:securityGroupId=sg-0f68b61e6566235...>. The page displays the 'Edit inbound rules' section for a security group. A single rule is listed: an HTTP rule allowing traffic from anywhere (0.0.0.0/0) on port 80. Buttons for 'Add rule', 'Delete', 'Cancel', 'Preview changes', and 'Save rules' are visible.

41. Return to the web server tab that you previously opened and refresh the page.

You should see the message *Hello From Your Web Server!*

Congratulations! You have successfully modified your security group to permit HTTP traffic into your Amazon EC2 Instance.

The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab displays the message "Hello From Your Web Server!" on a white background. The browser's address bar shows the URL <http://3.238.164.142>. The status bar at the bottom of the screen shows the date and time as 06-08-2021 04:50 PM.

Task 4: Resize Your Instance: Instance Type and EBS Volume

As your needs change, you might find that your instance is over-utilized (too small) or under-utilized (too large). If so, you can change the *instance type*. For example, if a *t2.micro* instance is too small for its workload, you can change it to an *m5.medium* instance. Similarly, you can change the size of a disk.

Stop Your Instance

Before you can resize an instance, you must *stop* it.

When you stop an instance, it is shut down. There is no charge for a stopped EC2 instance, but the storage charge for attached Amazon EBS volumes remains.

42. On the **EC2 Management Console**, in the left navigation pane, click **Instances**.

Web Server should already be selected.

43. In the **Instance State** menu, select **Stop instance**.

44. Choose **Stop**

Your instance will perform a normal shutdown and then will stop running.

45. Wait for the **Instance State** to display: stopped

The screenshot shows the AWS EC2 Management Console interface. The left sidebar includes 'New EC2 Experience', 'EC2 Dashboard', 'Events', 'Tags', 'Limits', 'Instances' (selected), 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', 'Scheduled Instances', 'Capacity Reservations', 'Images', 'AMIs', and 'Elastic Block Store' with 'Volumes' and 'Snapshots'. The main content area displays the 'Instances (1/2) Info' section with a table of running instances. The 'Web Server' instance (i-001add7f70ddc985) is selected. A context menu is open over the 'Web Server' instance, with 'Stop instance' highlighted. The 'Actions' dropdown also shows 'Start instance', 'Reboot instance', 'Hibernate instance', and 'Terminate instance' options. The table shows the following data:

Name	Instance ID	Instance state	Instance type	Status
Web Server	i-001add7f70ddc985	Running	t2.micro	2/2
Bastion Host	i-0ff645e572f44c46b2	Running	t2.micro	2/2 checks passed No alarms

Below the table, the 'Instance: i-001add7f70ddc985 (Web Server)' details are shown, including Security groups (sg-0f68b61e656623570) and Inbound rules. The status bar at the bottom indicates: 25°C, AQI 41, ENG, 04:51 PM, 06-08-2021.

The screenshot shows the AWS EC2 Instances page. There are two instances listed: 'Web Server' (running, t2.micro) and 'Bastion Host' (running, t2.micro). A modal dialog titled 'Stop instance?' is open for the 'Web Server' instance, asking for confirmation to stop it. The modal shows the instance ID and its security group.

Change The Instance Type

46. In the **Actions** menu, select **Instance Settings Change Instance Type**, then configure:

- **Instance Type:** *t2.small*
- Choose **Apply**

47. When the instance is started again it will be a *t2.small*, which has twice as much memory as a *t2.micro* instance. **NOTE:** You may be restricted from using other instance types in this lab.

The screenshot shows the AWS EC2 Instances page. The 'Web Server' instance is now stopped. The Actions menu is open, and 'Change instance type' is selected. The modal shows the current instance type as 't2.micro' and the proposed new type as 't2.small'.

The screenshot shows the 'Change instance type' dialog box. At the top, it says 'EC2 > Instances > i-001add7f70ddc985 > Change instance type'. The main area has a heading 'Change instance type' with a 'Info' link. It states: 'You can change the instance type only if the current instance type and the instance type that you want are compatible.' Below this, 'Instance ID' is listed as 'i-001add7f70ddc985 (Web Server)'. The 'Current instance type' is 't2.micro'. Under 'Instance type', a dropdown menu shows 't2.small' is selected. A note says 'EBS-optimized' is not supported for this instance type. At the bottom are 'Cancel' and 'Apply' buttons.

Resize the EBS Volume

47. In the left navigation menu, click **Volumes**.

48. In the **Actions** menu, select **Modify Volume**.

The disk volume currently has a size of 8 GiB. You will now increase the size of this disk.

49. Change the size to: 10 **NOTE:** You may be restricted from creating large Amazon EBS volumes in this lab.

50. Choose **Modify**

51. Choose **Yes** to confirm and increase the size of the volume.

52. Choose **Close**

The screenshot shows the 'Volumes' page in the AWS EC2 Management Console. The left sidebar includes 'New EC2 Experience', 'EC2 Dashboard', 'Events', 'Tags', 'Limits', 'Instances' (selected), 'Images', 'AMIs', 'Elastic Block Store' (selected), 'Volumes' (selected), and 'Snapshots'. The main area lists two volumes: 'vol-0c2a03fd9b9266c27 (Web Server)' and 'gp2'. An 'Actions' menu is open over the first volume, showing options: 'Modify Volume' (highlighted in blue), 'Create Snapshot', 'Create Snapshot Lifecycle Policy', 'Delete Volume', 'Attach Volume', 'Detach Volume', 'Force Detach Volume', 'Change Auto-Enable IO Setting', and 'Add/Edit Tags'. Below the volumes, a table shows detailed information for 'vol-0c2a03fd9b9266c27'. The table columns include Volume Type, IOPS, Throughput, Snapshot, Created, Availability Zone, State, and Alarm Status. The volume details are: Volume ID: vol-0c2a03fd9b9266c27, Size: 8 GiB, Created: August 6, 2021 at 4:38:01 PM UTC+5:30, State: in-use, and Availability Zone: us-east-1b. The screenshot also shows the Windows taskbar at the bottom.

Screenshot of the AWS Cloud Computing Practical File - Lab 3 - Introduction to Amazon Volumes page. The 'Modify Volume' dialog is open, showing the volume ID vol-0c2a03fd9266c27. The volume type is set to General Purpose SSD (gp2), and the size is being modified from 8 GiB to 10 GiB. The IOPS value is set to 100 / 3000. A confirmation message at the bottom states: "Are you sure that you want to modify volume vol-0c2a03fd9266c27? It may take some time for performance changes to take full effect. You may need to extend the OS file system on the volume to use any newly-allocated space." The 'Yes' button is highlighted.

Screenshot of the AWS Cloud Computing Practical File - Lab 3 - Introduction to Amazon Volumes page. The 'Modify Volume' dialog is open, showing the volume ID vol-0c2a03fd9266c27. The volume type is set to General Purpose SSD (gp2), and the size is being modified from 8 GiB to 10 GiB. The IOPS value is set to 100 / 3000. A confirmation message at the bottom states: "Are you sure that you want to modify volume vol-0c2a03fd9266c27? It may take some time for performance changes to take full effect. You may need to extend the OS file system on the volume to use any newly-allocated space." The 'Yes' button is highlighted.

The screenshot shows the AWS EC2 Management Console interface. On the left, the navigation pane includes 'Instances' (selected), 'Images', and 'Elastic Block Store'. In the main area, a 'Modify Volume' dialog is open, displaying a green success message: 'Modify Volume Request Succeeded' and 'Your volume is now being modified.' Below this, the 'Volumes' section shows two volumes: 'Web Server' (vol-0c2a03fdb9266c27) and another unnamed volume. The 'Instances' section lists two instances: 'Web Server' (pending) and 'Bastion Host' (running). The status bar at the bottom indicates the instance ID as i-001add7f70ddc985.

Start the Resized Instance

You will now start the instance again, which will now have more memory and more disk space.

53. In left navigation pane, click **Instances**.
54. In the **Instance State** menu, select **Start instance**.
55. Choose **Start**

Congratulations! You have successfully resized your Amazon EC2 Instance. In this task

you changed your instance type from *t2.micro* to *t2.small*. You also modified your root disk volume from 8 GiB to 10 GiB.

Task 5: Explore EC2 Limits

Amazon EC2 provides different resources that you can use. These resources include images, instances, volumes, and snapshots. When you create an AWS account, there are default limits on these resources on a per-region basis.

56. In the left navigation pane, click **Limits**.

Name	Limit type	Current limit	Description
Reserved Instances	Running instances	20	The total number of instances corresponding to new reserv...
Security groups	Running instances	-	The total number of security groups for this Region.
Security groups per instance	Running instances	8	The number of security groups per instance
Running On-Demand All G instan...	Running instances	0 vCPUs	Running On-Demand G instances
Running On-Demand All Inf insta...	Running instances	0 vCPUs	Running On-Demand Inf instances
Running On-Demand All P instan...	Running instances	0 vCPUs	Running On-Demand P instances
Running On-Demand All Standar...	Running instances	32 vCPUs	Running On-Demand Standard (A, C, D, H, I, M, R, T, Z) insta...
Running On-Demand All High M...	Running instances	0 vCPUs	Running On-Demand High Memory instances
Running On-Demand All X instan...	Running instances	0 vCPUs	Running On-Demand X instances
Running On-Demand All F instan...	Running instances	0 vCPUs	Running On-Demand F instances

57. From the drop down list, choose **Running instances**.

Note that there is a limit on the number of instances that you can launch in this region. When launching an instance, the request must not cause your usage to exceed the current instance limit in that region.

You can request an increase for many of these limits.

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*.

58. In left navigation pane, click **Instances**.

59. In the **Instance State** menu, select **Terminate instance**.

60. 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.*

This is a safeguard to prevent the accidental termination of an instance. If you really want to terminate the instance, you will need to disable the termination protection.

61. In the **Actions** menu, select **Instance Settings Change Termination Protection**.

62. Remove the check next to **Enable**.

63. Choose **Save**

You can now terminate the instance.

64. In the **Instance State** menu, select **Terminate**.

65. Choose **Terminate**

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

The screenshot shows the AWS EC2 Instances page. On the left, the navigation pane includes 'EC2 Dashboard', 'Events', 'Tags', 'Limits', 'Instances' (selected), 'Images' (AMIs), and 'Elastic Block Store' (Volumes, Snapshots). The main area displays two instances: 'Web Server' (i-001addd7f70ddc985) and 'Bastion Host' (i-0f645e372f44c46b2). Both are listed as 'Running'. The 'Actions' dropdown for the Web Server instance has 'Terminate instance' highlighted. Below the table, the details for the selected instance (i-001addd7f70ddc985) are shown, including its Public IPv4 address (44.195.32.62), Private IPv4 addresses (10.0.2.93), and Public IPv4 DNS (ec2-44-195-32-62.compute-1.amazonaws.com).

Screenshot of the AWS EC2 Management Console showing the Instances page. A modal dialog titled "Terminate instance?" is open, asking if the user wants to terminate the selected instance. The modal includes a warning message about the default action for EBS-backed instances.

The main table shows two instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Web Server	i-001add7f70ddc985	Running	t2.small	Initializing	No alarms	us-east-1b	ec2-44-195-32-6
Bastion Host	i-0f645e372f44c46b2	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-18-232-114-

The modal contains the following text:

⚠️ On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost.

Are you sure you want to terminate these instances?

Instance: i-001add7f70ddc985 (Web Server)

To confirm that you want to terminate the instances, choose the terminate button below. Terminating the instance cannot be undone.

Cancel **Terminate**

Feedback English (US) ▾ Type here to search © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences 25°C Rain ENG 04:57 PM 06-08-2021

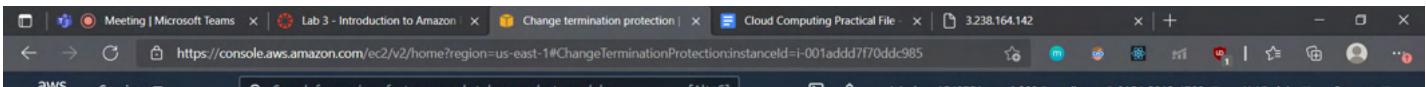
Failed to terminate an instance: The instance 'i-001add7f70ddc985' may not be terminated. Modify its 'disableApiTermination' instance attribute and try again.

The modal is red and displays the error message: Failed to terminate an instance: The instance 'i-001add7f70ddc985' may not be terminated. Modify its 'disableApiTermination' instance attribute and try again.

The main table shows the same two instances as before:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Web Server	i-001add7f70ddc985	Running	t2.small	Initializing	No alarms	us-east-1b	ec2-44-195-32-6
Bastion Host	i-0f645e372f44c46b2	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-18-232-114-

Feedback English (US) ▾ Type here to search © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences 25°C Rain ENG 04:57 PM 06-08-2021



EC2 > Instances > i-001add7f70ddc985 > Change termination protection

Change termination protection Info

Enable termination protection to prevent your instance from being accidentally terminated.

Instance ID: i-001add7f70ddc985 (Web Server)

Termination protection: Enable

Termination protection disabled.
The instance is no longer protected against accidental termination. If the instance is terminated, data stored on ephemeral storage is lost.

Cancel **Save**

Feedback English (US) ▾ Type here to search 25°C Rain 04:57 PM 06-08-2021

Meeting | Microsoft Teams Lab 3 - Introduction to Amazon Instances | EC2 Management Con Cloud Computing Practical File 3.238.164.142

New EC2 Experience Learn more

Instances (2) Info

Disabled termination protection for i-001add7f70ddc985

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Web Server	i-001add7f70ddc985	Running	t2.small	2/2 checks passed	No alarms	us-east-1b	ec2-44-195-32-6
Bastion Host	i-0ff645e372f44c46b2	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-18-232-114-

Select an instance above

Feedback English (US) ▾ Type here to search 25°C Rain 04:57 PM 06-08-2021

Screenshot of the AWS Cloud Computing Practical File - Instances | EC2 Management Console showing the termination of an EC2 instance.

The browser tabs are:

- Meeting | Microsoft Teams
- Lab 3 - Introduction to Amazon
- Instances | EC2 Management Con...
- Cloud Computing Practical File -
- 3.238.164.142

The AWS Cloud Computing Practical File - Instances | EC2 Management Console shows the following information:

Disabled termination protection for i-001add7f70ddc985

Successfully terminated i-001add7f70ddc985

Instances (1/2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Web Server	i-001add7f70ddc985	Shutting-down	t2.small	2/2 checks passed	No alarms	us-east-1b	ec2-44-195-32-6
Bastion Host	i-0f645e372f44c46b2	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-18-232-114-

Instance: i-001add7f70ddc985 (Web Server)

Details Security Networking Storage Status checks Monitoring Tags

Instance summary

Instance ID	Public IPv4 address	Private IPv4 addresses
i-001add7f70ddc985 (Web Server)	44.195.32.62 open address	10.0.2.93
IPv6 address	Instance state	Public IPv4 DNS
-	Shutting-down	ec2-44-195-32-62.compute-1.amazonaws.com open address

Feedback English (US) ▾ Type here to search © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences 25°C Rain ENG 04:58 PM 06-08-2021

Disabled termination protection for i-001add7f70ddc985

Successfully terminated i-001add7f70ddc985

Instances (1/2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Web Server	i-001add7f70ddc985	Terminated	t2.small	-	No alarms	us-east-1b	-
Bastion Host	i-0f645e372f44c46b2	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-18-232-114-

Instance: i-001add7f70ddc985 (Web Server)

Details Security Networking Storage Status checks Monitoring Tags

Instance summary

Instance ID	Public IPv4 address	Private IPv4 addresses
i-001add7f70ddc985 (Web Server)	-	-
IPv6 address	Instance state	Public IPv4 DNS
-	Terminated	-
Private IPv4 DNS	Instance type	Elastic IP addresses
-	-	-

Feedback English (US) ▾ Type here to search © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences 25°C Rain ENG 04:58 PM 06-08-2021

Practical 2

AIM

Build your VPC and Launch a Web Server

THEORY

OBJECTIVE

- Create a VPC.
- Create subnets.
- Configure a security group.
- Launch an EC2 instance into a VPC.

PROCEDURE

Task 1: Create Your VPC

In this task, you will use the VPC Wizard to create a VPC, an Internet Gateway and two subnets in a single Availability Zone. An Internet gateway (IGW) is a VPC component that allows communication between instances in your VPC and the Internet.

After creating a VPC, you can add subnets. Each subnet resides entirely within one Availability Zone and cannot span zones. If a subnet's traffic is routed to an Internet Gateway, the subnet is known as a public subnet. If a subnet does not have a route to the Internet gateway, the subnet is known as a private subnet.

The wizard will also create a NAT Gateway, which is used to provide internet connectivity to EC2 instances in the private subnets.

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

2. Click **Launch VPC Wizard**

The screenshot shows the AWS VPC Management Console dashboard. On the left, there's a navigation pane with sections like 'New VPC Experience', 'VPC Dashboard', 'Your VPCs', 'Subnets', 'Route Tables', etc. The main area displays 'Resources by Region' with categories such as VPCs, Subnets, Route Tables, Internet Gateways, Carrier Gateways, Security Groups, and more. Each category shows the number of resources and a 'See all regions' link. To the right, there are sections for 'Service Health' (Amazon EC2 - US East (N. Virginia) is operating normally), 'Settings' (Zones, Console Experiments), 'Additional Information' (VPC Documentation, All VPC Resources, Forums, Report an Issue), and 'Transit Gateway Network Manager' (Network Manager enables centrally manage your global network across AWS and on-premises. Learn more). At the bottom, there are links for 'Feedback', 'English (US)', and other AWS services.

3. In the left navigation pane, click **VPC with Public and Private Subnets** (the second option).

The screenshot shows the 'Step 1: Select a VPC Configuration' page of the VPC Wizard. The left sidebar lists four options: 'VPC with a Single Public Subnet' (selected), 'VPC with Public and Private Subnets' (highlighted in blue), 'VPC with Public and Private Subnets and Hardware VPN Access', and 'VPC with a Private Subnet Only and Hardware VPN Access'. The main content area describes the 'VPC with Public and Private Subnets' configuration, stating it adds a private subnet whose instances are not addressable from the Internet. It mentions instances in the private subnet can establish outbound connections to the Internet via the public subnet using Network Address Translation (NAT). A diagram illustrates the setup: 'Internet, S3, DynamoDB, SNS, SQS, etc.' connects to an 'Amazon Virtual Private Cloud' which contains a 'Public Subnet' and a 'Private Subnet'. A 'NAT' device is shown between them. An 'Important:' note says: 'If you are using a Local Zone with your VPC follow this link to create your VPC.' A 'Select' button is at the bottom right, and a 'Cancel and Exit' link is at the bottom center.

4. Click **Select** then configure:

- **VPC name:** Lab VPC
- **Availability Zone:** Select the *first* Availability Zone
- **Public subnet name:** Public Subnet 1
- **Availability Zone:** Select the *first* Availability Zone (the same as used above)
- **Private subnet name:** Private Subnet 1
- **Elastic IP Allocation ID:** Click in the box and select the displayed IP address

Step 2: VPC with Public and Private Subnets

IPv4 CIDR block:	10.0.0.0/16	(65531 IP addresses available)
IPv6 CIDR block:	<input checked="" type="radio"/> No IPv6 CIDR Block <input type="radio"/> Amazon provided IPv6 CIDR block <input type="radio"/> IPv6 CIDR block owned by me	
VPC name:	Lab VPC	
Public subnet's IPv4 CIDR:	10.0.0.0/24	(251 IP addresses available)
Availability Zone:	us-east-1a	
Public subnet name:	Public subnet 1	
Private subnet's IPv4 CIDR:	10.0.1.0/24	(251 IP addresses available)
Availability Zone:	us-east-1a	
Private subnet name:	Private subnet 1	
You can add more subnets after Amazon Web Services creates the VPC.		
Specify the details of your NAT gateway (NAT gateway rates apply).		
Elastic IP Allocation ID:	<input type="text"/> Allocation ID <input type="text"/> Elastic IP Address elipalloc-07795d3dd79beea94 44.196.49.125	
Enable DNS hostnames:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Hardware tenancy:	<input type="text"/> Default	
Cancel and Exit Back Create VPC		

Feedback English (US) © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences

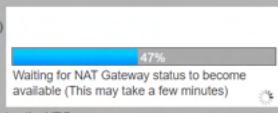
5. Click **Create VPC**.

The wizard will create your VPC.

Step 2: VPC with Public and Private Subnets

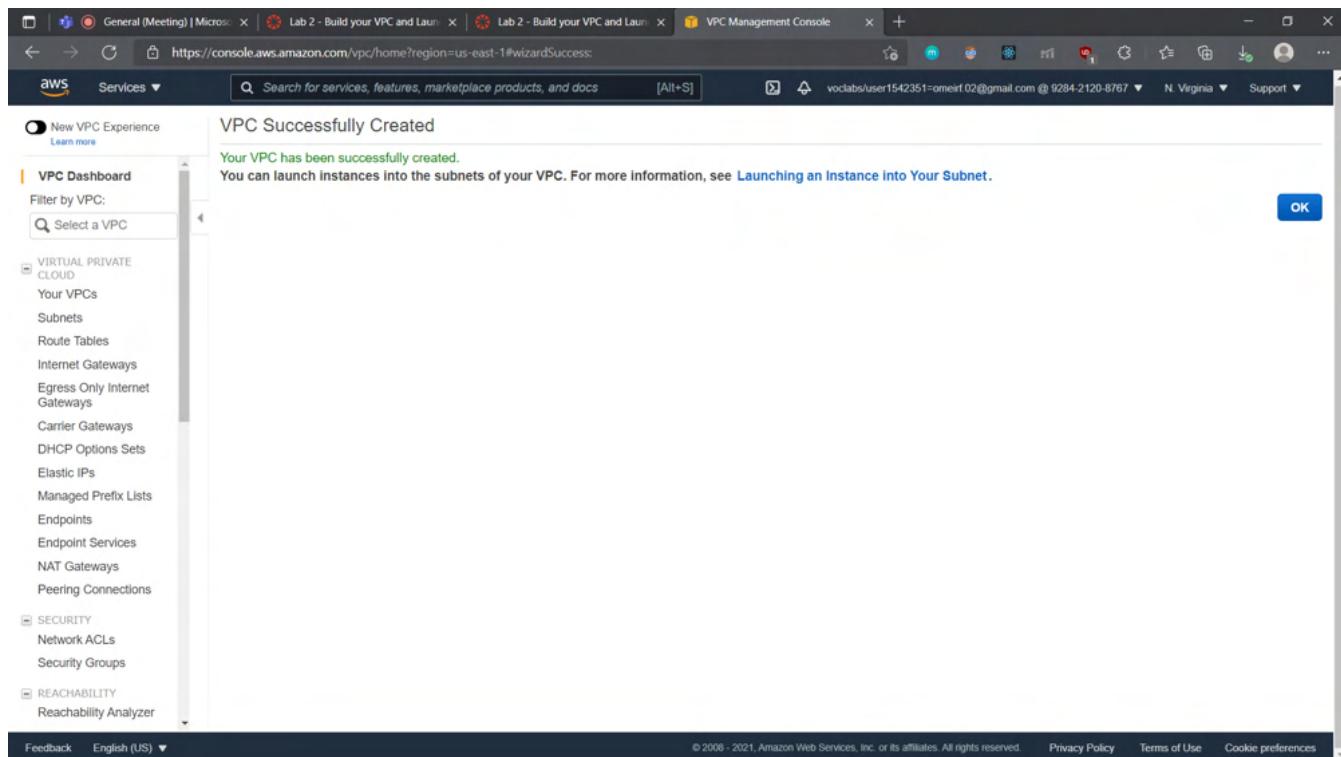
IPv4 CIDR block:	10.0.0.0/16	(65531 IP addresses available)
IPv6 CIDR block:	<input checked="" type="radio"/> No IPv6 CIDR Block <input type="radio"/> Amazon provided IPv6 CIDR block <input type="radio"/> IPv6 CIDR block owned by me	
VPC name:	Lab VPC	
Public subnet's IPv4 CIDR:	10.0.0.0/24	(251 IP addresses available)
Availability Zone:	us-east-1a	
Public subnet name:	Public subnet 1	
Private subnet's IPv4 CIDR:	10.0.1.0/24	(251 IP addresses available)
Availability Zone:	us-east-1a	
Private subnet name:	Private subnet 1	
You can add more subnets after Amazon Web Services creates the VPC.		
Specify the details of your NAT gateway (NAT gateway rates apply).		
Elastic IP Allocation ID:	<input type="text"/> elipalloc-07795d3dd79beea94	
Service endpoints	Add Endpoint	
Enable DNS hostnames:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Hardware tenancy:	<input type="text"/> Default	
Cancel and Exit Back Create VPC		

Feedback English (US) © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences

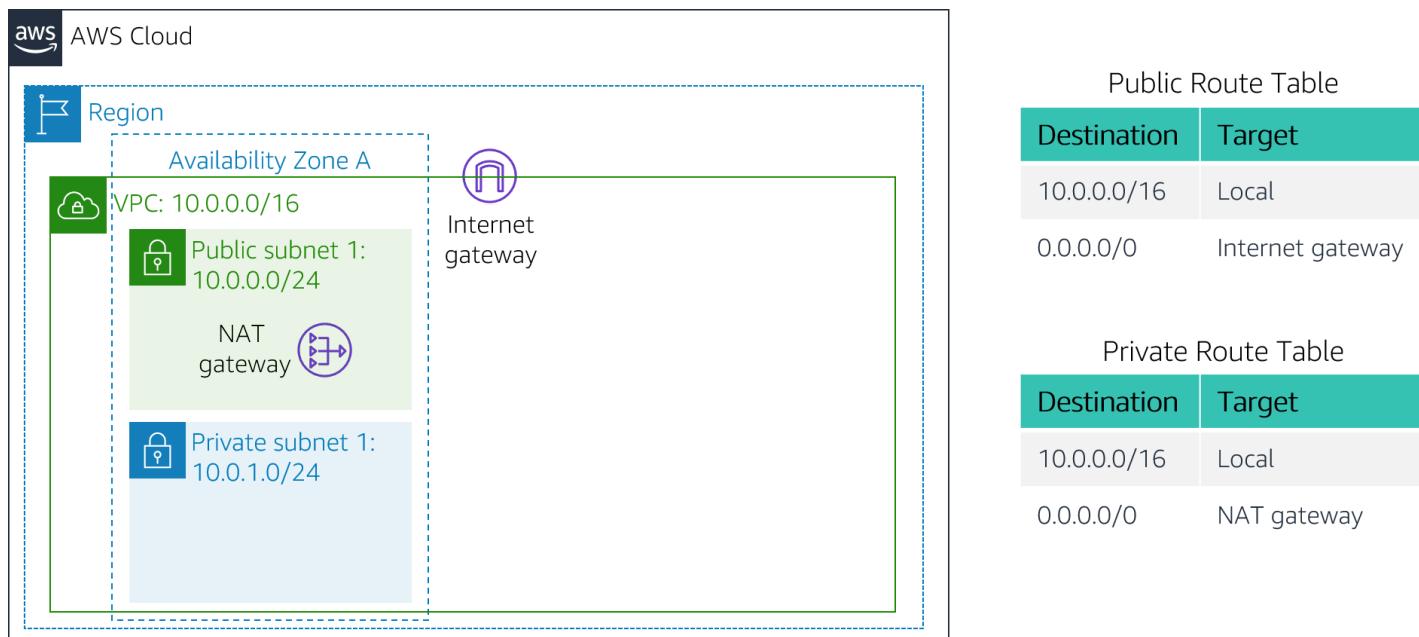


Waiting for NAT Gateway status to become available (This may take a few minutes)

6. Once it is complete, click **OK**



The wizard has provisioned a VPC with a public subnet and a private subnet in the same Availability Zone, together with route tables for each subnet:



The Public Subnet has a CIDR of **10.0.0.0/24**, which means that it contains all IP addresses starting with **10.0.0.x**.

The Private Subnet has a CIDR of **10.0.1.0/24**, which means that it contains all IP addresses starting with **10.0.1.x**.

Task 2: Create Additional Subnets

In this task, you will create two additional subnets in a second Availability Zone. This is useful for creating resources in multiple Availability Zones to provide *High Availability*.

7. In the left navigation pane, click **Subnets**.

First, you will create a second Public Subnet.

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
Work Public Subnet	subnet-084b5bc7a69cbde7a	Available	vpc-0b2db02f7a9e249f7 Wo...	10.0.0.0/24	-
-	subnet-33dcfa6c	Available	vpc-4a710037	172.31.32.0/20	-
Private subnet 1	subnet-004632aad62623063	Available	vpc-0d63cb6f9374a3ffb Lab ...	10.0.1.0/24	-
-	subnet-04d7be35	Available	vpc-4a710037	172.31.48.0/20	-
-	subnet-cd46b381	Available	vpc-4a710037	172.31.16.0/20	-
Public subnet 1	subnet-09bb0c2e7460186ae	Available	vpc-0d63cb6f9374a3ffb Lab ...	10.0.0.0/24	-
-	subnet-3b5a791a	Available	vpc-4a710037	172.31.80.0/20	-
Public subnet 2					

8. Click **Create subnet** then configure:

- **VPC ID:** Lab VPC
- **Subnet name:** Public Subnet 2
- **Availability Zone:** Select the second Availability Zone
- **IPv4 CIDR block:** 10.0.2.0/24

VPC

VPC ID
Create subnets in this VPC.
vpc-0d63cb6f9374a3ffb (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.
Public Subnet 2
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
Q. 10.0.2.0/24

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

10. Click **Create subnet**

You will now create a second Private Subnet.

The screenshot shows the AWS VPC Management Console interface. A modal window titled "Subnet 1 of 1" is open, prompting for subnet configuration. The "Subnet name" field contains "Public Subnet 2". The "Availability Zone" dropdown is set to "US East (N. Virginia) / us-east-1b". The "IPv4 CIDR block" field shows "10.0.2.0/24". Under "Tags - optional", a single tag named "Name" with value "Public Subnet 2" is added. At the bottom right of the modal is a prominent orange "Create subnet" button. Below the modal, the main VPC Management Console page displays a success message: "You have successfully created 1 subnet: subnet-0d41fc5aeac3859db". The "Subnets" table lists this subnet with details: Name: Public Subnet 2, Subnet ID: subnet-0d41fc5aeac3859db, State: Available, VPC: vpc-0d63cb6f9374a3ffb | Lab ..., IPv4 CIDR: 10.0.2.0/24. The left sidebar shows the navigation menu for VPC management, including sections for VPC Dashboard, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, Carrier Gateways, DHCP Options Sets, Elastic IPs, Managed Prefix Lists, Endpoints, Endpoint Services, NAT Gateways, and Peering Connections.

11. Click **Create subnet** then configure:

- **VPC ID:** Lab VPC
- **Subnet name:** Private Subnet 2
- **Availability Zone:** Select the *second* Availability Zone
- **CIDR block:** 10.0.3.0/24

VPC ID: vpc-0d63cb6f9374a3ffb (Lab VPC)

Associated VPC CIDRs: 10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name: Private subnet 2

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

IPv4 CIDR block: 10.0.3.0/24

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

13. Click **Create subnet**

You will now configure the Private Subnets to route internet-bound traffic to the NAT Gateway so that resources in the Private Subnet are able to connect to the Internet, while still keeping the resources private. This is done by configuring a *Route Table*.

A *route table* contains a set of rules, called *routes*, that are used to determine where network traffic is directed. Each subnet in a VPC must be associated with a route table; the route table controls routing for the subnet.

14. In the left navigation pane, click **Route Tables**.

15. Select the route table with **Main = Yes** and **VPC = Lab VPC**. (Expand the **VPC ID** column if necessary to view the VPC name.)

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
rtb-a51be7d4	-	-	-	Yes	vpc-4a710037
rtb-07b6760956d6479b3	-	-	-	Yes	vpc-0b2db02f7a9e249f7 Work VPC
rtb-0a78ed9c8ba43417c	-	-	-	Yes	vpc-0d63cb6f9374a3ffb Lab VPC
Work Public Route ...	rtb-08a554c3c67554a78	subnet-084b5bc7a69cb...	-	No	vpc-0b2db02f7a9e249f7 Work VPC
-	rtb-02ea00ca7665d1b50	subnet-09bb0c2e74601...	-	No	vpc-0d63cb6f9374a3ffb Lab VPC

16. In the lower pane, click the **Routes** tab.

Note that **Destination 0.0.0.0/0** is set to **Target nat-xxxxxxxx**. This means that traffic destined for the internet (0.0.0.0/0) will be sent to the NAT Gateway. The NAT Gateway will then forward the traffic to the internet.

This route table is therefore being used to route traffic from Private Subnets. You will now add a name to the Route Table to make this easier to recognize in future.

The screenshot shows the AWS VPC Route Table configuration page for a route table named 'rtb-0a78ed9c8ba43417c'. The 'Routes' tab is selected. There are two entries:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	nat-027cb761d260825f7	Active	No

17. In the **Name** column for this route table, click the pencil then type **Private Route Table** and click **Save**.

The screenshot shows the AWS VPC NAT gateway configuration page. A modal dialog is open over a list of NAT gateways. The dialog is titled 'Edit Name' and contains the text 'Private Route Table'. At the bottom of the dialog are 'Cancel' and 'Save' buttons. The main table below shows one NAT gateway entry:

Name	NAT gateway ID	Connectivit...	State	State message	Elastic IP address	Private IP
Private Route Table	5f7	Public	Available	-	44.196.49.125	10.0.0.24

18. In the lower pane, click the **Subnet Associations** tab.

You will now associate this route table to the Private Subnets.

19. Click **Edit subnet associations**

20. Select both **Private Subnet 1** and **Private Subnet 2**.

You can expand the *Subnet ID* column to view the Subnet names.

The screenshot shows the AWS VPC Management Console with the URL [https://console.aws.amazon.com/vpc/home?region=us-east-1#EditRouteTableSubnetAssociations\(RouteTableId=rtb-0a78ed9c8ba43417c\)](https://console.aws.amazon.com/vpc/home?region=us-east-1#EditRouteTableSubnetAssociations(RouteTableId=rtb-0a78ed9c8ba43417c)). The page title is "Edit subnet associations".

Available subnets (2/4)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
Private subnet 1	subnet-004632aad62623063	10.0.1.0/24	-	Main (rtb-0a78ed9c8ba43417c)
Private subnet 2	subnet-0214db5d857559b9b	10.0.3.0/24	-	Main (rtb-0a78ed9c8ba43417c)
Public subnet 1	subnet-09bb0c2e7460186a	10.0.0.0/24	-	rtb-02ea00ca7665d1b50
Public Subnet 2	subnet-0d41fc5aeac3859db	10.0.2.0/24	-	Main (rtb-0a78ed9c8ba43417c)

Selected subnets

- subnet-0214db5d857559b9b / Private subnet 2
- subnet-004632aad62623063 / Private subnet 1

Buttons: Cancel, Save associations

21. Click **Save associations**

You will now configure the Route Table that is used by the Public Subnets.

22. Select the route table with **Main = No** and **VPC = Lab VPC** (and deselect any other subnets).

23. In the **Name** column for this route table, click the pencil then type **Public Route Table**, and click **Save**

24. In the lower pane, click the **Routes** tab.

Note that **Destination 0.0.0.0/0** is set to **Target igw-xxxxxxxx**, which is the Internet Gateway. This means that internet-bound traffic will be sent straight to the internet via the Internet Gateway.

You will now associate this route table to the Public Subnets.

The screenshot shows the AWS VPC Management Console with the URL <https://console.aws.amazon.com/vpc/home?region=us-east-1#RouteTables>. The page title is "Route tables (1/5)".

Route tables (1/5)

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
Work Public Route ...	rtb-08a5543c67554a78	subnet-084b5bc7a69cb...	-	No	vpc-0b2db02f7a9e249f7 Work VPC
-	rtb-a51be7d4	-	-	Yes	vpc-4a710037
rtb-02ea00ca7665d1b50	rtb-02ea00ca7665d1b50	subnet-09bb0c2e74601...	-	No	vpc-0d63cb6f9374a3ffb Lab VPC
-	rtb-07b670956d6479b3	-	-	Yes	vpc-0b2db02f7a9e249f7 Work VPC
-	rtb-0a78ed9c8ba43417c	2 subnets	-	Yes	vpc-0d63cb6f9374a3ffb Lab VPC

Routes (2)

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-0b9f27e9ccb7b14c4	Active	No

25. Click the Subnet Associations tab.

26. Click Edit subnet associations

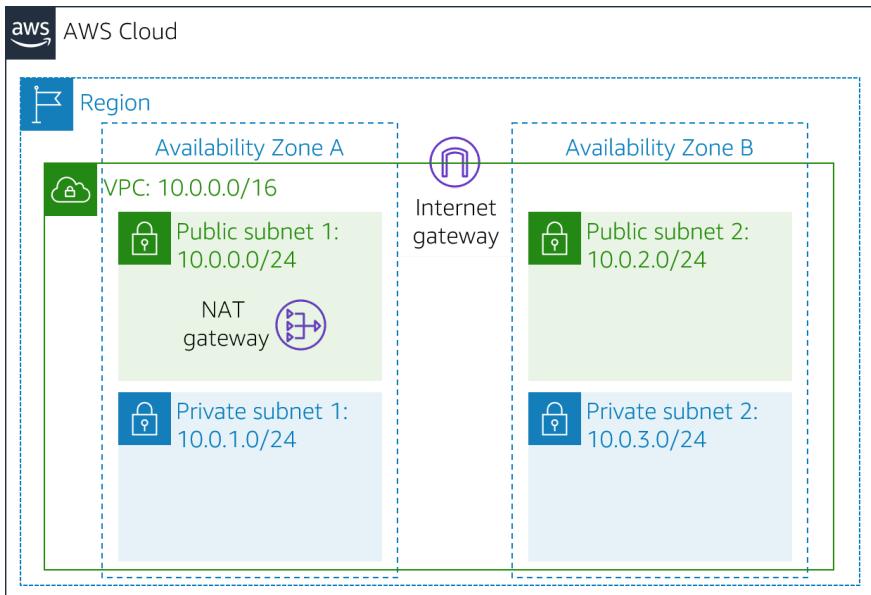
The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar with various VPC-related services like Internet Gateways, Carrier Gateways, and Route Tables. The main area displays a table of route tables, with one specific route table, 'rtb-02ea00ca7665d1b50', selected. Below the table, there's a detailed view of this route table, specifically its 'Subnet associations' tab. It lists one association: 'subnet-09bb0c2e7460186ae / Public subnet 1' with an IPv4 CIDR of 10.0.0.0/24.

27. Select both Public Subnet 1 and Public Subnet 2.

28. Click Save associations

This screenshot shows the 'Edit subnet associations' dialog box. At the top, it says 'Available subnets (2/4)' and shows a list of subnets: 'Private subnet 1', 'Private subnet 2', 'Public subnet 1', and 'Public Subnet 2'. The last two are checked. Below that is a 'Selected subnets' section containing the same two subnets. At the bottom right, there are 'Cancel' and 'Save associations' buttons.

Your VPC now has public and private subnets configured in two Availability Zones:



Public Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Internet gateway

Private Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	NAT gateway

Task 3: Create a VPC Security Group

In this task, you will create a VPC security group, which acts as a virtual firewall. When you launch an instance, you associate one or more security groups with the instance. You can add rules to each security group that allow traffic to or from its associated instances.

29. In the left navigation pane, click **Security Groups**.

30. Click **Create security group** and then configure:

- Security group name:** Web Security Group
- Description:** Enable HTTP access
- VPC:** Lab VPC

The screenshot shows the AWS VPC Management Console with the Security Groups page open. The page displays a list of existing security groups, each with a Name, Security group ID, VPC ID, Description, and Owner. The 'Create security group' button is located at the top right of the table header. The left sidebar shows the navigation menu for VPC management, including options like New VPC Experience, VPC Dashboard, and various network components.

Name	Security group ID	VPC ID	Description	Owner
default	sg-05bd67743dfd2bd7b	vpc-0d63cb6f9374a3ffb	default VPC security gr...	928421208767
default	sg-097f72b9c592aa650	vpc-0b2db02f7a9e249f7	default VPC security gr...	928421208767
Ec2SecurityGroup	sg-0c899f3850d13dff2	vpc-0b2db02f7a9e249f7	VPC Security Group	928421208767
default	sg-f04b16ef	vpc-4a710037	default VPC security gr...	928421208767

Basic details

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

Description [Info](#)
Enable HTTP Access

VPC [Info](#)
vpc-0d63cb6f9374a3ffb (Lab VPC)

Inbound rules [Info](#)

This security group has no inbound rules.

Add rule

31. In the **Inbound rules** pane, choose **Add rule**

32. Configure the following settings:

- Type: **HTTP**
- Source: **Anywhere**
- Description: **Permit web requests**

Basic details

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

Description [Info](#)
Enable HTTP Access

VPC [Info](#)
vpc-0d63cb6f9374a3ffb (Lab VPC)

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
HTTP	TCP	80	Anywhere	Permit web requests

Feedback English (US) ▾ © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences

33. Scroll to the bottom of the page and choose **Create security group**

You will use this security group in the next task when launching an Amazon EC2 instance.

The screenshot shows the AWS VPC Management Console. A green banner at the top indicates that a security group named "sg-0e4cfb943f2e335db | Web Security Group" was created successfully. Below the banner, the "sg-0e4cfb943f2e335db - Web Security Group" page is displayed. The "Details" section shows the following information:

Security group name	sg-0e4cfb943f2e335db	Description	VPC ID
Owner	928421208767	Inbound rules count	vpc-0d63cb6f9374a3ff
		Outbound rules count	
		1 Permission entry	

The "Inbound rules" tab is selected, showing one rule: "You can now check network connectivity with Reachability Analyzer". There is a "Run Reachability Analyzer" button.

Task 4: Launch a Web Server Instance

In this task, you will launch an Amazon EC2 instance into the new VPC. You will configure the instance to act as a web server.

34. On the **Services** menu, click **EC2**.

The screenshot shows the AWS Services menu. The "EC2" option is highlighted in the "Recently visited" section. The main menu lists various AWS services under categories such as Favorites, All services, Containers, Storage, Database, Customer Enablement, Robotics, Blockchain, Quantum Technologies, Management & Governance, and many others.

35. Click **Launch Instance**, and then choose **Launch Instance**

First, you will select an *Amazon Machine Image (AMI)*, which contains the desired Operating System.

The screenshot shows the AWS EC2 Management console with the URL <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard>. The left sidebar has sections for EC2 Dashboard, Instances, Images, and Elastic Block Store. The main area shows 'Resources' with counts for Instances (running), Dedicated Hosts, Elastic IPs, Instances, Key pairs, Load balancers, Placement groups, Security groups, Snapshots, and Volumes. A callout 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'. Below this is the 'Launch instance' section with a 'Launch instance' button. To the right is the 'Service health' dashboard showing the US East (N. Virginia) region is operating normally. The right sidebar shows 'Account attributes' like Supported platforms (VPC), Default VPC (vpc-4a710037), and 'Explore AWS' sections for ML Inference and Best Price-Performance.

36. In the row for **Amazon Linux 2** (at the top), click **Select**

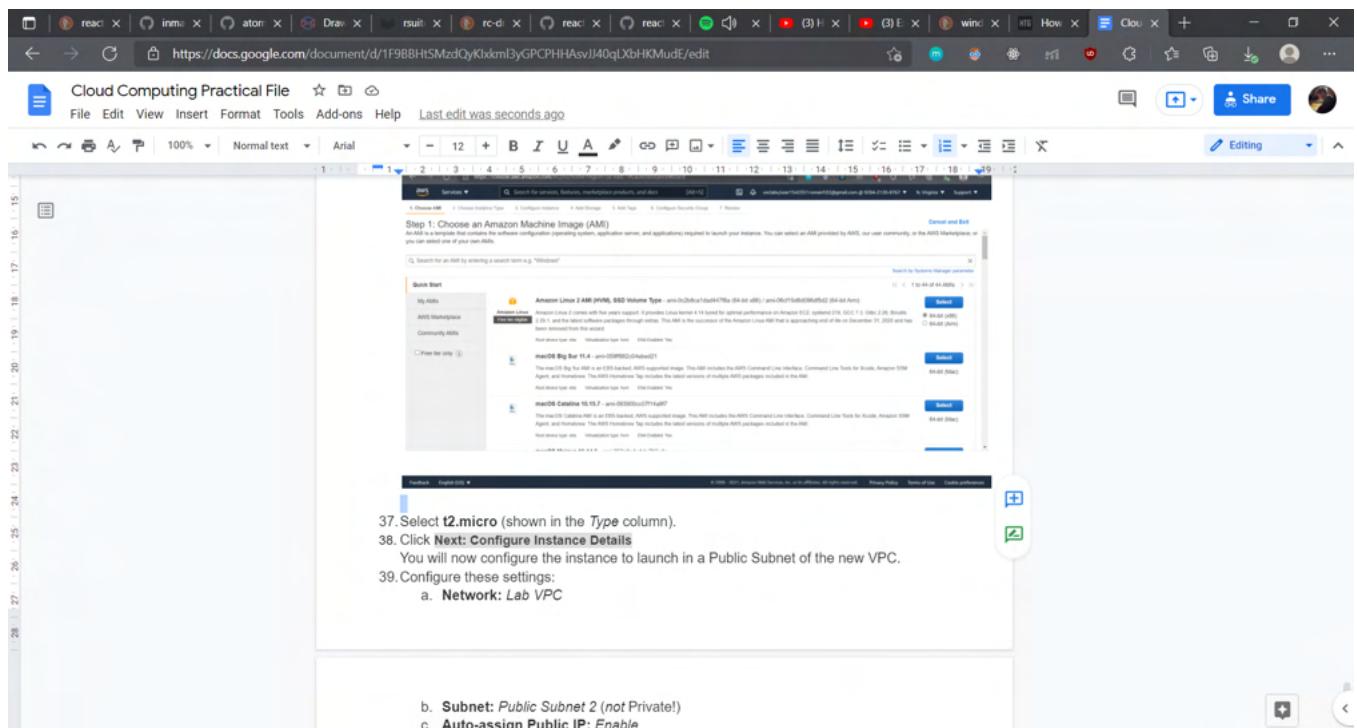
The *Instance Type* defines the hardware resources assigned to the instance.

The screenshot shows the 'Launch instance wizard | EC2 Management' page at step 1: Choose AMI. The URL is <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard>. The left sidebar shows steps 1-7. The main area lists AMIs: 'Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0c2b8ca1dad447f8a (64-bit x86) / ami-06cf15d6d096df5d2 (64-bit Arm)', 'macOS Big Sur 11.4 - ami-059ff882c04ebcd21 (64-bit Mac)', and 'macOS Catalina 10.15.7 - ami-093900cc07f14a8f7 (64-bit Mac)'. Each item has a 'Select' button and a radio button for 64-bit (x86) or 64-bit (Arm). The right sidebar shows 'Cancel and Exit' and 'Search by Systems Manager parameter'.

37. Select **t2.micro** (shown in the *Type* column).

38. Click **Next: Configure Instance Details**

You will now configure the instance to launch in a Public Subnet of the new VPC.



39. Configure these settings:

- Network: Lab VPC**
- Subnet: Public Subnet 2 (not Private!)**
- Auto-assign Public IP: Enable**

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	1	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-0d63cb6f9374a3ff Lab VPC	<input type="button"/> Create new VPC
Subnet	subnet-0d41fc5aeac3859db Public Subnet 2 us-east-1	<input type="button"/> Create new subnet 251 IP Addresses available
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	
Domain join directory	No directory	<input type="button"/> Create new directory
IAM role	None	<input type="button"/> Create new IAM role
Shutdown behavior	Stop	
Stop - Hibernate behavior	<input type="checkbox"/> Enable hibernation as an additional stop behavior	
Enable termination protection	<input type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring Additional charges apply.	

Review and Launch **Cancel** **Previous** **Next: Add Storage**

40. Expand the **Advanced Details** section (at the bottom of the page).

41. Copy and paste this code into the **User data** box:

```

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

```

This script will be run automatically when the instance launches for the first time. The script loads and configures a PHP web application.

The screenshot shows the AWS Launch Instance Wizard at Step 3: Configure Instance Details. In the 'User data' section, the following shell script is pasted:

```

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

```

42. Click **Next: Add Storage**

You will use the default settings for storage.

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-090e9376979c86d7b	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Cancel Previous Review and Launch Next: Add Tags

43. Click **Next: Add Tags**

Tags can be used to identify resources. You will use a tag to assign a Name to the instance.

44. Click **Add Tag** then configure:

- a. **Key:** Name
- b. **Value:** Web Server 1

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key	(128 characters maximum)	Value	(256 characters maximum)	Instances	Volumes	Network Interfaces
Name		Web Server 1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

45. Click **Next: Configure Security Group**

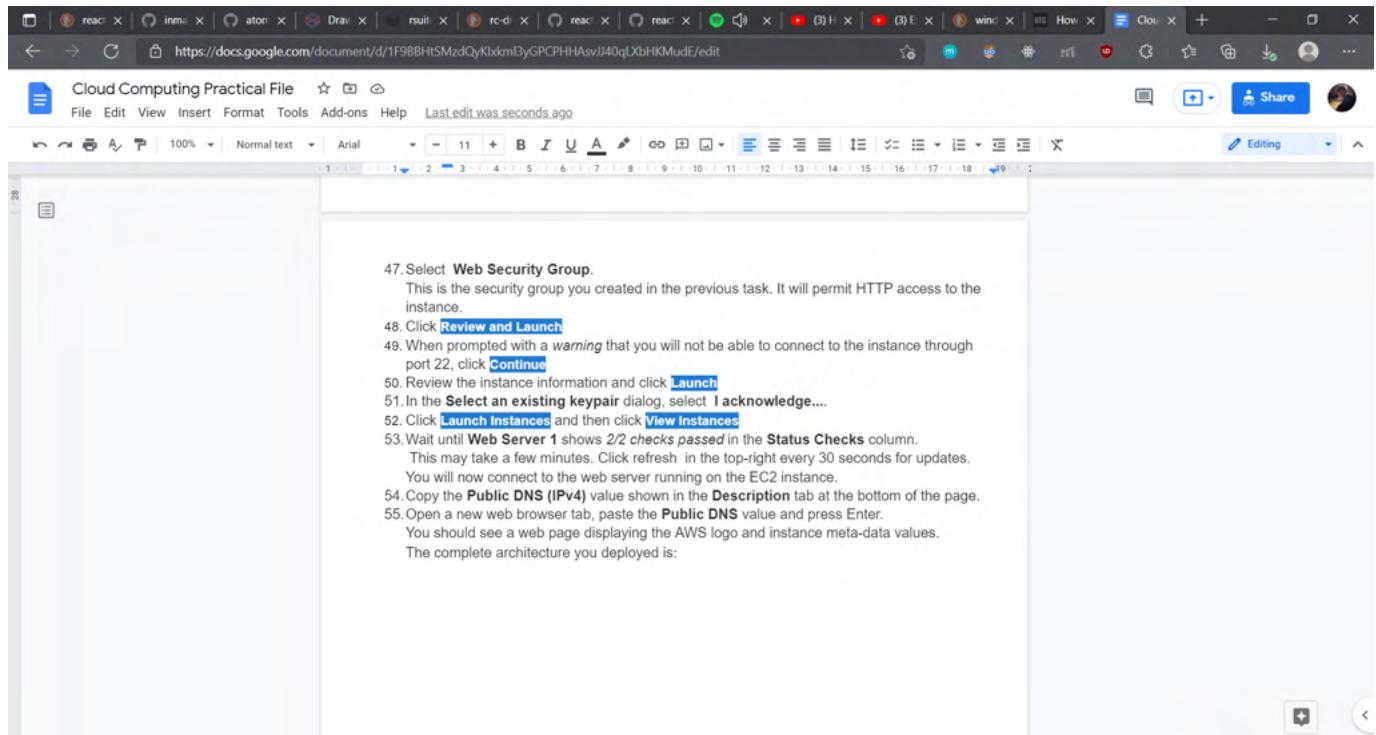
You will configure the instance to use the *Web Security Group* that you created earlier.

46. Select **Select an existing security group**

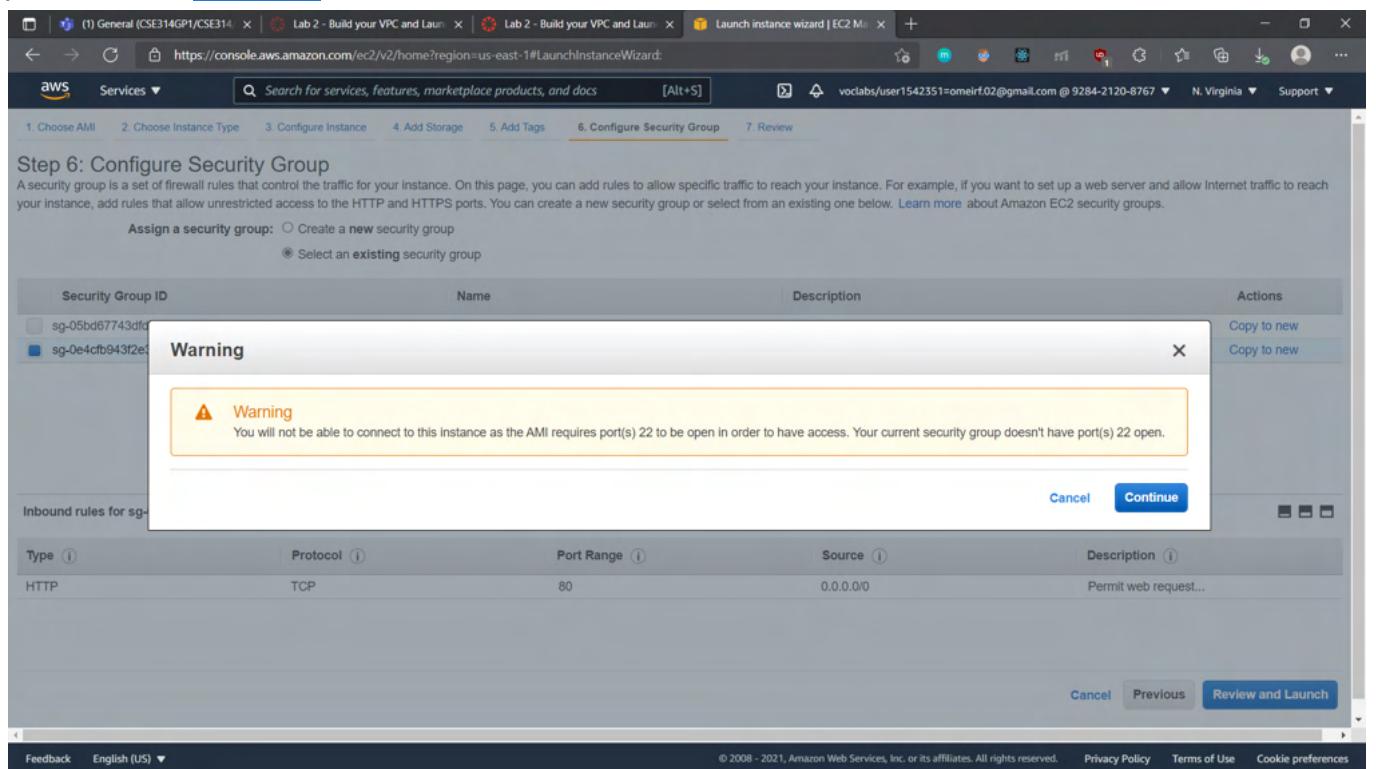
47. Select Web Security Group.

This is the security group you created in the previous task. It will permit HTTP access to the instance.

48. Click Review and Launch



49. When prompted with a *warning* that you will not be able to connect to the instance through port 22, click **Continue**



50. Review the instance information and click **Launch**

The screenshot shows the AWS Launch Instance Wizard Step 7: Review Instance Launch page. The page displays the configuration details for launching an instance. It includes sections for AMI Details, Instance Type, Security Groups, and a summary of selected security group inbound rules. The instance type chosen is t2.micro with 1 vCPU and 1 GiB of memory. The security group 'Web Security Group' is selected, allowing HTTP access on port 80. The review step is the final step before launching the instance.

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0c2b8ca1dad447f8a

Free tier eligible

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is a...
Root Device Type: ebs Virtualization type: hvm

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

Security Groups

Security Group ID	Name	Description
sg-0e4cfb943f2e335db	Web Security Group	Enable HTTP Access

All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	Permit web request...

Feedback English (US) ▾ © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. **Privacy Policy** **Terms of Use** **Cookie preferences**

Cancel Previous Launch

Step 7: Review Instance Launch

Security Group ID

Security Group ID	Name	Description
sg-0e4cfb943f2e335db	Web Security Group	Enable HTTP Access

All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	Permit web request...

Instance Details

Storage

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	snap-090e9376979c86d7b	8	gp2	100 / 3000	N/A	Yes	Not Encrypted

Tags

Key	Value	Instances	Volumes	Network Interfaces
Name	Web Server 1	□	□	□

Feedback English (US) ▾ © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. **Privacy Policy** **Terms of Use** **Cookie preferences**

Cancel Previous Launch

51. In the **Select an existing keypair** dialog, select **I acknowledge....**

52. Click **Launch Instances** and then click **View Instances**

The screenshot shows the AWS EC2 Launch Instance Wizard at Step 7: Review Instance Launch. On the left, there are sections for Instance Details, Storage (with a table for Volume Type, Device, Snapshot), and Tags (with a table for Name and Value). On the right, there are tabs for Description, Edit instance details, Edit storage, Encrypted (checkbox), Not Encrypted, Network Interfaces, and Edit tags. At the bottom, there are buttons for Cancel, Previous, and Launch.

Launch Status

Your instances are now launching. The following instance launches have been initiated: i-0a2f5eb800d4a6bf9 [View launch log](#)

Get notified of estimated charges [Create billing alerts](#) to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click [View Instances](#) to monitor your instances' status. Once your instances are in the **running** state, you can [connect](#) to them from the Instances screen. [Find out](#) how to connect to your instances.

Here are some helpful resources to get you started

- How to connect to your Linux instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes (Additional charges may apply)
- Manage security groups

[View Instances](#)

53. Wait until **Web Server 1** shows **2/2 checks passed** in the **Status Checks** column.

This may take a few minutes. Click **refresh** in the top-right every 30 seconds for updates. You will now connect to the web server running on the EC2 instance.

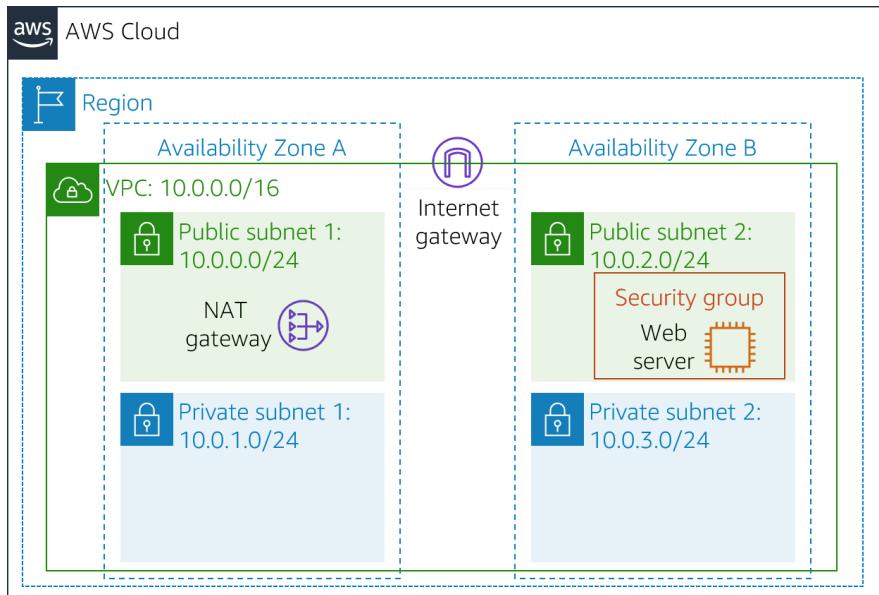
54. Copy the **Public DNS (IPv4)** value shown in the **Description** tab at the bottom of the page.

The screenshot shows the AWS EC2 Instances page. On the left sidebar, under 'Instances', 'Instances New' is selected. The main table lists two instances: 'Web Server 1' (running, t2.micro, Public IPv4 DNS: ec2-3-234-146-198.compute-1.amazonaws.com) and 'Bastion Host' (running, t2.micro, Public IPv4 DNS: ec2-52-201-252-). A tooltip on the right indicates that the Public IPv4 DNS has been copied. The 'Instance: i-0a2f5eb800d4a6bf9 (Web Server 1)' details pane is open, showing fields like IPv6 address, Instance state (Running), Instance type (t2.micro), Private IPv4 DNS (ip-10-0-2-7.ec2.internal), VPC ID (vpc-0d63cb6f9374a3ffb (Lab VPC)), AWS Compute Optimizer finding (User: arn:aws:sst:928421208767:assumed-role/voclabs/user1542351=omeirf.02@gmail.com is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: *), and IAM Role.

55. 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.

The screenshot shows a web browser window with the URL ec2-3-234-146-198.compute-1.amazonaws.com. The page displays the AWS logo and a table of instance meta-data. The table has two columns: 'Meta-Data' and 'Value'. The rows show 'InstanceId' with value 'i-0a2f5eb800d4a6bf9' and 'Availability Zone' with value 'us-east-1b'. Below the table, a message says 'Current CPU Load: 0%'.

The complete architecture you deployed is:



Public Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Internet gateway

Private Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	NAT gateway

Practical 3

AIM

Working with EBS (Elastic Block Storage)

THEORY

This lab focuses on Amazon Elastic Block Store (Amazon EBS), a key underlying storage mechanism for Amazon EC2 instances. In this lab, you will learn how to create an Amazon EBS volume, attach it to an instance, apply a file system to the volume, and then take a snapshot backup.



What is Amazon Elastic Block Store?

Amazon Elastic Block Store (Amazon EBS) offers persistent storage for Amazon EC2 instances. Amazon EBS volumes are network-attached and persist independently from the life of an instance. Amazon EBS volumes are highly available, highly reliable volumes that can be leveraged as an Amazon EC2 instances boot partition or attached to a running Amazon EC2 instance as a standard block device.

When used as a boot partition, Amazon EC2 instances can be stopped and subsequently restarted, enabling you to pay only for the storage resources used while maintaining your instance's state. Amazon EBS volumes offer greatly improved durability over local Amazon EC2 instance stores because Amazon EBS volumes are automatically replicated on the backend (in a single Availability Zone).

For those wanting even more durability, Amazon EBS provides the ability to create point-in-time consistent snapshots of your volumes that are then stored in Amazon Simple Storage Service (Amazon S3) and automatically replicated across multiple Availability Zones. These snapshots can be used as the starting point for new Amazon EBS volumes and can protect your data for long-term durability. You can also easily share these snapshots with co-workers and other AWS developers.

This lab guide explains basic concepts of Amazon EBS in a step-by-step fashion. However, it can only give a brief overview of Amazon EBS concepts. For further information, see the [Amazon EBS documentation](#).

Amazon EBS Volume Features

Amazon EBS volumes deliver the following features:

- **Persistent storage:** Volume lifetime is independent of any particular Amazon EC2 instance.

- **General purpose:** Amazon EBS volumes are raw, unformatted block devices that can be used from any operating system.
- **High performance:** Amazon EBS volumes are equal to or better than local Amazon EC2 drives.
- **High reliability:** Amazon EBS volumes have built-in redundancy within an Availability Zone.
- **Designed for resiliency:** The AFR (Annual Failure Rate) of Amazon EBS is between 0.1% and 1%.
- **Variable size:** Volume sizes range from 1 GB to 16 TB.
- **Easy to use:** Amazon EBS volumes can be easily created, attached, backed up, restored, and deleted.

PROCEDURE

Task 1: Create a New EBS Volume

1. In the AWS Management Console, on the Services menu, click EC2.
 2. In the left navigation pane, click Instances.
- An Amazon EC2 instance named Lab has already been launched for your lab.
3. Note the Availability Zone of the instance. It will look similar to us-west-2a.

The screenshot shows the AWS Management Console interface for the EC2 service. The left sidebar has a tree view with 'Instances' selected, which is further expanded to show 'Instances' (New). Other options like 'Images' and 'Elastic Block Store' are also visible. The main content area is titled 'Instances (2) Info' and lists two instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Lab	i-0cb27959ff252216b	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-3-237-197-8
Bastion Host	i-07675701405a1dec3	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-3-237-199-2

A modal window titled 'Select an instance above' is open over the list, indicating that an instance needs to be chosen for the next step.

4. In the left navigation pane, click 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.

The screenshot shows the AWS Cloud Computing Practical File interface. On the left, there's a sidebar with various AWS services like Instances, Images, and Elastic Block Store. The main area is titled 'Create Volume' and shows a table of existing volumes. A message at the bottom says 'Select a volume above'.

5. Click **Create Volume** then configure:

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

The screenshot shows the 'Create Volume' dialog box. It has fields for Volume Type (set to General Purpose SSD gp2), Size (1 GiB), IOPS (100 / 3000), Availability Zone (set to us-east-1a), Snapshot ID (Select a snapshot), and Encryption (Encrypt this volume). Below these, there's a 'Tags' section with a table for adding tags. One tag is added: Key: Name, Value: My Volume. At the bottom right are 'Cancel' and 'Create Volume' buttons.

6. Click **Create Volume** then click **Close**

Your new volume will appear in the list, and will move from the *creating* state to the *available* state.

state. You may need to click **refresh** to see your new volume.

The screenshot shows a browser window with the AWS Cloud Computing Practical File tab open. The URL is https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateVolume. The page displays a success message: "Volume created successfully" with a green checkmark icon. Below it, the Volume ID is listed as vol-0ca8a16e5d15112f6. A "Close" button is at the bottom right of the message box. At the bottom of the screen, there is a footer bar with links for Feedback, English (US), Privacy Policy, Terms of Use, and Cookie preferences.

Task 2: Attach the Volume to an Instance

You can now attach your new volume to the Amazon EC2 instance.

7. Select **My Volume**.

8. In the Actions menu, click **Attach Volume**.

The screenshot shows the AWS Cloud Computing Practical File interface. The left sidebar has "New EC2 Experience" selected. Under "Instances", "Instances" is highlighted. The main area shows a table of volumes. A context menu is open over a row for a volume named "My Volume". The menu options include: Modify Volume, Create Snapshot, Create Snapshot Lifecycle Policy, Delete Volume, **Attach Volume** (which is highlighted in blue), Detach Volume, Force Detach Volume, and Change Auto-Enable IO Setting. Below the table, a detailed view of the selected volume "vol-0ca8a16e5d15112f6 (My Volume)" is shown. The "Description" tab is selected, displaying details like Volume ID, Alarm status, Snapshot, Availability Zone, and State. Other tabs include Status Checks, Monitoring, and Tags. The footer bar at the bottom includes links for Feedback, English (US), Privacy Policy, Terms of Use, and Cookie preferences.

9. Click in the **Instance** field, then select the instance that appears (Lab).

The screenshot shows the AWS EC2 Attach Volume dialog box overlaid on the EC2 Management Console. In the dialog, the 'Volume' dropdown is set to 'vol-0ca8a16e5d15112f6 (My Volume) in us-east-1a'. The 'Instance' dropdown contains the value 'i-0cb27959ff252216b' with '(Lab) (running)' displayed below it. The 'Device' dropdown is set to '/dev/sdf'. A note at the bottom states: 'Note: 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.' At the bottom right of the dialog are 'Cancel' and 'Attach' buttons.

Note that the **Device** field is set to */dev/sdf*. You will use this device identifier in a later task.

This screenshot is identical to the one above, showing the Attach Volume dialog. The 'Device' field now has the value '/dev/sdf' entered. The rest of the dialog and the underlying EC2 Management Console interface remain the same.

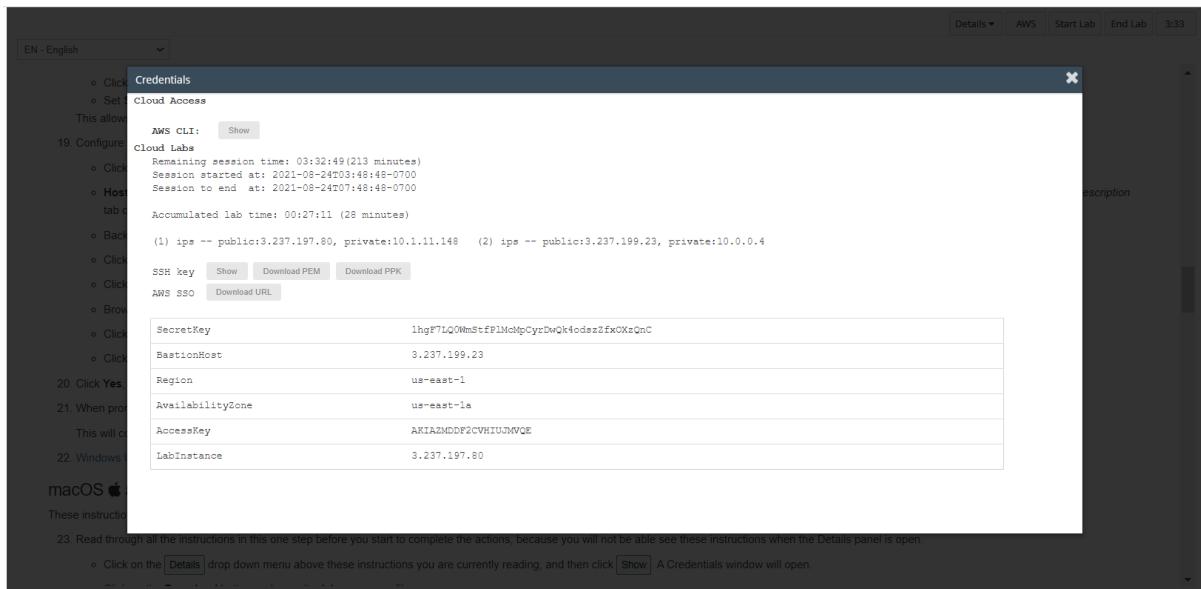
10. Click **Attach** The volume state is now *in-use*.

Task 3: Connect to Your Amazon EC2 Instance

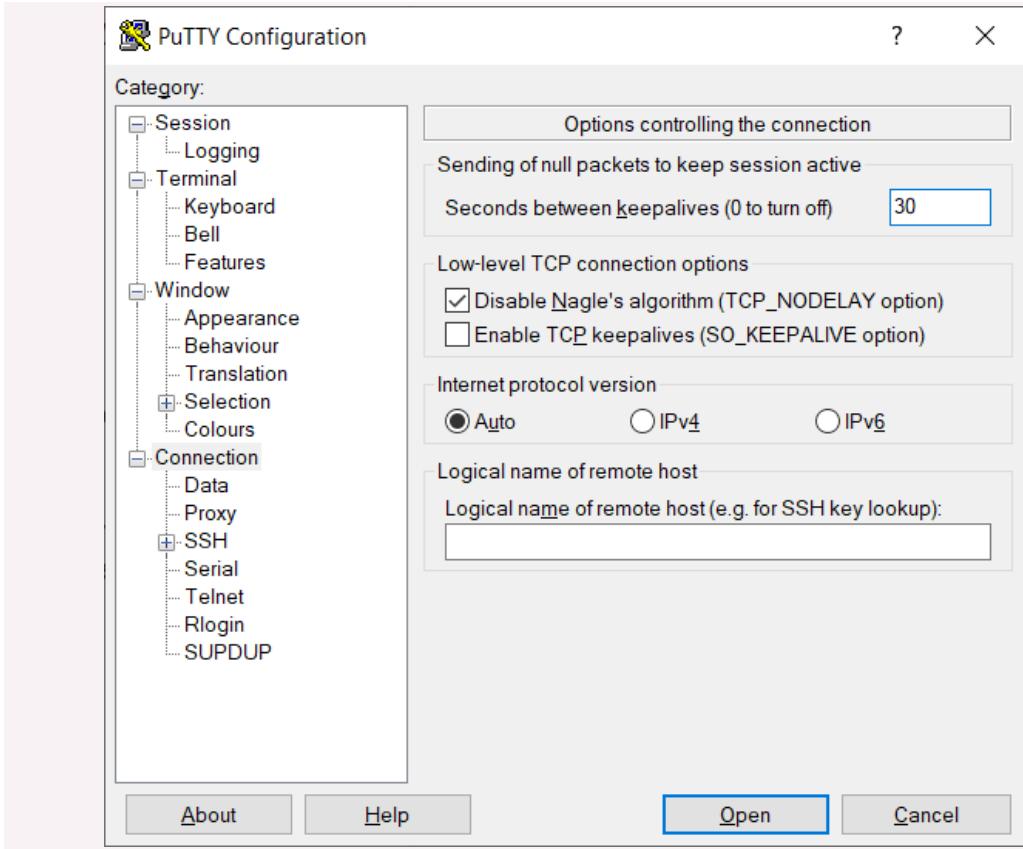
Windows Users: Using SSH to Connect

These instructions are for Windows users only.

1. Read through the three bullet points in this step before you start to complete the actions, because you will not be able see these instructions when the Details panel is open.
 - a. Click on the Details drop down menu above these instructions you are currently reading, and then click Show. A Credentials window will open.



- b. Click on the **Download PPK** button and save the **labsuser.ppk** file. Typically your browser will save it to the Downloads directory.
 - c. Then exit the Details panel by clicking on the **X**.
2. Download needed software.
 - a. You will use **PuTTY** to SSH to Amazon EC2 instances. If you do not have PuTTY installed on your computer, [download it here](#).
3. Open **putty.exe**
4. Configure PuTTY to not timeout:
 - a. Click **Connection**
 - b. Set **Seconds between keepalives** to **30**

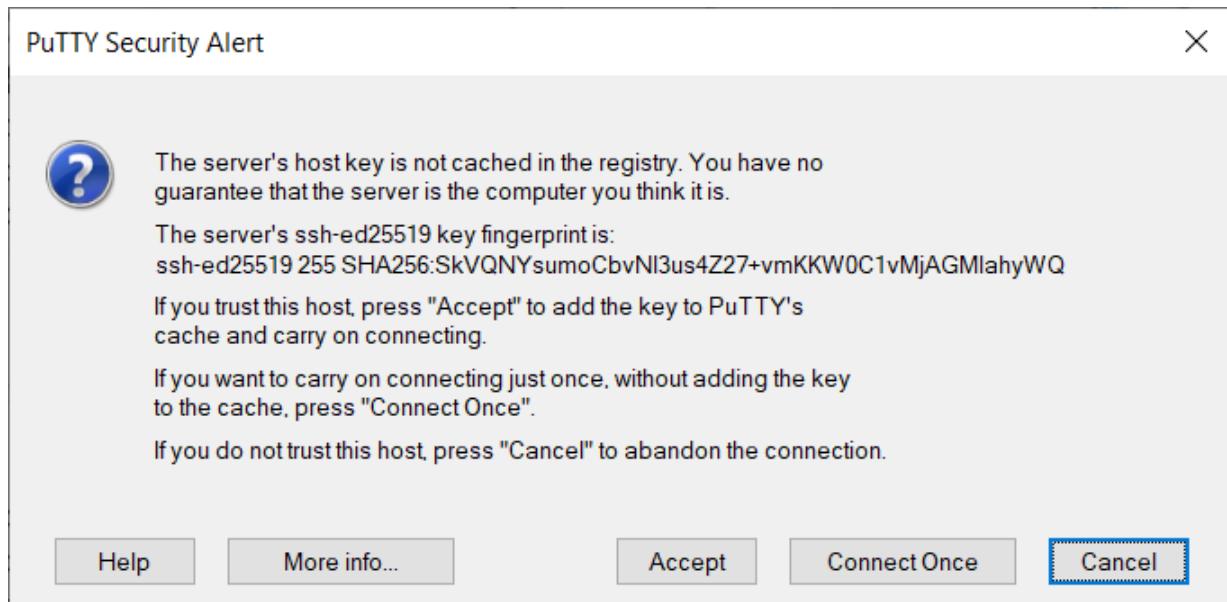


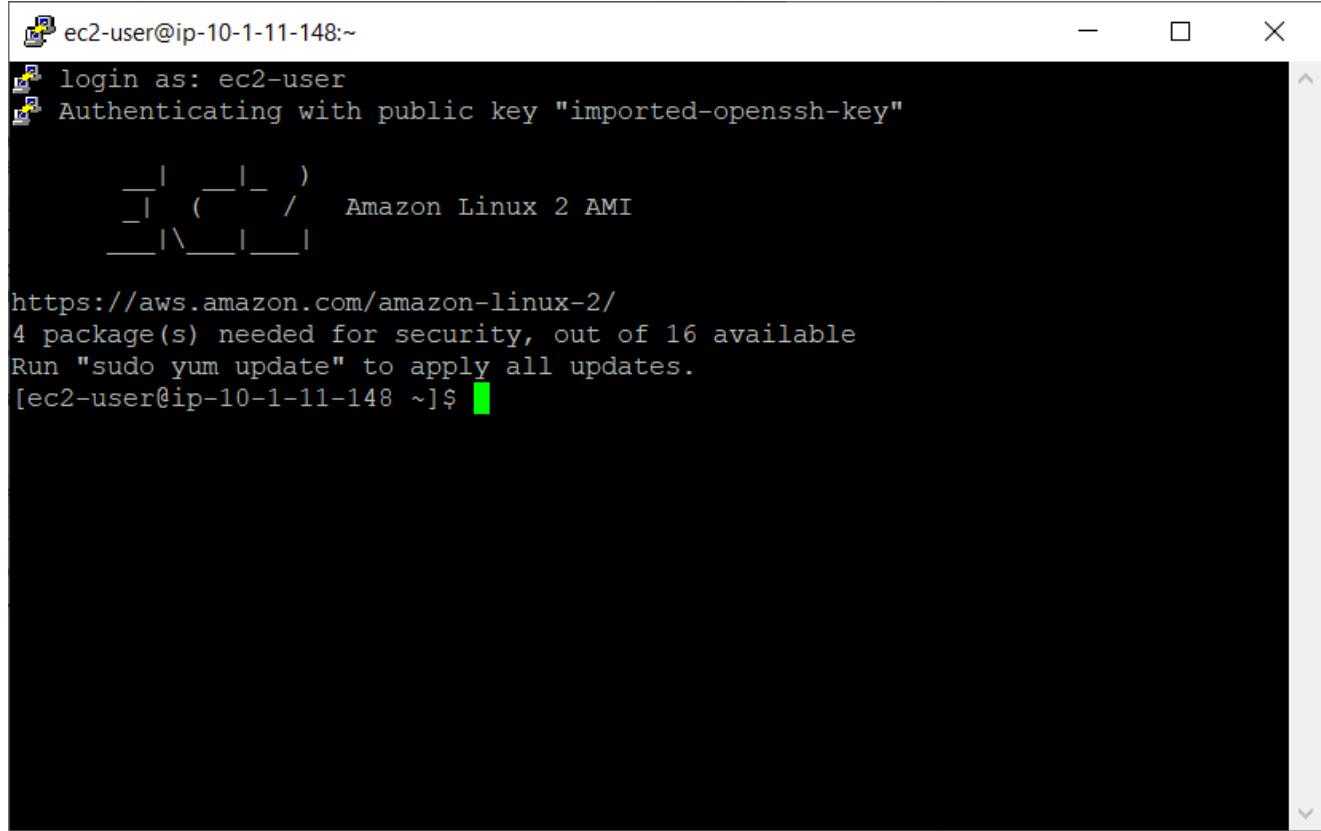
5. This allows you to keep the PuTTY session open for a longer period of time.
6. Configure your PuTTY session:
 - a. Click **Session**
 - b. **Host Name (or IP address)**: Copy and paste the **IPv4 Public IP address** for the instance. To find it, return to the EC2 Console and click on **Instances**. Check the box next to the instance and in the *Description* tab copy the **IPv4 Public IP** value.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Lab	i-0cb27959ff252216b	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-3-237-197-8
Bastion Host	i-07675701405a1dec3	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-3-237-199-2

- c. Back in PuTTY, in the **Connection** list, expand **SSH**
- d. Click **Auth** (don't expand it)
- e. Click **Browse**
- f. Browse to and select the labsuser.ppk file that you downloaded

- g. Click **Open** to select it
 - h. Click **Open**
7. Click **Yes**, to trust the host and connect to it.



8. When prompted **login as**, enter: **ec2-user**
This will connect you to the EC2 instance.
- 
- The terminal window shows the following output:
- ```
ec2-user@ip-10-1-11-148:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
[ec2-user@ip-10-1-11-148 ~]$
```
- The terminal window has a black background and white text. The prompt is "ec2-user@ip-10-1-11-148:~". The command "login as: ec2-user" is entered. The message "Authenticating with public key "imported-openssh-key"" follows. A logo consisting of four blue squares is displayed. The text "Amazon Linux 2 AMI" is shown below the logo. The URL "https://aws.amazon.com/amazon-linux-2/" is listed, followed by the message "4 package(s) needed for security, out of 16 available". The command "[ec2-user@ip-10-1-11-148 ~]\$" is at the bottom, with a green cursor bar.

## 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.

If you are using PuTTY, you can paste text by right-clicking in the PuTTY window.

1. View the storage available on your instance:

```
df -h
```

You should see output similar to:

| Filesystem | Size | Used | Avail | Use% | Mounted on |
|------------|------|------|-------|------|------------|
| devtmpfs   | 488M | 60K  | 488M  | 1%   | /dev       |
| tmpfs      | 497M | 0    | 497M  | 0%   | /dev/shm   |
| /dev/xvda1 | 7.8G | 982M | 6.7G  | 13%  | /          |

The screenshot shows a PuTTY terminal window. The title bar says "ec2-user@ip-10-1-11-148:~". The session log shows:

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"

 _\ _
 _ \ | _ / Amazon Linux 2 AMI
 __| __|_|

https://aws.amazon.com/amazon-linux-2/
4 package(s) needed for security, out of 16 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-1-11-148 ~]$ df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 482M 0 482M 0% /dev
tmpfs 492M 0 492M 0% /dev/shm
tmpfs 492M 460K 492M 1% /run
tmpfs 492M 0 492M 0% /sys/fs/cgroup
/dev/xvda1 8.0G 1.5G 6.6G 19% /
tmpfs 99M 0 99M 0% /run/user/0
tmpfs 99M 0 99M 0% /run/user/1000
[ec2-user@ip-10-1-11-148 ~]$
```

This is showing the original 8GB disk volume. Your new volume is not yet shown.

2. Create an ext3 file system on the new volume:

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

```
ec2-user@ip-10-1-11-148:~$ sudo mkfs -t ext3 /dev/sdf
mke2fs 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
8 block groups
32768 blocks per group, 32768 fragments per group
8192 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-10-1-11-148 ~]$
```

3. Create a directory for mounting the new storage volume:

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

4. 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
```

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

```
cat /etc/fstab
```

6. View the available storage again:

```
df -h
```

The output will now contain an additional line - `/dev/xvdf`:

| Filesystem | Size | Used | Avail | Use% | Mounted on      |
|------------|------|------|-------|------|-----------------|
| devtmpfs   | 488M | 60K  | 488M  | 1%   | /dev            |
| tmpfs      | 497M | 0    | 497M  | 0%   | /dev/shm        |
| /dev/xvda1 | 7.8G | 982M | 6.7G  | 13%  | /               |
| /dev/xvdf  | 976M | 1.3M | 924M  | 1%   | /mnt/data-store |

7. 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"
```

8. Verify that the text has been written to your volume.

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

```

[ec2-user@ip-10-1-11-148 ~]$ sudo mkdir /mnt/data-store
[ec2-user@ip-10-1-11-148 ~]$ sudo mount /dev/sdf /mnt/data-store
[ec2-user@ip-10-1-11-148 ~]$ 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-10-1-11-148 ~]$ cat /etc/fstab
#
UUID=04b92f2f-4366-4687-868b-7c403cc59901 /
/dev/sdf /mnt/data-store ext3 defaults,noatime 1 2
[ec2-user@ip-10-1-11-148 ~]$ df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 482M 0B 482M 0% /dev
tmpfs 492M 0B 492M 0% /dev/shm
tmpfs 492M 460K 492M 1% /run
tmpfs 492M 0B 492M 0% /sys/fs/cgroup
/dev/xvda1 8.0G 1.5G 6.6G 19% /
tmpfs 99M 0B 99M 0% /run/user/0
tmpfs 99M 0B 99M 0% /run/user/1000
/dev/xvdf 976M 1.3M 924M 1% /mnt/data-store
[ec2-user@ip-10-1-11-148 ~]$ sudo sh -c "echo some text has been written > /mnt/data-store/file.txt"
[ec2-user@ip-10-1-11-148 ~]$ cat /mnt/data-store/file.txt
some text has been written
[ec2-user@ip-10-1-11-148 ~]$

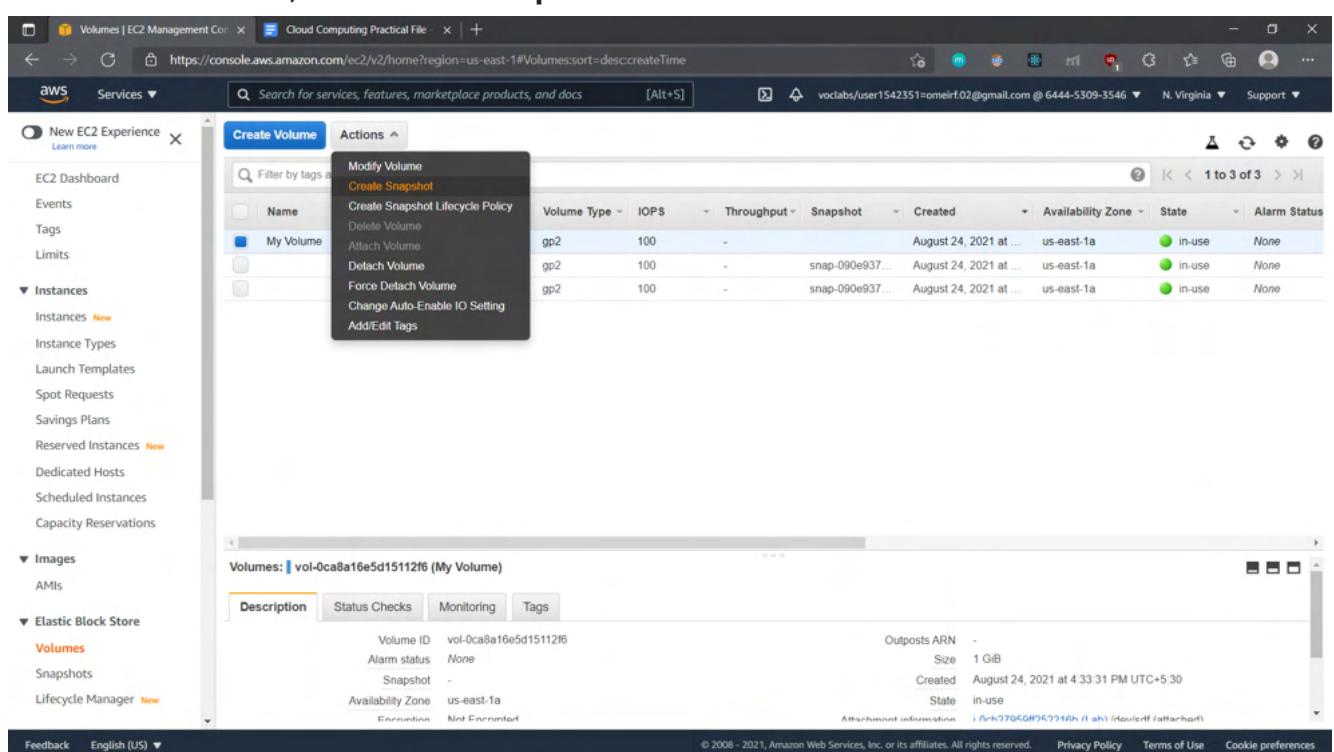
```

## Task 5: Create an Amazon EBS Snapshot

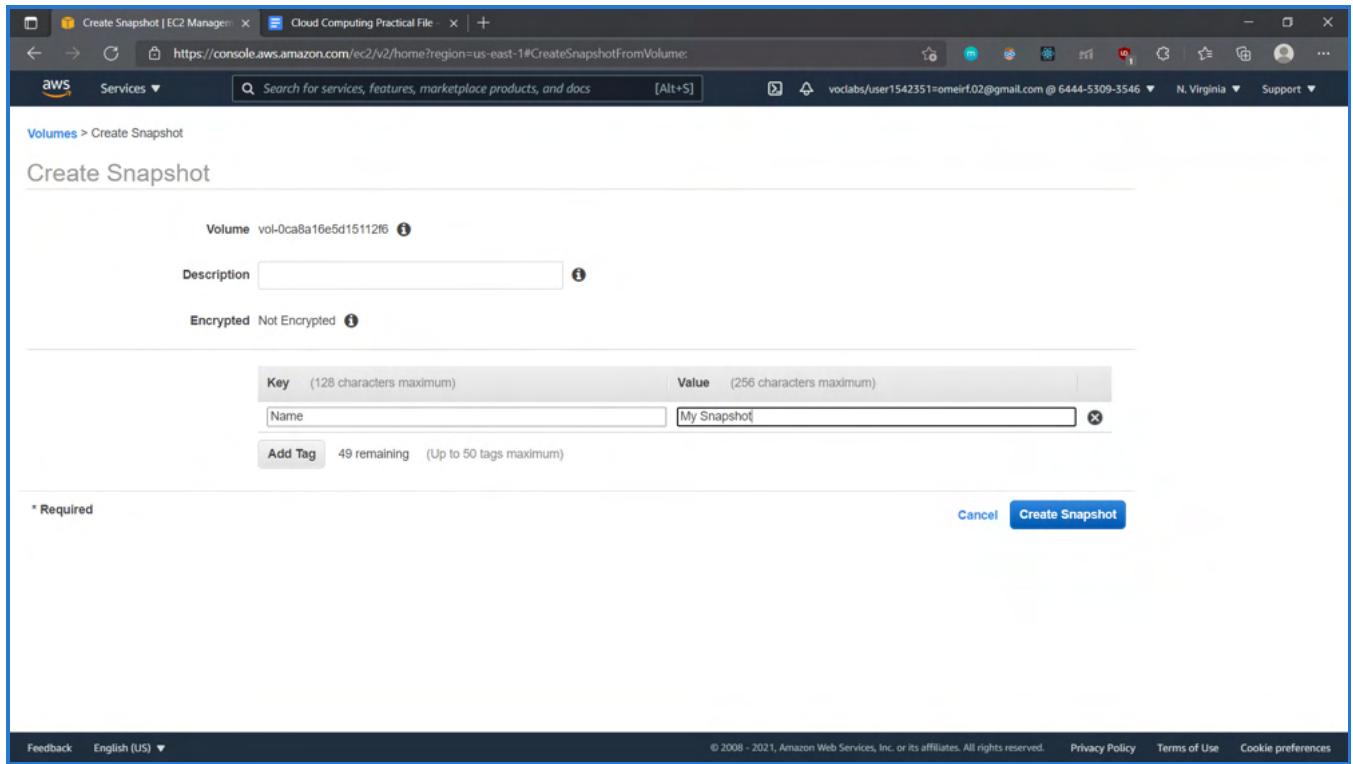
In this task, you will create a snapshot of your EBS volume.

You can create any number of point-in-time, consistent snapshots from Amazon EBS volumes at any time. Amazon EBS snapshots are stored in Amazon S3 with high durability. New Amazon EBS volumes can be created out of snapshots for cloning or restoring backups. Amazon EBS snapshots can also be easily shared among AWS users or copied over AWS regions.

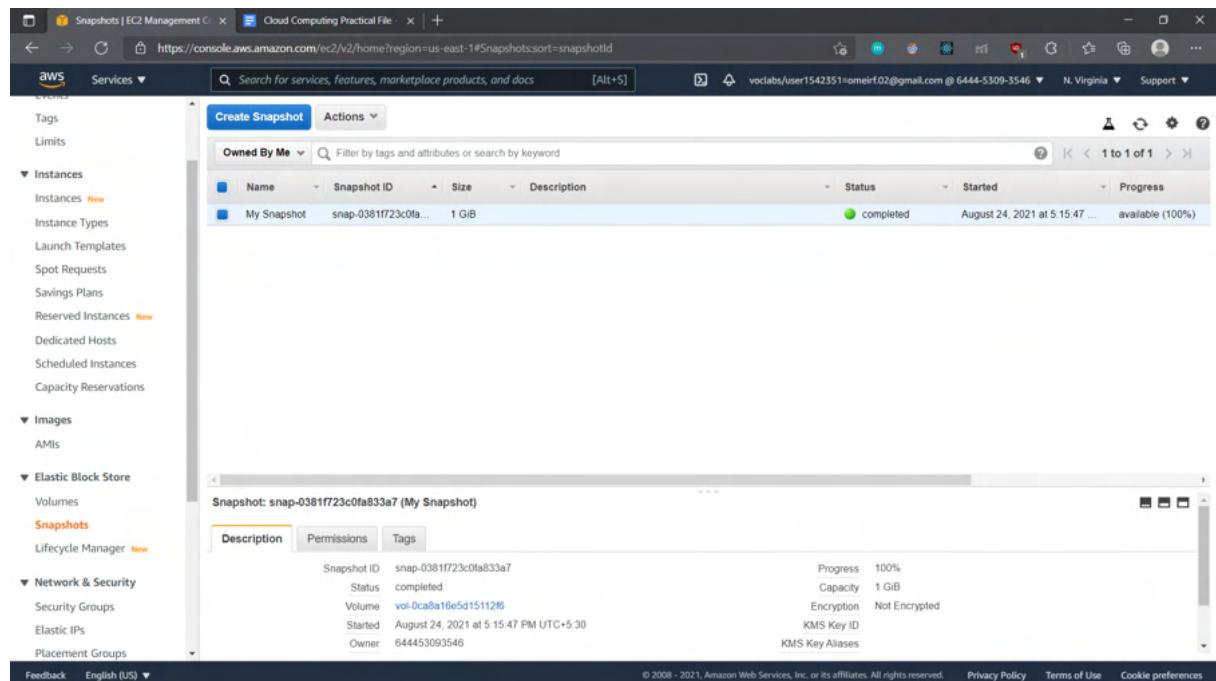
1. In the **AWS Management Console**, click on **Volumes** and select **My Volume**.
2. In the **Actions** menu, click **Create Snapshot**.



3. Click **Add Tag** then configure:
  - a. **Key:** Name
  - b. **Value:** My Snapshot
  - c. Click **Create Snapshot** then click **Close**



4. Your snapshot will be listed in the **Snapshots** console.
5. In the left navigation pane, click **Snapshots**.  
Your snapshot is displayed. It will start with a state of *pending*, which means that the snapshot is being created. It will then change to a state of *completed*. Only used storage blocks are copied to snapshots, so empty blocks do not take any snapshot storage space.



6. In your remote SSH session, delete the file that you created on your volume.  
`sudo rm /mnt/data-store/file.txt`

7. Verify that the file has been deleted.

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

Your file has been deleted.

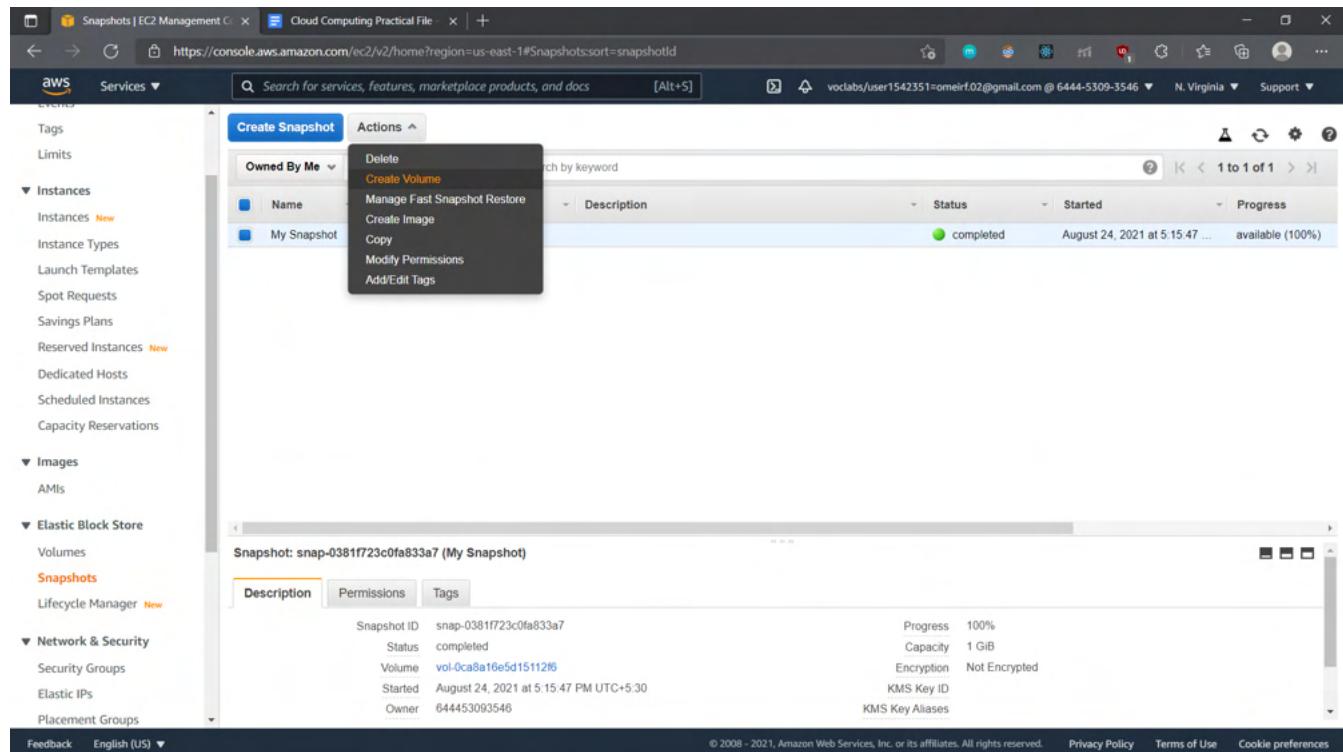
```
[ec2-user@ip-10-1-11-148 ~]$ sudo rm /mnt/data-store/file.txt
[ec2-user@ip-10-1-11-148 ~]$ ls /mnt/data-store/
lost+found
[ec2-user@ip-10-1-11-148 ~]$
```

## Task 6: Restore the Amazon EBS Snapshot

If you ever wish to retrieve data stored in a snapshot, you can **Restore** the snapshot to a new EBS volume.

### Create a Volume Using Your Snapshot

1. In the **AWS Management Console**, select **My Snapshot**.
2. In the **Actions** menu, click **Create Volume**.



3. For **Availability Zone** Select the same availability zone that you used earlier.
4. Click **Add Tag** then configure:
  - a. **Key:** `Name`
  - b. **Value:** `Restored Volume`

Screenshot of the AWS Cloud Computing Practical File showing the 'Create Volume' wizard. The 'Volume Type' is set to 'General Purpose SSD (gp2)'. The 'Size (GiB)' is set to 1. The 'IOPS' is set to 100 / 3000. The 'Throughput (MB/s)' is set to 'Not applicable'. The 'Availability Zone' is set to 'us-east-1a'. The 'Encryption' checkbox is unchecked. A tag 'Name' is added with the value 'Restored Volume'. The 'Create Volume' button is highlighted.

5. Click **Create Volume**
6. Click **Close**

When restoring a snapshot to a new volume, you can also modify the configuration, such as changing the volume type, size or Availability Zone.

## Attach the Restored Volume to Your EC2 Instance

1. In the left navigation pane, click **Volumes**.
2. Select **Restored Volume**.
3. In the Actions menu, click **Attach Volume**.

Screenshot of the AWS Cloud Computing Practical File showing the 'Volumes' section. The 'Actions' menu for a 'Restored Volume' is open, with 'Attach Volume' selected. The main table lists four volumes, all of which are currently attached ('in-use') to EC2 instances in the 'us-east-1a' availability zone. The bottom section shows detailed information for the selected volume, including its ID, snapshot, and creation date.

| Volume Type | IOPS | Snapshot               | Created                | Availability Zone | State     | Alarm Status |
|-------------|------|------------------------|------------------------|-------------------|-----------|--------------|
| gp2         | 100  | snap-0381f723c0fa833a7 | August 24, 2021 at ... | us-east-1a        | available | None         |
| gp2         | 100  | snap-090e937...        | August 24, 2021 at ... | us-east-1a        | in-use    | None         |
| gp2         | 100  | snap-090e937...        | August 24, 2021 at ... | us-east-1a        | in-use    | None         |
| gp2         | 100  | snap-090e937...        | August 24, 2021 at ... | us-east-1a        | in-use    | None         |

4. Click in the **Instance** field, then select the instance that appears (Lab).

The screenshot shows the AWS Cloud Computing Practical File interface. On the left, the navigation pane includes 'EC2 Dashboard', 'Events', 'Tags', 'Limits', 'Instances' (selected), 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', 'Scheduled Instances', 'Capacity Reservations', 'Images', 'AMIs', and 'Elastic Block Store' (selected). In the center, a table lists volumes: 'Restored Vol...', 'My Volume', 'vol-0e4092ef...', and 'vol-0e9d9...'. Below the table, a modal window titled 'Attach Volume' is open. It shows the 'Volume' as 'vol-03e73db5a44094c55 (Restored Volume) in us-east-1a'. The 'Instance' field contains 'Search Instance ID or Name tag' and 'i-0cb27959ff252216b (Lab) (running)'. The 'Device' field is set to '/dev/sdg'. At the bottom right of the modal are 'Cancel' and 'Attach' buttons.

Note that the **Device** field is set to **/dev/sdg**. You will use this device identifier in a later task.

This screenshot is identical to the previous one, but the 'Device' field in the 'Attach Volume' dialog is explicitly set to '/dev/sdg'.

5. Click **Attach**

The volume state is now *in-use*.

## Mount the Restored Volume

53. Create a directory for mounting the new storage volume:

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

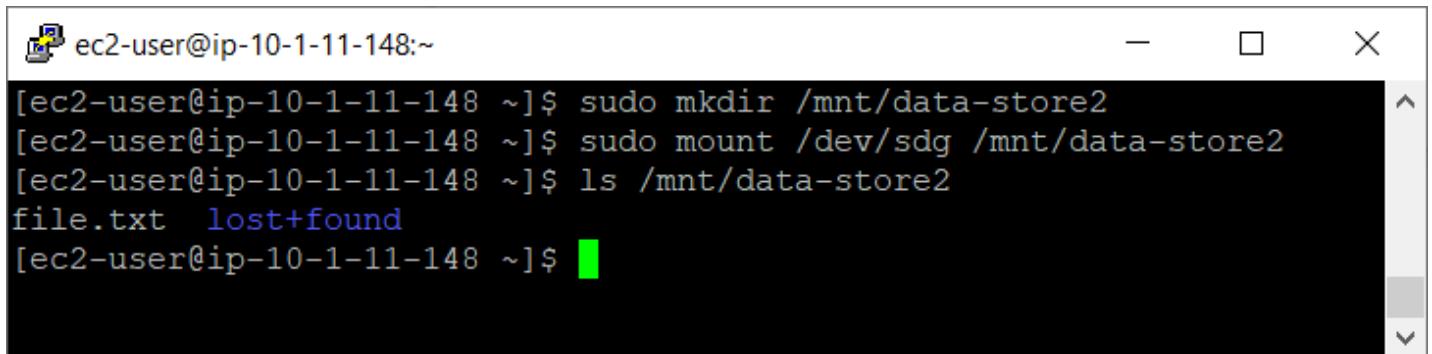
54. Mount the new volume:

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

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

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

You should see file.txt.



```
ec2-user@ip-10-1-11-148:~$ sudo mkdir /mnt/data-store2
[ec2-user@ip-10-1-11-148 ~]$ sudo mount /dev/sdg /mnt/data-store2
[ec2-user@ip-10-1-11-148 ~]$ ls /mnt/data-store2
file.txt lost+found
[ec2-user@ip-10-1-11-148 ~]$
```

## CONCLUSION

Congratulations! You now have successfully:

- Created an Amazon EBS volume
- Attached the volume to an EC2 instance
- Created a file system on the volume
- Added a file to volume
- Created a snapshot of your volume
- Created a new volume from the snapshot
- Attached and mounted the new volume to your EC2 instance
- Verified that the file you created earlier was on the newly created volume

# Practical 4

## AIM

Build Your DB Server and Interact With Your DB Using an App

## THEORY

This lab is designed to reinforce the concept of leveraging an AWS-managed database instance for solving relational database needs.

**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.

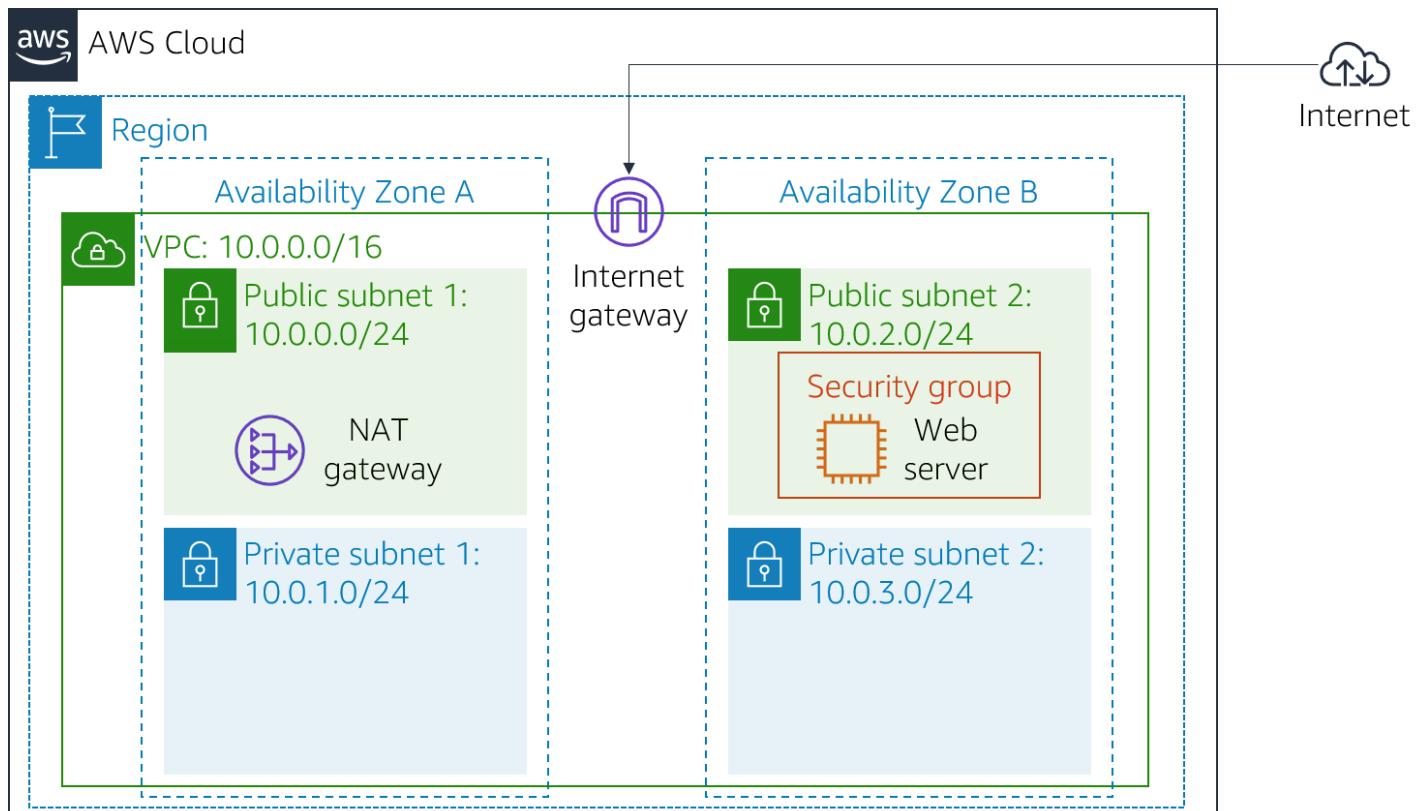
## OBJECTIVES

After completing this lab, you can:

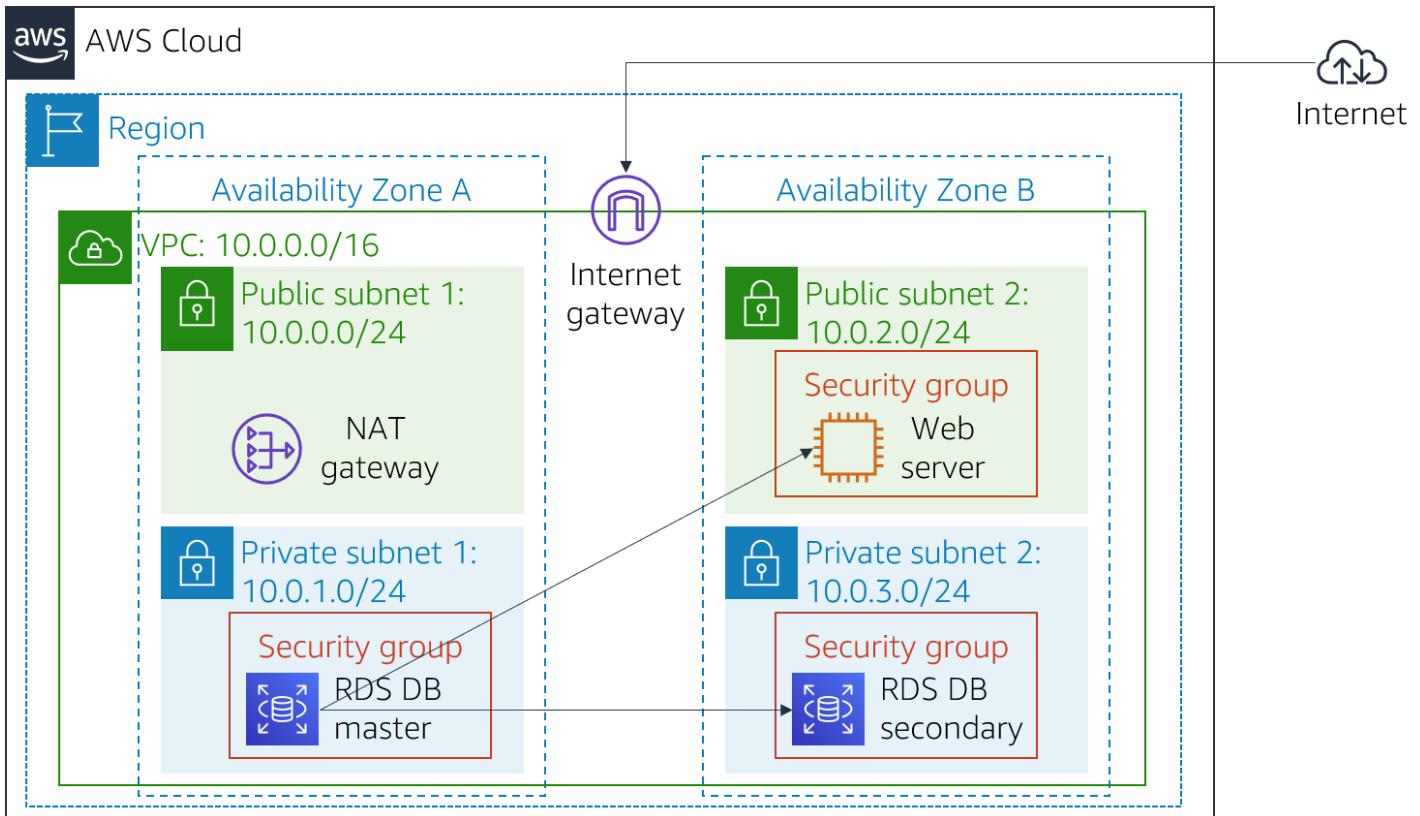
- Launch an Amazon RDS DB instance with high availability.
- Configure the DB instance to permit connections from your web server.
- Open a web application and interact with your database.

## PROCEDURE

Infrastructure before this lab:



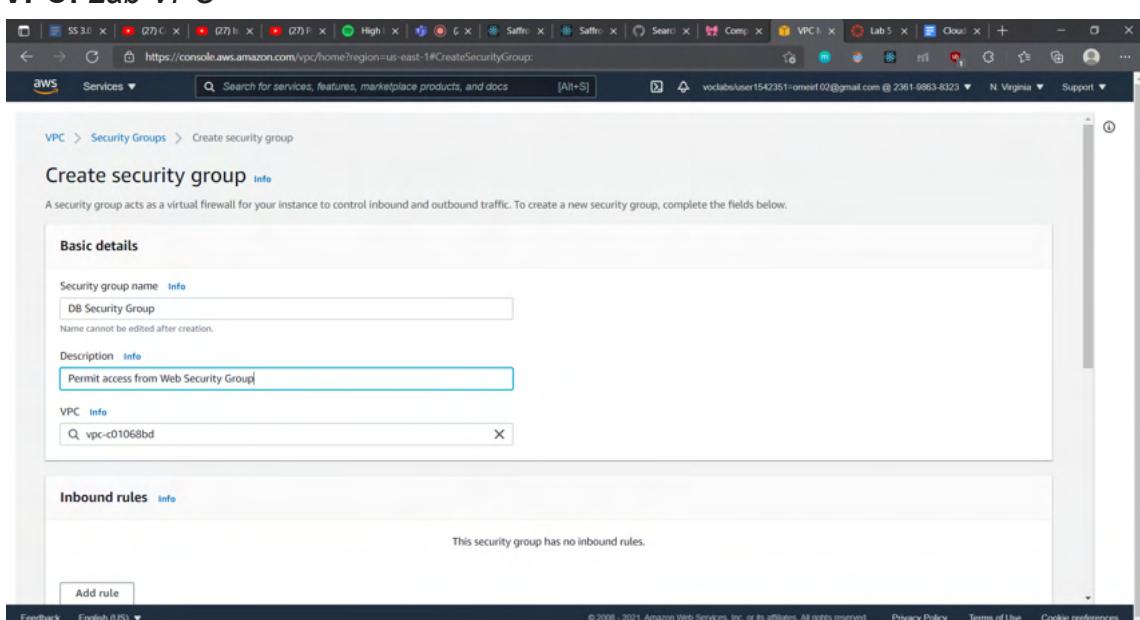
Infrastructure after this lab:



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

In this task, you will create a security group to allow your web server to access your RDS DB instance. The security group will be used when you launch the database instance.

5. In the **AWS Management Console**, on the **Services** menu, click **VPC**.
6. In the left navigation pane, click **Security Groups**.
7. Click **Create security group** and then configure:
  - o **Security group name:** DB Security Group
  - o **Description:** Permit access from Web Security Group
  - o **VPC:** Lab VPC



8. You will now add a rule to the security group to permit inbound database requests.
9. In the **Inbound rules** pane, choose **Add rule**  
The security group currently has no rules. You will add a rule to permit access from the *Web Security Group*.
10. Configure the following settings:
  - **Type:** MySQL/Aurora (3306)
  - **CIDR, IP, Security Group or Prefix List:** Type sg and then select *Web Security Group*.
11. This configures the Database security group to permit inbound traffic on port 3306 from any EC2 instance that is associated with the *Web Security Group*.
12. Choose **Create security group**

You will use this security group when launching the Amazon RDS database.

| Security group rule ID | Type         | Protocol | Port range | Source | Description - optional |
|------------------------|--------------|----------|------------|--------|------------------------|
| sgr-0fb1f29bedb11ca8   | SSH          | TCP      | 22         | Custom | 0.0.0.0/0              |
| sgr-0227c3377ce1b1021  | HTTP         | TCP      | 80         | Custom | 0.0.0.0/0              |
| -                      | MySQL/Aurora | TCP      | 3306       | Custom | sg-0bb9fe462a8835e5f   |

## Task 2: Create a DB Subnet Group

In this task, you will create a *DB subnet group* that is used to tell RDS which subnets can be used for the database. Each DB subnet group requires subnets in at least two Availability Zones.

11. On the **Services** menu, click **RDS**.
12. In the left navigation pane, click **Subnet groups**.  
If the navigation pane is not visible, click the **menu** icon in the top-left corner.
13. Click **Create DB Subnet Group** then configure:
  - **Name:** DB-Subnet-Group
  - **Description:** DB Subnet Group
  - **VPC:** Lab VPC

Amazon RDS > Subnet groups > Create DB Subnet Group

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.

**Add subnets**

Availability Zones

Feedback English (US) ▾ Type here to search Privacy Policy Terms of Use Cookie preferences 04:36 PM 03-09-2021

14. Scroll down to the **Add Subnets** section.

15. Expand the list of values under **Availability Zones** and select the first two zones: **us-east-1a** and **us-east-1b**.

Amazon RDS > Subnet groups > Create DB Subnet Group

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.

**Add subnets**

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

us-east-1a  
 us-east-1b  
 us-east-1c  
 us-east-1d  
 us-east-1e  
 us-east-1f

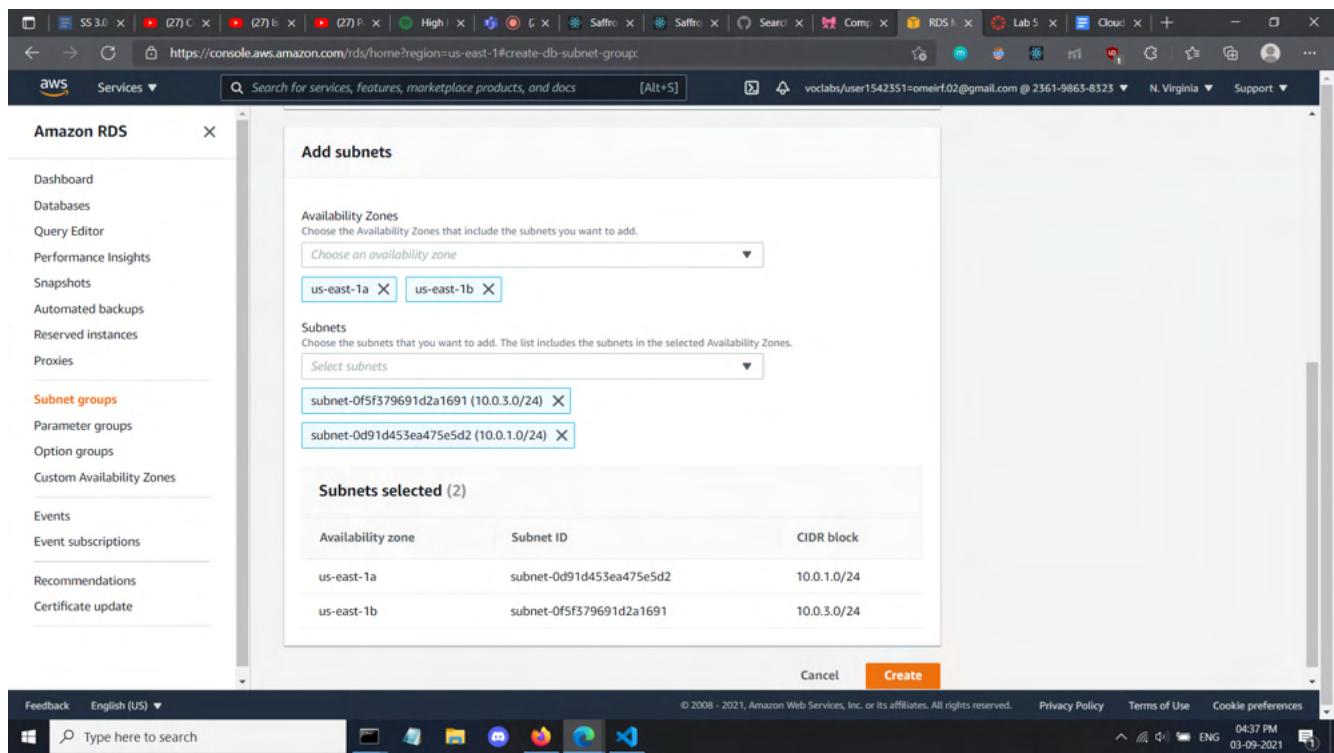
**Subnets selected (0)**

| Availability zone              | Subnet ID | CIDR block |
|--------------------------------|-----------|------------|
| No subnets added to this group |           |            |

Feedback English (US) ▾ Type here to search Privacy Policy Terms of Use Cookie preferences 04:36 PM 03-09-2021

16. 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.



## 17. Click **Create**

You will use this DB subnet group when creating the database in the next task.

## Task 3: Create an Amazon RDS DB Instance

In this task, you will configure and launch a Multi-AZ Amazon RDS for MySQL database instance.

Amazon RDS **Multi-AZ** deployments provide enhanced availability and durability for Database (DB) instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB instance, Amazon RDS automatically creates a primary DB instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ).

## 18. In the left navigation pane, click **Databases**.

## 19. Click **Create database**

If you see **Switch to the new database creation flow** at the top of the screen, please click.

The screenshot shows the AWS RDS console with the URL <https://console.aws.amazon.com/rds/home?region=us-east-1#databases>. A green banner at the top says "Successfully created DB-Subnet-Group. View subnet group". The left sidebar is titled "Amazon RDS" and includes sections like Dashboard, Databases (selected), Query Editor, Performance Insights, Snapshots, Automated backups, Reserved instances, Proxies, Subnet groups, Parameter groups, Option groups, Custom Availability Zones, Events, Event subscriptions, Recommendations, and Certificate update. The main content area shows a table titled "Databases" with a single row: "DB identifier" (lab-db). The table has columns for Role, Engine, Region & AZ, Size, Status, CPU, and Current activity. A message at the bottom says "No instances found". The bottom of the screen shows the Windows taskbar with various icons and the system tray.

## 20. Select MySQL.

### 21. Under Settings, configure:

- **DB instance identifier:** lab-db
- **Master username:** main
- **Master password:** lab-password
- **Confirm password:** lab-password

The screenshot shows the "Settings" configuration page for a new DB instance. The "DB instance identifier" field is set to "lab-db". The "Master username" field is set to "main". The "Master password" field contains "\*\*\*\*\*". The "Confirm password" field also contains "\*\*\*\*\*". Below the master password field, a note states: "Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote), "(double quote) and @ (at sign)." The "Credentials Settings" section is expanded, showing the "Auto generate a password" checkbox is unchecked. The "Master password" field has a note: "1 to 16 alphanumeric characters. First character must be a letter".

### 22. Under DB instance size, configure:

- Select **Burstable classes (includes t classes)**.
- Select ***db.t3.micro***

## DB instance class

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

23. Under **Storage**, configure:

- **Storage type: General Purpose (SSD)**
- **Allocated storage: 20**

## Storage

Storage type [Info](#)

General Purpose SSD (gp2)



Allocated storage

20

GiB

(Minimum: 20 GiB. Maximum: 16,384 GiB) Higher allocated storage [may improve](#) IOPS performance.

**i** Provisioning less than 100 GiB of General Purpose (SSD) storage for high throughput workloads could result in higher latencies upon exhaustion of the initial General Purpose (SSD) IO credit balance. [Learn more](#)

## Storage autoscaling [Info](#)

Provides dynamic scaling support for your database's storage based on your application's needs.

Enable storage autoscaling

Enabling this feature will allow the storage to increase once the specified threshold is exceeded.

## Maximum storage threshold [Info](#)

Charges will apply when your database autoscales to the specified threshold

1000

GiB

Minimum: 21 GiB. Maximum: 16,384 GiB

24. Under **Connectivity**, configure:

- **Virtual Private Cloud (VPC): Lab VPC**

## Connectivity



### Virtual private cloud (VPC) [Info](#)

VPC that defines the virtual networking environment for this DB instance.

Lab VPC (vpc-0a1f91d6fc63c5c8c)



Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

### Subnet group [Info](#)

DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

db-subnet-group



### Public access [Info](#)

Yes

Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.

No

RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

### VPC security group

Choose a VPC security group to allow access to your database. Ensure that the security group rules allow the appropriate incoming traffic.

Choose existing

Choose existing VPC security groups

Create new

Create new VPC security group

25. Under **Existing VPC security groups**, from the dropdown list:

- Choose *DB Security Group*.
- Deselect *default*.

### Existing VPC security groups

Choose VPC security groups



Web Security Group

26. Expand **Additional configuration**, then configure:

- Initial database name:** lab
- Uncheck **Enable automatic backups**.
- Uncheck **Enable Enhanced monitoring**.

## ▼ Additional configuration

Database options, encryption enabled, backup disabled, backtrack disabled, Enhanced Monitoring disabled, maintenance, CloudWatch Logs, delete protection enabled

### Database options

Initial database name [Info](#)

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

DB parameter group [Info](#)



Option group [Info](#)



### 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](#)

AWS KMS Key [Info](#)



### Account

236198638323

### KMS key ID

alias/aws/rds

### Monitoring

Enable Enhanced monitoring

Enabling Enhanced monitoring metrics are useful when you want to see how different processes or threads use the CPU

### Log exports

Select the log types to publish to Amazon CloudWatch Logs

- Audit log
- Error log
- General log
- Slow query log

### IAM role

The following service-linked role is used for publishing logs to CloudWatch Logs.

Ensure that general, slow query, and audit logs are turned on. Error logs are enabled by default. [Learn more](#)

### Maintenance

Auto minor version upgrade [Info](#)

Enable auto minor version upgrade

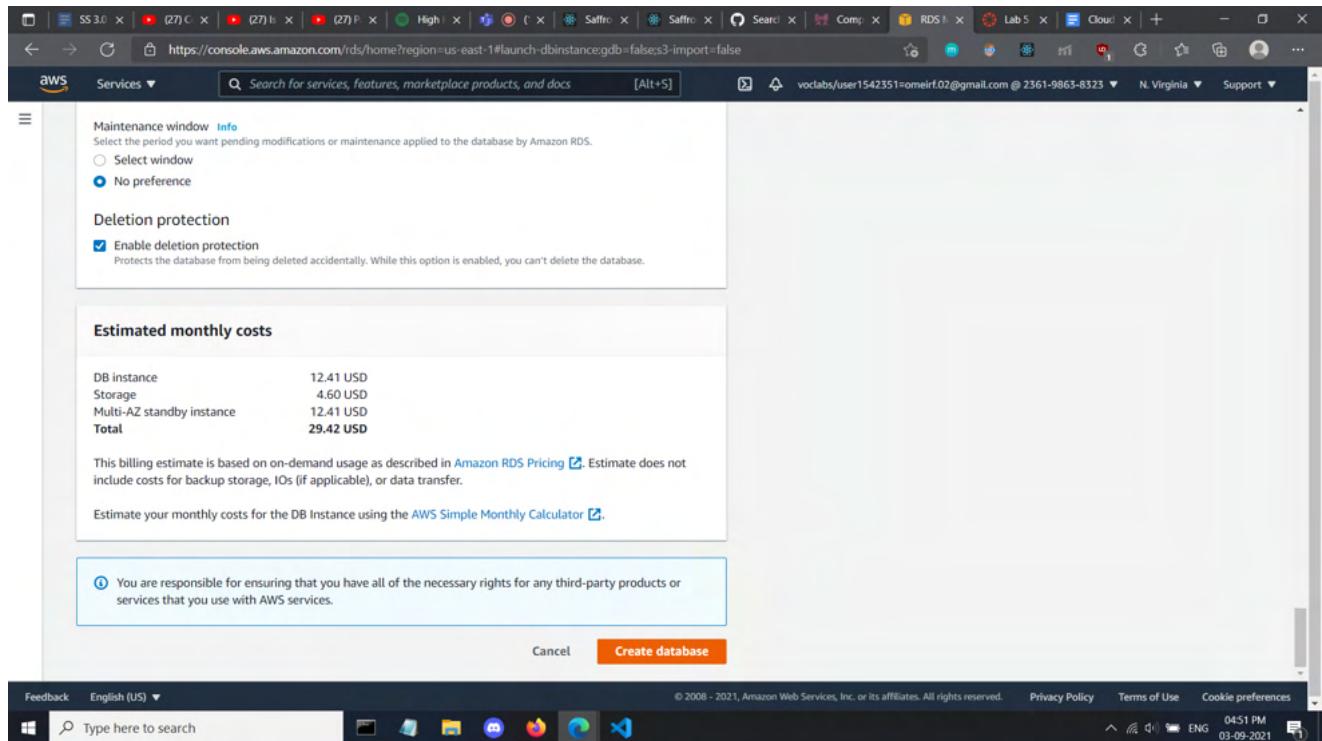
Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the

27. This will turn off backups, which is not normally recommended, but will make the database deploy faster for this lab.

28. Click **Create database**

Your database will now be launched.

If you receive an error that mentions "not authorized to perform: iam:CreateRole", make sure you unchecked *Enable Enhanced monitoring* in the previous step.



29. Click **lab-db** (click the link itself).

You will now need to wait **approximately 4 minutes** for the database to be available. The deployment process is deploying a database in two different Availability zones.

While you are waiting, you might want to review the [Amazon RDS FAQs](#) or grab a cup of coffee.

The screenshot shows the AWS RDS console with the URL <https://console.aws.amazon.com/rds/home?region=us-east-1#databases>. On the left, a sidebar menu is open under 'Databases', showing various options like Dashboard, Query Editor, and Performance Insights. The main area is titled 'Creating database lab-db' and displays a table of databases. A single row for 'lab-db' is visible, showing it's an 'Instance' of 'MySQL Community' engine, size 'db.t3.micro', and status 'Creating'. At the top right of the main area, there is a red 'Create database' button.

### 30. Wait until Info changes to Modifying or Available.

The screenshot shows the AWS RDS console with the URL <https://console.aws.amazon.com/rds/home?region=us-east-1#databaseid=lab-db&is-cluster=false>. The left sidebar is identical to the previous screenshot. The main page shows the 'lab-db' database details. In the 'Summary' section, the 'Status' field is now 'Modifying'. Below this, the 'Connectivity & security' tab is selected, showing the 'Endpoint & port' section with the value 'lab-db.cg5zs8byoxn.us-east-1.rds.amazonaws.com'.

### 31. Scroll down to the **Connectivity & security** section and copy the **Endpoint** field.

It will look similar to: *lab-db.cg5zs8byoxn.us-east-1.rds.amazonaws.com*

### 32. Paste the Endpoint value into a text editor. You will use it later in the lab.

## Task 4: Interact with Your Database

In this task, you will open a web application running on your web server and configure it to use the database.

32. To copy the **WebServer** IP address, click on the Details drop down menu above these instructions, and then click Show.

EN - English

AWS: **Show**

You will now need to wait **approximately 4 minutes** for the database to be available. The deployment process is deploying a database in two different Availability zones.

While you are waiting, you might want to review the [Amazon RDS FAQs](#) or grab a cup of coffee.

29. Wait until Info changes to **Modifying** or **Available**.

30. Scroll down to the **Connectivity & security** section and copy the **Endpoint** field.

It will look similar to: `lab-db.cggq8lhnxvm.us-west-2.rds.amazonaws.com`

31. Paste the Endpoint value into a text editor. You will use it later in the lab.

**Task 4: Interact with Your Database**

In this task, you will open a web application running on your web server and configure it to use the database.

32. To copy the **WebServer** IP address, click on the **Details** drop down menu above these instructions, and then click **Show**.

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

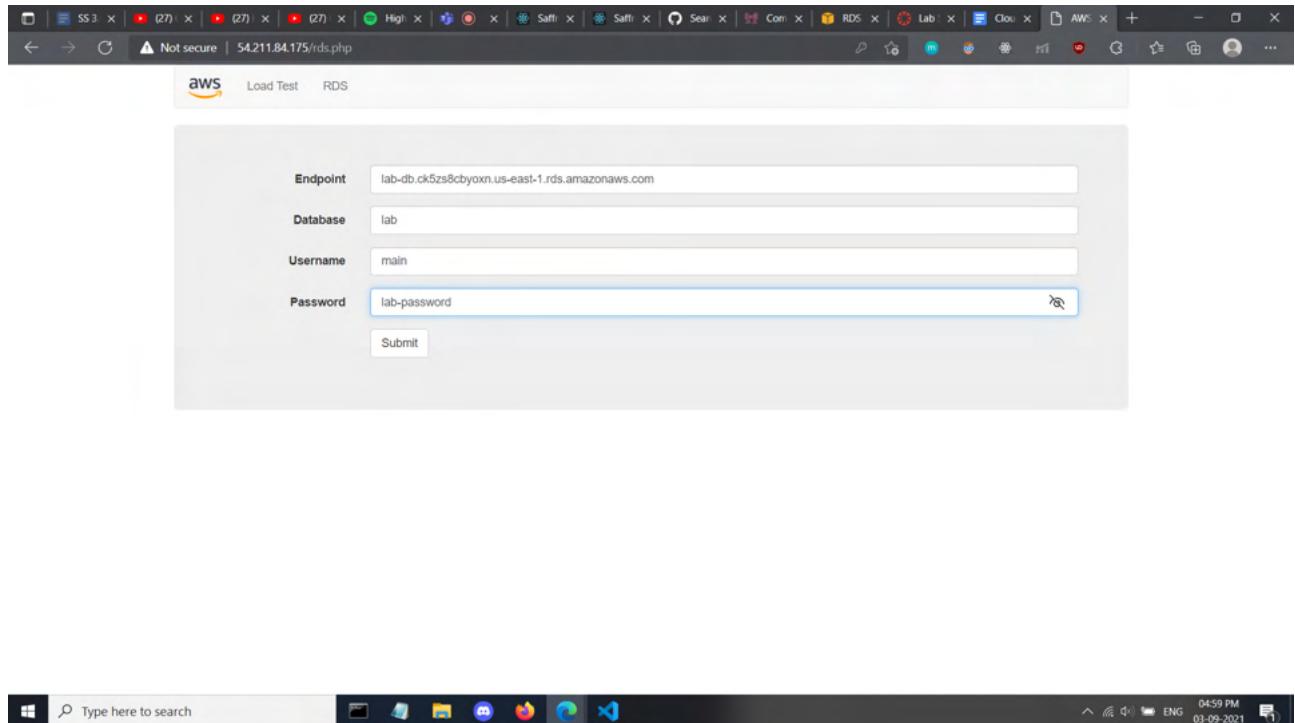
| Meta-Data         | Value               |
|-------------------|---------------------|
| InstanceId        | i-0821337bb6ae0a29e |
| Availability Zone | us-east-1b          |

Current CPU Load: 0%

34. Click the **RDS** link at the top of the page.  
You will now configure the application to connect to your database.

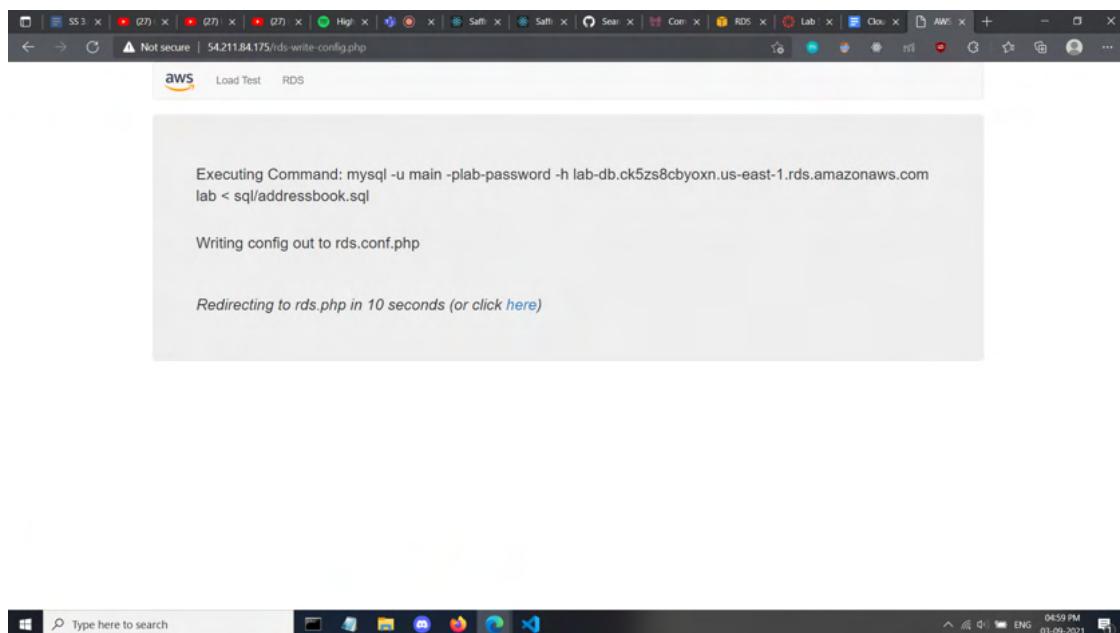
35. Configure the following settings:

- **Endpoint:** Paste the Endpoint you copied to a text editor earlier
- **Database:** lab
- **Username:** main
- **Password:** lab-password
- Click **Submit**



36. A message will appear explaining that the application is running a command to copy information to the database. After a few seconds the application will display an **Address Book**.

The Address Book application is using the RDS database to store information.



37. Test the web application by adding, editing and removing contacts.

The data is being persisted to the database and is automatically replicating to the second Availability Zone.

A screenshot of a web browser window titled "Address Book". The URL is 54.211.84.175/rds.php?mode=add. The page has a form for adding a contact with fields for Last Name (Shah), First Name (Akas), Phone (8989898989), and Email (abc@xyz.com). Below the form is a table showing existing contacts: Doe (Jane, 010-110-1101, janed@someotheraddress.org) and Johnson (Roberto, 123-456-7890, robertoj@someaddress.com). There are "Edit" and "Remove" links for each row. A "Submit" button is at the bottom of the form. The browser's address bar shows "Not secure" and the IP address.



A screenshot of the "Address Book" application window. The title bar says "Address Book". Below it is a table with columns: Last name, First name, Phone, Email, and Admin. The table contains three rows: Doe (Jane, 010-110-1101, janed@someotheraddress.org), Johnson (Roberto, 123-456-7890, robertoj@someaddress.com), and Shah (Akas, 8989898989, abc@xyz.com). Each row has "Edit" and "Remove" links. An "Add Contact" link is located at the top right of the table area.

A screenshot of the "Address Book" application window. The title bar says "Address Book". A message "Entry has been removed" is displayed above the contact table. The table below shows two rows: Johnson (Roberto, 123-456-7890, robertoj@someaddress.com) and Shah (Akas, 8989898989, abc@xyz.com). Each row has "Edit" and "Remove" links. An "Add Contact" link is located at the top right of the table area.

# Practical 5

## AIM

Scale and Load Balance Your Architecture

## THEORY

Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances. It enables you to achieve fault tolerance in your applications by seamlessly providing the required amount of load balancing capacity needed to route application traffic.

Auto Scaling helps you maintain application availability and allows you to scale your Amazon EC2 capacity out or in automatically according to conditions you define. You can use Auto Scaling to help ensure that you are running your desired number of Amazon EC2 instances. Auto Scaling can also automatically increase the number of Amazon EC2 instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs. Auto Scaling is well suited to applications that have stable demand patterns or that experience hourly, daily, or weekly variability in usage.

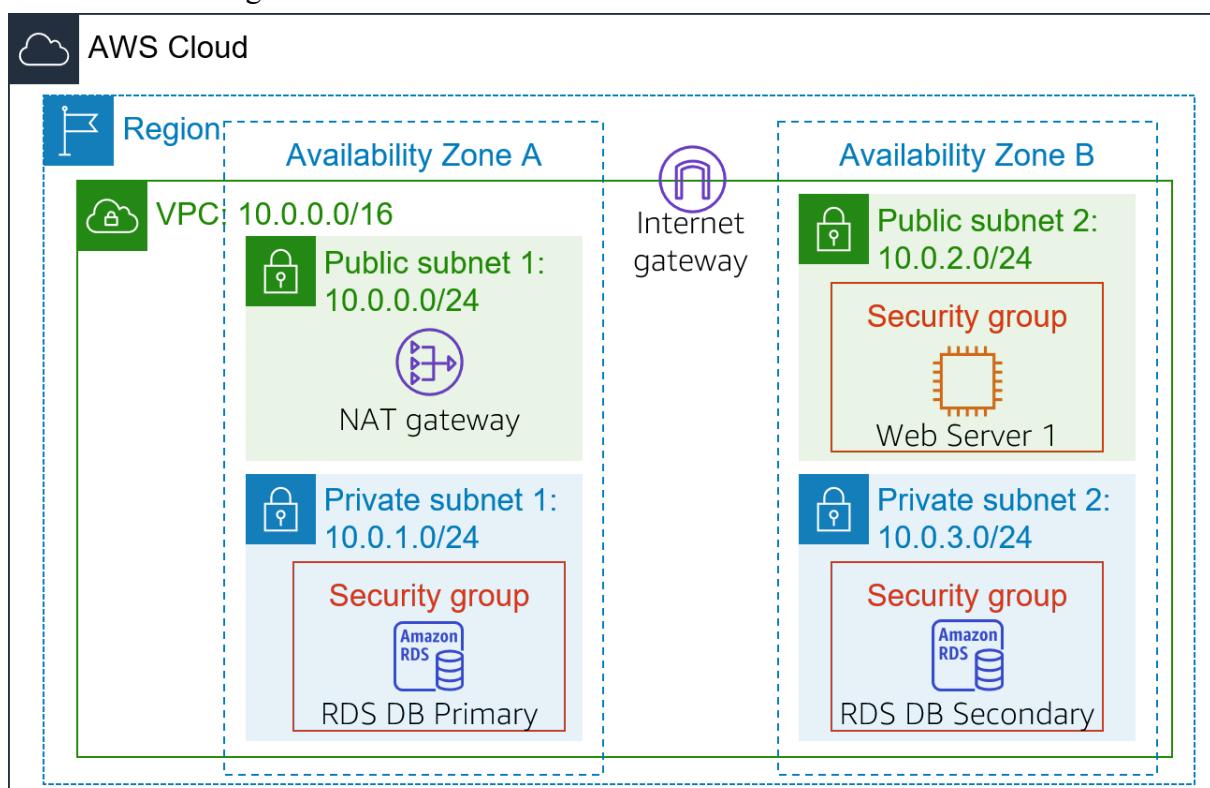
## OBJECTIVES

After completing this lab, you can:

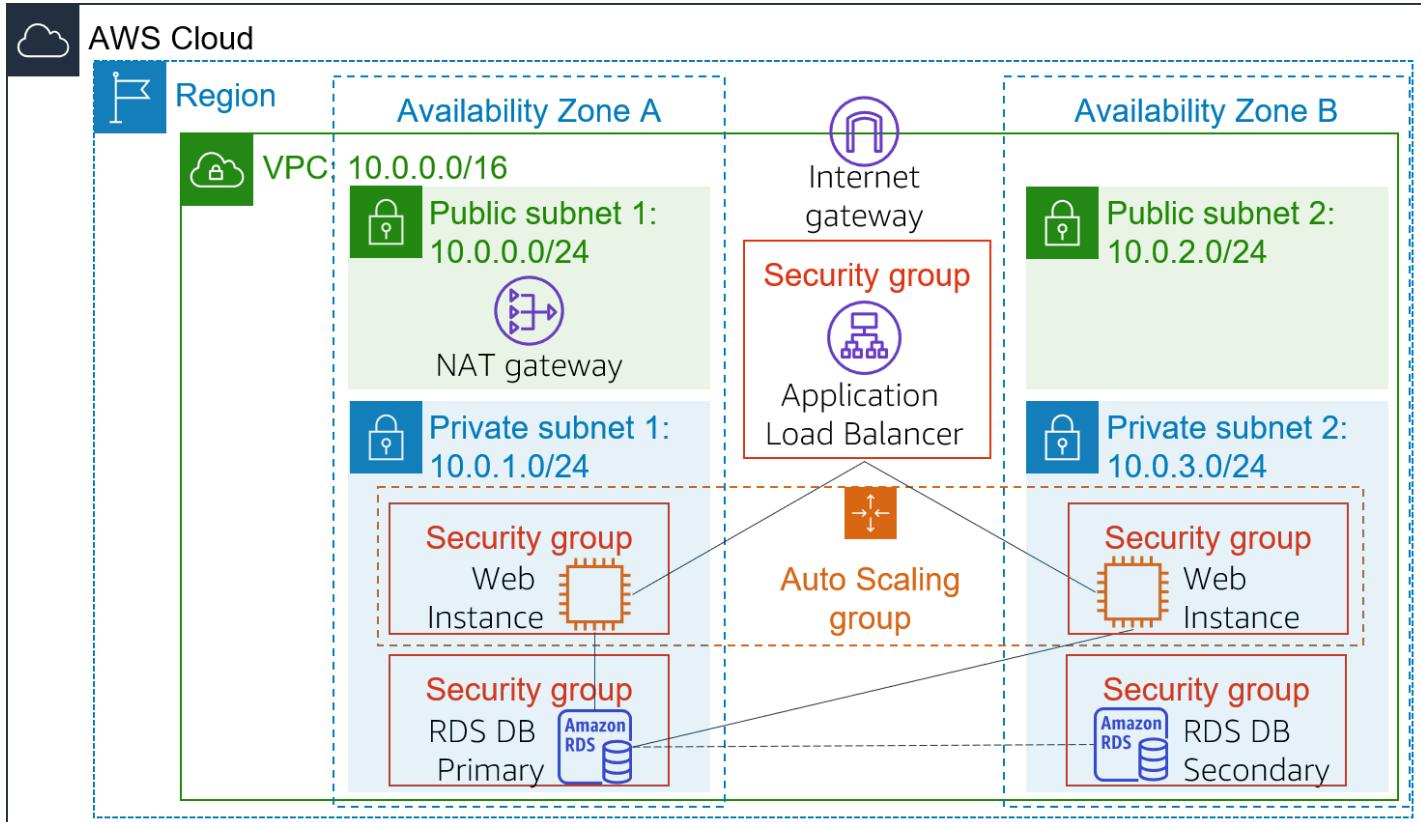
- Create an Amazon Machine Image (AMI) from a running instance.
- Create a load balancer.
- Create a launch configuration and an Auto Scaling group.
- Automatically scale new instances within a private subnet
- Create Amazon CloudWatch alarms and monitor performance of your infrastructure.

## PROCEDURE

You start with the following infrastructure:



The final state of the infrastructure is:



## Task 1: Create an AMI for Auto Scaling

In this task, you will create an AMI from the existing *Web Server 1*. This will save the contents of the boot disk so that new instances can be launched with identical content.

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**.

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with options like EC2 Dashboard, Events, Tags, Limits, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, Images (AMIs), and Elastic Block Store (Volumes, Snapshots). The main area displays a table of instances:

| Name         | Instance ID         | Instance state | Instance type | Status check      | Alarm status | Availability Zone | Public IPv4 |
|--------------|---------------------|----------------|---------------|-------------------|--------------|-------------------|-------------|
| Web Server 1 | i-0ba8f50cc39295660 | Running        | t2.micro      | 2/2 checks passed | No alarms    | us-east-1a        | -           |
| Bastion Host | i-06c4ce8e746a4d00a | Running        | t2.micro      | 2/2 checks passed | No alarms    | us-east-1a        | -           |

Below the table, a detailed view for 'Web Server 1' is shown with tabs for Details, Security, Networking, Storage, Status checks, Monitoring, and Tags. The Details tab shows instance summary information including Instance ID (i-0ba8f50cc39295660), Public IPv4 address (18.206.40.64), Private IPv4 address (10.0.0.52), Instance state (Running), and Instance type (t2.micro).

- In the Actions menu, click **Image and templates > Create image**, then configure:
  - Image name:** WebServerAMI
  - Image description:** Lab AMI for Web Server

The screenshot shows the Actions menu for an EC2 instance. The menu includes options like Connect, View details, Manage instance state, Instance settings, Networking, Security, Image and templates (which is highlighted with a blue background), and Monitor and troubleshoot.

The screenshot shows the 'Create image' configuration page. It includes fields for Instance ID (i-0ba8f50cc39295660), Image name (WebServerAMI), and Image description (optional) (Lab AMI for Web Server). Under Instance volumes, there's a table for EBS volumes:

| Volume type | Device    | Snapshot                  | Size | Volume type               | IOPS | Throughput | Delete on termination                      | Encrypted                       |
|-------------|-----------|---------------------------|------|---------------------------|------|------------|--------------------------------------------|---------------------------------|
| EBS         | /dev/x... | Create new snapshot fr... | 8    | EBS General Purpose SS... | 100  |            | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |

## 10. Click **Create image**

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

You will use this AMI when launching the Auto Scaling group later in the lab.

ID: ami-0efba6ca7e398ef63

The screenshot shows the AWS EC2 Instances page. A green confirmation banner at the top states: "Successfully created ami-0efba6ca7e398ef63 from instance i-0ba8f50cc39295660." Below the banner, the "Instances (2)" table lists two items:

| Name         | Instance ID         | Instance state | Instance type | Status check      | Alarm status | Availability Zone | Public IPv |
|--------------|---------------------|----------------|---------------|-------------------|--------------|-------------------|------------|
| Web Server 1 | i-0ba8f50cc39295660 | Running        | t2.micro      | 2/2 checks passed | No alarms    | + us-east-1a      | -          |
| Bastion Host | i-06c4ce8e746a4d00a | Running        | t2.micro      | 2/2 checks passed | No alarms    | + us-east-1a      | -          |

A modal dialog box titled "Select an instance above" is open, prompting the user to choose an instance to proceed with creating the AMI.

## Task 2: Create a Load Balancer

In this task, you will create a load balancer that can balance traffic across multiple EC2 instances and Availability Zones.

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

### 12. Click **Create Load Balancer**

Several different types of load balancer are displayed. You will be using an *Application Load Balancer* that operates at the request level (layer 7), routing traffic to targets – EC2 instances, containers, IP addresses and Lambda functions – based on the content of the request. For more information, see: [Comparison of Load Balancers](#)

Select load balancer type

Elastic Load Balancing supports four types of load balancers: Application Load Balancers, Network Load Balancers, Gateway Load Balancers, and Classic Load Balancers. Choose the load balancer type that meets your needs. Learn more about which load balancer is right for you.

| Application Load Balancer                                                                                                                                                                                                                                                                                                                                     | Network Load Balancer                                                                                                                                                                                                                                                                                                                                                                                 | Gateway Load Balancer                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                       |
| <b>Create</b>                                                                                                                                                                                                                                                                                                                                                 | <b>Create</b>                                                                                                                                                                                                                                                                                                                                                                                         | <b>Create</b>                                                                                                                                                                                                                                         |
| Choose an Application Load Balancer when you need a flexible feature set for your web applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.<br><a href="#">Learn more &gt;</a> | Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your application. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.<br><a href="#">Learn more &gt;</a> | Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.<br><a href="#">Learn more &gt;</a> |
| <b>Classic Load Balancer</b>                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                       |

**Cancel**

Feedback English (US) ▾ © 2008–2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences

13. Under **Application Load Balancer** click **Create** and configure:

- **Name:** LabELB
- **VPC:** Lab VPC (In the **Availability Zones** section)
- **Availability Zones:** Select both to see the available subnets.
- **Select Public Subnet 1 and Public Subnet 2**

Step 1: Configure Load Balancer

Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network with a listener that receives HTTP traffic on port 80.

|                 |                                                                                    |
|-----------------|------------------------------------------------------------------------------------|
| Name            | LabELB                                                                             |
| Scheme          | <input checked="" type="radio"/> internet-facing<br><input type="radio"/> internal |
| IP address type | IPv4                                                                               |

#### Availability Zones

Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You must specify subnets from at least two Availability Zones to increase the availability of your load balancer.

|                    |                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------|
| VPC                | vpc-044c05b60fc9f5015 (10.0.0.0/16)   Lab VPC                                                                             |
| Availability Zones | <input checked="" type="checkbox"/> us-east-1a subnet-06257ffce68b5ab02 (Public Subnet 1)<br>IPv4 address Assigned by AWS |
|                    | <input checked="" type="checkbox"/> us-east-1b subnet-02be67f5cb73a42bd (Public Subnet 2)<br>IPv4 address Assigned by AWS |

14. This configures the load balancer to operate across multiple Availability Zones.

15. Click **Next: Configure Security Settings**

You can ignore the "Improve your load balancer's security." warning.

Step 2: Configure Security Settings

**⚠ Improve your load balancer's security.** Your load balancer is not using any secure listener.  
If your traffic to the load balancer needs to be secure, use the HTTPS protocol for your front-end connection. You can go back to the first step to add/configure secure listeners under [Basic Configuration](#) section. You can also continue with current settings.

[Cancel](#) [Previous](#) [Next: Configure Security Groups](#)

## 16. Click **Next: Configure Security Groups**

A Web Security Group has already been created for you, which permits HTTP access.

## 17. Select **Web Security Group** and deselect **default**.

Step 3: Configure Security Groups

A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to reach your load balancer. First, decide whether to create a new security group or select an existing one.

Assign a security group  Create a **new** security group  Select an **existing** security group

| Security Group ID    | Name                                                                  | Description                | Actions                     |
|----------------------|-----------------------------------------------------------------------|----------------------------|-----------------------------|
| sg-0fa86d44f0b8c59   | c36908a47455910192371w300060053754-BastionSecurityGroup-132MIOZAS4901 | Enables SSH access.        | <a href="#">Copy to new</a> |
| sg-09f42cc9b1870e84f | DB Security Group                                                     | DB Security Group          | <a href="#">Copy to new</a> |
| sg-0446c03613c7fa610 | default                                                               | default VPC security group | <a href="#">Copy to new</a> |
| sg-0297bea08cf354e67 | Web Security Group                                                    | Enable HTTP access         | <a href="#">Copy to new</a> |

[Cancel](#) [Previous](#) [Next: Configure Routing](#)

## 18. Click **Next: Configure Routing**

Routing configures where to send requests that are sent to the load balancer. You will create a *Target Group* that will be used by Auto Scaling.

## 19. For **Name**, enter: *LabGroup*

## 20. Click **Next: Register Targets**

Auto Scaling will automatically register instances as targets later in the lab.

**Step 4: Configure Routing**

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify here. It also performs health checks on the targets using these settings. The target group you specify in this step will apply to all of the listeners configured on this load balancer. You can edit or add listeners after the load balancer is created.

**Target group**

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target group     | New target group                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Name             | LabGroup                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Target type      | <input checked="" type="radio"/> Instance                                                                                                                                                                                                                                                                                                                                                                                                      |
| Protocol         | HTTP                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Port             | 80                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Protocol version | <input checked="" type="radio"/> HTTP1<br>Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.<br><input type="radio"/> HTTP2<br>Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.<br><input type="radio"/> gRPC<br>Send requests to targets using gRPC. Supported when the request protocol is gRPC. |

**Cancel** **Previous** **Next: Register Targets**

## 21. Click **Next: Review**

**Step 5: Register Targets**

Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

**Registered targets**

To deregister instances, select one or more registered instances and then click Remove.

| Remove                  | Instance | Name | Port | State | Security groups | Zone |
|-------------------------|----------|------|------|-------|-----------------|------|
| No instances available. |          |      |      |       |                 |      |

**Instances**

To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

Add to registered on port 80

Search Instances

| Instance            | Name         | State   | Security groups      | Zone       | Subnet ID                | Subnet CIDR |
|---------------------|--------------|---------|----------------------|------------|--------------------------|-------------|
| i-0ba8f50cc39295660 | Web Server 1 | running | Web Security Group   | us-east-1a | subnet-06257ffce68b5ab02 | 10.0.0.0/24 |
| i-06c4ce8e746a4d00a | Bastion Host | running | c36908a4745591019... | us-east-1a | subnet-06257ffce68b5ab02 | 10.0.0.0/24 |

**Cancel** **Previous** **Next: Review**

## 22. Click **Create** then click **Close**

The load balancer will show a state of *provisioning*. There is no need to wait until it is ready. Please continue with the next task.

The screenshot shows the AWS Lambda console with the URL <https://console.aws.amazon.com/lambda/home?region=us-east-1#V2CreateELBWizard?type=application>. The page is titled "Step 6: Review" and displays the configuration details for a new Lambda function named "LabELB". The configuration includes:

- Name:** LabELB
- Scheme:** Internet-facing
- Listeners:** Port:80 - Protocol:HTTP
- IP address type:** ipv4
- VPC:** vpc-044c05b60fc9f5015 (Lab VPC)
- Subnets:** subnet-06257ffce68b5ab02 (Public Subnet 1), subnet-02be67f5cb73a42bd (Public Subnet 2)
- Tags:**

Below this, there are sections for "Security groups" and "Routing". Under "Routing", the target group is set to "New target group" with the name "LabGroup". The port is 80, target type is instance, protocol is HTTP, and protocol version is HTTP1. The health check protocol is HTTP, path is /, health check port is traffic port, and healthy threshold is 5.

At the bottom right, there are "Cancel", "Previous", and "Create" buttons. The "Create" button is highlighted in blue.

The screenshot shows the AWS Lambda console with the URL <https://console.aws.amazon.com/lambda/home?region=us-east-1#V2CreateELBWizard?type=application>. The page is titled "Load Balancer Creation Status" and displays a success message:

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

**Suggested next steps**

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

At the bottom right, there is a "Close" button.

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

In this task, you will create a *launch configuration* for your Auto Scaling group. A launch configuration is a template that an Auto Scaling group uses to launch EC2 instances. When you create a launch configuration, you specify information for the instances such as the AMI, the instance type, a key pair, security group and disks.

22. In the left navigation pane, click **Launch Configurations**.

23. Click **Create launch configuration**

The screenshot shows the AWS Management Console interface for the EC2 service. The left sidebar has a tree view of services: Capacity Reservations, Images (selected), AMIs, 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), and Auto Scaling (Launch Configurations selected, Auto Scaling Groups). The main content area is titled 'Launch configurations (0)' and contains a table with columns: Name, AMI ID, Instance type, Spot price, and Creation time. Below the table, it says 'No launch configurations found in this region.' At the bottom right of the main area, there is a large orange button labeled 'Create launch configuration'.

24. Configure these settings:

- **Launch configuration name:** LabConfig
- **Amazon Machine Image (AMI)** Choose Web Server AMI
- **Instance type:**
  - Choose Choose instance type
  - Select t3.micro
  - Choose Choose
- **Note:** If you have launched the lab in the us-east-1 Region, select the **t2.micro** instance type. To find the Region, look in the upper right-hand corner of the Amazon EC2 console.  
**Note:** If you receive the error message "Something went wrong. Please refresh and try again.", you may ignore it and continue with the exercise.
- **Additional configuration**
  - **Monitoring:** Select *Enable EC2 instance detailed monitoring within CloudWatch*
- This allows Auto Scaling to react quickly to changing utilization.

Screenshot of the AWS CloudFormation 'Create launch configuration' wizard.

**Launch configuration name**

Name: LabConfig

**Amazon machine image (AMI)**

AMI: WebServerAMI

**Instance type**

Instance type: t3.micro (2 vCPUs, 1 GiB, EBS Only) | Choose instance type

**Additional configuration - optional**

Purchasing option [Info](#)  
 Request Spot Instances

IAM instance profile [Info](#)  
Select IAM role ▾

Monitoring [Info](#)  
 Enable EC2 instance detailed monitoring within CloudWatch

EBS-optimized instance  
 Launch as EBS-optimized instance

► Advanced details

**Tip:** 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.

25. Under **Security groups**, you will configure the launch configuration to use the **Web Security Group** that has already been created for you.
- Choose **Select an existing security group**
  - Select **Web Security Group**

**Security groups** [Info](#)

Assign a security group

Create a new security group  
 Select an existing security group

| Security groups                             |                      |                                                                        |                                                        |                            |
|---------------------------------------------|----------------------|------------------------------------------------------------------------|--------------------------------------------------------|----------------------------|
| <input type="text"/> Search security groups |                      |                                                                        | <a href="#">Copy to new</a> <a href="#">View rules</a> |                            |
|                                             | Security group ID    | Name                                                                   | VPC ID                                                 |                            |
|                                             |                      |                                                                        | Description                                            |                            |
| <input type="checkbox"/>                    | sg-027b9854db5fd7dd3 | DB Security Group                                                      | vpc-044c05b60fc9f5015                                  | DB Security Group          |
| <input type="checkbox"/>                    | sg-081b799306948de91 | default                                                                | vpc-044c05b60fc9f5015                                  | default VPC security group |
| <input type="checkbox"/>                    | sg-083ff2badcae1c003 | c36908a4745591019237t1w300060053754-BastionSecurityGroup-1V42BQEAXRWP6 | vpc-044c05b60fc9f5015                                  | Enables SSH access.        |
| <input checked="" type="checkbox"/>         | sg-0cd5a31412e1a648f | Web Security Group                                                     | vpc-044c05b60fc9f5015                                  | Enable HTTP access         |
| <input type="checkbox"/>                    | sg-0e04360dba83db3c0 | default                                                                | vpc-082a9593f0085f456                                  | default VPC security group |

⚠ 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.

## 26. Under Key pair configure:

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

**Key pair (login)** [Info](#)

Key pair options

Existing key pair

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

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

27. You will now create an Auto Scaling group that uses this Launch Configuration.

28. Select the checkbox for the *LabConfig* Launch Configuration.

29. From the Actions menu, choose *Create Auto Scaling group*

The screenshot shows the AWS EC2 Launch Configuration page. On the left, there's a sidebar with options like EC2 Dashboard, Instances, Images, and Elastic Block Store. The main area displays a table titled 'Launch configurations (1/1)'. It shows one entry: 'LabConfig' with AMI ID 'ami-0efba6ca7e3...' and Instance type 't3.micro'. The creation time is listed as 'Fri Sep 17 2021 16:46:34 GMT+...'. There are buttons for 'Actions', 'Copy to launch template', and 'Create launch configuration'.

30. Enter Auto Scaling group name:

- **Name:** Lab Auto Scaling Group

31. Choose **Next**

The screenshot shows the 'Choose launch template or configuration' step of the Auto Scaling group creation wizard. On the left, a sidebar lists various AWS services. The main form has several steps: Step 1 (Choose launch template or configuration), Step 2 (Configure settings), 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, and Step 7 (optional) Review. The 'Name' section is filled with 'Lab Auto Scaling Group'. The 'Launch configuration' section shows 'LabConfig' selected. At the bottom right, there are 'Cancel' and 'Next' buttons.

32. On the **Network** page configure

- **Network:** Lab VPC  
You can ignore the message regarding "No public IP address"
- **Subnet:** Select *Private Subnet 1 (10.0.1.0/24)* and *Private Subnet 2 (10.0.3.0/24)*

Configure settings [Info](#)

Configure the settings below. Depending on whether you chose a launch template, these settings may include options to help you make optimal use of EC2 resources.

**Network [Info](#)**

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

**VPC**

vpc-044c05b60fc9f5015 (Lab VPC)  
10.0.0.0/16

**Create a VPC [?](#)**

**Subnets**

Select subnets

us-east-1a | subnet-023c55b2929c09df7 (Private Subnet 1)  
10.0.1.0/24

us-east-1b | subnet-0e20ba4407543488f (Private Subnet 2)  
10.0.3.0/24

**Create a subnet [?](#)**

**Cancel** **Previous** **Skip to review** **Next**

33. This will launch EC2 instances in private subnets across both Availability Zones.

34. Choose **Next**.

35. In the **Load balancing - optional** pane, choose **Attach to an existing load balancer**

36. In the **Attach to an existing load balancer** pane, use the dropdown list to select *LabGroup*.

Auto Scaling groups > Create Auto Scaling group

Configure advanced options [Info](#)

Choose a load balancer to distribute incoming traffic for your application across instances to make it more reliable and easily scalable. You can also set options that give you more control over health check replacements and monitoring.

**Load balancing - optional [Info](#)**

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

No load balancer  
Traffic to your Auto Scaling group will not be fronted by a load balancer.

Attach to an existing load balancer  
Choose from your existing load balancers.

Attach to a new load balancer  
Quickly create a basic load balancer to attach to your Auto Scaling group.

**Attach to an existing load balancer**

Select the load balancers that you want to attach to your Auto Scaling group.

Choose from your load balancer target groups  
This option allows you to attach Application, Network, or Gateway Load Balancers.

Choose from Classic Load Balancers

Existing load balancer target groups  
Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups

LabGroup | HTTP  
Application Load Balancer: LabELB

© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences

37. 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.

38. Choose **Next**

**Additional settings - optional**

Monitoring [Info](#)

Enable group metrics collection within CloudWatch

**Cancel** **Previous** **Skip to review** **Next**

39. Under **Group size**, configure:

- Desired capacity:** 2
- Minimum capacity:** 2
- Maximum capacity:** 6

40. This will allow Auto Scaling to automatically add/remove instances, always keeping between 2 and 6 instances running.

**Configure group size and scaling policies [Info](#)**

Set the desired, minimum, and maximum capacity of your Auto Scaling group. You can optionally add a scaling policy to dynamically scale the number of instances in the group.

**Group size - optional [Info](#)**

Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum capacity limits. Your desired capacity must be within the limit range.

Desired capacity  
2

Minimum capacity  
2

Maximum capacity  
6

**Scaling policies - optional**

Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand. [Info](#)

41. Under **Scaling policies**, choose *Target tracking scaling policy* and configure:

- Lab policy name:** `LabScalingPolicy`
- Metric type:** *Average CPU Utilization*
- Target value:** 60

## Scaling policies - optional

Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand. [Info](#)

Target tracking scaling policy

Choose a desired outcome and leave it to the scaling policy to add and remove capacity as needed to achieve that outcome.

None

Scaling policy name

LabScalingPolicy

Metric type

Average CPU utilization

Target value

60

Instances need

300

seconds warm up before including in metric

Disable scale in to create only a scale-out policy

42. 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.

43. Choose **Next**

Auto Scaling can send a notification when a scaling event takes place. You will use the default settings.

The screenshot shows the AWS EC2 Auto Scaling group creation wizard at Step 5: Add notifications. The left sidebar shows navigation options like EC2 Dashboard, Events, Tags, Limits, Instances, Images, and Elastic Block Store. The main content area has a title 'Add notifications' with a 'Info' link. It explains that notifications are sent to SNS topics whenever instances are launched or terminated. A button 'Add notification' is present. Below it are other optional steps: Step 2 (Configure settings), Step 3 (optional) Configure advanced options, Step 4 (optional) Configure group size and scaling policies, Step 5 (optional) Add notifications (which is currently selected), Step 6 (optional) Add tags, and Step 7 Review. At the bottom right are buttons for Cancel, Previous, Skip to review, and Next.

#### 44. Choose **Next**

Tags applied to the Auto Scaling group will be automatically propagated to the instances that are launched.

#### 45. Choose **Add tag** and Configure the following:

- Key:** Name
- Value:** Lab Instance

#### 46. Click **Next**

The screenshot shows the AWS EC2 Auto Scaling group creation wizard at Step 6: Add tags. The left sidebar is identical to the previous screenshot. The main content area has a title 'Add tags' with an 'Info' link. It explains that tags help search, filter, and track the Auto Scaling group. A note states that you can optionally choose to add tags to instances by specifying tags in your launch template. A callout box highlights that tag values from the launch template will be overridden if there are any duplicate keys. Below this is a 'Tags (1)' section showing one tag: Key 'Name' and Value 'Lab Instance'. A checkbox 'Tag new instances' is checked. Buttons for 'Add tag' and 'Remove' are available. At the bottom right are buttons for Cancel, Previous, and Next.

47. 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 6: Add tags**

| Tags (1) |              |                   |
|----------|--------------|-------------------|
| Key      | Value        | Tag new instances |
| Name     | Lab Instance | Yes               |

**Create Auto Scaling group**

**Auto Scaling groups (1)**

| Name             | Launch template/configuration | Instances | Status            | Desired capacity | Min | Max |
|------------------|-------------------------------|-----------|-------------------|------------------|-----|-----|
| Lab Auto Scaling | LabConfig                     | 0         | Updating capacity | 2                | 2   | 6   |

| Auto Scaling groups (1)  |                  |                               |           |        |                  |     |     |
|--------------------------|------------------|-------------------------------|-----------|--------|------------------|-----|-----|
|                          | Name             | Launch template/configuration | Instances | Status | Desired capacity | Min | Max |
| <input type="checkbox"/> | Lab Auto Scaling | LabConfig                     | 2         | -      | 2                | 2   | 6   |

## Task 4: Verify that Load Balancing is Working

In this task, you will verify that Load Balancing is working correctly.

44. In the left navigation pane, click **Instances**.

You should see two new instances named **Lab Instance**. These were launched by Auto Scaling.

If the instances or names are not displayed, wait 30 seconds and click refresh in the top-right.

First, you will confirm that the new instances have passed their Health Check.

| Instances (4) <a href="#">Info</a> |              |                     |                      |               |                                |              |                   |
|------------------------------------|--------------|---------------------|----------------------|---------------|--------------------------------|--------------|-------------------|
|                                    | Name         | Instance ID         | Instance state       | Instance type | Status check                   | Alarm status | Availability Zone |
| <a href="#">Filter instances</a>   |              |                     |                      |               |                                |              |                   |
| <input type="checkbox"/>           | Web Server 1 | i-0ba8f50cc39295660 | <span>Running</span> | t2.micro      | <span>2/2 checks passed</span> | No alarms    | us-east-1a        |
| <input type="checkbox"/>           | Bastion Host | i-06c4ce8e746a4d00a | <span>Running</span> | t2.micro      | <span>2/2 checks passed</span> | No alarms    | us-east-1a        |
| <input type="checkbox"/>           | Lab Instance | i-0ed163ed9ba3d2b0a | <span>Running</span> | t3.micro      | <span>2/2 checks passed</span> | No alarms    | us-east-1a        |
| <input type="checkbox"/>           | Lab Instance | i-01bf522e2afc500a5 | <span>Running</span> | t3.micro      | <span>2/2 checks passed</span> | No alarms    | us-east-1b        |

45. In the left navigation pane, click **Target Groups** (in the *Load Balancing* section).

46. Choose *LabGroup*

47. Click the **Targets** tab.

Two **Lab Instance** targets should be listed for this target group.

48. Wait until the **Status** of both instances transitions to *healthy*. Click Refresh in the upper-right to check for updates.

*Healthy* indicates that an instance has passed the Load Balancer's health check. This means that the Load Balancer will send traffic to the instance.

You can now access the Auto Scaling group via the Load Balancer.

**Target groups (1/1) [Info](#)**

| <input checked="" type="checkbox"/> | Name     | ARN                                                                                       | Port | Protocol | Target type | Load balancer |
|-------------------------------------|----------|-------------------------------------------------------------------------------------------|------|----------|-------------|---------------|
| <input checked="" type="checkbox"/> | LabGroup | arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/LabGroup/5555555555555555 | 80   | HTTP     | Instance    | LabELB        |

Details    Targets **Targets**    Monitoring    Health checks    Attributes    Tags

**Registered targets (2)**

| <input type="checkbox"/> | Instance ID         | Name         | Port | Zone       | Health status                              | Health status details |
|--------------------------|---------------------|--------------|------|------------|--------------------------------------------|-----------------------|
| <input type="checkbox"/> | i-01bf522e2afc500a5 | Lab Instance | 80   | us-east-1b | <span style="color: green;">healthy</span> |                       |
| <input type="checkbox"/> | i-0ed163ed9ba3d2b0a | Lab Instance | 80   | us-east-1a | <span style="color: green;">healthy</span> |                       |

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

50. In the lower pane, copy the **DNS name** of the load balancer, making sure to omit "(A Record)".

It should look similar to: *LabELB-1998580470.us-west-2.elb.amazonaws.com*

DNS Name: LabELB-108156777.us-east-1.elb.amazonaws.com

51. Open a new web browser tab, paste the DNS Name you just copied, and press Enter.

The application should appear in your browser. This indicates that the Load Balancer received the request, sent it to one of the EC2 instances, then passed back the result.

| Meta-Data         | Value               |
|-------------------|---------------------|
| InstanceId        | i-03b1dd609a4923e1a |
| Availability Zone | us-east-1a          |

Current CPU Load: 0%

# Task 5: Test Auto Scaling

You created an Auto Scaling group with a minimum of two instances and a maximum of six instances. Currently two instances are running because the minimum size is two and the group is currently not under any load. You will now increase the load to cause Auto Scaling to add additional instances.

52. Return to the AWS management console, but do not close the application tab – you will return to it soon.

53. On the **Services** menu, click **CloudWatch**.

54. In the left navigation pane, click **Alarms** (not **ALARM**).

Two alarms will be displayed. These were created automatically by the Auto Scaling group.

They will automatically keep the average CPU load close to 60% while also staying within the limitation of having two to six instances.

**Note:** Please follow these steps only if you do not see the alarms in 60 seconds.

- On the **Services** menu, click **EC2**.
- In the left navigation pane, choose **Auto Scaling Groups**.
- Select **Lab Auto Scaling Group**.
- In the bottom half of the page, choose the **Automatic Scaling** tab.
- Select **LabScalingPolicy**.
- Click **Actions** and **Edit**.
- Change the **Target Value** to **50**.
- Click **Update**
- On the **Services** menu, click **CloudWatch**.
- In the left navigation pane, click **Alarms** (not **ALARM**) and verify you see two alarms.

The screenshot shows the AWS CloudWatch Alarms page. The left sidebar has 'CloudWatch' selected. Under 'Alarms', 'All alarms' is selected. The main area displays two alarms:

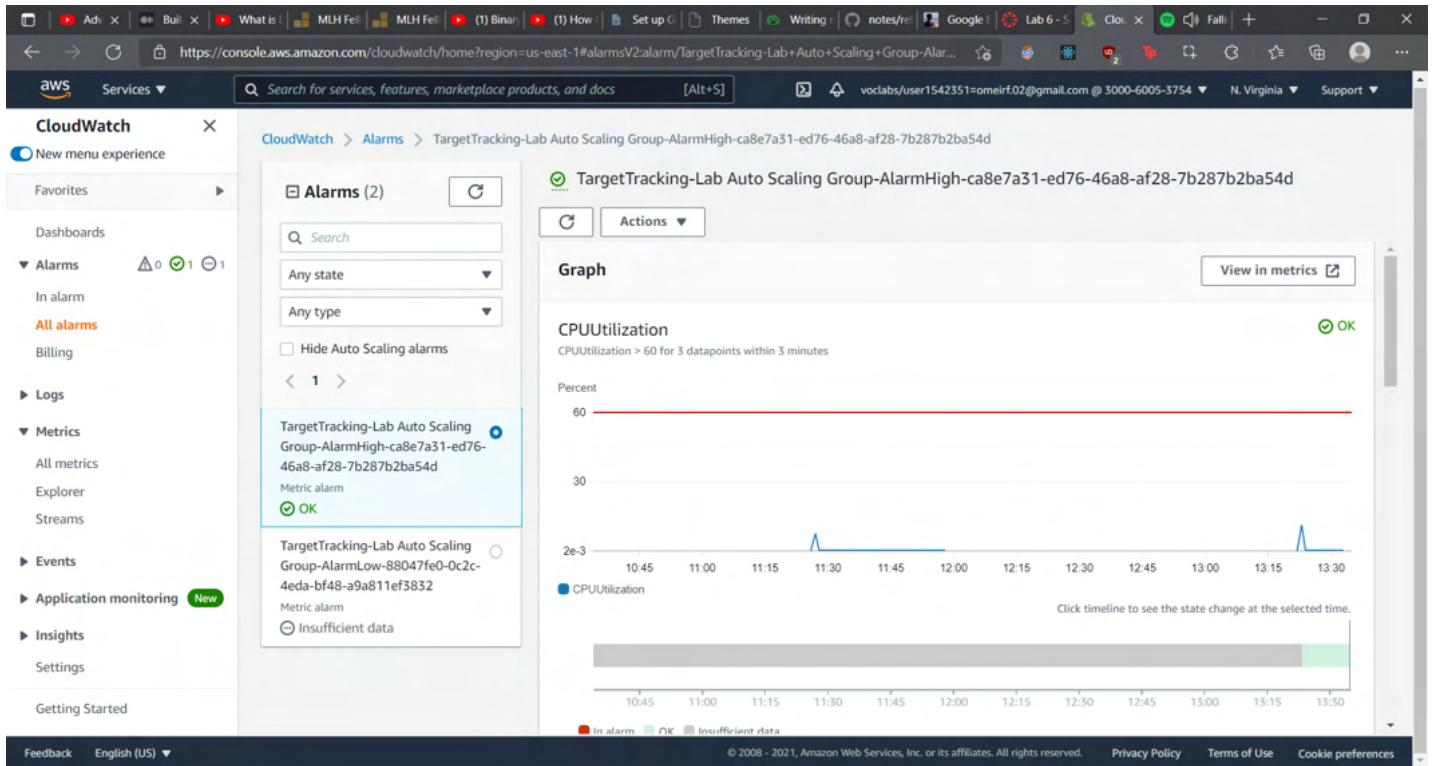
| Name                                                                                 | State             | Last state update   | Conditions                                              | Actions         |
|--------------------------------------------------------------------------------------|-------------------|---------------------|---------------------------------------------------------|-----------------|
| TargetTracking-Lab Auto Scaling Group-AlarmHigh-ca8e7a31-ed76-46a8-af28-7b287b2ba54d | OK                | 2021-09-17 18:53:28 | CPUUtilization > 60 for 3 datapoints within 3 minutes   | Actions enabled |
| TargetTracking-Lab Auto Scaling Group-AlarmLow-88047fe0-0c2c-4eda-bf48-a9a811ef3832  | Insufficient data | 2021-09-17 18:52:01 | CPUUtilization < 54 for 15 datapoints within 15 minutes | Actions enabled |

55. Click the **OK** alarm, which has *AlarmHigh* in its name.

If no alarm is showing **OK**, wait a minute then click refresh in the top-right until the alarm status changes.

The **OK** indicates that the alarm has *not* been triggered. It is the alarm for **CPU Utilization > 60**, which will add instances when average CPU is high. The chart should show very low levels of CPU at the moment.

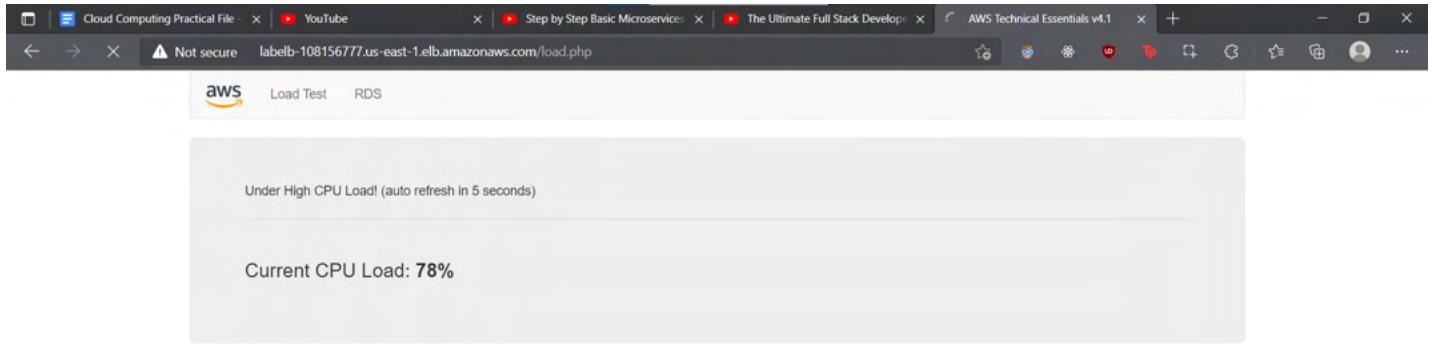
You will now tell the application to perform calculations that should raise the CPU level.



56. Return to the browser tab with the web application.

57. Click **Load Test** beside the AWS logo.

This will cause the application to generate high loads. The browser page will automatically refresh so that all instances in the Auto Scaling group will generate load. Do not close this tab.



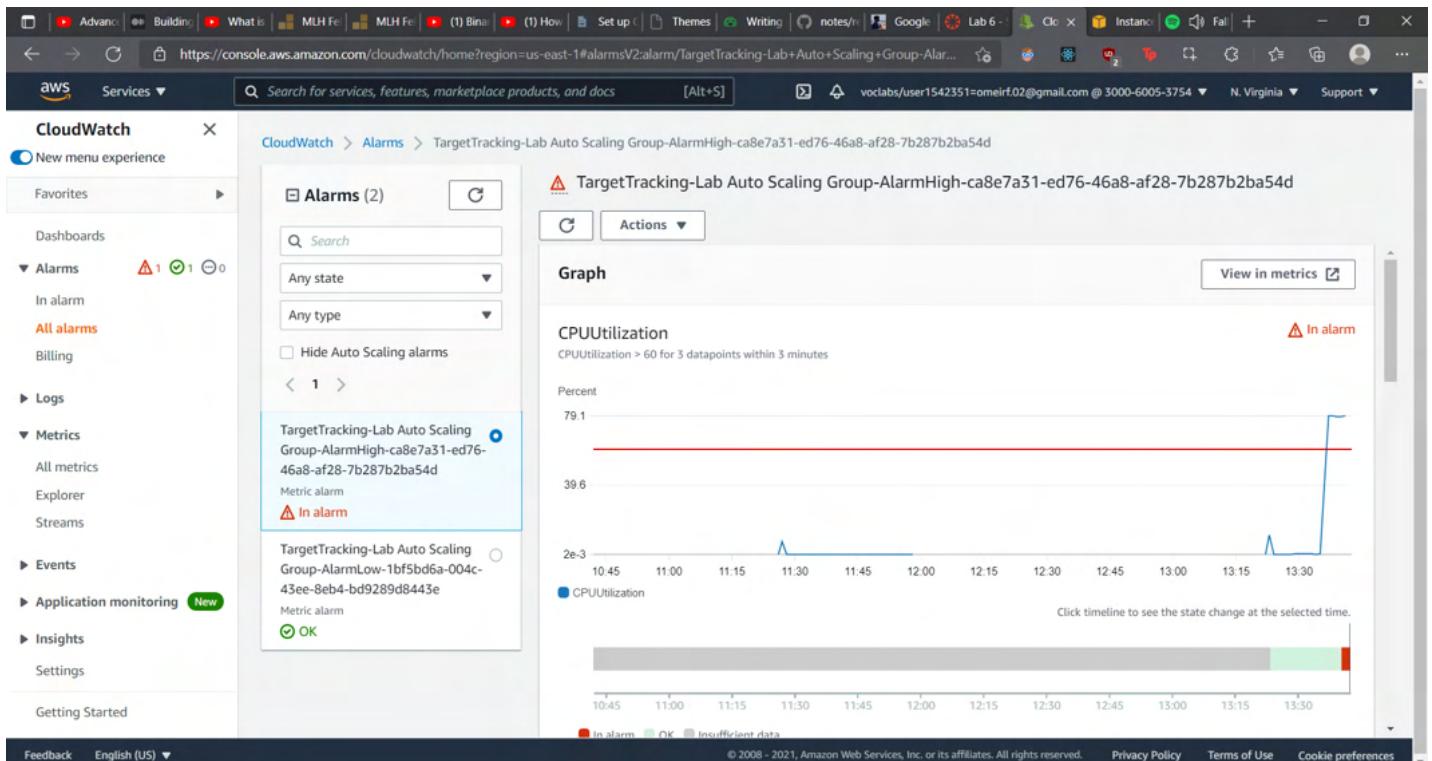
58. Return to the browser tab with the **CloudWatch** console.

In less than 5 minutes, the **AlarmLow** alarm should change to **OK** and the **AlarmHigh** alarm status should change to **ALARM**.

You can click Refresh in the top-right every 60 seconds to update the display.

You should see the **AlarmHigh** chart indicating an increasing CPU percentage. Once it crosses the 60% line for more than 3 minutes, it will trigger Auto Scaling to add additional instances.

| Alarms (2)               |                                                                                      |                                             |                     |                                                         | <input type="checkbox"/> Hide Auto Scaling alarms    | <button>Clear selection</button> | <button>C</button> | <button>Create composite alarm</button> | <button>Actions ▾</button> | <button>Create alarm</button> |
|--------------------------|--------------------------------------------------------------------------------------|---------------------------------------------|---------------------|---------------------------------------------------------|------------------------------------------------------|----------------------------------|--------------------|-----------------------------------------|----------------------------|-------------------------------|
| <input type="checkbox"/> | Name                                                                                 | State                                       | Last state update   | Conditions                                              | Actions                                              |                                  |                    |                                         |                            |                               |
| <input type="checkbox"/> | TargetTracking-Lab Auto Scaling Group-AlarmHigh-ca8e7a31-ed76-46a8-af28-7b287b2ba54d | <span style="color: red;">⚠ In alarm</span> | 2021-09-17 19:10:28 | CPUUtilization > 60 for 3 datapoints within 3 minutes   | <span style="color: green;">↻ Actions enabled</span> |                                  |                    |                                         |                            |                               |
| <input type="checkbox"/> | TargetTracking-Lab Auto Scaling Group-AlarmLow-1bf5bd6a-004c-43ee-8eb4-bd9289d8443e  | <span style="color: green;">🕒 OK</span>     | 2021-09-17 19:09:01 | CPUUtilization < 42 for 15 datapoints within 15 minutes | <span style="color: green;">↻ Actions enabled</span> |                                  |                    |                                         |                            |                               |



59. Wait until the **AlarmHigh** alarm enters the **ALARM** state.

You can now view the additional instance(s) that were launched.

60. On the **Services** menu, click **EC2**.

61. In the left navigation pane, click **Instances**.

More than two instances labeled **Lab Instance** should now be running. The new instance(s) were created by Auto Scaling in response to the Alarm.

| Instances (5) <a href="#">Info</a> |              |                     |                                              |                                       |              |                                                      |                   |                 | <button>C</button> | <button>Connect</button> | <button>Instance state ▾</button> | <button>Actions ▾</button> | <button>Launch instances</button> | <button>▼</button> |
|------------------------------------|--------------|---------------------|----------------------------------------------|---------------------------------------|--------------|------------------------------------------------------|-------------------|-----------------|--------------------|--------------------------|-----------------------------------|----------------------------|-----------------------------------|--------------------|
| <input type="checkbox"/>           | Name         | Instance ID         | Instance state                               | Instance type                         | Status check | Alarm status                                         | Availability Zone | Public IPv4 DN: |                    |                          |                                   |                            |                                   |                    |
| <input type="checkbox"/>           | Web Server 1 | i-03fbfdff2bc1c6de  | <span style="color: green;">🕒 Running</span> | <span style="color: green;">QQ</span> | t2.micro     | <span style="color: green;">2/2 checks passed</span> | No alarms         | + us-east-1a    |                    |                          |                                   |                            |                                   |                    |
| <input type="checkbox"/>           | Bastion Host | i-08b96885d4d717324 | <span style="color: green;">🕒 Running</span> | <span style="color: green;">QQ</span> | t2.micro     | <span style="color: green;">2/2 checks passed</span> | No alarms         | + us-east-1a    |                    |                          |                                   |                            |                                   |                    |
| <input type="checkbox"/>           | Lab Instance | i-03b1dd609a4923e1a | <span style="color: green;">🕒 Running</span> | <span style="color: green;">QQ</span> | t3.micro     | <span style="color: green;">2/2 checks passed</span> | No alarms         | + us-east-1a    |                    |                          |                                   |                            |                                   |                    |
| <input type="checkbox"/>           | Lab Instance | i-0071612e34227b349 | <span style="color: green;">🕒 Running</span> | <span style="color: green;">QQ</span> | t3.micro     | <span style="color: green;">1 Initializing</span>    | No alarms         | + us-east-1a    |                    |                          |                                   |                            |                                   |                    |
| <input type="checkbox"/>           | Lab Instance | i-02007c97052d492cf | <span style="color: green;">🕒 Running</span> | <span style="color: green;">QQ</span> | t3.micro     | <span style="color: green;">2/2 checks passed</span> | No alarms         | + us-east-1b    |                    |                          |                                   |                            |                                   |                    |

# Task 6: Terminate Web Server 1

In this task, you will terminate **Web Server 1**. This instance was used to create the AMI used by your Auto Scaling group, but it is no longer needed.

62. Select **Web Server 1** (and ensure it is the only instance selected).
63. In the **Instance state** menu, click **Instance State > Terminate Instance**.

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with various navigation links like EC2 Dashboard, Instances, Images, and Elastic Block Store. The main area displays a table of instances. One instance, "Web Server 1" (with ID i-03fbfdfbf2bc1c6de), is selected and highlighted with a blue border. In the "Actions" column for this instance, the "Terminate instance" option is highlighted with a red box. Below the table, a modal window titled "Instance: i-03fbfdfbf2bc1c6de (Web Server 1)" is open, showing details about the instance and its summary.

64. Choose **Terminate**

The screenshot shows the same AWS EC2 Instances page as before, but now a modal dialog box titled "Terminate instance?" is centered over the table. The dialog contains a warning message: "On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost." Below the message, there's a question: "Are you sure you want to terminate these instances?", followed by a list of instance IDs: i-03fbfdfbf2bc1c6de (Web Server 1). At the bottom of the dialog, there are "Cancel" and "Terminate" buttons, with "Terminate" being highlighted with a red box.

https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:

New EC2 Experience [Learn more](#)

Services ▾

EC2 Dashboard

Events

Tags

Limits

Instances

- Instances [New](#)
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances [New](#)
- Dedicated Hosts
- Scheduled Instances
- Capacity Reservations

Images

- AMIs

Elastic Block Store

- Volumes
- Snapshots

Successfully terminated i-03fbfdfbf2bc1c6de

Instances (1/5) [Info](#)

Filter instances

| Name                                             | Instance ID         | Instance state       | Instance type | Status check                   | Alarm status | Availability Zone | Public IPv4 DNS |
|--------------------------------------------------|---------------------|----------------------|---------------|--------------------------------|--------------|-------------------|-----------------|
| <input checked="" type="checkbox"/> Web Server 1 | i-03fbfdfbf2bc1c6de | <span>Running</span> | t2.micro      | <span>2/2 checks passed</span> | No alarms    | + us-east-1a      | -               |
| <input type="checkbox"/> Bastion Host            | i-08b96885d4d717324 | <span>Running</span> | t2.micro      | <span>2/2 checks passed</span> | No alarms    | + us-east-1a      | -               |
| <input type="checkbox"/> Lab Instance            | i-03b1dd609a4923e1a | <span>Running</span> | t3.micro      | <span>2/2 checks passed</span> | No alarms    | + us-east-1a      | -               |
| <input type="checkbox"/> Lab Instance            | i-0071612e34227b349 | <span>Running</span> | t3.micro      | <span>Initializing</span>      | No alarms    | + us-east-1a      | -               |
| <input type="checkbox"/> Lab Instance            | i-02007c97052d492cf | <span>Running</span> | t3.micro      | <span>2/2 checks passed</span> | No alarms    | + us-east-1b      | -               |

Instance: i-03fbfdfbf2bc1c6de (Web Server 1)

Details Security Networking Storage Status checks Monitoring Tags

Instance summary Info

|                                    |                                               |                        |
|------------------------------------|-----------------------------------------------|------------------------|
| Instance ID                        | Public IPv4 address                           | Private IPv4 addresses |
| i-03fbfdfbf2bc1c6de (Web Server 1) | 34.239.125.167   <a href="#">open address</a> | 10.0.0.175             |
| IPv6 address                       | Instance state                                | Public IPv4 DNS        |
| -                                  | <span>Running</span>                          | -                      |
| Private IP DNS name (IPv4 only)    | Instance type                                 | Elastic IP addresses   |
|                                    |                                               |                        |

Feedback English (US) ▾

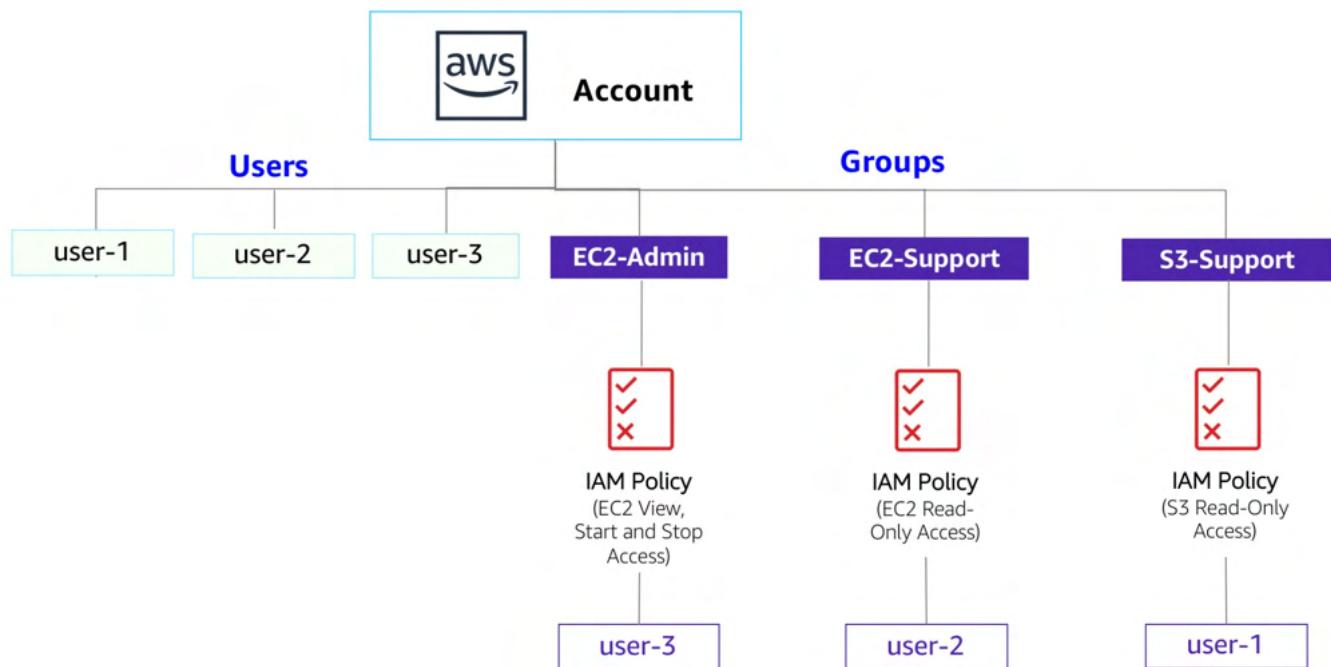
© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#) [Cookie preferences](#)

# Practical 6

## AIM

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.

## THEORY



This lab will demonstrate:

- 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

## Other AWS Services

During this lab, you may receive error messages when performing actions beyond the steps in this lab guide. These messages will not impact your ability to complete the lab.

## AWS Identity and Access Management

*AWS IAM can be used to:*

- Manage IAM Users and their access: You can create Users and assign them individual security credentials (access keys, passwords, and multi-factor authentication devices). You can manage permissions to control which operations a User can perform.
- Manage IAM Roles and their permissions: An IAM Role is similar to a User, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a Role is intended to be assumable by anyone who needs it.

- *Manage federated users and their permissions: You can enable identity federation to allow existing users in your enterprise to access the AWS Management Console, to call AWS APIs and to access resources, without the need to create an IAM User for each identity.*

## PROCEDURE

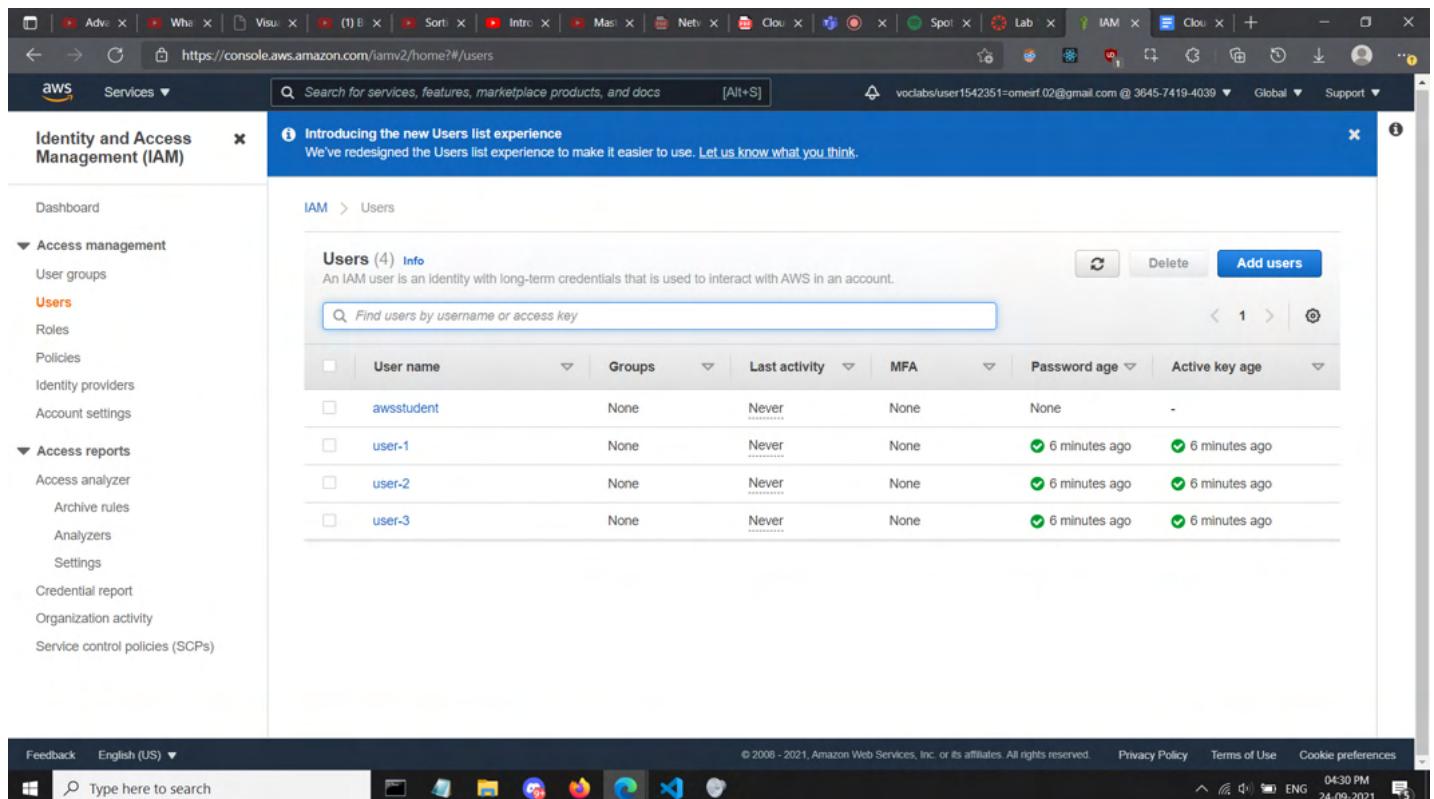
# Task 1: Explore the Users and Groups

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

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

The following IAM Users have been created for you:

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



The screenshot shows the AWS IAM service in the AWS Management Console. The left sidebar has 'Identity and Access Management (IAM)' selected. The main content area is titled 'Users (4)'. It displays a table with columns: User name, Groups, Last activity, MFA, Password age, and Active key age. The table rows are as follows:

| User name  | Groups | Last activity | MFA  | Password age  | Active key age |
|------------|--------|---------------|------|---------------|----------------|
| awsstudent | None   | Never         | None | None          | -              |
| user-1     | None   | Never         | None | 6 minutes ago | 6 minutes ago  |
| user-2     | None   | Never         | None | 6 minutes ago | 6 minutes ago  |
| user-3     | None   | Never         | None | 6 minutes ago | 6 minutes ago  |

7. Click **user-1**.

This will bring to a summary page for user-1. The **Permissions** tab will be displayed.

8. Notice that user-1 does not have any permissions.

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, a navigation pane lists various IAM management options like Dashboard, Access management, and Users. The 'Users' option is selected. The main content area displays details for a user named 'user-1'. At the top, there's a message about CloudTrail events generating policies. Below it, the 'Summary' tab is active, showing the User ARN (arn:aws:iam::364574194039:user/spl66/user-1), Path (/spl66/), and Creation time (2021-09-24 16:23 UTC+0530). There are tabs for Permissions, Groups, Tags (1), Security credentials, and Access Advisor. Under the 'Permissions' tab, there's a section titled 'Get started with permissions' with a 'Add permissions' button and a 'Add inline policy' link. A note says 'This user doesn't have any permissions yet.' Below this, another section 'Permissions boundary (not set)' is shown. The bottom of the page includes a search bar, feedback links, and a system status bar.

9. Click the **Groups** tab.  
user-1 also is not a member of any groups.

This screenshot shows the same IAM user details page for 'user-1', but the 'Groups' tab is now active. The summary information remains the same. Below the tabs, a large blue button labeled 'Add user to groups' is visible. The main content area has two sections: 'Group name' (with a dropdown arrow) and 'Attached permissions'. A note below the first section says 'No results'. The bottom of the page includes a search bar, feedback links, and a system status bar.

10. Click the **Security credentials** tab.  
user-1 is assigned a **Console password**

## Summary

[Delete user](#) [?](#)

User ARN arn:aws:iam::364574194039:user/spl66/user-1 [Copy](#)  
Path /spl66/  
Creation time 2021-09-24 16:23 UTC+0530

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

### Sign-in credentials

**Summary** • Console sign-in link: <https://364574194039.signin.aws.amazon.com/console> [Copy](#)

**Console password** Enabled (never signed in) | [Manage](#)

**Assigned MFA device** Not assigned | [Manage](#)

**Signing certificates** None [Edit](#)

### Access keys

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.

If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. [Learn more](#)

[Create access key](#)

## 11. In the navigation pane on the left, click **Groups**.

The following groups have already been created for you:

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

The screenshot shows the AWS IAM User Groups page. The left sidebar is collapsed, and the main content area displays the following information:

**User groups (3)** [Info](#)  
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

| <input type="checkbox"/> | Group name  | Users | Permissions | Creation time |
|--------------------------|-------------|-------|-------------|---------------|
| <input type="checkbox"/> | EC2-Admin   | ▲ 0   | Defined     | 8 minutes ago |
| <input type="checkbox"/> | EC2-Support | ▲ 0   | Defined     | 8 minutes ago |
| <input type="checkbox"/> | S3-Support  | ▲ 0   | Defined     | 8 minutes ago |

## 12. Click the **EC2-Support** group.

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

## 13. Click 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

Delete

### Summary

Edit

| User group name<br>EC2-Support                                                                                                                                                                                                                                                                       | Creation time<br>September 24, 2021, 16:24 (UTC+05:30) | ARN<br>arn:aws:iam::364574194039:group/spl66/EC2-Support |                                   |             |      |             |                          |                                         |             |                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|----------------------------------------------------------|-----------------------------------|-------------|------|-------------|--------------------------|-----------------------------------------|-------------|-----------------------------------|
| <hr/>                                                                                                                                                                                                                                                                                                |                                                        |                                                          |                                   |             |      |             |                          |                                         |             |                                   |
| <a href="#">Users</a> <a href="#">Permissions</a> <a href="#">Access advisor</a>                                                                                                                                                                                                                     |                                                        |                                                          |                                   |             |      |             |                          |                                         |             |                                   |
| <hr/>                                                                                                                                                                                                                                                                                                |                                                        |                                                          |                                   |             |      |             |                          |                                         |             |                                   |
| <b>Permissions policies (1)</b> <a href="#">Info</a>                                                                                                                                                                                                                                                 |                                                        |                                                          |                                   |             |      |             |                          |                                         |             |                                   |
| You can attach up to 10 managed policies.                                                                                                                                                                                                                                                            |                                                        |                                                          |                                   |             |      |             |                          |                                         |             |                                   |
| <a href="#">Filter policies by property or policy name and press enter</a>                                                                                                                                                                                                                           |                                                        |                                                          |                                   |             |      |             |                          |                                         |             |                                   |
| <a href="#">Simulate</a> <a href="#">Remove</a> <a href="#">Add permissions</a> ▾                                                                                                                                                                                                                    |                                                        |                                                          |                                   |             |      |             |                          |                                         |             |                                   |
| <hr/>                                                                                                                                                                                                                                                                                                |                                                        |                                                          |                                   |             |      |             |                          |                                         |             |                                   |
| <table><thead><tr><th><input type="checkbox"/></th><th>Policy Name</th><th>Type</th><th>Description</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td><a href="#">AmazonEC2ReadOnlyAccess</a></td><td>AWS managed</td><td>Provides read only access to Amaz</td></tr></tbody></table> |                                                        |                                                          | <input type="checkbox"/>          | Policy Name | Type | Description | <input type="checkbox"/> | <a href="#">AmazonEC2ReadOnlyAccess</a> | AWS managed | Provides read only access to Amaz |
| <input type="checkbox"/>                                                                                                                                                                                                                                                                             | Policy Name                                            | Type                                                     | Description                       |             |      |             |                          |                                         |             |                                   |
| <input type="checkbox"/>                                                                                                                                                                                                                                                                             | <a href="#">AmazonEC2ReadOnlyAccess</a>                | AWS managed                                              | Provides read only access to Amaz |             |      |             |                          |                                         |             |                                   |
| <hr/>                                                                                                                                                                                                                                                                                                |                                                        |                                                          |                                   |             |      |             |                          |                                         |             |                                   |

#### 14. Under **Actions**, click the **Show Policy** link.

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. This ability to view resources, but not modify them, is ideal for assigning to a Support role.

The basic structure of the statements in an IAM Policy is:

- **Effect** says whether to *Allow* or *Deny* the permissions.
- **Action** specifies the API calls that can be made against an AWS Service (eg *cloudwatch:ListMetrics*).
- **Resource** defines the scope of entities covered by the policy rule (eg a specific Amazon S3 bucket or Amazon EC2 instance, or \* which means *any resource*).

| <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Policy Name             | Type        | Description                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-------------|-------------------------------------------------------------------------|
| <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | AmazonEC2ReadOnlyAccess | AWS managed | Provides read only access to Amazon EC2 via the AWS Management Console. |
| <b>AmazonEC2ReadOnlyAccess</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                         |             |                                                                         |
| Provides read only access to Amazon EC2 via the AWS Management Console.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                         |             |                                                                         |
| <pre> 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 }</pre> |                         |             |                                                                         |

15. Close the **Show Policy** window.

16. In the navigation pane on the left, click **Groups**.

17. Click the **S3-Support** group.

The S3-Support group has the **AmazonS3ReadOnlyAccess** policy attached.

IAM > User groups > S3-Support

## S3-Support

[Delete](#)

### Summary

[Edit](#)

|                 |                                       |                                                                  |
|-----------------|---------------------------------------|------------------------------------------------------------------|
| User group name | Creation time                         | ARN                                                              |
| S3-Support      | September 24, 2021, 16:24 (UTC+05:30) | <a href="#">arn:aws:iam::364574194039:group/spl66/S3-Support</a> |

| <input type="checkbox"/>                                                                                                                                                                                               | Users                  | Permissions | Access advisor                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|-------------|-------------------------------------|
| <b>Permissions policies (1) <a href="#">Info</a></b>                                                                                                                                                                   |                        |             |                                     |
| You can attach up to 10 managed policies.                                                                                                                                                                              |                        |             |                                     |
| <input type="text"/> Filter policies by property or policy name and press enter <span style="float: right;"><a href="#">⟳</a> <a href="#">Simulate</a> <a href="#">Remove</a> <a href="#">Add permissions</a> ▾</span> |                        |             |                                     |
| <input type="checkbox"/>                                                                                                                                                                                               | Policy Name            | Type        | Description                         |
| <input type="checkbox"/>                                                                                                                                                                                               | AmazonS3ReadOnlyAccess | AWS managed | Provides read only access to all bu |

18. Below the **Actions** menu, click the **Show Policy** link.

This policy has permissions to Get and List resources in Amazon S3.

| Policy Name                   | Type        | Description                        |
|-------------------------------|-------------|------------------------------------|
| AmazonS3ReadOnlyAccess        | AWS managed | Provides read only access to all t |
| <b>AmazonS3ReadOnlyAccess</b> |             |                                    |

Provides read only access to all buckets via the AWS Management Console.

```

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

19. Close the **Show Policy** window.

20. In the navigation pane on the left, click **Groups**.

21. Click the **EC2-Admin** group.

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.

## EC2-Admin

[Delete](#)

### Summary

[Edit](#)

|                 |                                       |                                                                 |
|-----------------|---------------------------------------|-----------------------------------------------------------------|
| User group name | Creation time                         | ARN                                                             |
| EC2-Admin       | September 24, 2021, 16:24 (UTC+05:30) | <a href="#">arn:aws:iam::364574194039:group/spl66/EC2-Admin</a> |

[Users](#)

[Permissions](#)

[Access advisor](#)

### Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

[Filter policies by property or policy name and press enter](#)

[Simulate](#)

[Remove](#)

[Add permissions](#) ▾

| Policy Name                      | Type            | Description |
|----------------------------------|-----------------|-------------|
| <a href="#">EC2-Admin-Policy</a> | Customer inline |             |

22. Under **Actions**, click **Show Policy** to view the policy.

This policy grants permission to view (Describe) information about Amazon EC2 and also the ability to Start and Stop instances.

The screenshot shows the AWS IAM Policy Editor interface. At the top, there's a header with 'Policy Name' (set to 'EC2-Admin-Policy'), 'Type' (set to 'Customer inline'), and 'Description'. Below the header, the policy document is displayed in JSON format:

```
1 {
2 "Version": "2012-10-17",
3 "Statement": [
4 {
5 "Action": [
6 "ec2:Describe*",
7 "ec2:StartInstances",
8 "ec2:StopInstances"
9],
10 "Resource": ["*"],
11 "Effect": "Allow"
12 }
13]
14}
15 }
16]
```

On the right side of the JSON editor, there's a 'Copy' button.

23. At the bottom of the screen, click **Cancel** to close the policy.

## Business Scenario

For the remainder of this lab, you will work with these Users and Groups to enable permissions supporting the following business scenario:

Your company is growing its use of Amazon Web Services, and is using many Amazon EC2 instances and a great deal of Amazon S3 storage. You wish to give access to new staff depending upon their job function:

| User   | In Group    | Permissions                               |
|--------|-------------|-------------------------------------------|
| user-1 | S3-Support  | Read-Only access to Amazon S3             |
| user-2 | EC2-Support | Read-Only access to Amazon EC2            |
| user-3 | EC2-Admin   | View, Start and Stop Amazon EC2 instances |

## Task 2: Add Users to Groups

You have recently hired **user-1** into a role where they will provide support for Amazon S3. You will add them to the **S3-Support** group so that they inherit the necessary permissions via the attached *AmazonS3ReadOnlyAccess* policy.

You can ignore any "not authorized" errors that appear during this task. They are caused by your lab account having limited permissions and will not impact your ability to complete the lab.

## Add user-1 to the S3-Support Group

24. In the left navigation pane, click **Groups**.

25. Click the **S3-Support** group.

26. Click the **Users** tab.

The screenshot shows the AWS IAM Groups page. At the top, there's a summary for the 'S3-Support' group, including its name, creation time (September 24, 2021, 16:24 UTC+05:30), and ARN (arn:aws:iam::364574194039:group/spl66/S3-Support). Below the summary, there are three tabs: 'Users' (which is selected and highlighted in orange), 'Permissions', and 'Access advisor'. Under the 'Users' tab, there's a section titled 'Users in this group (0)'. It includes a search bar, a refresh button, and buttons for 'Remove users' and 'Add users'. A note states: 'An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.' Below this, there's a table header with columns: 'User name' (with a dropdown arrow), 'Groups' (with a dropdown arrow), 'Last activity' (with a dropdown arrow), and 'Creation time' (with a dropdown arrow). The table body is empty, displaying the message 'No resources to display'.

27. In the **Users** tab, click **Add Users to Group**.

28. In the **Add Users to Group** window, configure the following:

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

The screenshot shows the AWS IAM console. On the left, a sidebar lists 'Identity and Access Management (IAM)' with sections for Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)). The main content area is titled 'Add users to S3-Support'. It shows a table of 'Other users in this account (Selected 1/4)'. The table has columns: User name, Groups, Last activity, and Creation time. A checkbox next to 'awsstudent' is unchecked. A checked checkbox next to 'user-1' highlights it. Other users listed are 'user-2' and 'user-3', both with unchecked checkboxes. At the bottom right are 'Cancel' and 'Add users' buttons.

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

The screenshot shows the 'Users' tab in the AWS IAM console. The top navigation bar includes 'Feedback', 'English (US)', 'Privacy Policy', 'Terms of Use', and 'Cookie preferences'. Below the navigation is a search bar and a toolbar with icons for various services. The main content area is titled 'Users in this group (1)'. It shows a table with one user, 'user-1', listed. The table columns are: User name, Groups, Last activity, and Creation time. The 'Groups' column shows 'S3-Support'. At the bottom right are 'Remove users' and 'Add users' buttons.

## Add user-2 to the EC2-Support Group

You have hired **user-2** into a role where they will provide support for Amazon EC2.

29. 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.

## EC2-Support

[Delete](#) [Edit](#)

### Summary

|                                |                                                        |                                                          |
|--------------------------------|--------------------------------------------------------|----------------------------------------------------------|
| User group name<br>EC2-Support | Creation time<br>September 24, 2021, 16:24 (UTC+05:30) | ARN<br>arn:aws:iam::364574194039:group/spl66/EC2-Support |
|--------------------------------|--------------------------------------------------------|----------------------------------------------------------|

[Users](#) [Permissions](#) [Access advisor](#)

#### Users in this group (1) [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

| <input type="checkbox"/> | User name | Groups | Last activity | Creation time  |
|--------------------------|-----------|--------|---------------|----------------|
| <input type="checkbox"/> | user-2    | 1      | None          | 21 minutes ago |

## Add user-3 to the EC2-Admin Group

You have hired **user-3** as your Amazon EC2 administrator, who will manage your EC2 instances.

30. 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.

## EC2-Admin

[Delete](#) [Edit](#)

### Summary

|                              |                                                        |                                                        |
|------------------------------|--------------------------------------------------------|--------------------------------------------------------|
| User group name<br>EC2-Admin | Creation time<br>September 24, 2021, 16:24 (UTC+05:30) | ARN<br>arn:aws:iam::364574194039:group/spl66/EC2-Admin |
|------------------------------|--------------------------------------------------------|--------------------------------------------------------|

[Users](#) [Permissions](#) [Access advisor](#)

#### Users in this group (1) [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

| <input type="checkbox"/> | User name | Groups | Last activity | Creation time  |
|--------------------------|-----------|--------|---------------|----------------|
| <input type="checkbox"/> | user-3    | 1      | None          | 22 minutes ago |

31. In the navigation pane on the left, click **Groups**.  
Each Group should 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 to ensure that each user is assigned to a Group, as shown in the table in the Business Scenario section.

| User groups (3) <small>Info</small>                                                                     |             |       |             |                | <small>Delete</small> | <small>Create group</small> |
|---------------------------------------------------------------------------------------------------------|-------------|-------|-------------|----------------|-----------------------|-----------------------------|
| A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. |             |       |             |                |                       |                             |
| Group name                                                                                              |             | Users | Permissions | Creation time  |                       |                             |
| <input type="checkbox"/>                                                                                | EC2-Admin   | 1     | Defined     | 22 minutes ago |                       |                             |
| <input type="checkbox"/>                                                                                | EC2-Support | 1     | Defined     | 22 minutes ago |                       |                             |
| <input type="checkbox"/>                                                                                | S3-Support  | 1     | Defined     | 22 minutes ago |                       |                             |

## Task 3: Sign-In and Test Users

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

32. In the navigation pane on the left, click **Dashboard**.

An **IAM users sign-in link** is displayed It will look similar to:

<https://123456789012.signin.aws.amazon.com/console>

This link can be used to sign-in to the AWS Account you are currently using.

The screenshot shows the AWS IAM Dashboard. On the left, the navigation pane includes sections for Identity and Access Management (IAM), Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)). The main content area features a banner about the new IAM dashboard experience. Below it, the "IAM dashboard" section displays "Security recommendations" (Add MFA for root user) and "IAM resources" (User groups: 3, Users: 4, Roles: 14, Policies: 1, Identity providers: 0). A "What's new" section lists recent updates from the IAM Access Analyzer and AWS Amplify. To the right, there are sections for "AWS Account" (Account ID: 364574194039, Account Alias: 364574194039, Sign-In URL: https://364574194039.signin.aws.amazon.com/console) and "Tools" (Policy simulator, Web identity federation playground). The bottom of the screen shows a Windows taskbar with various icons and system status.

33. Copy the **IAM users sign-in link** to a text editor.

34. Open a private window.

#### Mozilla Firefox

- Click the menu bars at the top-right of the screen
- Select **New Private Window**

35. Google Chrome

- Click the ellipsis at the top-right of the screen
- Click **New incognito window**

36. Microsoft Edge

- Click the ellipsis at the top-right of the screen
- Click **New InPrivate window**

37. Microsoft Internet Explorer

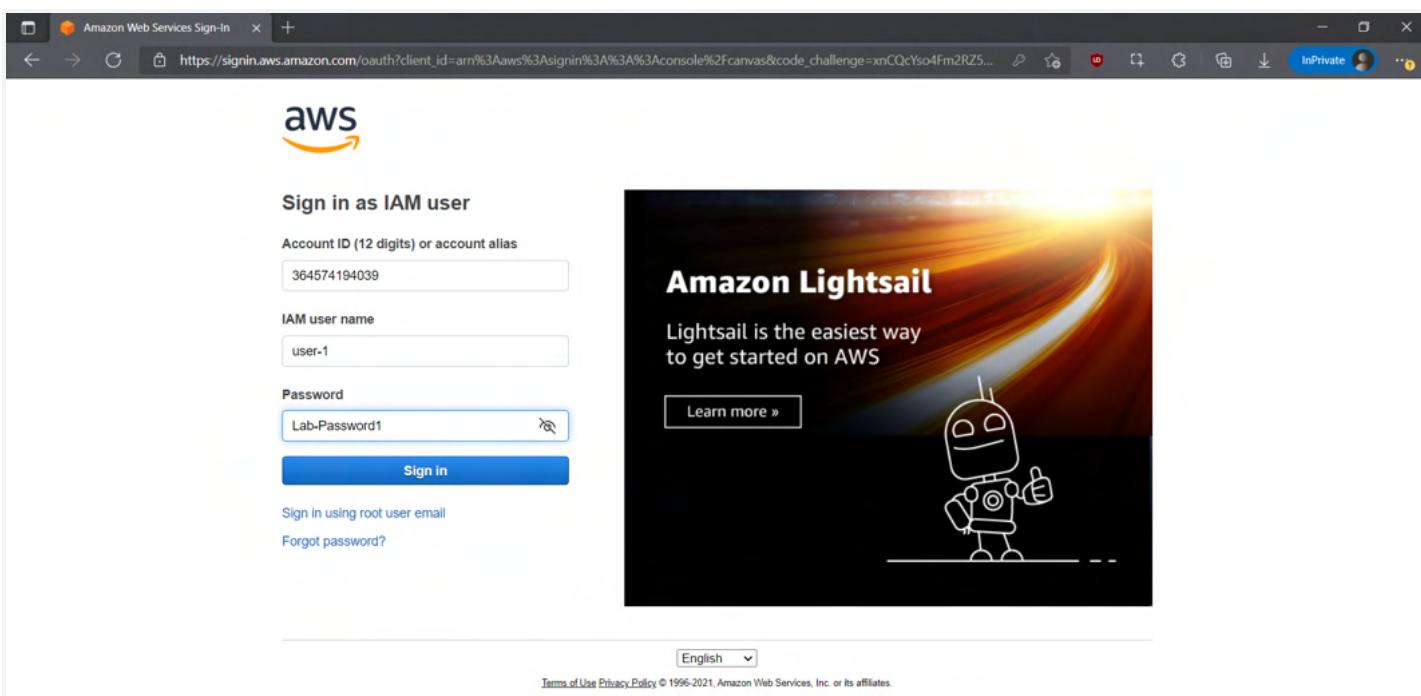
- Click the **Tools** menu option
- Click **InPrivate Browsing**

38. Paste the IAM users sign-in link into your private window and press **Enter**.

You will now sign-in as **user-1**, who has been hired as your Amazon S3 storage support staff.

39. Sign-in with:

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



40. In the **Services** menu, click **S3**.

41. Click the name of one of your buckets 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 their contents.

Now, test whether they have access to Amazon EC2.

The screenshot shows the AWS S3 Management Console. On the left, there's a navigation pane with sections like Buckets, Storage Lens, and Feature spotlight. The main area displays an 'Account snapshot' with a link to 'View Storage Lens dashboard'. Below it is a table titled 'Buckets (1) Info' showing one bucket named 'samplebucket--a7efaa60' located in 'US East (N. Virginia) us-east-1'. The bucket has 'Objects can be public' access and was created on 'September 24, 2021, 16:23:38 (UTC+05:30)'. There are buttons for Copy ARN, Empty, Delete, and Create bucket.

This screenshot shows the 'Objects' tab for the 'samplebucket--a7efaa60' bucket. The top navigation bar includes tabs for Objects, Properties, Permissions, Metrics, Management, and Access Points. The 'Objects (0)' section indicates there are no objects in the bucket. It features a search bar and buttons for Upload, Copy S3 URI, Copy URL, Download, Open, Delete, Actions, and Create folder. A note at the bottom says 'No objects' and 'You don't have any objects in this bucket.'

42. In the **Services** menu, click **EC2**.

43. In the left navigation pane, click **Instances**.

You cannot see any instances! Instead, it says *You do not have any instances in this region.*

This is because your user has not been assigned any permissions to use Amazon EC2.

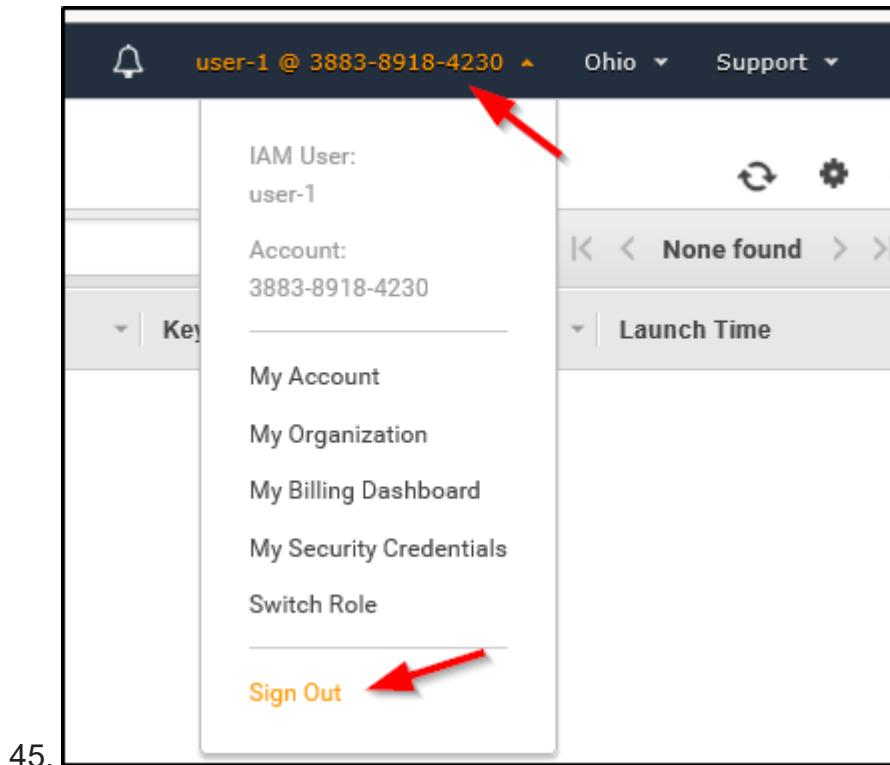
You will now sign-in as **user-2**, who has been hired as your Amazon EC2 support person.

The screenshot shows the AWS Management Console for the EC2 service. The left sidebar includes links for EC2 Dashboard, Instances (with sub-links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, and Capacity Reservations), Images (AMIs), and Elastic Block Store (Volumes, Snapshots). The main content area has a 'Resources' section listing various EC2 components with 'API Error' status icons. Below this is a callout for Microsoft SQL Server Always On availability groups. To the right is a 'Service health' section showing the US East (Ohio) region with a green status indicator for 'This service is operating normally'. A sidebar on the right contains 'Account attributes' like Supported platforms, Default VPC, and EBS encryption.

This screenshot shows the 'Instances' page within the EC2 Management service. The left sidebar is identical to the previous one. The main area features a table titled 'Instances Info' with columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. A message 'You are not authorized to perform this operation.' is centered above the table. At the bottom, a modal window titled 'Select an instance above' is open, indicating that no specific instance is selected.

44. Sign user-1 out of the **AWS Management Console** by configuring the following:

- At the top of the screen, click **user-1**
- Click **Sign Out**



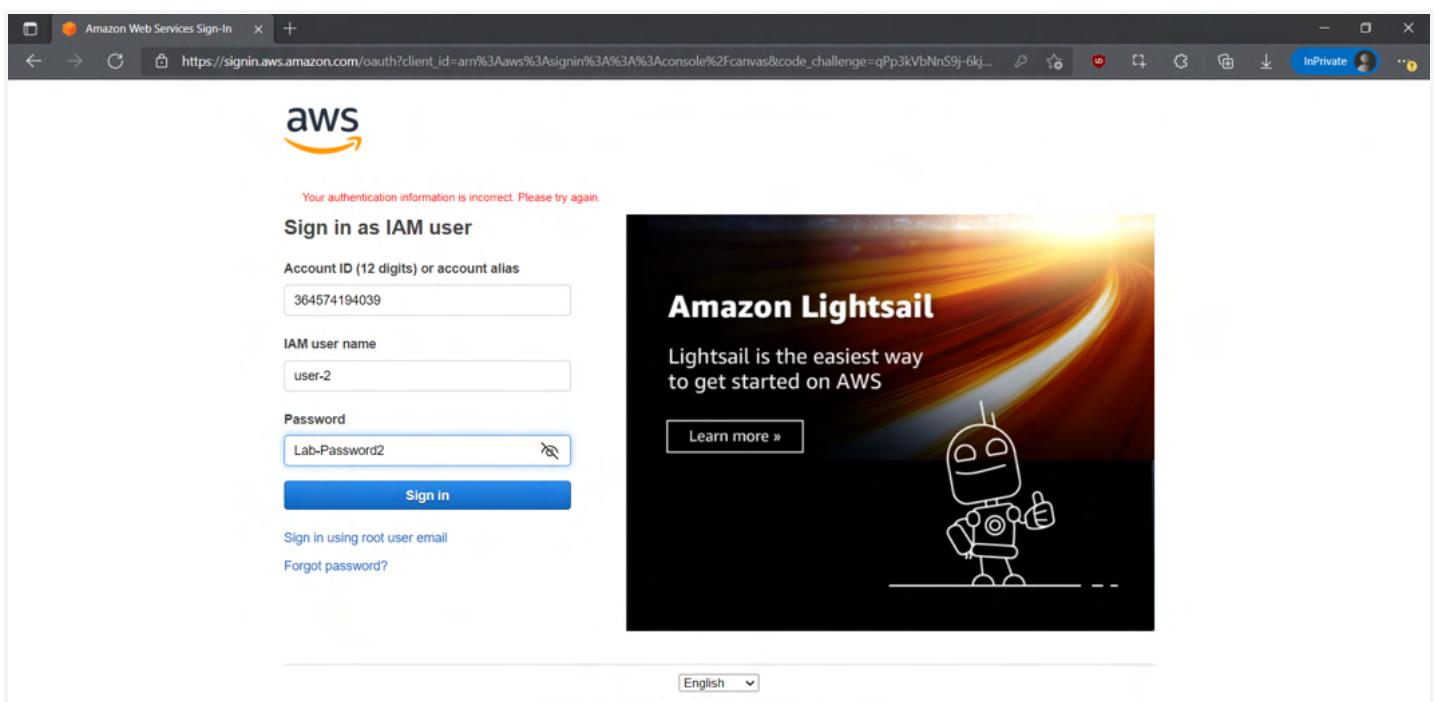
45.

46. Paste the **IAM users sign-in** link into your private window and press **Enter**.

This links should be in your text editor.

47. Sign-in with:

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

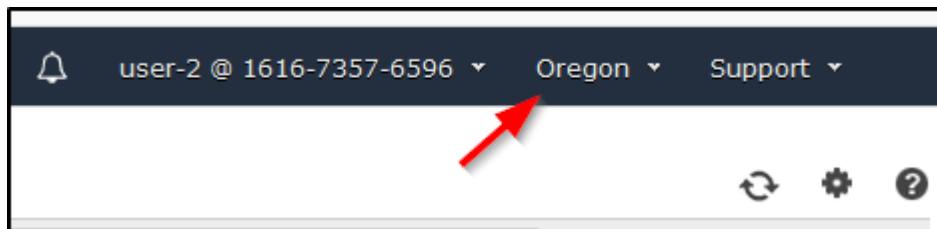


48. In the **Services** menu, click **EC2**.

49. In the navigation pane on the left, click **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 (e.g., **N. Virginia**).



Your EC2 instance should be selected . If it is not selected, select the instance named *LabHost* .

A screenshot of the AWS EC2 Instances page. The left sidebar shows navigation options like EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (selected), Images, and Elastic Block Store. The main content area shows a table of instances. One instance, "LabHost" (ID i-03278d4a7782d5164), is selected and highlighted with a blue checkmark. Its details are shown in a modal window below. The "Bastion Host" (ID i-06022c13118850666) is also listed but not selected. The modal window for "LabHost" displays its instance ID, public and private IP addresses, and state as "Running".

| Name         | Instance ID         | Instance state | Instance type | Status check      | Alarm status | Availability Zone | Public IPv4 DNS |
|--------------|---------------------|----------------|---------------|-------------------|--------------|-------------------|-----------------|
| LabHost      | i-03278d4a7782d5164 | Running        | t2.micro      | 2/2 checks passed | No alarms    | us-east-1a        | ec2-3-80-234-16 |
| Bastion Host | i-06022c13118850666 | Running        | t2.micro      | 2/2 checks passed | No alarms    | us-east-1a        | ec2-54-80-93-85 |

50. In the **Instance state** menu, choose **Stop instance**.

The screenshot shows the AWS EC2 Management Console interface. On the left, a sidebar lists various EC2-related options like Instances, Images, and Elastic Block Store. The main area displays two instances: 'LabHost' and 'Bastion Host', both in the 'running' state. A modal window titled 'Stop instance?' is centered over the 'LabHost' row, prompting the user to confirm the action. The modal contains the instance ID 'i-03278d4a7782d5164 (LabHost)' and a confirmation message. At the bottom of the modal are 'Cancel' and 'Stop' buttons.

## 51. In the **Stop Instance** window, click **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.

The screenshot shows the same EC2 Management Console interface as before, but the 'Stop instance?' modal has been closed. Instead, an error message is displayed in a red box at the top of the page: 'Failed to stop the instance i-03278d4a7782d5164. You are not authorized to perform this operation. Encoded authorization failure message: 4CWRq28jH0kCSLUt0TbJU85U6ej8-NDMDWaVtzkeFxlidwrHUF824Q5Gv7...'. Below the error message, the instance list and details are visible, showing the two instances and their current states.

## 52. At the **Stop instances** window, click **Cancel**.

Next, check if user-2 can access Amazon S3.

53. In the **Services**, click **S3**.

You will receive an **Error Access Denied** because user-2 does not have permission to use Amazon S3.

The screenshot shows the AWS S3 Management Console interface. On the left, there's a sidebar with options like Buckets, Storage Lens, and Feature spotlight. The main area has a heading 'Amazon S3' and a section titled 'Account snapshot'. Below it is a table for 'Buckets (0)'. A red box highlights an error message: 'You don't have permissions to list buckets. After you or your AWS administrator have updated your permissions to allow the s3>ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3'. At the bottom of the screen, the Windows taskbar is visible with various icons and the date/time '24-09-2021 04:59 PM'.

You will now sign-in as **user-3**, who has been hired as your Amazon EC2 administrator.

54. Sign user-2 out of the **AWS Management Console** by configuring the following:

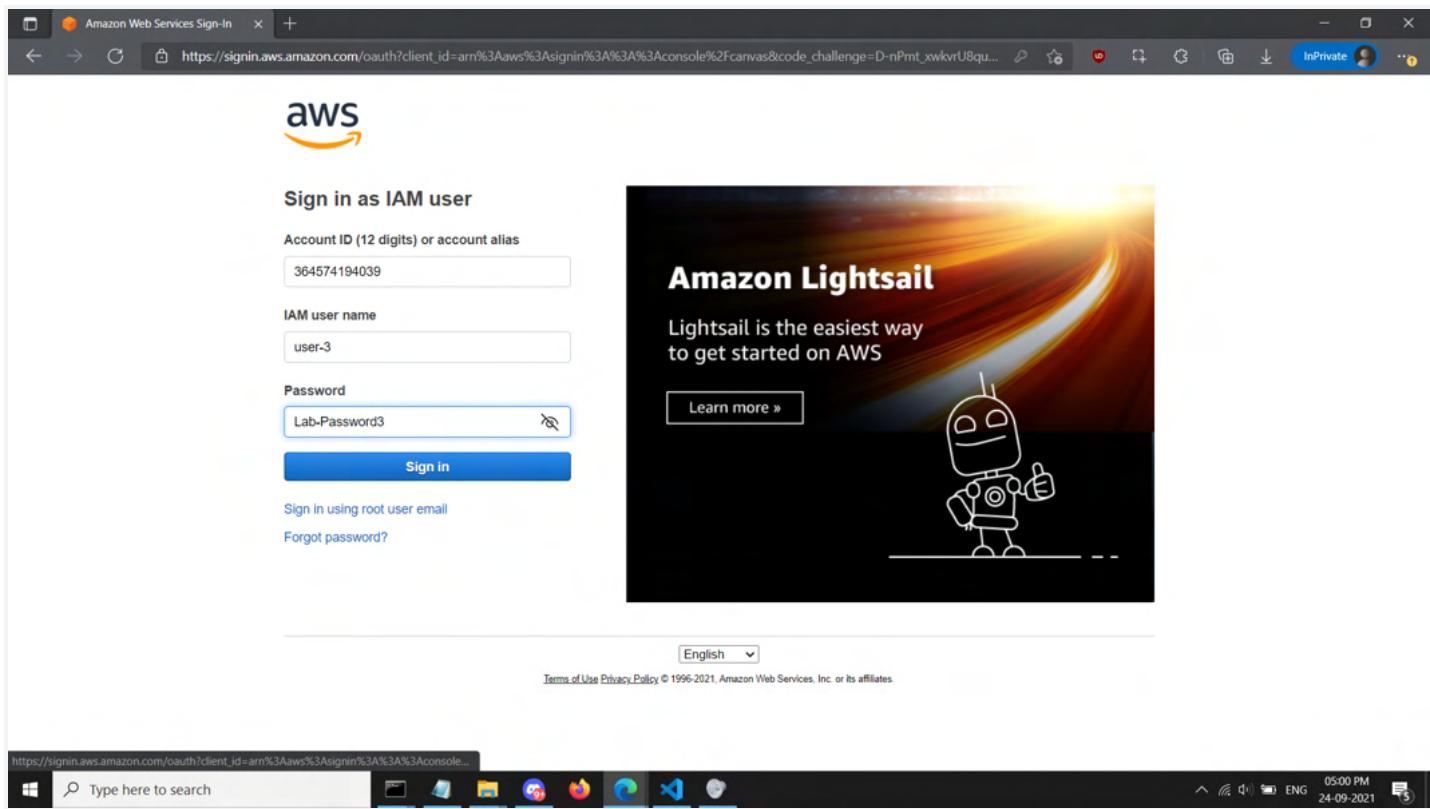
- At the top of the screen, click **user-2**
- Click **Sign Out**

55. Paste the **IAM users sign-in** link into your private window and press **Enter**.

56. Paste the sign-in link into your web browser address bar again. If it is not in your clipboard, retrieve it from the text editor where you stored it earlier.

57. Sign-in with:

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



58. In the **Services** menu, click **EC2**.

59. In the navigation pane on the left, click **Instances**.

As an EC2 Administrator, you should now have permissions to Stop the Amazon EC2 instance.

Your EC2 instance should be selected . If it is not, please select the instance named *LabHost* .

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

60. In the **Instance state** menu, choose **Stop instance**.

The screenshot shows the AWS EC2 Management Console. On the left, there's a navigation sidebar with options like EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (selected), Images, and Elastic Block Store. The main area displays a table of instances. One instance, 'LabHost' (ID: i-03278d4a7782d5164), is selected and highlighted in blue. A context menu is open over this instance, with 'Stop instance' being the chosen option. Below the table, a detailed view of 'LabHost' is shown, including its instance ID, public and private IP addresses, and current state (Running). The status bar at the bottom indicates the user is in an InPrivate window.

61. In the **Stop instance** window, click **Stop**.

The instance will enter the *stopping* state and will shutdown.

This screenshot shows the same EC2 Management Console interface after the instance has been stopped. The 'LabHost' instance is now listed with a status of 'Stopping'. A prominent green banner at the top of the page reads 'Successfully stopped i-03278d4a7782d5164'. The rest of the interface remains largely the same, with the instance details page still visible below.

62. Close your private window.

## CONCLUSION

Congratulations! You now have successfully:

- Explored pre-created IAM users and groups
- Inspected IAM policies as applied to the pre-created groups
- Followed a real-world scenario, adding users to groups with specific capabilities enabled
- Located and used the IAM sign-in URL
- Experimented with the effects of policies on service access

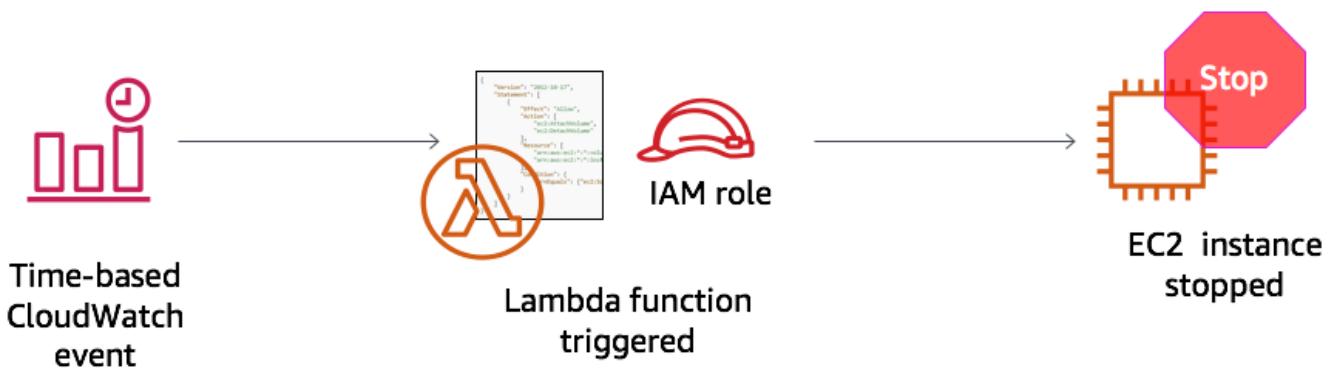
# Activity 1

## AIM

AWS Lambda

## THEORY

In this hands-on activity, you will create an AWS Lambda function. You will also create an Amazon CloudWatch event to trigger the function every minute. The function uses an AWS Identity and Access Management (IAM) role. This IAM role allows the function to stop an Amazon Elastic Compute Cloud (Amazon EC2) instance that is running in the Amazon Web Services (AWS) account.



## PROCEDURE

### Task 1: Create a Lambda function

5. In the AWS Management Console, from the Services menu, choose Lambda.  
Note: If you see a warning message that says *tags failed to load*, you can ignore it.

The screenshot shows the AWS Lambda Functions page in the AWS Management Console. The browser address bar shows the URL <https://console.aws.amazon.com/lambda/home?region=us-east-1#/functions>. The page displays a message: 'Tags failed to load. The filter doesn't include tags.' Below this, there is a 'Functions (0)' section with a 'Create function' button. A search bar and a table header with columns for 'Function name', 'Description', 'Package type', 'Runtime', 'Code size', and 'Last modified' are visible. The message 'There is no data to display.' is centered at the bottom of the table area.

6. Click **Create function**.
7. In the Create function screen, configure these settings:

- Choose Author from scratch
- Function name: myStopinator
- Runtime: Python 3.8
- Click Choose or create an execution role
- Execution role: Use an existing role
- Existing role: From the dropdown list, choose myStopinatorRole

Lambda > Functions > Create function

## Create function Info

Choose one of the following options to create your function.

**Author from scratch**

Start with a simple Hello World example.

**Use a blueprint**

Build a Lambda application from sample code and configuration presets for common use cases.

**Container image**

Select a container image to deploy for your function.

**Browse serverless app repository**

Deploy a sample Lambda application from the AWS Serverless Application Repository.

---

### Basic information

Function name Info  
Enter a name that describes the purpose of your function.  
  
Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info  
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.

---

### Permissions Info

By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

▼ Change default execution role

Execution role  
Choose a role that defines the permissions of your function. To create a custom role, go to the [IAM console](#).

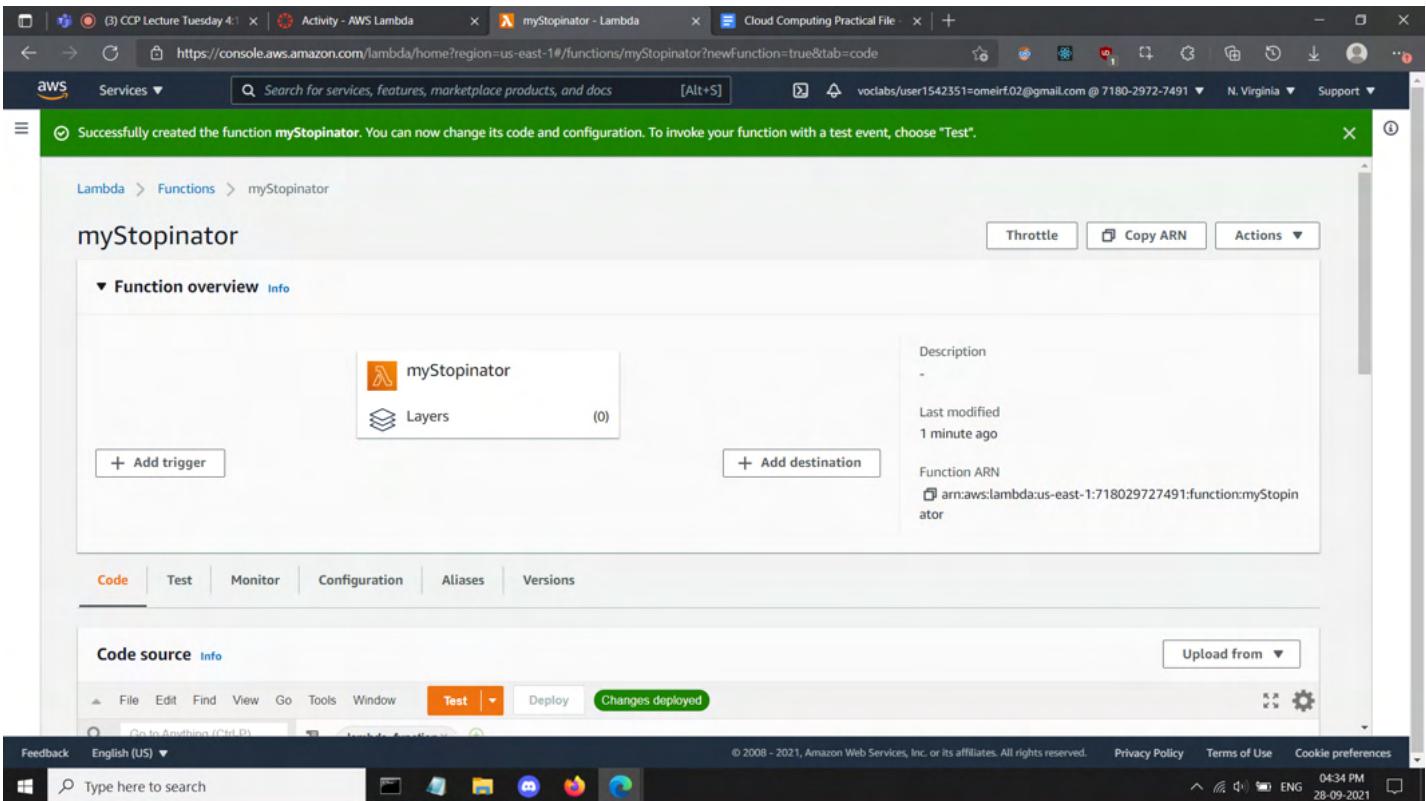
Create a new role with basic Lambda permissions

Use an existing role

- [myStopinatorRole](#)
- [robomaker\\_students](#)
- [myStopinatorRole](#)

[View the myStopinatorRole role on the IAM console.](#)

8. Click **Create function**.



## Task 2: Configure the trigger

In this task, you will configure a scheduled event to trigger the Lambda function by setting a CloudWatch event as the event source (or trigger). The Lambda function can be configured to operate much like a cron job on a Linux server, or a scheduled task on a Microsoft Windows server. However, you do not need to have a server running to host it.

9. Click **+ Add trigger**.
10. Click the **Select a trigger** dropdown menu, and choose **EventBridge (CloudWatch Events)**.
11. For the rule, choose **Create a new rule** and configure these settings:
  - Rule name: everyMinute
  - Rule type: **Schedule expression**
  - Schedule expression: rate(1 minute)

## Trigger configuration



EventBridge (CloudWatch Events)  
aws events management-tools



### Rule

Pick an existing rule, or create a new one.

- Create a new rule
- Existing rules

### Rule name\*

Enter a name to uniquely identify your rule.

### Rule description

Provide an optional description for your rule.

### Rule type

Trigger your target based on an event pattern, or based on an automated schedule.

- Event pattern
- Schedule expression

### Schedule expression\*

Self-trigger your target on an automated schedule using Cron or rate expressions. Cron expressions are in UTC.

e.g. rate(1 day), cron(0 17 ? \* MON-FRI \*)

Lambda will add the necessary permissions for Amazon EventBridge (CloudWatch Events) to invoke your Lambda function from this trigger. [Learn more](#) about the Lambda permissions model.

Cancel

Add

12. **Note:** A more realistic, schedule-based stopinator Lambda function would probably be triggered by using a cron expression instead of a rate expression. However, for the purposes of this activity, using a rate expression ensures that the Lambda function will be triggered soon enough that you can see the results.

13. Click **Add**.

The trigger everyMinute was successfully added to function myStopinator. The function is now receiving events from the trigger.

Description

Last modified 4 minutes ago

Function ARN arn:aws:lambda:us-east-1:718029727491:function:myStopinator

## Task 3: Configure the Lambda function

In this task, you will paste a few lines of code to update two values in the function code. You do not need to write code to complete this task.

13. Below the **Function overview** pane, choose **Code**, and then choose *lambda\_function.py* to display and edit the Lambda function code.
14. In the **Code source** pane, delete the existing code. Copy the following code, and paste it in the box:

```
import json
def lambda_handler(event, context):
 # TODO implement
 return {
 'statusCode': 200,
 'body': json.dumps('Hello from Lambda!')
 }
```

```

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

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

```

**Note:** After pasting the code into the **Code source** box, review line 5. If a period (.) was added, delete it.

15. Replace the <REPLACE\_WITH\_REGION> placeholder with the actual Region that you are using.

To do this:

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

**Important:** Keep the single quotation marks (' ') around the Region in your code. For example, for the N. Virginia, it would be '*us-east-1*'

16. **Challenge section:** Verify that an EC2 instance named *instance1* is running in your account, and copy the *instance1* **instance ID**.

| Instances (1/2)                     |              | Info                |                                                                                                          |               | C                                                                                                                   | Connect                                                                                         | Instance state ▾  | Actions |
|-------------------------------------|--------------|---------------------|----------------------------------------------------------------------------------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-------------------|---------|
|                                     |              | Filter instances    |                                                                                                          |               |                                                                                                                     |                                                                                                 |                   |         |
|                                     | Name         | Instance ID         | Instance state                                                                                           | Instance type | Status check                                                                                                        | Alarm status                                                                                    | Availability Zone |         |
| <input checked="" type="checkbox"/> | instance1    | i-0432614646be41923 | <span>Running</span>  | t2.micro      | <span>2/2 checks passed</span>  | No alarms  | us-east-1a        |         |
| <input type="checkbox"/>            | Bastion Host | i-0d62733a011503a84 | <span>Running</span>  | t2.micro      | <span>2/2 checks passed</span>  | No alarms  | us-east-1a        |         |

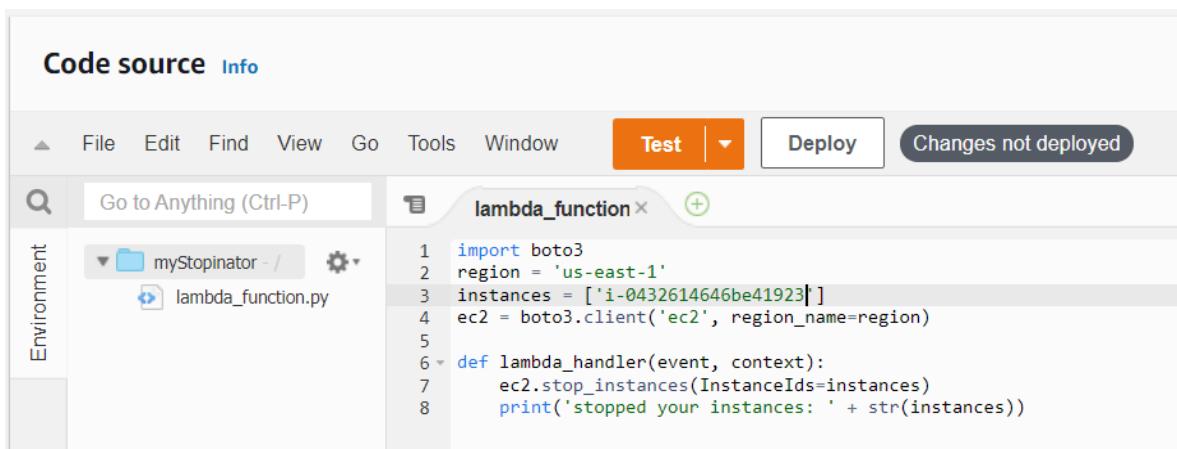
You are encouraged to figure out how to do this task without specific step-by-step guidance. However, if you need detailed guidance, [click here](#).

17. Return to the **AWS Lambda console** browser tab, and replace

<REPLACE\_WITH\_INSTANCE\_ID> with the actual instance ID that you just copied.

**Important:** Keep the single quotation marks (' ') around the instance ID in your code.

Your code should now look similar to the following example. However, you might have a different value for the Region, and you will have a different value for the instance ID:



The screenshot shows the AWS Lambda Code source editor interface. The top navigation bar includes File, Edit, Find, View, Go, Tools, Window, Test, Deploy, and Changes not deployed. The main area is titled 'lambda\_function' and contains the following Python code:

```

1 import boto3
2 region = 'us-east-1'
3 instances = ['i-0432614646be41923']
4 ec2 = boto3.client('ec2', region_name=region)
5
6 def lambda_handler(event, context):
7 ec2.stop_instances(InstanceIds=instances)
8 print('stopped your instances: ' + str(instances))

```

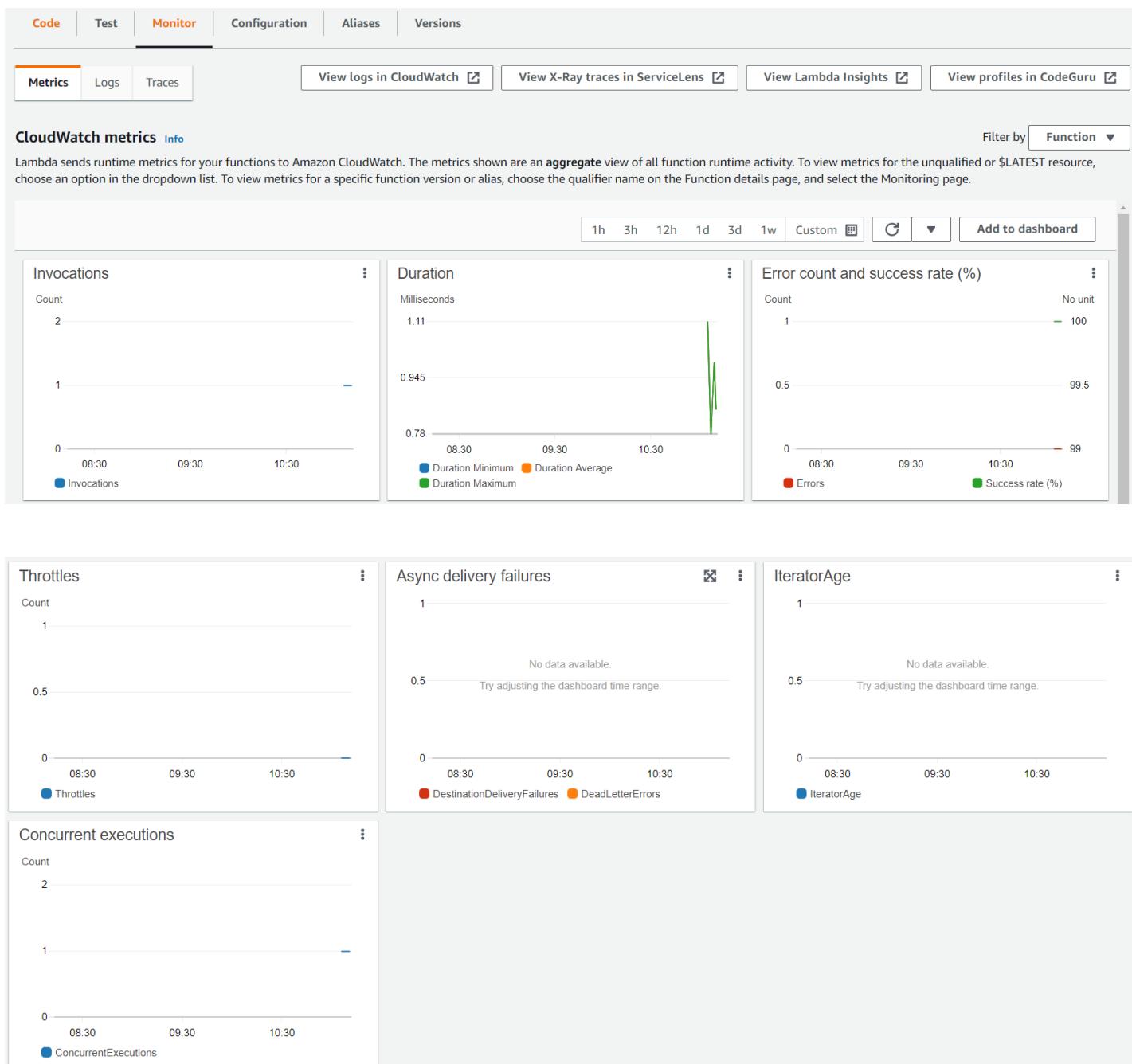
18. In the top-right corner of the **Code source** box, choose **Deploy**.

Your Lambda function is now fully configured. It should attempt to stop your instance every minute.

19. Click **Monitor** (the tab near the top of the page).

Note that one of the charts shows you how many times your function has been invoked.

There is also a chart that shows the error count and the success rate as a percentage.



## Task 4: Verify that the Lambda function worked

20. Return to the **Amazon EC2 console** browser tab and see if your instance was stopped.

**Tip:** You can click the refresh icon or refresh the browser page to see the change in state more quickly.

## Instances (2) [Info](#)

[Filter instances](#)

| <input type="checkbox"/> | Name         | Instance ID         | Instance state |  |
|--------------------------|--------------|---------------------|----------------|--|
| <input type="checkbox"/> | instance1    | i-0432614646be41923 | Stopping       |  |
| <input type="checkbox"/> | Bastion Host | i-0d62733a011503a84 | Running        |  |

21. Try starting the instance again. What do you think will happen?

*The instance will be stopped again within 1 minute.*

Successfully started i-0432614646be41923

## Instances (2) [Info](#)

[Connect](#)

Instance state

Actions

[Filter instances](#)

| <input type="checkbox"/> | Name         | Instance ID         | Instance state | Instance type | Status check      | Alarm status |
|--------------------------|--------------|---------------------|----------------|---------------|-------------------|--------------|
| <input type="checkbox"/> | instance1    | i-0432614646be41923 | Pending        | t2.micro      | -                 | No alarms    |
| <input type="checkbox"/> | Bastion Host | i-0d62733a011503a84 | Running        | t2.micro      | 2/2 checks passed | No alarms    |

Successfully started i-0432614646be41923

## Instances (1/2) [Info](#)

[Connect](#)

Instance state

Actions

[Filter instances](#)

| <input type="checkbox"/>            | Name         | Instance ID         | Instance state | Instance type | Status check      | Alarm status |
|-------------------------------------|--------------|---------------------|----------------|---------------|-------------------|--------------|
| <input checked="" type="checkbox"/> | instance1    | i-0432614646be41923 | Stopped        | t2.micro      | -                 | No alarms    |
| <input type="checkbox"/>            | Bastion Host | i-0d62733a011503a84 | Running        | t2.micro      | 2/2 checks passed | No alarms    |

# Activity 2

## AIM

AWS Elastic Beanstalk

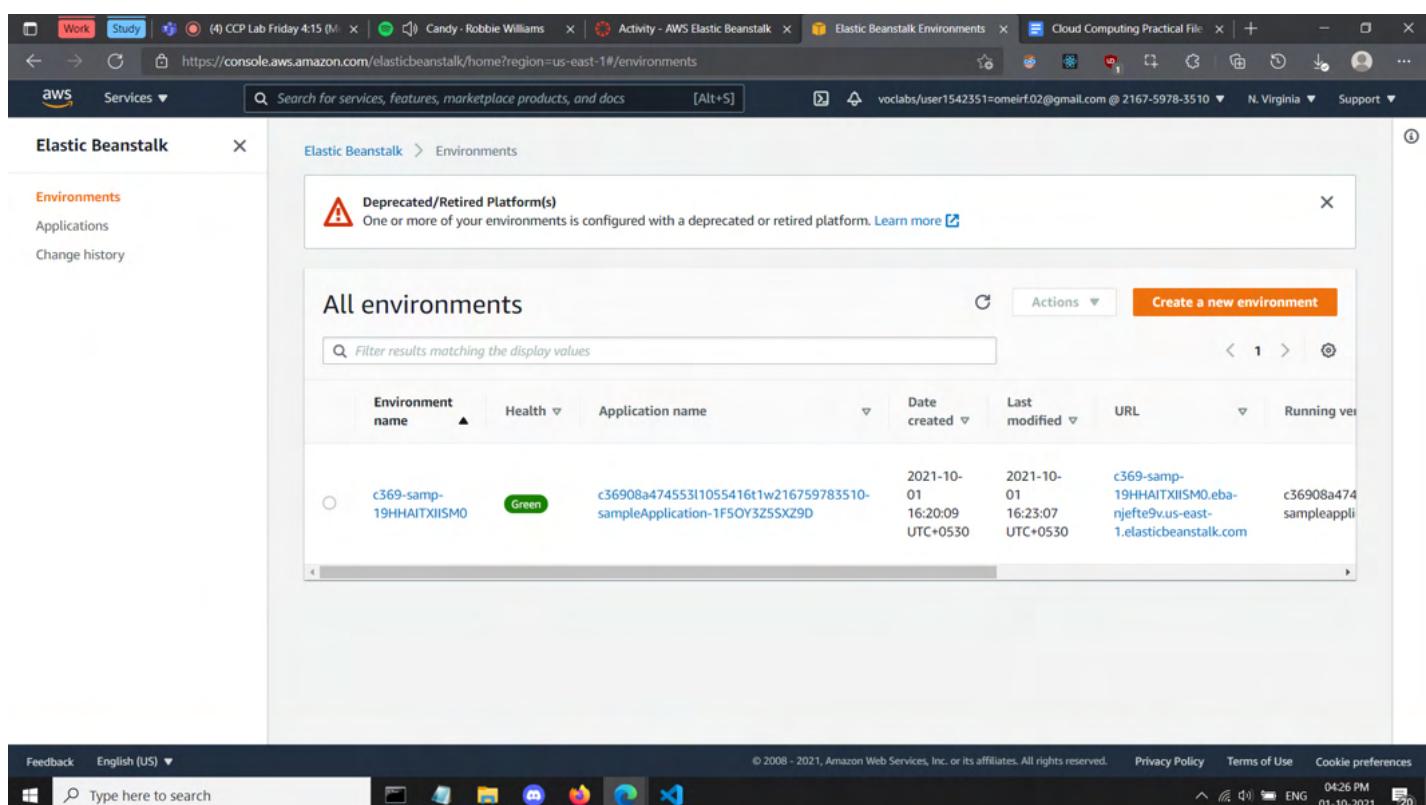
## THEORY

This activity provides you with an Amazon Web Services (AWS) account where an AWS Elastic Beanstalk environment has been pre-created for you. You will deploy code to it and observe the AWS resources that make up the Elastic Beanstalk environment.

## PROCEDURE

### Task 1: Access the Elastic Beanstalk environment

5. In the **AWS Management Console**, from the **Services** menu, choose **Elastic Beanstalk**. A page titled **All environments** should open, and it should show a table that lists the details for an existing Elastic Beanstalk application.  
**Note:** If the status in the **Health** column is not Green, it has not finished starting yet. Wait a few moments, and it should change to Green.



| Environment name       | Health | Application name                | Date created                 | Last modified                | URL                                                               | Running ver                                                         |
|------------------------|--------|---------------------------------|------------------------------|------------------------------|-------------------------------------------------------------------|---------------------------------------------------------------------|
| c369-samp-19HHAITXISM0 | Green  | sampleApplication-1F5OY3ZSSXZ9D | 2021-10-01 16:20:09 UTC+0530 | 2021-10-01 16:23:07 UTC+0530 | c369-samp-19HHAITXISM0.eba-njeftev.us-east-1.elasticbeanstalk.com | c36908a4745531055416t1w216759783510-sampleapplication-1F5OY3ZSSXZ9D |

6. Under the **Environment name** column, click on the name of the environment. The **Dashboard** page for your Elastic Beanstalk environment opens.

7. Notice that the page shows that the health of your application is Green (good).  
The Elastic Beanstalk environment is ready to host an application. However, it does not yet have running code.
8. Near the top of the page, click the URL (the URL ends in *elasticbeanstalk.com*).  
When you click the URL, a new browser tab opens. However, you should see that it displays an "*HTTP Status 404 - Not Found*" message. *This behavior is expected* because this application server doesn't have an application running on it yet. Return to the Elastic Beanstalk console.

The screenshot shows a browser window with multiple tabs open. The active tab displays an 'HTTP Status 404 – Not Found' error page. The page includes sections for 'Type' (Status Report), 'Message' (The requested resource [/] is not available), and 'Description' (The origin server did not find a current representation for the target resource or is not willing to disclose that one exists.). Below this, it says 'Apache Tomcat/8.5.63'. The URL in the address bar is 'c369-samp-19hhaitxiism0.eba-njefte9v.us-east-1.elasticbeanstalk.com'.

## HTTP Status 404 – Not Found

### Type Status Report

**Message** The requested resource [/] is not available

**Description** The origin server did not find a current representation for the target resource or is not willing to disclose that one exists.

### Apache Tomcat/8.5.63

In the next step, you will deploy code in your Elastic Beanstalk environment.

## Task 2: Deploy a sample application to Elastic Beanstalk

9. To download a sample application, click this link:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/samples/tomcat.zip>

10. Back in the Elastic Beanstalk Dashboard, click **Upload and Deploy**.

11. Click **Browse or Choose File**, then navigate to and open the **tomcat.zip** file that you just downloaded.

The screenshot shows the AWS Elastic Beanstalk console. On the left, there's a sidebar with options like Environments, Applications, Change history, Application versions, and Saved configurations. The main area shows an environment named 'c369-samp-19hhaitxiism0'. A modal window titled 'Upload and deploy' is open. It contains a message to deploy a previous version, a 'Choose file' button with 'tomcat.zip' selected, a 'Version label' input field with 'c36908a4745531055416t1w216759783510-samp', and a 'Deployment Preferences' section indicating 'All at once' policy with 2 instances. At the bottom are 'Cancel' and 'Deploy' buttons. The right side of the screen shows the environment details: Tomcat 8.5 with Java 8 running on 64bit Amazon Linux/3.4.10, with a 'Deployed' status and a yellow cat icon.

12. Click **Deploy**.

It will take a minute or two for Elastic Beanstalk to update your environment and deploy the application.

**Note:** If you see a warning in the Elastic Beanstalk dashboard page that an instance profile is required to integrate with the AWS X-Ray service, you can ignore the warning.

Elastic Beanstalk is updating your environment.  
To cancel this operation select Abort Current Operation from the Actions dropdown.  
[View Events](#)

**Deprecated platform**  
This environment uses a deprecated platform branch. We recommend that you upgrade to a supported platform branch. A deprecated branch may have a scheduled retirement date. It still receives ongoing maintenance updates. [Info](#)

**c369-samp-19HHAITXIISM0**

c369-samp-19HHAITXIISM0.eba-njfte9v.us-east-1.elasticbeanstalk.com (e-spet2n3gnq)  
Application name: c36908a474553l1055416t1w216759783510-sampleApplication-1F50Y3Z5SXZ9D

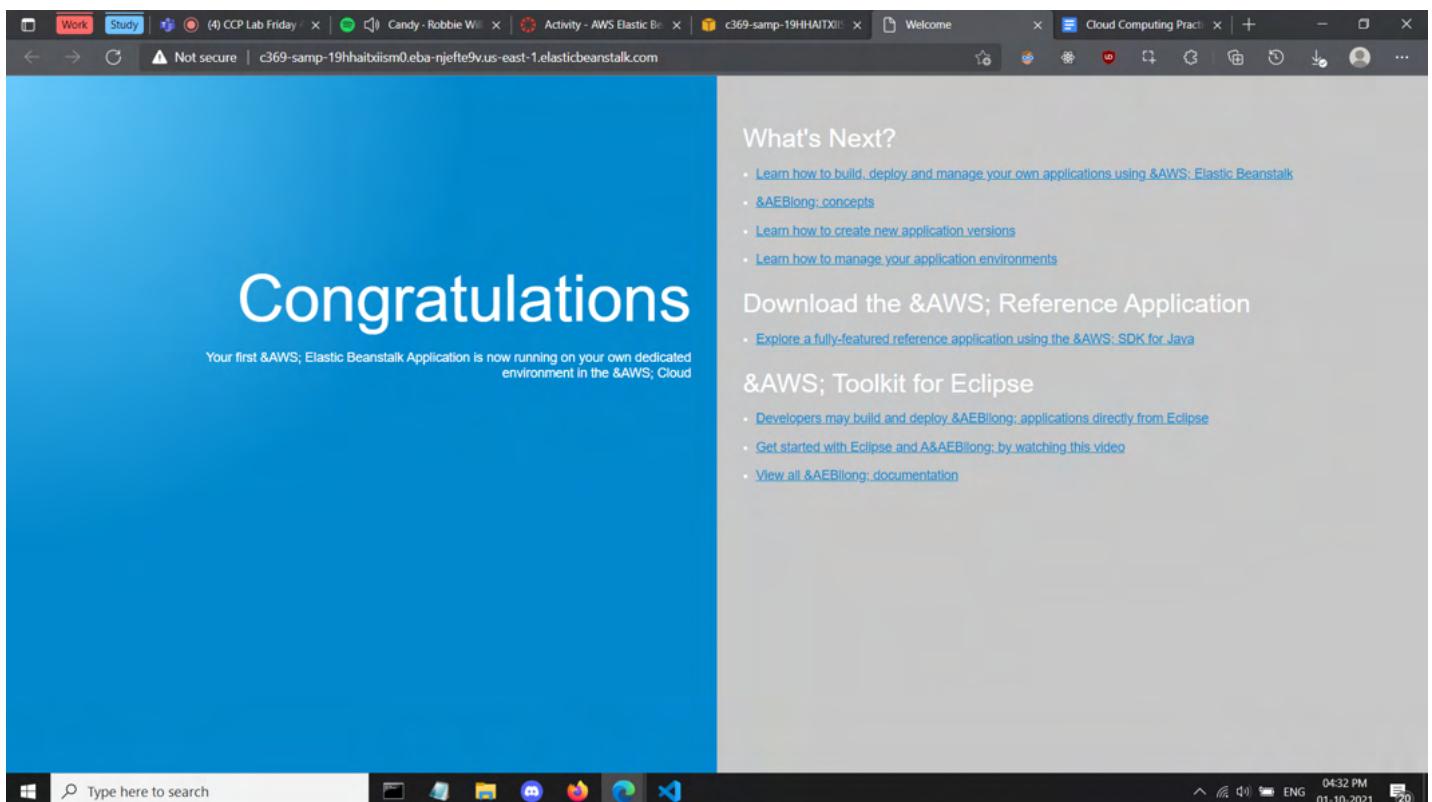
**Health**  
  
Grey  
[Causes](#)

**Running version**  
c36908a474553l1055416t1w216  
759783510-  
sampleapplicationversion-  
6tenhpdlztu4  
[Upload and deploy](#)

**Platform**  
  
Tomcat 8.5 with Java 8 running  
on 64bit Amazon Linux/3.4.10  
[Deprecated](#)  
[Change](#)

13. After the deployment is complete, click the URL value near the top of the screen (or, if you still have the browser tab that displayed the 404 status, refresh that page).  
The web application that you deployed displays.

Congratulations, you have successfully deployed an application on Elastic Beanstalk!



The screenshot shows a web browser window with multiple tabs open. The active tab displays a "Congratulations" message from AWS Elastic Beanstalk, stating: "Your first &AWS; Elastic Beanstalk Application is now running on your own dedicated environment in the &AWS; Cloud". To the right of this message is a sidebar titled "What's Next?" containing links to learn how to build, deploy, and manage applications using &AWS; Elastic Beanstalk, &AEBlong; concepts, create new application versions, and manage application environments. Below this is a section titled "Download the &AWS; Reference Application" with a link to explore a fully-featured reference application using the &AWS; SDK for Java. At the bottom of the sidebar is a section titled "&AWS; Toolkit for Eclipse" with links to developer documentation and a video for getting started with Eclipse and &AEBlong;. The browser's address bar shows the URL: "Not secure | c369-samp-19hhaixism0.eba-njfte9v.us-east-1.elasticbeanstalk.com". The operating system taskbar at the bottom includes icons for search, file explorer, messaging, browser, and file manager, along with system status indicators like battery level and network connection.

14. Back in the Elastic Beanstalk console, click **Configuration** in the left pane.

▼ **c369-samp-19HHAITXIISMO**

[Go to environment](#)

[Configuration](#)

[Logs](#)

[Health](#)

[Monitoring](#)

[Alarms](#)

[Managed updates](#)

[Events](#)

[Tags](#)

Notice the details here.

For example, in the **Instances** row, it indicates the Monitoring interval, EC2 Security groups, and Root volume type details of the Amazon Elastic Compute Cloud (Amazon EC2) instances that are hosting your web application.

| Category  | Options                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Actions              |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| Software  | Environment properties: JDBC_CONNECTION_STRING<br>Gzip compression: enabled<br>Initial JVM heap size (Xms): 256m<br>JVM options: --<br>Log streaming: disabled<br>Max JVM heap size (Xmx): 256m<br>Proxy server: apache<br>Rotate logs: disabled<br>X-Ray daemon: disabled<br>XX:MaxPermSize: 64m                                                                                                                                                               | <a href="#">Edit</a> |
| Instances | EC2 security groups: awseb-e-spet2n3gnq-stack-AWSEBSecurityGroup-1O4IIIVQTJGD7C<br>IOPS: container default<br>Monitoring interval: 5 minute<br>Root volume type: container default<br>Size: container default<br>Throughput: container default                                                                                                                                                                                                                  | <a href="#">Edit</a> |
| Capacity  | AMI ID: ami-0ed7054c38dad8473<br>Availability Zones: Any<br>Breach duration: 5<br>Capacity rebalancing: disabled<br>Environment type: load balancing, auto scaling<br>Instance types: t2.micro,t2.small<br>Lower threshold: 2000000<br>Max: 6<br>Metric: NetworkOut<br>Min: 2<br>Period: 5<br>Placement:<br>Scale down increment: -1<br>Scale up increment: 1<br>Scaling cooldown: 360 seconds<br>Statistic: Average<br>Unit: Bytes<br>Upper threshold: 6000000 | <a href="#">Edit</a> |

15. Scroll to the bottom of the page to the **Database** row.

The **Database** row does not have any details because the environment does not include a database.

16. In the **Database** row, click **Edit**.

Note that you could easily add a database to this environment if you wanted to: you only need to set a few basic configurations and click **Apply**. (However, for the purposes of this activity, you do not need to add a database.)

Database settings

Choose an engine and instance type for your environment's database.

Engine

Engine version

Instance class

Storage  
Choose a number between GB and GB.  
Allocated storage must be a number.

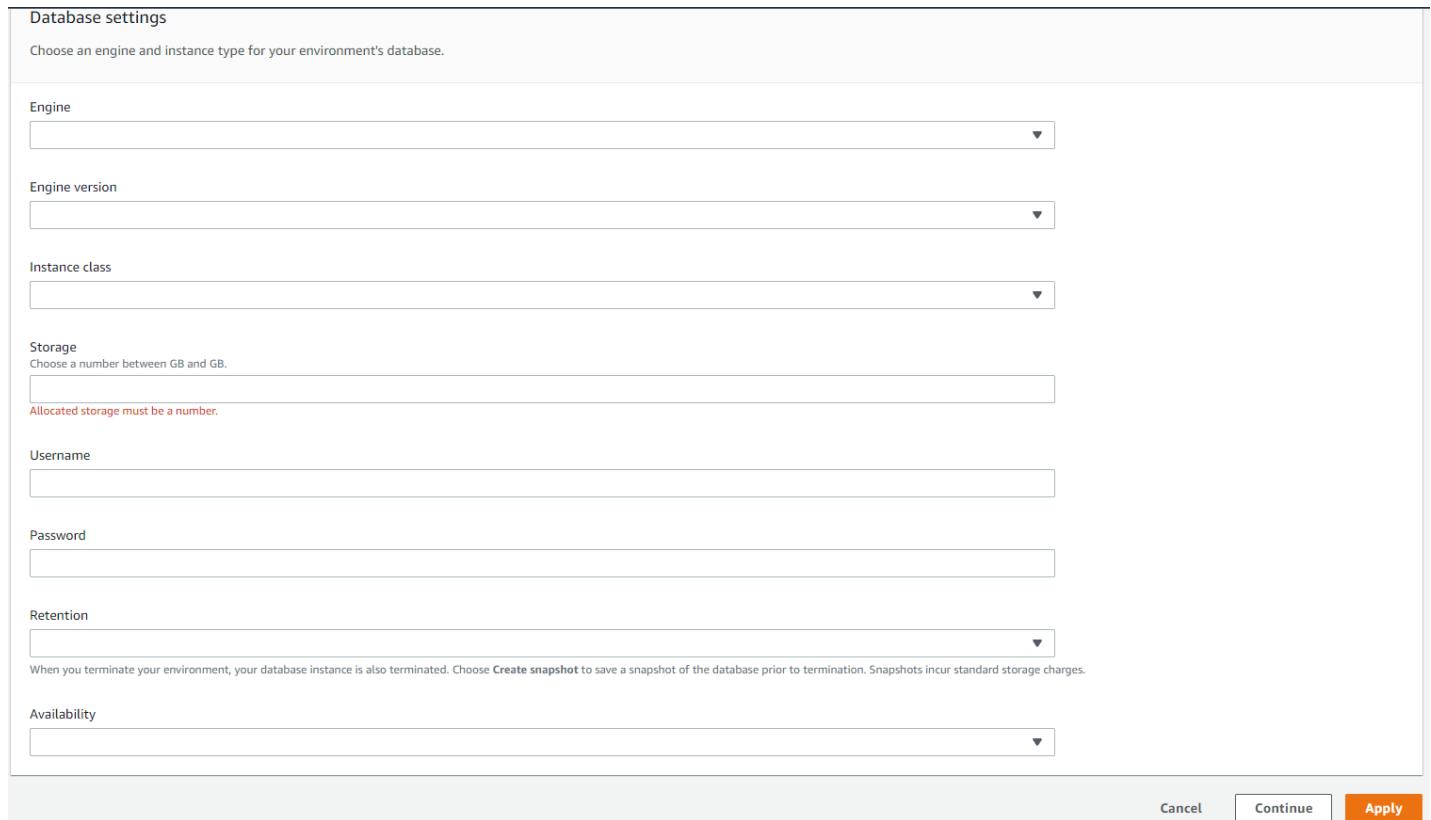
Username

Password

Retention  
When you terminate your environment, your database instance is also terminated. Choose **Create snapshot** to save a snapshot of the database prior to termination. Snapshots incur standard storage charges.

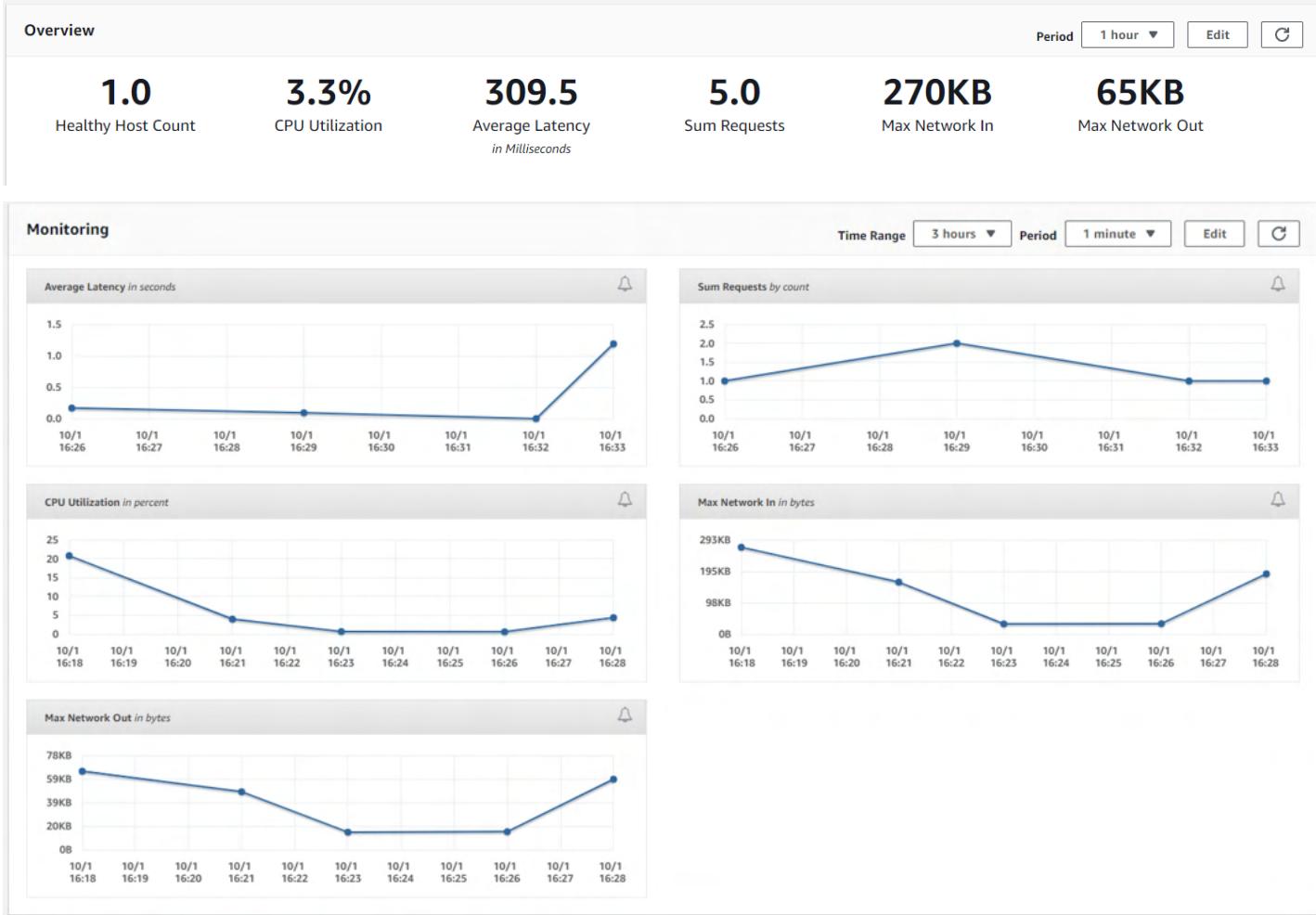
Availability

Cancel Continue **Apply**



17. In the left panel, click **Monitoring**.

Browse through the charts to see the kinds of information that are available to you.



## Task 3: Explore the AWS resources that support your application

18. From the **Services** menu, choose **EC2**

19. Click **Instances**.

Note that two instances are running (they both contain *samp* in their names). Both instances support your web application.

| Instances (3) <a href="#">Info</a> |                         |                     |                      |               |                                |              |                   |                                            |
|------------------------------------|-------------------------|---------------------|----------------------|---------------|--------------------------------|--------------|-------------------|--------------------------------------------|
| <input type="checkbox"/>           | Name                    | Instance ID         | Instance state       | Instance type | Status check                   | Alarm status | Availability Zone | Public IPv4 DNS                            |
| <input type="checkbox"/>           | Bastion Host            | i-08c13d45249b0304b | <span>Running</span> | t3.micro      | <span>2/2 checks passed</span> | No alarms    | + us-east-1a      | ec2-54-81-122-43.compute-1.amazonaws.com   |
| <input type="checkbox"/>           | c369-samp-19HHAITXIISMO | i-040a7451c769a74b0 | <span>Running</span> | t2.micro      | <span>2/2 checks passed</span> | No alarms    | + us-east-1a      | ec2-184-73-118-129.compute-1.amazonaws.com |
| <input type="checkbox"/>           | c369-samp-19HHAITXIISMO | i-063509af62326d45e | <span>Running</span> | t2.micro      | <span>2/2 checks passed</span> | No alarms    | + us-east-1b      | ec2-35-172-228-61.compute-1.amazonaws.com  |

20. If you want to continue exploring the Amazon EC2 service resources that were created by Elastic Beanstalk, feel free to explore them. You will find:

- A security group with port 80 open

| <input checked="" type="checkbox"/>                                                                                                                                 | c369-samp-19HHAITXIISM0               | i-040a7451c769a74b0  | <span>Running</span>                                      | <span>2/2 checks passed</span> |  |  |  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|----------------------|-----------------------------------------------------------|--------------------------------|--|--|--|
| <input type="checkbox"/>                                                                                                                                            | c369-samp-19HHAITXIISM0               | i-063509af62326d45e  | <span>Running</span>                                      | <span>2/2 checks passed</span> |  |  |  |
| <b>Instance: i-040a7451c769a74b0 (c369-samp-19HHAITXIISM0)</b>                                                                                                      |                                       |                      |                                                           |                                |  |  |  |
| IAM Role                                                                                                                                                            | Owner ID                              | Launch time          |                                                           |                                |  |  |  |
| <input type="checkbox"/> c36908a474553l1055416t1w216759783510-EBRole-D1LTWZQQKP3A  | <input type="checkbox"/> 216759783510 | Fri Oct 01 2021 16:2 |                                                           |                                |  |  |  |
| Security groups                                                                                                                                                     |                                       |                      |                                                           |                                |  |  |  |
| <input type="checkbox"/> sg-0cf132bfbaaa2f642 (awseb-e-spet2n3gnq-stack-AWSEBSecurityGroup-1O4IIVQTJGD7C)                                                           |                                       |                      |                                                           |                                |  |  |  |
| <b>Inbound rules</b>                                                                                                                                                |                                       |                      |                                                           |                                |  |  |  |
| <input type="text"/> Filter rules                                                                                                                                   |                                       |                      |                                                           |                                |  |  |  |
| Port range                                                                                                                                                          | Protocol                              | Source               | Security groups                                           |                                |  |  |  |
| 80                                                                                                                                                                  | TCP                                   | sg-0db5e015eaa888c2e | awseb-e-spet2n3gnq-stack-AWSEBSecurityGroup-1O4IIVQTJGD7C |                                |  |  |  |

- A *load balancer* that both instances belong to

**Create Load Balancer** Actions ▾

| Name                      | DNS name                  | State                 | VPC ID                      | Availability Zones | Type |
|---------------------------|---------------------------|-----------------------|-----------------------------|--------------------|------|
| awseb-e-s-AWSEBLoa-1MH... | awseb-e-s-AWSEBLoa-1MH... | vpc-00b1803afae95b8aa | us-east-1c, us-east-1b, ... | classic            |      |

Load balancer: awseb-e-s-AWSEBLoa-1MH6EWL62QOV

Description Instances Health check Listeners Monitoring Tags Migration

### Basic Configuration

|                    |                                                                                                                           |               |                                        |
|--------------------|---------------------------------------------------------------------------------------------------------------------------|---------------|----------------------------------------|
| Name               | awseb-e-s-AWSEBLoa-1MH6EWL62QOV                                                                                           | Creation time | October 1, 2021 at 4:20:36 PM UTC+5:30 |
| * DNS name         | awseb-e-s-AWSEBLoa-1MH6EWL62QOV-2137680416.us-east-1.elb.amazonaws.com (A Record)                                         | Hosted zone   | Z35SXDOTRQ7X7K                         |
| Type               | Classic ( <a href="#">Migrate Now</a> )                                                                                   | Status        | 2 of 2 instances in service            |
| Scheme             | internet-facing                                                                                                           | VPC           | vpc-00b1803afae95b8aa                  |
| Availability Zones | subnet-0a6dcdbe5c8c84a83 - us-east-1a,<br>subnet-0d954b99db2cc53cf - us-east-1c,<br>subnet-0ed7cf7f9218794a4 - us-east-1b |               |                                        |

### Port Configuration

- An *Auto Scaling group* that runs from two to six instances, depending on the network load

| Auto Scaling groups (1/1)                                                                                                                                                                                                                                                    |                                      |                                                                                                                                                                                                                  |           |        |                  |     |     |           |  |  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|--------|------------------|-----|-----|-----------|--|--|
| <input type="button" value="Create an Auto Scaling group"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>                                                                                                                                        |                                      |                                                                                                                                                                                                                  |           |        |                  |     |     |           |  |  |
|                                                                                                                                                                                                                                                                              | Name                                 | Launch template/configuration                                                                                                                                                                                    | Instances | Status | Desired capacity | Min | Max | Available |  |  |
| <input checked="" type="checkbox"/>                                                                                                                                                                                                                                          | awseb-e-spet2n3gnq-stack-AWSEBAut... | awseb-e-spet2n3gnq-stack-AWSEBAutoScali...                                                                                                                                                                       | 2         | -      | 2                | 2   | 6   | us-east-1 |  |  |
| <input type="button" value="Details"/> <input type="button" value="Activity"/> <input type="button" value="Automatic scaling"/> <input type="button" value="Instance management"/> <input type="button" value="Monitoring"/> <input type="button" value="Instance refresh"/> |                                      |                                                                                                                                                                                                                  |           |        |                  |     |     |           |  |  |
| <b>Group details</b>                                                                                                                                                                                                                                                         |                                      |                                                                                                                                                                                                                  |           |        |                  |     |     |           |  |  |
| Desired capacity                                                                                                                                                                                                                                                             |                                      | Auto Scaling group name<br>awseb-e-spet2n3gnq-stack-AWSEBAutoScalingGroup-1B9RTFVG9H1QM                                                                                                                          |           |        |                  |     |     |           |  |  |
| Minimum capacity                                                                                                                                                                                                                                                             | 2                                    | Date created<br>Fri Oct 01 2021 16:20:52 GMT+0530 (India Standard Time)                                                                                                                                          |           |        |                  |     |     |           |  |  |
| Maximum capacity                                                                                                                                                                                                                                                             | 6                                    | Amazon Resource Name (ARN)<br>arn:aws:autoscaling:us-east-1:216759783510:autoScalingGroup:675b1b7f-ece9-4f40-836f-51a47dd8a1e7:autoScalingGroupName/awseb-e-spet2n3gnq-stack-AWSEBAutoScalingGroup-1B9RTFVG9H1QM |           |        |                  |     |     |           |  |  |

21. Though Elastic Beanstalk created these resources for you, you still have access to them.

# Activity 3

## AIM

To explore the sandbox environment

## THEORY

This lab describes how to use the sandbox environment for ad-hoc exploration of Amazon Web Services (AWS) products and services.

You will be restricted to the following services and usage:

- Amazon Elastic Compute Cloud (Amazon EC2)
  - Amazon Machine Images (AMIs) – You can use Amazon provided Linux and Microsoft Windows AMIs
  - Instances – You can only launch the following instance types: t2.nano, t2.micro, t2.small, t2.medium, t3.nano, t3.micro, t3.small, t3.medium
  - Amazon Elastic Block Store (Amazon EBS) volumes – You can use volumes in sizes up to 35 GB and of type General Purpose SSD (gp2)
  - On-Demand Instances
- Amazon EC2 Auto Scaling
- Elastic Load Balancing
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Storage Service Glacier
- Amazon Relational Database Service (Amazon RDS)
  - DB Instance Class Types – You can use db.t2 and db.t3 instances of type db.t\*.micro to db.t\*.medium
  - EBS volumes – You can use volumes in sizes up to 100 GB and of type General Purpose SSD (gp2)
  - On-Demand DB Instance class types
  - DatabaseEngine – Amazon Aurora, MySQL, PostgreSQL, and MariaDB
  - Multi-AZ deployments are not supported – You can choose the Dev/Test or AWS Free Tier templates if prompted, and you can't create a standby instance
  - Enhanced monitoring is not supported – You must clear this default setting
- Amazon DynamoDB
- AWS Identity and Access Management (IAM) – You have read-only access
- AWS CloudFormation
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Route 53
- Amazon CloudFront
- AWS CloudTrail
- AWS Key Management Service (AWS KMS) – You have list access
- Tagging

## PROCEDURE

# Using the terminal in the browser

A terminal window displays to the right of these instructions.

You can toggle the visibility of the terminal window by selecting or clearing the check box in the *Terminal* box at the top of the screen.

The terminal in the browser provides access to a Linux shell on a server that exists *outside* of the AWS account that you use when your lab is running.

## Running AWS CLI commands

After you start the lab, the terminal will be preconfigured with the credentials that you need to use the AWS Command Line Interface (AWS CLI).

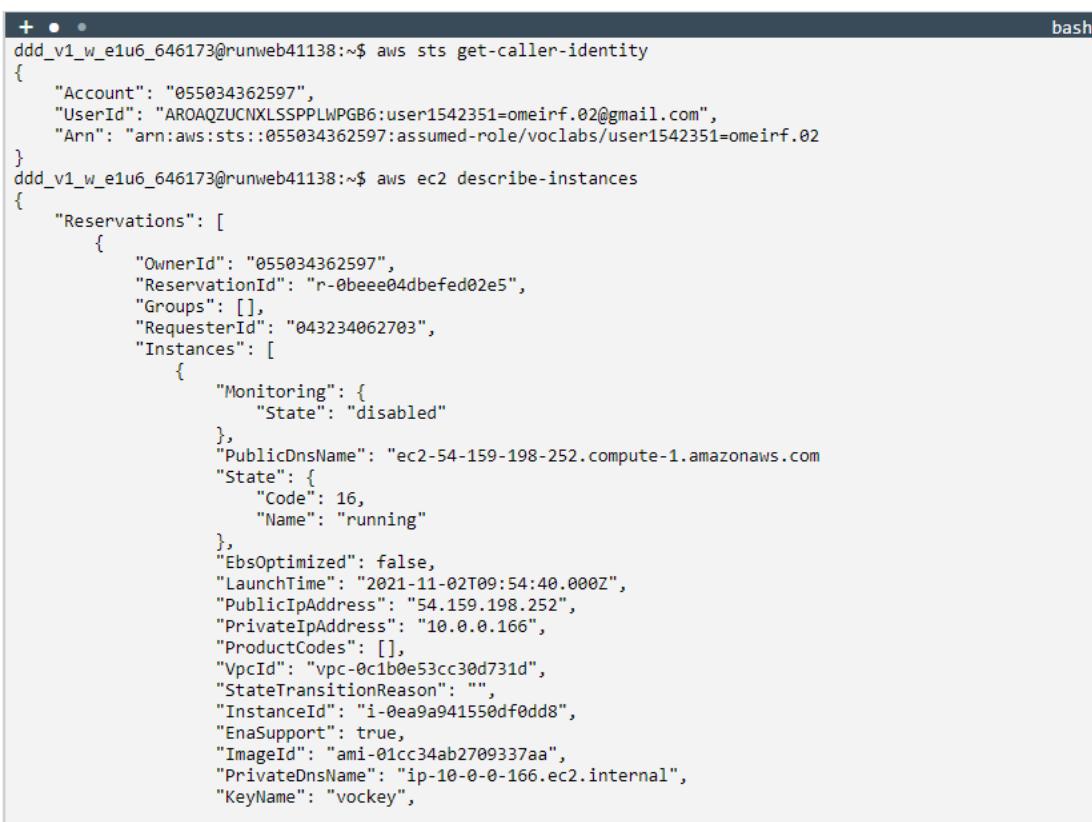
For example, to retrieve the account number and your user ID, run the following command:

```
aws sts get-caller-identity
```

If you have any EC2 instances that are running in the sandbox, this command provides information about them:

```
aws ec2 describe-instances
```

For details about how to use the AWS CLI, refer to the [AWS CLI command reference](#) documentation.

A screenshot of a terminal window titled "bash". The window contains two lines of AWS CLI command output. The first line shows the user's account ID, user ID, and assumed role ARN. The second line shows detailed information about a single EC2 instance, including its owner ID, reservation ID, group, requester ID, instance ID, monitoring state, public DNS name, state code, and private IP address.

```
ddd_v1_w_e1u6_646173@runweb41138:~$ aws sts get-caller-identity
{
 "Account": "055034362597",
 "UserId": "AROAQZUCNXLSSPPLWPGB6:user1542351=omeirf.02@gmail.com",
 "Arn": "arn:aws:sts::055034362597:assumed-role/voclabs/user1542351=omeirf.02
}
ddd_v1_w_e1u6_646173@runweb41138:~$ aws ec2 describe-instances
{
 "Reservations": [
 {
 "OwnerId": "055034362597",
 "ReservationId": "r-0beeee04dbefed02e5",
 "Groups": [],
 "RequesterId": "043234062703",
 "Instances": [
 {
 "Monitoring": {
 "State": "disabled"
 },
 "PublicDnsName": "ec2-54-159-198-252.compute-1.amazonaws.com",
 "State": {
 "Code": 16,
 "Name": "running"
 },
 "EbsOptimized": false,
 "LaunchTime": "2021-11-02T09:54:40.000Z",
 "PublicIpAddress": "54.159.198.252",
 "PrivateIpAddress": "10.0.0.166",
 "ProductCodes": [],
 "VpcId": "vpc-0c1b0e53cc30d731d",
 "StateTransitionReason": "",
 "InstanceId": "i-0ea9a941550df0dd8",
 "EnaSupport": true,
 "ImageId": "ami-01cc34ab2709337aa",
 "PrivateDnsName": "ip-10-0-0-166.ec2.internal",
 "KeyName": "vockey",
 "NetworkInterfaces": [
 {
 "Description": "Amazon VPC interface card for interface i-0ea9a941550df0dd8",
 "MacAddress": "54:19:47:0C:00:02",
 "NetworkInterfaceId": "eni-0c1b0e53cc30d731d",
 "PrivateDnsName": "ip-10-0-0-166.ec2.internal",
 "PrivateIpAddress": "10.0.0.166",
 "Status": "in-use"
 }
]
 }
]
 }
]
}
```

# Using the AWS SDK for Python

Python V3 is installed in the terminal, with access to the AWS software development kit (SDK) for Python (Boto3) library. You can use this library to run AWS SDK for Python code. For example:

```
$ python3
>>> import boto3
>>> ec2 = boto3.client('ec2', region_name='us-east-1')
>>> ec2.describe_regions()
>>> exit()
$
```

```
ddd_v1_w_e1u6_646173@runweb41138:~$ python3
Python 3.6.4 (default, Feb 9 2018, 18:50:54)
[GCC 5.4.1 20160904] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import boto3
>>> ec2 = boto3.client('ec2', region_name='us-east-1')
>>> ec2.describe_regions()
{'Regions': [{'Endpoint': 'ec2.eu-north-1.amazonaws.com', 'RegionName': 'eu-north-1'}, {'Endpoint': 'ec2.ap-south-1.amazonaws.com', 'RegionName': 'ap-south-1'}, {'Endpoint': 'ec2.eu-west-3.amazonaws.com', 'RegionName': 'eu-west-3'}, {'Endpoint': 'ec2.eu-west-2.amazonaws.com', 'RegionName': 'eu-west-2'}, {'Endpoint': 'ec2.eu-west-1.amazonaws.com', 'RegionName': 'eu-west-1'}, {'Endpoint': 'ec2.ap-northeast-3.amazonaws.com', 'RegionName': 'ap-northeast-3'}, {'Endpoint': 'ec2.ap-northeast-2.amazonaws.com', 'RegionName': 'ap-northeast-2'}, {'Endpoint': 'ec2.ap-northeast-1.amazonaws.com', 'RegionName': 'ap-northeast-1'}, {"Endpoint": "ec2.sa-east-1.amazonaws.com", "RegionName": "sa-east-1"}, {"Endpoint": "ec2.ca-central-1.amazonaws.com", "RegionName": "ca-central-1"}, {"Endpoint": "ec2.ap-southeast-1.amazonaws.com", "RegionName": "ap-southeast-1"}, {"Endpoint": "ec2.ap-southeast-2.amazonaws.com", "RegionName": "ap-southeast-2"}, {"Endpoint": "ec2.eu-central-1.amazonaws.com", "RegionName": "eu-central-1"}, {"Endpoint": "ec2.us-east-1.amazonaws.com", "RegionName": "us-east-1"}, {"Endpoint": "ec2.us-east-2.amazonaws.com", "RegionName": "us-east-2"}, {"Endpoint": "ec2.us-west-1.amazonaws.com", "RegionName": "us-west-1"}, {"Endpoint": "ec2.us-west-2.amazonaws.com", "RegionName": "us-west-2"}], 'ResponseMetadata': {'RequestId': '3b3a6414-4621-4fe8-a85c-4013f0034193', 'HTTPStatusCode': 200, 'HTTPHeaders': {'x-amzn-requestid': '3b3a6414-4621-4fe8-a85c-4013f0034193', 'cache-control': 'no-cache, no-store', 'strict-transport-security': 'max-age=31536000; includeSubDomains', 'vary': 'accept-encoding', 'content-type': 'text/xml; charset=UTF-8', 'content-length': '3875', 'date': 'Tue, 02 Nov 2021 10:01:00 GMT', 'server': 'AmazonEC2'}, 'RetryAttempts': 0}}
>>> exit()
ddd_v1_w_e1u6_646173@runweb41138:~$
```

For details about how to use the AWS SDK for Python, refer to the [Boto3 documentation](#) page.

## Accessing EC2 instances

When you launch EC2 instances in the sandbox environment, choose the option to use the existing key pair that's named *vockey* at the time of launch. Then:

- Above these instructions (that you are currently reading), choose the Details dropdown menu.
- Choose Show  
A **Credentials** window opens.

AWS CLI: Show

**Cloud Labs**

```
Remaining session time: 03:50:36(231 minutes)
Session started at: 2021-11-02T02:52:12-0700
Session to end at: 2021-11-02T06:52:12-0700

Accumulated lab time: 00:09:24 (10 minutes)

ips -- public:54.159.198.252, private:10.0.0.166
```

SSH key Show Download PEM Download PPK

AWS SSO Download URL

|             |                                          |
|-------------|------------------------------------------|
| SecretKey   | mQkyYxb1uqjZ4n/qKE53NaC23QxcKICl6FTYwIxa |
| BastionHost | 54.159.198.252                           |
| Region      | us-east-1                                |
| AccessKey   | AKIAQZUCNXLSQLIYWXXR                     |

Instances (1/1) Info

Filter instances

| Name         | Instance ID         | Instance state | Instance type | Status check      | Alarm status | Availability Zone | Public IPv4 DNS        |
|--------------|---------------------|----------------|---------------|-------------------|--------------|-------------------|------------------------|
| Bastion Host | i-0ea9a941550df0dd8 | Running        | t2.micro      | 2/2 checks passed | No alarms    | us-east-1a        | ec2-54-159-198-252.com |

Instance: i-0ea9a941550df0dd8 (Bastion Host)

Details Security Networking Storage Status checks Monitoring Tags

Instance summary Info

|                  |                                                           |                        |
|------------------|-----------------------------------------------------------|------------------------|
| Instance ID      | 54.159.198.252   open address                             | Private IPv4 addresses |
| IPv6 address     | -                                                         | Public IPv4 DNS        |
| Private IPv4 DNS | 10.0.0.166                                                | Elastic IP addresses   |
| VPC ID           | ec2-54-159-198-252.compute-1.amazonaws.com   open address | IAM Role               |

Public IPv4 address copied

- If you use a *Microsoft Windows computer* and want to connect to a Linux instance, or connect to a Microsoft Windows instance by using Secure Shell (SSH): Choose **Download PPK** and save the **labsuser.ppk** file.
- If you want to connect to a Windows instance desktop from any computer: Choose **Download PEM** and save the **labsuser.pem** file.
- If you use *macOS* and want to connect to a Linux instance by using SSH: Choose **Download PEM** and save the **labsuser.pem** file.
- Typically, your browser will save the **labsuser.pem** or the **labsuser.ppk** file to your **Downloads** directory.
- Exit the **Credentials** window by choosing the **X**.
- *To connect to the desktop of a Microsoft Windows instance:*

- In the EC2 console, choose **Instances** and then choose the instance that you want to connect to.
- From the **Actions** menu, choose **Get Windows Password**.
- Next to *Key Pair Path*, choose **Browse**.
- Browse to and select the labsuser.pem file that you downloaded earlier.
- Choose **Decrypt Password**.
- The connection information should display, including the instance's public Domain Name System (DNS), administrator user name, and the decrypted password.
- Use a Remote Desktop Protocol (RDP) client to connect to the desktop of the EC2 instance by using these connection details.
- *To connect to a Linux instance by using SSH, see the next section.*

## Using SSH to access any EC2 instances that you launch

---

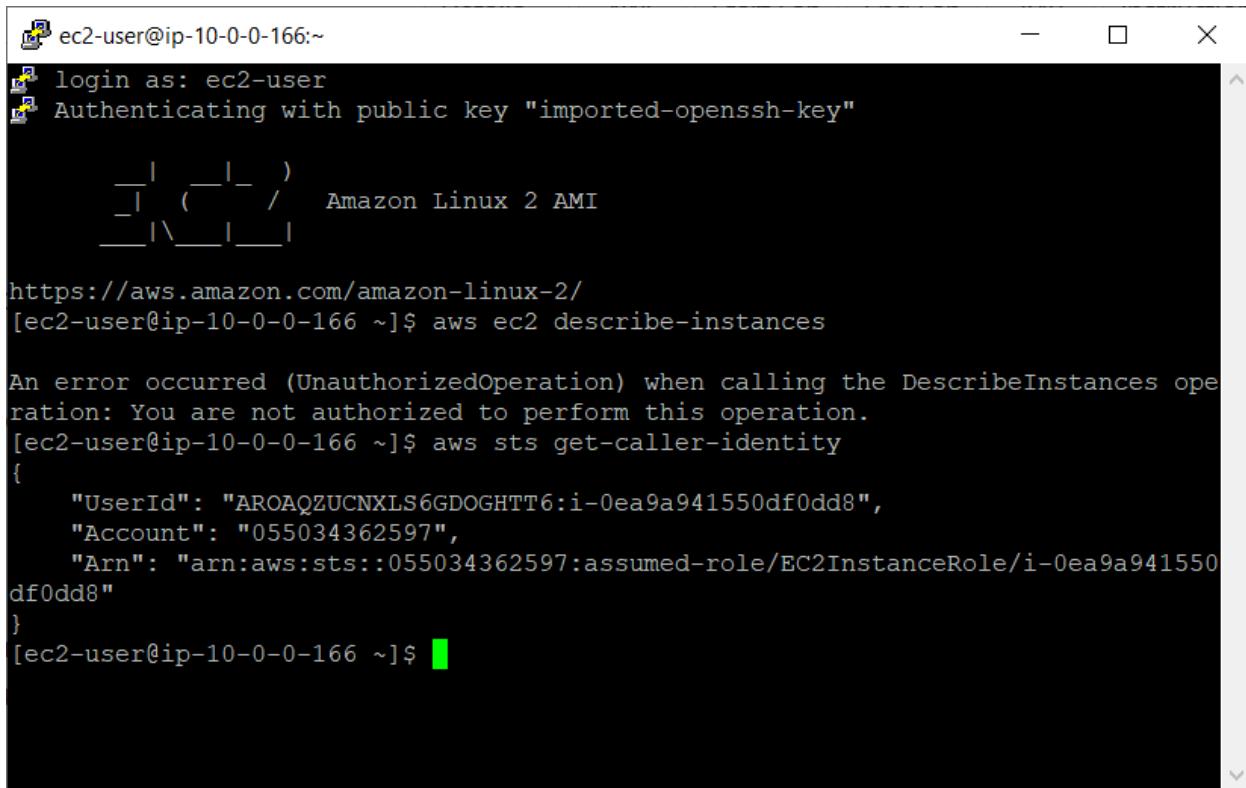
The following steps describe how to use the SSH key to connect to your instance.

### Microsoft Windows users

These instructions are for Windows users only.

If you use macOS or Linux, [skip to the next section](#).

6. Download the required software.
  - You will use *PuTTY* to use SSH to connect to EC2 instances. If you do not have PuTTY installed on your computer, [download it here](#).
7. Open **putty.exe**
8. Configure PuTTY to not timeout:
  - Choose **Connection**
  - Set **Seconds between keepalives** to 30
9. This setting enables you to keep the PuTTY session open for a longer time.
10. Configure your PuTTY session:
  - Choose **Session**
  - **Host Name (or IP address)**: Copy and paste the **IPv4 Public IP address** for the instance. To find it, return to the Amazon EC2 console and choose **Instances**. Select the box next to the instance and in the **Description** tab, copy the **IPv4 Public IP** value.
  - Back in PuTTY, in the **Connection** list, expand **SSH**
  - Choose **Auth** (don't expand it).
  - Choose **Browse**.
  - Browse to and select the .ppk file that you downloaded
  - Choose **Open** to select it
  - Choose **Open**
11. Choose **Yes**, to trust the host and connect to it.
12. When prompted to **login as**, enter: **ec2-user**  
This step will connect you to the EC2 instance.
13. [Microsoft Windows users: Click here to skip ahead to the next task.](#)



A screenshot of a terminal window titled "ec2-user@ip-10-0-0-166:~". The window shows the following text:

```
login as: ec2-user
Authenticating with public key "imported-ssh-key"

Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-166 ~]$ aws ec2 describe-instances

An error occurred (UnauthorizedOperation) when calling the DescribeInstances operation: You are not authorized to perform this operation.
[ec2-user@ip-10-0-0-166 ~]$ aws sts get-caller-identity
{
 "UserId": "AROAQZUCNXLS6GDOGHTT6:i-0ea9a941550df0dd8",
 "Account": "055034362597",
 "Arn": "arn:aws:sts::055034362597:assumed-role/EC2InstanceRole/i-0ea9a941550df0dd8"
}
[ec2-user@ip-10-0-0-166 ~]$
```

## macOS and Linux Users - Using SSH to Connect

These instructions are only for macOS or Linux users.

13. Read through the three bullet points in this step before you start to complete the actions. You will not be able see these instructions when the **Details** panel is open.
  - Above these instructions you are currently reading, choose the Details dropdown menu, and then choose Show
14. A **Credentials** window will open.
  - Choose the **Download PEM** button and save the **labsuser.pem** file. Typically, your browser will save it to the **Downloads** directory.
  - Then, exit the Details panel by choosing the **X**.
15. Open a terminal window, and change directory (`cd`) to the directory where the `.pem` file was downloaded.  
For example, if it was saved to your **Downloads** directory, run this command:  
`16. cd ~/Downloads`
17. Change the permissions on the key to be *read only* by running this command:  
`18. chmod 400 <filename>.pem`
19. Return to the AWS Management Console, and in the EC2 service, choose **Instances**.  
Check the box next to the instance you want to connect to.
20. In the **Description** tab, copy the **IPv4 Public IP** value.
21. Return to the terminal window and run this command (replace `<public-ip-address>` with the actual public IP address that you copied):  
`22. ssh -i <filename>.pem ec2-user@<public-ip-address>`
23. When you are prompted to allow a first connection to this remote SSH server, enter yes.  
Because you are using a key pair for authentication, you will not be prompted for a password.

