



# ACF Lab 3

# Introduction to EC2

---

COS 20019- Cloud Computing Architecture

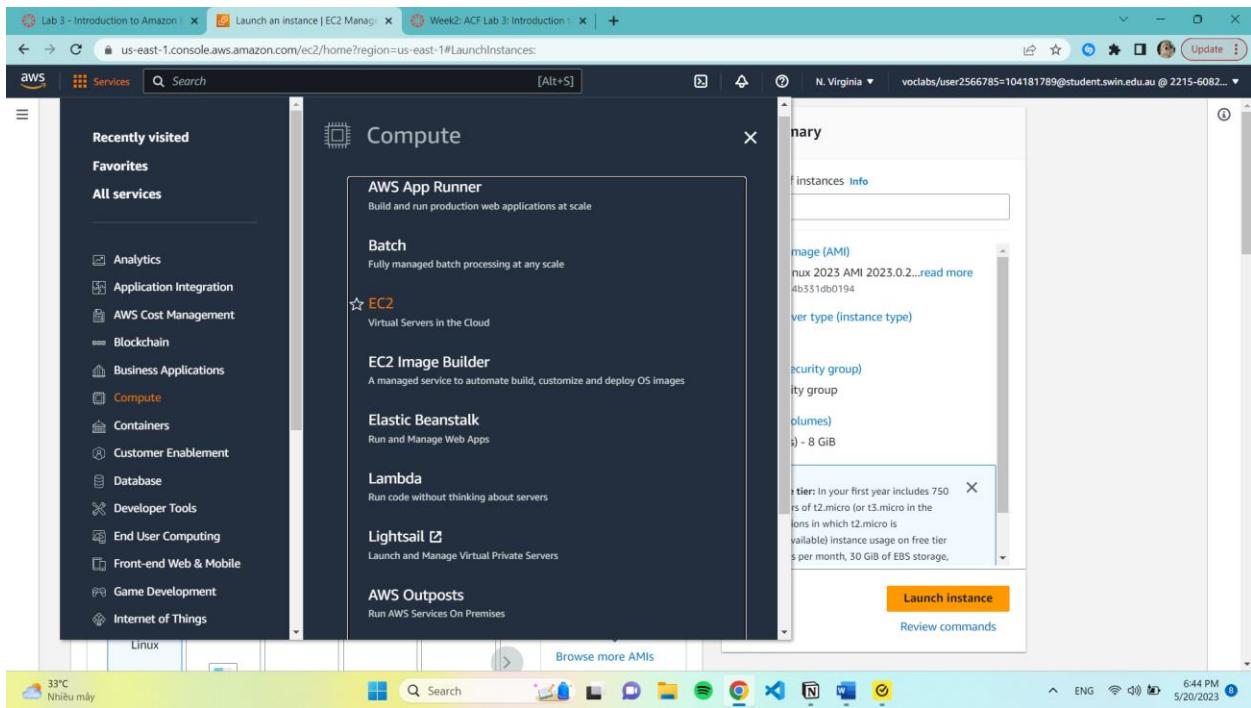
Nguyen Manh Dung

20/5/2023

So this is my screenshot for Lab 3, including explanation in every image.

Task 1: Lauch Amazon EC2 Instance.

5. Select Services, Compute, and then EC2 in the AWS Management Console.



## 6. Choose Launch instance menu and select Launch instance

The screenshot shows the AWS EC2 Management Console with the 'Launch instance' wizard open. The 'Launch instance' step is selected. The 'Service health' section indicates that the service is operating normally. The 'Explore AWS' section promotes better price performance and spot instances.

The screenshot shows the 'Launch an instance' configuration page. The 'Name and tags' section has 'Web Server' entered. The 'Application and OS Images (Amazon Machine Image)' section shows a search bar and a list of AMIs. The 'Summary' section shows 1 instance and includes a note about the Free tier.

## Step 1: Name and tags

7. The name “Web Server” will be stored as a tag. Tags enable us to categorize our AWS resources in different ways. The tag be created will consist a key called Name with a value of Web Server.

The screenshot shows two windows side-by-side. On the left is the 'EC2 Management Console' showing the 'Launch an instance' wizard. It has a 'Name and tags' section where 'Name' is set to 'Web Server'. Below it is an 'Application and OS Images (Amazon Machine Image)' section with a search bar and a 'Quick Start' tab selected. On the right is a browser window titled 'Lab 3 - Introduction to Amazon EC2' showing a step-by-step guide. Step 6 says 'Choose the Launch instance menu and select **Launch instance**'. Step 7 says 'Give the instance the name **Web Server**'. The guide explains that the Name tag will be stored as a tag and can be used to categorize resources. The EC2 Instances page is also visible at the bottom of the browser window.

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

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

The screenshot shows two windows side-by-side. On the left is the AWS Management Console EC2 service, displaying a search bar for 'Application and OS Images (Amazon Machine Image)' and a list of quick start AMIs including Amazon Linux, macOS, Ubuntu, and Windows. On the right is a browser window for 'Lab 3 - Introduction to Amazon EC2' titled 'ACFv2EN-47408'. The page contains instructions for selecting the default Amazon Linux AMI and highlights the definition of an AMI.

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

8. In the list of available **Quick Start** AMIs, keep the default **Amazon Linux** AMI selected.

9. Also keep the default **Amazon Linux 2023 AMI** selected.

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

- o A template for the root volume for the instance (for example, an operating system or an application server with applications)
- o Launch permissions that control which AWS accounts can use the AMI to launch instances

## Step 3: Instance Type

10. t2.micro in 'Instance type' panel is selected.

The screenshot shows two windows side-by-side. On the left is the AWS Management Console EC2 service, displaying the 'Instance type' panel where 't2.micro' is selected. On the right is a browser window for 'Lab 3 - Introduction to Amazon EC2' titled 'ACFv2EN-47408'. The page contains instructions for keeping the default t2.micro instance type selected and highlights the features of the t2.micro instance type.

**Step 3: Instance type**

10. In the *Instance type* panel, keep the default **t2.micro** selected.

Amazon EC2 provides a wide selection of *instance types* optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications. Each instance type includes one or more *instance sizes*, allowing you to scale your resources to the requirements of your target workload.

The t2.micro instance type has 1 virtual CPU and 1 GiB of memory.

**Note:** You may be restricted from using other instance types in this lab.

#### Step 4: Key pair (login)

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

To make sure you can log in to the guest OS of the instance you build. A block device mapping that designates the volumes that will be attached to the instance when it is started.

The screenshot shows two windows side-by-side. On the left is the AWS Management Console EC2 service, displaying the 'Instance type' configuration page. It shows a selected 't2.micro' instance type with details like Family: t2, 1 vCPU, 1 GiB Memory, Current generation: true, and various On-Demand pricing options. Below this is the 'Key pair (login)' section, which has 'vockey' selected as the key pair name. On the right is a browser window for 'Lab 3 - Introduction to Amazon EC2' titled 'ACFV2EN-47408'. This window displays the 'Step 4: Key pair (login)' instructions, which include the requirement to choose a key pair name and a note about how Amazon EC2 uses public-key cryptography for login. The browser also shows navigation buttons for 'Previous' and 'Next'.

## Step 5: Network Settings

Edit and select Lab VPC. The Lab VPC was created using an AWS CloudFormation template during the setup process of our lab.

The screenshot shows two windows side-by-side. On the left is the AWS Management Console's EC2 Management Console, specifically the 'Subnet' settings page. It displays a subnet named 'No preference' with a VPC ID of 'vpc-c0ff1e274cbc5e2832'. On the right is a browser window titled 'Lab 3 - Introduction to Amazon EC2' with a URL like 'awsacademy.instructure.com/courses/4...'. The page is titled 'ACFv2EN-47408 Lab 3 - Introduction to Amazon EC2'. It contains step-by-step instructions for creating a security group. Step 14 says: 'Under Firewall (security groups), choose Create security group and configure:'. Below this, it lists the configuration steps: 'Security group name: Web Server security group', 'Description: Security group for my web server', and 'Inbound security group rules: No security group rules are currently included in this template. Add a new rule to include it in the launch template.' There is also a note about keeping the default subnet.

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

Security group name: Web Server security group

Description: Security group for my web server

This screenshot shows the same two windows as the previous one. The left window is the 'Subnet' settings page, and the right window is the 'Lab 3 - Introduction to Amazon EC2' guide. The guide has moved to 'Step 14: Under Firewall (security groups), choose Create security group and configure:' and provides the configuration details: 'Security group name: Web Server security group', 'Description: Security group for my web server', and 'Inbound security group rules: No security group rules are currently included in this template. Add a new rule to include it in the launch template.' It also includes a note about the security group acting as a virtual firewall for instances.

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

## Step 6: Configure Storage

Keep default settings.

The screenshot shows the AWS EC2 Management Console and a browser-based lab interface side-by-side. The EC2 console shows a security group named 'Security group for my web server' with an inbound rule. Below it, the 'Configure storage' section is open, showing a root volume of 8 GiB gp3. A tooltip indicates that free-tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. The browser-based lab interface shows Step 6: Configure storage, which instructs to keep the default settings. It notes that one rule exists in the inbound security group and provides a link to remove it.

## Step 7: Advanced details

Enable 'Terminal protection'

The screenshot shows the AWS EC2 Management Console and a browser-based lab interface side-by-side. The EC2 console shows various advanced instance settings like IP name, DNS hostname, instance auto-recovery, shutdown behavior, stop-hibernate behavior, termination protection, stop protection, detailed CloudWatch monitoring, and elastic GPU info. The browser-based lab interface shows Step 7: Advanced details, which instructs to enable termination protection. It explains that when an instance is terminated, its resources are released and cannot be accessed again. It also provides instructions for enabling termination protection.

## 18. Add code to Data box

The screenshot shows two windows side-by-side. On the left is the AWS Management Console's EC2 Instances page, where a new instance is being configured. In the 'User data' section, a shell script is pasted:

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

On the right is a browser window titled 'Lab 3 - Introduction to Amazon EC2' from awsacademy.instructure.com. It contains instructions for step 18:

being terminated as long as this setting remains enabled.

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

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

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

Your instance is running Amazon Linux 2023. The *shell script* you have specified will run as the root guest OS user when the instance

When we launch an instance, we can pass user data to the instance that can be used to perform automated installation and configuration tasks after the instance starts.

### Step 8: Launch the instance

Success message included

The screenshot shows two windows side-by-side. On the left is the AWS Management Console's EC2 Instances page, showing a success message for launching an instance:

**Success**  
Successfully initiated launch of instance (i-045c657b227c71bcc)

On the right is a browser window titled 'Lab 3 - Introduction to Amazon EC2' from awsacademy.instructure.com. It contains instructions for step 19:

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

20. Choose View all instances

- o In the Instances list, select **Web Server**.
- o Review the information displayed in the **Details** tab. It includes information about the instance type, security settings and network settings.

The instance is assigned a *Public IPv4 DNS* that you can use to contact the instance from the Internet.

To view more information, drag the window divider upwards.

## 20. View all instances

Review all information.

The instance is assigned a Public IPv4 DNS that you can use to contact the instance from the Internet. To view more information, drag the window divider upwards. At first, the instance will appear in a Pending state, which means it is being launched. It will then change to Initializing, and finally to Running.

Instance will display:

Instance State: Running

Status Checks: 2/2 checks passed.

The screenshot shows the AWS EC2 Management Console. The main window displays a list of instances with two items: 'Web Server' (running, t2.micro, 2/2 checks passed) and 'Bastion Host' (running, t2.micro, 2/2 checks passed). Below this, a detailed view is open for the 'Web Server' instance (i-045c657b227c71bcc). The details page includes tabs for Details, Security, Networking, Storage, Status checks, Monitoring, and Tags. Under the Details tab, it shows the Instance ID (i-045c657b227c71bcc), Public IPv4 address (3.80.222.131), Private IP address (172.31.24.156), Public IPv4 DNS (ec2-3-80-222-131.compute-1.amazonaws.com), and Instance type (t2.micro). The status is listed as 'Running' with a green checkmark. The monitoring tab shows 2/2 checks passed. The status checks tab shows 2/2 checks passed. The monitoring tab shows 2/2 checks passed. The tags tab shows no tags. The bottom of the screen shows the Windows taskbar with various pinned icons and the date/time (7:04 PM, 5/20/2023).

## Task 2

### 22. Status checks tab:

both the **System reachability** and **Instance reachability** checks have passed.

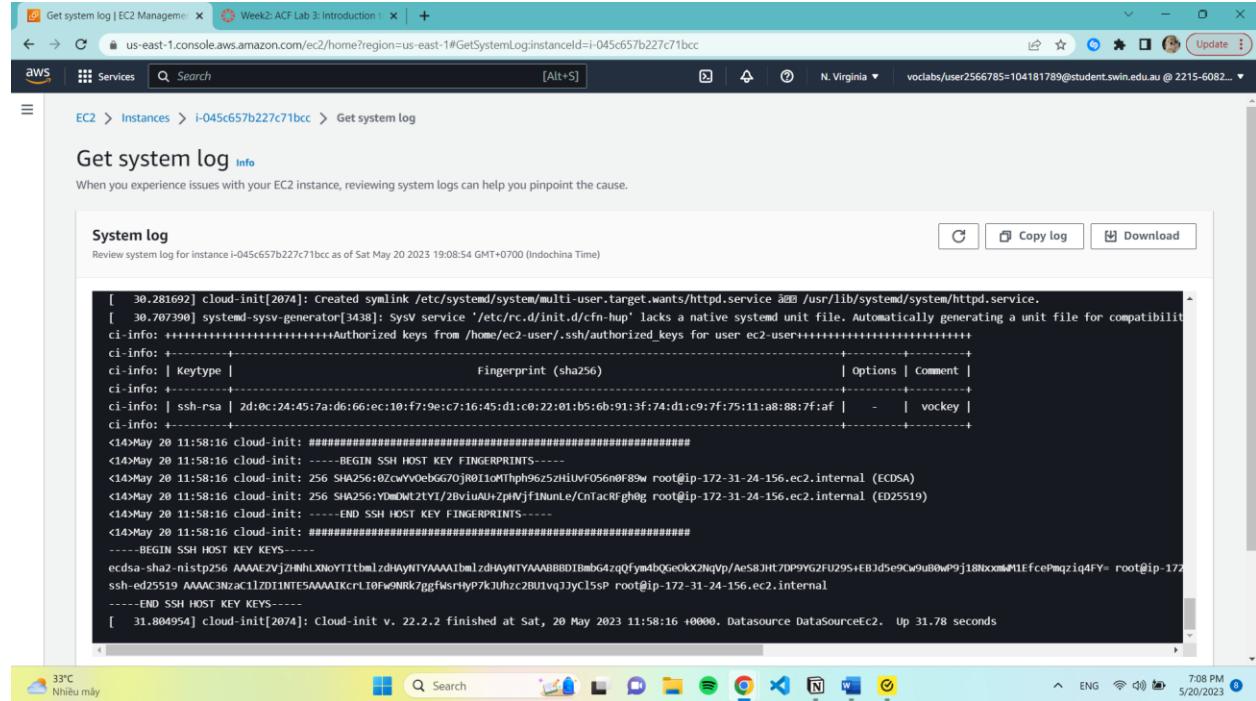
The screenshot shows the AWS EC2 Management Console. The main view displays two instances: a Web Server (running, t2.micro) and a Bastion Host (running, t2.micro). The status checks tab is selected for the Web Server instance. It shows two green status check entries: 'System reachability check passed' and 'Instance reachability check passed'. A 'Report instance status' button is visible. The bottom of the screen shows a Windows taskbar with various icons and system information.

### 23. Monitoring tab

This tab displays Amazon CloudWatch metrics for your instance.

The screenshot shows the AWS EC2 Management Console. The main view displays two instances: a Web Server (running, t2.micro) and a Bastion Host (running, t2.micro). The monitoring tab is selected for the Web Server instance. It displays three line charts: 'CPU utilization (%)', 'Status check failed (any) (count)', and 'Status check failed (instance) (count)'. The 'Status check failed (any) (count)' chart has a tooltip showing '11' at the top. Below the charts are three status check failed counts: 'No unit' (1), 'No unit' (0.5), and 'No unit' (0.5). The bottom of the screen shows a Windows taskbar with various icons and system information.

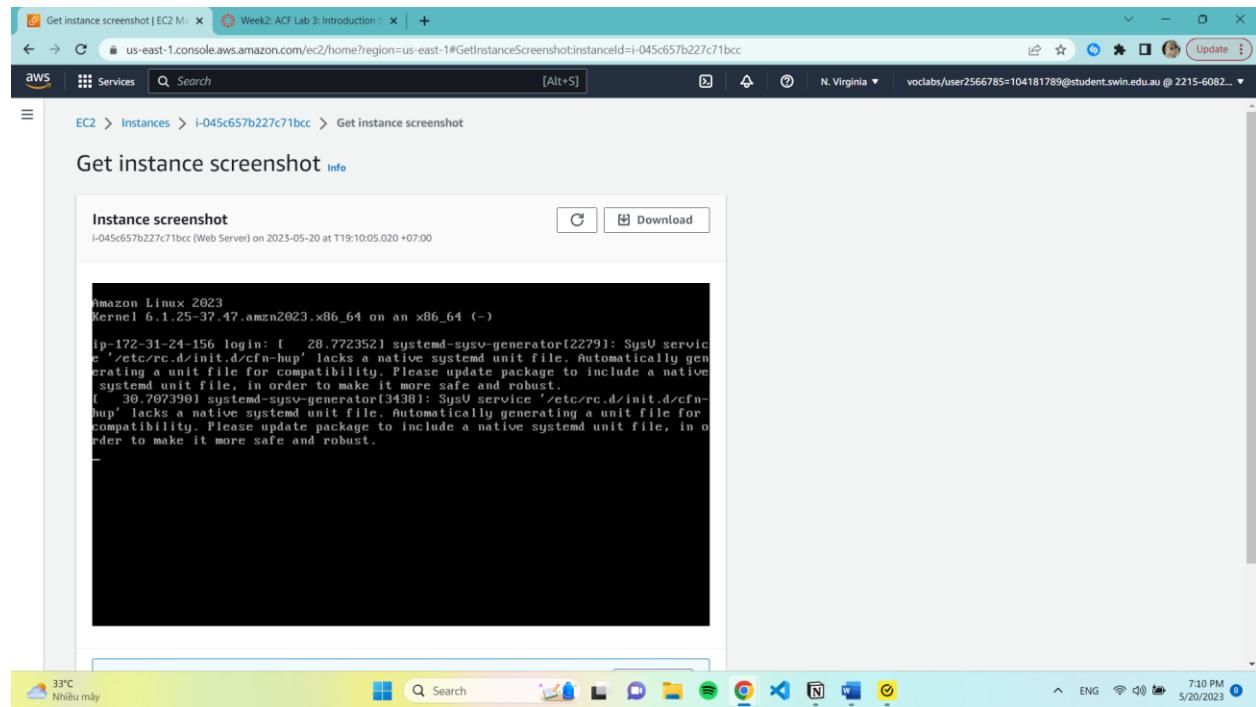
## 24. Monitor and troubleshoot -> Get system log.



The screenshot shows the AWS CloudWatch Logs interface for an EC2 instance. The log output is as follows:

```
[ 30.281692] cloud-init[2074]: Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[ 30.707390] systemd-sysv-generator[3438]: SysV service '/etc/rc.d/init.d/cfn-hup' lacks a native systemd unit file. Automatically generating a unit file for compatibility.
ci-info: +-----+-----+
ci-info | Keytype | Fingerprint (sha256) | Options | Comment |
ci-info: +-----+-----+
ci-info | ssh-rsa | 2d:0c:24:45:7a:d6:66:ec:10:f7:9e:c7:16:45:d1:c0:22:01:b5:b6:91:3f:74:d1:c9:7f:75:11:a8:88:7f:af | - | vockey |
ci-info: +-----+-----+
<14-May 20 11:58:16 cloud-init: #####
<14-May 20 11:58:16 cloud-init: -----BEGIN SSH HOST KEY FINGERPRINTS-----
<14-May 20 11:58:16 cloud-init: 256 SHA256:0zCwVOebG7OjR0l1MThph9z5zhliUvF056n0F89w root@ip-172-31-24-156.ec2.internal (ED25519)
<14-May 20 11:58:16 cloud-init: 256 SHA256:Y0DMz2tYl2BviuAUZpMVfIUnlCeCnacRfghg root@ip-172-31-24-156.ec2.internal (ED25519)
<14-May 20 11:58:16 cloud-init: -----END SSH HOST KEY FINGERPRINTS-----
<14-May 20 11:58:16 cloud-init: #####
-----BEGIN SSH HOST KEY KEYS-----
ecdsa-sha2-nistp256 AAAEAEyJZH#hILXNoYT1tbm1zdHhAyNTAAA1bm1zdHhAyNTAAAABBB0IBmbG4zQfym4bQGeokx2NqVp/AeS8JHt7DP9YG2FU295+EB)d5e9Cw9uB0dP9j18NxM#MIEfcePmqziq4FY= root@ip-172-31-24-156.ec2.internal
-----END SSH HOST KEY KEYS-----
[ 31.804954] cloud-init[2074]: Cloud-init v. 22.2.2 finished at Sat, 20 May 2023 11:58:16 +0000. Datasource DataSourceEc2. Up 31.78 seconds
```

## 27. in the Actions menu, select Monitor and troubleshoot Get instance screenshot.



The screenshot shows the AWS CloudWatch Metrics interface for an EC2 instance. The instance screenshot is displayed as a black terminal window with the following text:

Amazon Linux 2023  
Kernel 6.1.25-37.47.amzn2023.x86\_64 on an x86\_64 (-)

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

#### 33. Choose Security Groups.

The screenshot shows the AWS EC2 Management Console with the 'Security Groups' page open. The left sidebar shows various AWS services like Launch Templates, Spot Requests, Savings Plans, etc. Under 'Network & Security', 'Security Groups' is selected. The main pane displays a table of security groups with columns: Name, Security group ID, Security group name, VPC ID, Description, and Owner. There are five entries listed:

Name	Security group ID	Security group name	VPC ID	Description	Owner
-	sg-00f2250e0ab3d5bdd	Web Server security gr...	vpc-0ff1e274cbc5e2832	Security group for my ...	221560824866
-	sg-06b1f94e2e358b2c9	default	vpc-04e262c63082bc72	default VPC security gr...	221560824866
-	sg-05299d1d3de0e5604	default	vpc-011bd81f2727c91c6	default VPC security gr...	221560824866
-	sg-0e8737294160af07d	default	vpc-0ff1e274cbc5e2832	default VPC security gr...	221560824866
-	sg-0aaaf790c2317e52fb	Ec2SecurityGroup	vpc-04e262c63082bc72	VPC Security Group	221560824866

#### 25. Create Inbound rules

Type: HTTP

Source: Anywhere-IPv4

The screenshot shows the 'Edit inbound rules' page for the 'Web Server security group'. The URL in the browser is `us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ModifyInboundSecurityGroupRules:securityGroupId=sg-00f2250e0ab3d5bdd`. The page has a header with 'EC2 > Security Groups > sg-00f2250e0ab3d5bdd - Web Server security group > Edit inbound rules'. Below the header, it says 'Edit inbound rules [Info](#)'. A note states 'Inbound rules control the incoming traffic that's allowed to reach the instance.' The main area is titled 'Inbound rules [Info](#)' and contains a table with columns: Security group rule ID, Type, Protocol, Port range, Source, and Description - optional. One rule is listed: 'HTTP' (Type), 'TCP' (Protocol), '80' (Port range), 'Anywh...' (Source), and 'Description - optional' is empty. At the bottom right are 'Cancel', 'Preview changes', and 'Save rules' buttons.

### 33. Reopen to web server.



Hello From Your Web Server!



### Task 4: Resize Your Instance: Instances Type ans EBS Volume

We have to stop our instance. The Instance state will display 'Stopped'

The screenshot shows the AWS EC2 Management Console. At the top, it says 'Successfully stopped i-045c657b227c71bcc'. Below this, the 'Instances (1/2) info' table lists two instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
Web Server	i-045c657b227c71bcc	Stopping	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-3-80-222-131.com...	3.80.222.131
Bastion Host	i-09f3359779392867e	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-107-20-43-197.co...	107.20.43.197

Below the table, the 'Instance: i-045c657b227c71bcc (Web Server)' details page is shown. The 'Details' tab is selected, displaying information such as Public IPv4 address (3.80.222.131), Instance state (Running), and Instance type (t2.micro). The 'Security' tab is also visible.

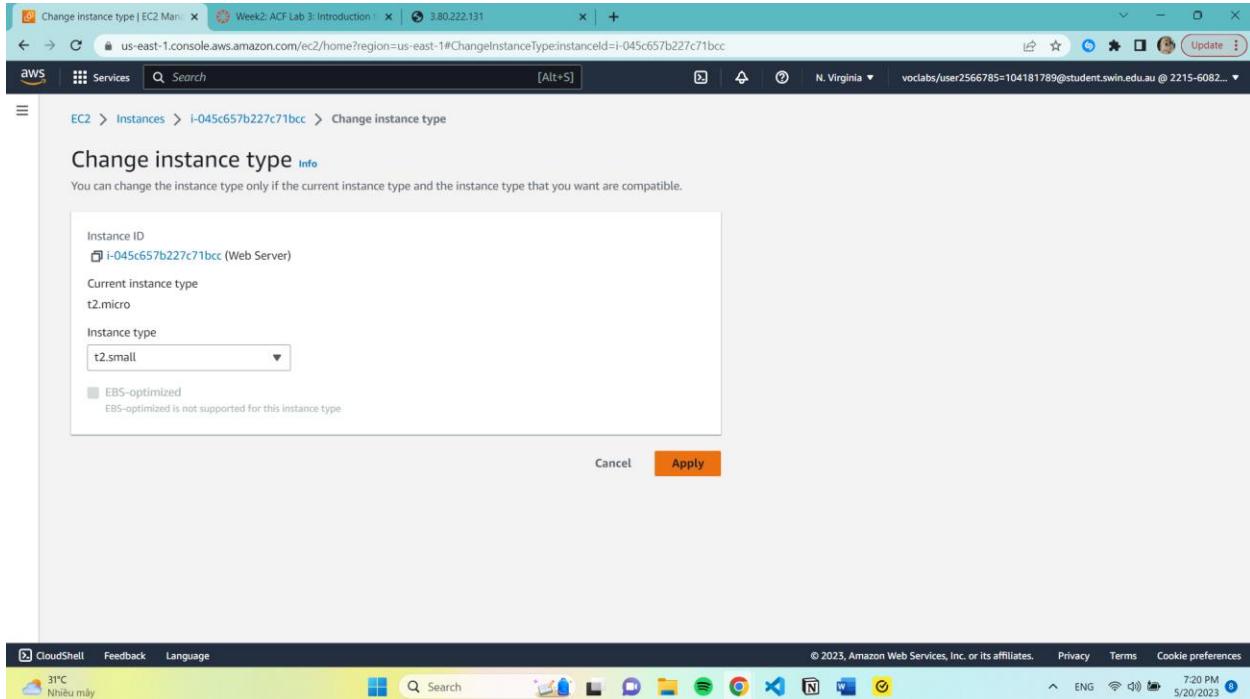
## Change The Instance Type

42. Select Instance settings. Change instance typ, then configure:

-Instance Type: t2.small

-Choose Apply

The instance will operate as a t2.small when it is restarted since it contains twice as much RAM as a t2.micro instance.



### Resize the EBS Volume:

Storage tab -> choose Volume ID then Modify Volume. We change the size of disk from 8 to 10Gb

### 47. Modify again and confirm the change

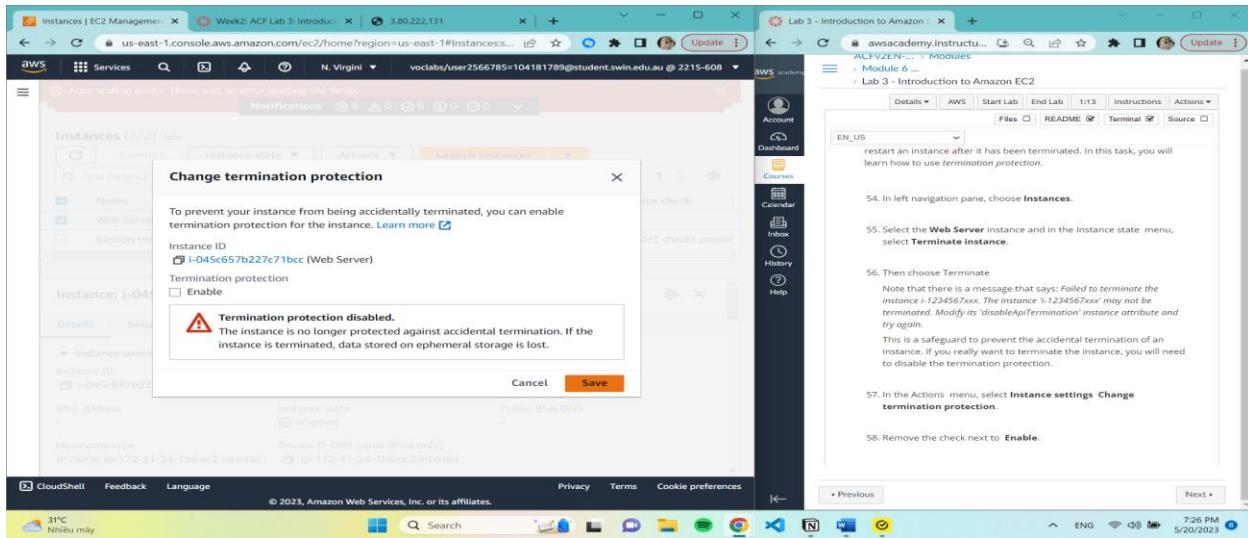
### 51. Start Instance.

### Task 5: Explore EC2 Limits (ignore)

### Task 6: Test Termination Protection

57. Select Instance settings -> Change termination protection.

Remove 'Enable' check.



### 61. Terminate Instance

