

Lab 3: Introduction to Amazon EC2

Name : Le Ngoc An Thu

Student ID : 103509814

Accessing the AWS Management Console

1. At the top of these instructions, choose Start Lab to launch your lab. A Start Lab panel opens displaying the lab status.

The screenshot shows the AWS Academy interface. On the left is a sidebar with icons for Account, Dashboard, Courses, Calendar, Inbox, History, and Help. The main area shows a breadcrumb trail: ACFv2EN... > Modules > Module 6 ... > Lab 3 - Introduction to Amazon EC2. Below the breadcrumb is a navigation bar with Details, AWS, Start Lab (highlighted in pink), End Lab, 00:00:00, Instructions, and Actions. A sub-navigation bar below the navigation bar includes Files, README (checked), Terminal (checked), and Source. A central panel titled "EN_US Accessing the AWS Management Console" contains two numbered steps: 1. At the top of these instructions, choose Start Lab to launch your lab. A Start Lab panel opens displaying the lab status. 2. Wait until you see the message "Lab status: ready", then choose the X to close the Start Lab panel. At the bottom of the panel are "Previous" and "Next" buttons.

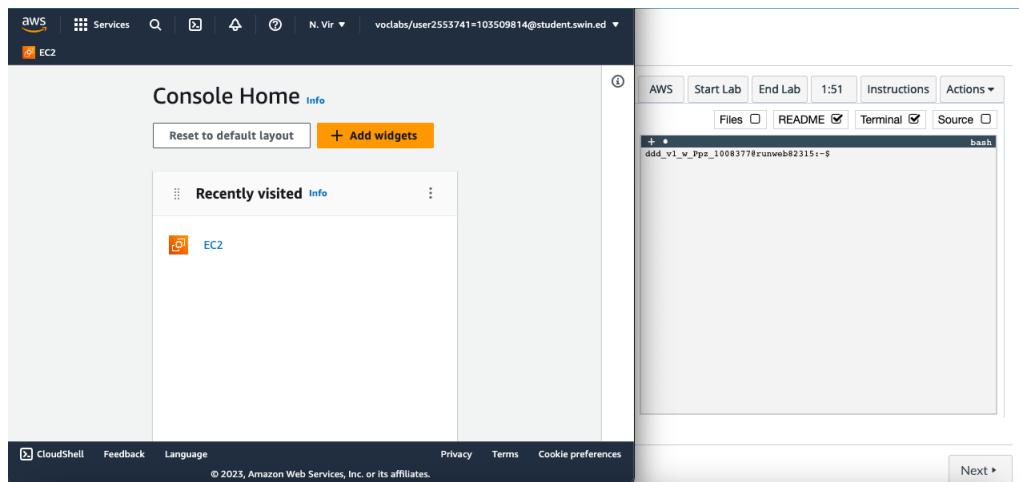
2. Wait until you see the message "**Lab status: ready**", then choose the X to close the Start Lab panel.

3. At the top of these instructions, choose AWS

This will open the AWS Management Console in a new browser tab. The system will automatically log you in.

Tip: If a new browser tab does not open, there will typically be a banner or icon at the top of your browser indicating that your browser is preventing the site from opening pop-up windows. Choose on the banner or icon and choose "Allow pop ups."

4. Arrange the AWS Management Console tab so that it displays along side these instructions. Ideally, you will be able to see both browser tabs at the same time, to make it easier to follow the lab steps.

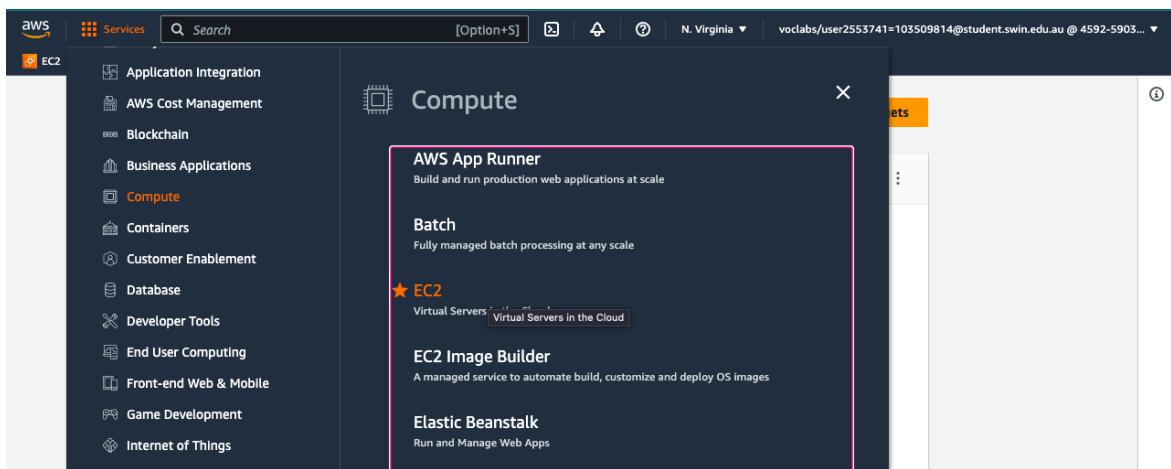


Task 1: Launch Your Amazon EC2 Instance

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** choose **Services**, choose **Compute** and then choose **EC2**.

Note: Verify that your EC2 console is currently managing resources in the **N. Virginia** (us-east-1) region. You can verify this by looking at the drop down menu at the top of the screen, to the left of your username. If it does not already indicate N. Virginia, choose the N. Virginia region from the region menu before



proceeding to the next step.

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

The screenshot shows the AWS EC2 console with the 'Launch instance' wizard open. The left sidebar shows various network and security options. The main panel has a 'Launch instance' button highlighted in orange. To the right, there's a 'Service health' section showing 'This service is operating normally' and a 'Zones' section. A banner at the top says 'Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server'. The URL in the address bar is <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstanceWizard>.

Step 1: Name and tags

7. Give the instance the name **Web Server**.

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

The screenshot shows the 'Launch an instance' wizard. In the 'Name and tags' section, the 'Name' field is filled with 'Web Server'. To the right, there's a 'Summary' pane showing 'Number of instances' set to 1, 'Software Image (AMI)' as Amazon Linux 2023 AMI 2023.0.2..., 'Virtual server type (instance type)' as t2.micro, and 'Firewall (security group)' as New security group.

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

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

The screenshot shows the AWS EC2 console with the 'Quick Start' tab selected. On the left, there's a grid of OS icons: Amazon Linux, macOS, Ubuntu, Windows, and Red Hat. Below the grid, the 'Amazon Machine Image (AMI)' section is highlighted. It displays the 'Amazon Linux 2023 AMI' with the ID 'ami-0889a44b331db0194'. The architecture is listed as '64-bit (x86)'. To the right, the 'Summary' pane shows the number of instances set to 1, the software image as 'Amazon Linux 2023 AMI 2023.0.2...', the virtual server type as 't2.micro', and the firewall as 'New security group'. At the bottom right of the summary pane is a prominent orange 'Launch instance' button.

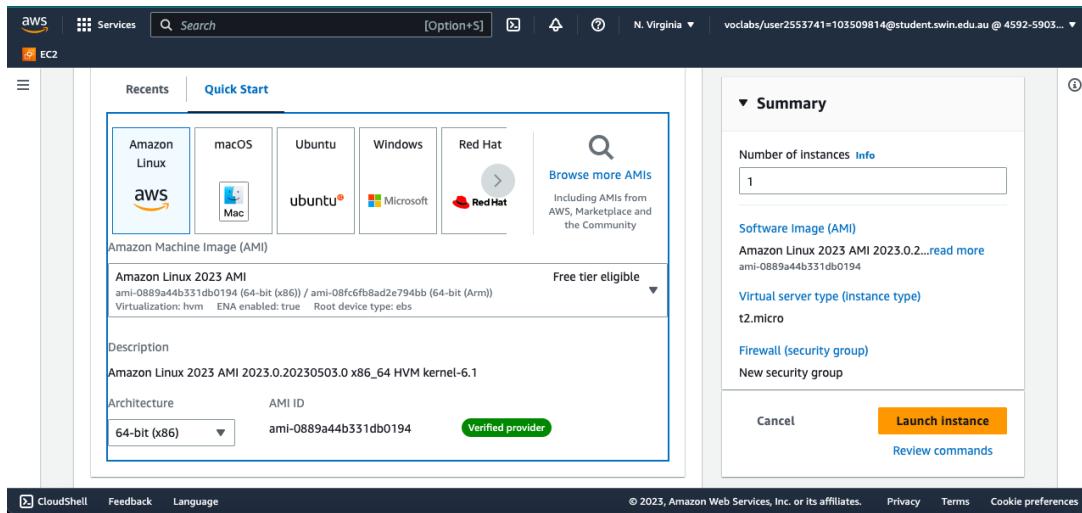
- Also keep the default **Amazon Linux 2023 AMI** selected.

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

- 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

This screenshot is identical to the one above, showing the AWS EC2 'Quick Start' interface. The 'Amazon Linux 2023 AMI' is selected, and the 'Summary' pane shows the same configuration: 1 instance, AMI ID 'ami-0889a44b331db0194', t2.micro instance type, and New security group. The 'Launch instance' button is again highlighted.

10. 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.



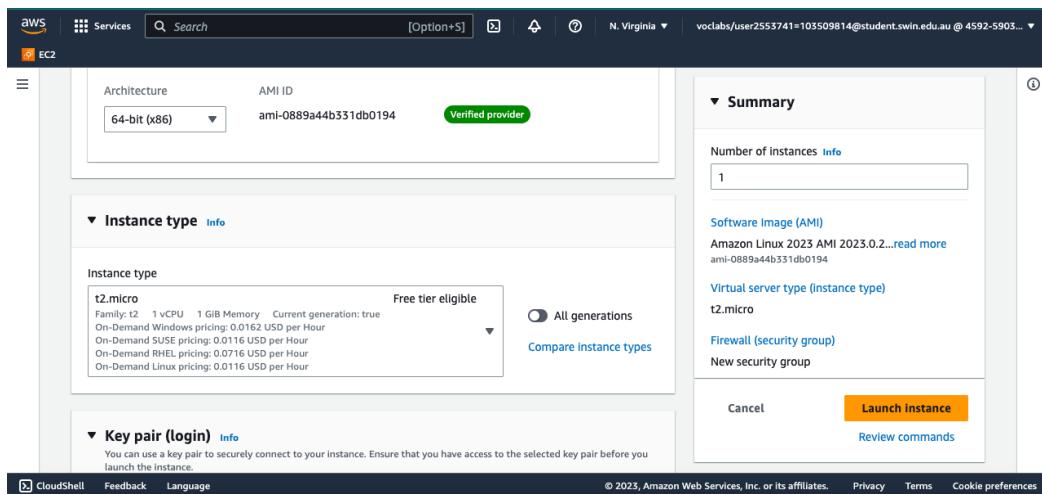
Step 3: Instance type

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.

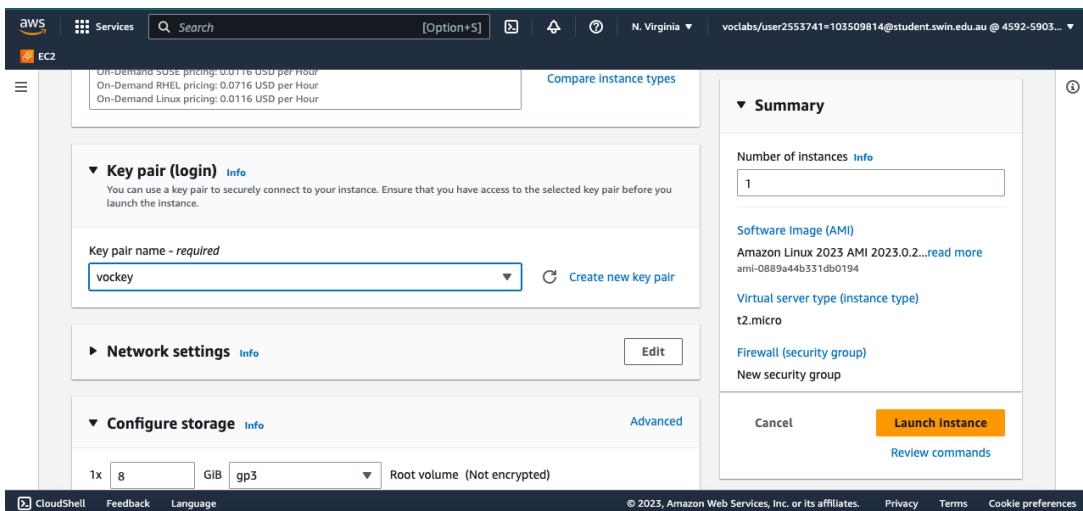
Note: You may be restricted from using other instance types in this lab.



Step 4: Key pair (login)

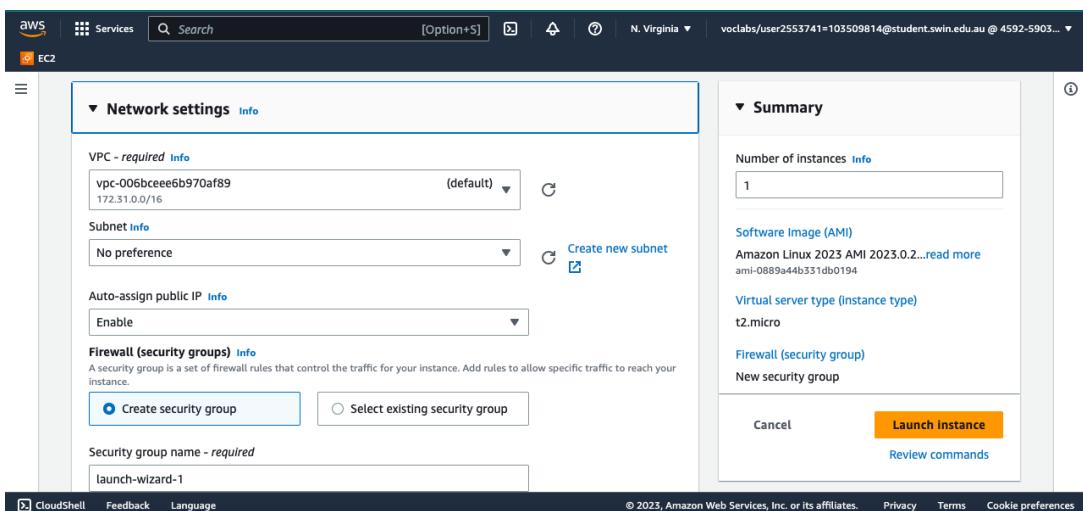
11. For Key pair name - *required*, choose **vockey**.

Amazon EC2 uses public–key cryptography to encrypt and decrypt login information. To ensure you will be able to log in to the guest OS of the instance you create, you identify an existing key pair or create a new key pair when launching the instance. Amazon EC2 then installs the key on the guest OS when the instance is launched. That way, when you attempt to login to the instance and you provide the private key, you will be authorized to connect to the instance. **Note:** In this lab you will not actually use the key pair you have specified to log into your instance.



Step 5: Network settings

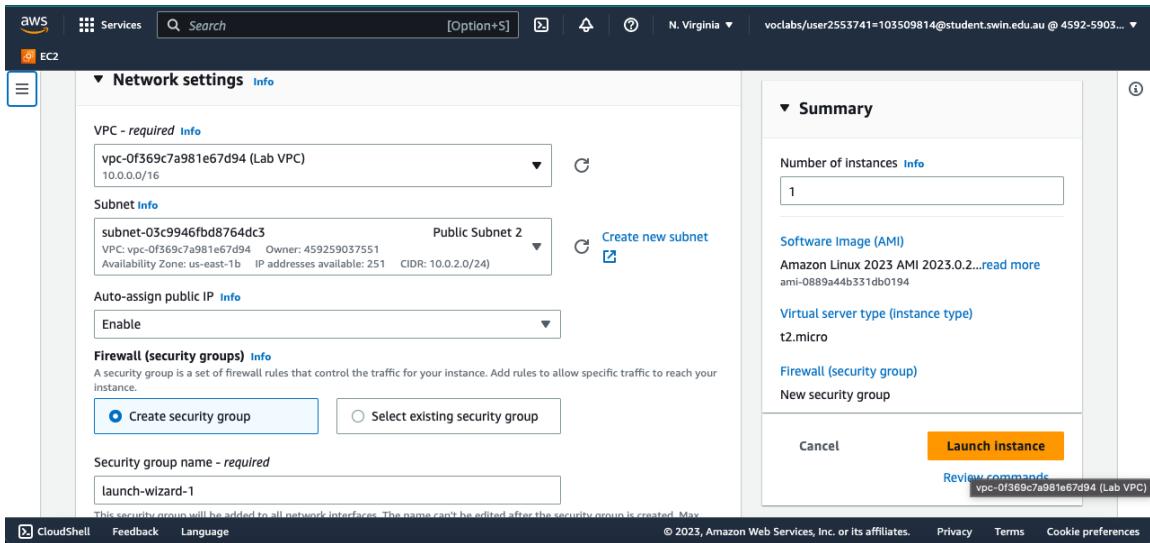
12. Next to Network settings, choose **Edit**.



13. For VPC, select Lab VPC.

The Lab VPC was created using an AWS CloudFormation template during the setup process of your lab. This VPC includes two public subnets in two different Availability Zones.

Note: Keep the default subnet. This is the subnet in which the instance will run. Notice also that by default, the instance will be assigned a public IP address.



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

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.

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

The screenshot shows the AWS EC2 Firewall (security groups) configuration page. The left sidebar has 'Create security group' and 'Select existing security group' options. The main area has fields for 'Security group name - required' (Web Server security group) and 'Description - required' (Security group for my web server). Below these are sections for 'Inbound security groups rules' (empty) and 'Advanced network configuration'. On the right, the 'Summary' section shows 'Number of instances' (1), 'Software Image (AMI)' (Amazon Linux 2023 AMI 2023.0.2), 'Virtual server type (instance type)' (t2.micro), and 'Firewall (security group)' (New security group). Buttons for 'Cancel', 'Launch instance' (highlighted in orange), and 'Review commands' are at the bottom.

Step 6: Configure storage

15. In the *Configure storage* section, keep the default settings.

Amazon EC2 stores data on a network-attached virtual disk called *Elastic Block Store*.

You will launch the Amazon EC2 instance using a default 8 GiB disk volume. This will be your root volume (also known as a 'boot' volume).

The screenshot shows the AWS EC2 instance configuration page. The left sidebar has 'Add security group rule' and 'Advanced network configuration' options. The main area has a 'Configure storage' section with a table showing 1x 8 GiB gp3 volume assigned as 'Root volume (Not encrypted)'. Buttons for 'Add new volume' and 'Edit' are below the table. On the right, the 'Summary' section shows 'Number of instances' (1), 'Software Image (AMI)' (Amazon Linux 2023 AMI 2023.0.2), 'Virtual server type (instance type)' (t2.micro), and 'Firewall (security group)' (New security group). Buttons for 'Cancel', 'Launch instance' (highlighted in orange), and 'Review commands' are at the bottom.

Step 7: Advanced details

16. Expand Advanced details.

The screenshot shows the AWS EC2 instance configuration page. The 'Advanced details' section is expanded, revealing various configuration options:

- Purchasing option: Request Spot Instances (checkbox)
- Domain join directory: Select dropdown with 'Select' option, 'Create new directory' button
- IAM instance profile: Select dropdown with 'Select' option, 'Create new IAM profile' button
- Hostname type: IP name (dropdown)
- DNS Hostname: Enable IP name IPv4 (A record) DNS requests (checkbox), Enable resource-based IPv4 (A record) DNS requests (checkbox)

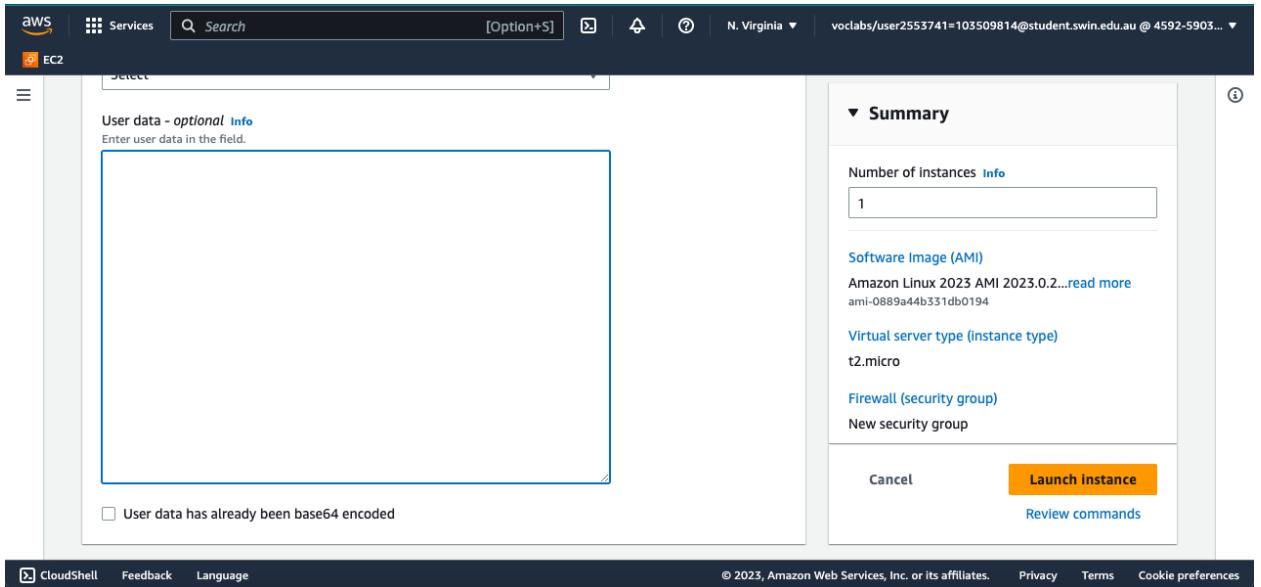
The right side of the screen displays detailed descriptions for these settings, such as the purchasing option and maximum price.

17. For Termination protection, select Enable.

When an Amazon EC2 instance is no longer required, it can be *terminated*, which means that the instance is deleted and its resources are released. A terminated instance cannot be accessed again and the data that was on it cannot be recovered. 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 as long as this setting remains enabled.

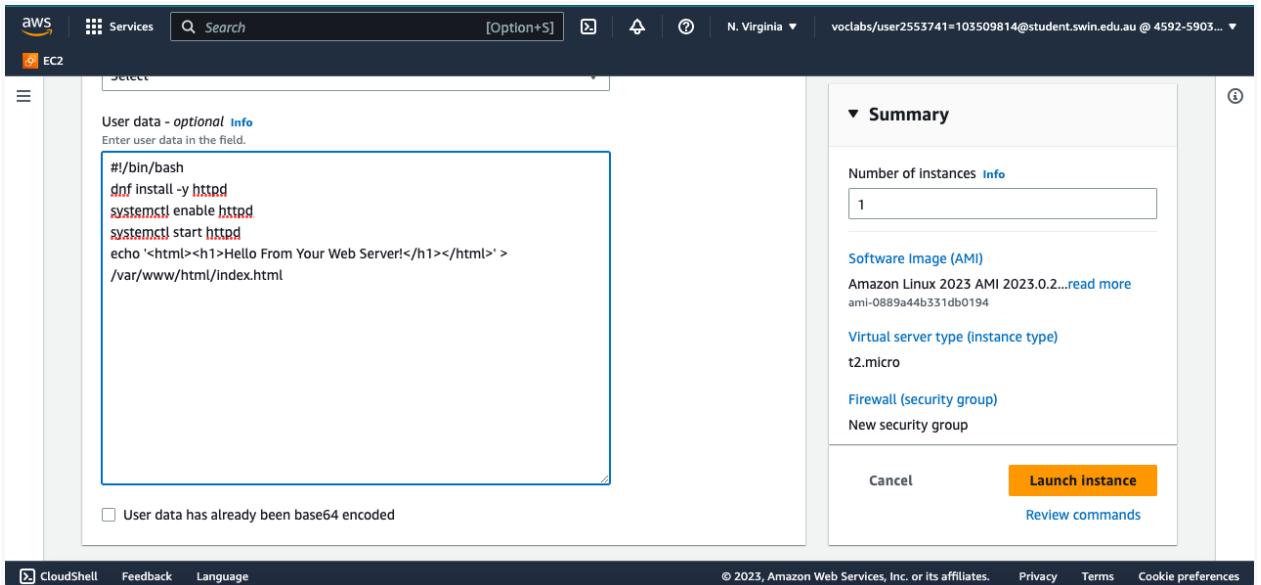
The screenshot shows the AWS EC2 instance configuration page. The 'Termination protection' setting is highlighted and set to 'Enable'. On the right side, the 'Summary' section shows the instance configuration, including the number of instances (1), software image (Amazon Linux 2023 AMI 2023.0.2...), virtual server type (t2.micro), and a prominent 'Launch instance' button.

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



19. #!/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
```



20. 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 starts. The script will:

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

The screenshot shows the AWS EC2 Instances Launch an Instance summary page. At the top, there's a success message: "Successfully initiated launch of instance (i-046271d9eb09d23f9)". Below this, there's a "Launch log" link. A "Next Steps" section follows, containing a search bar and six numbered steps: 1. Create billing and free tier usage alerts, 2. Connect to your instance, 3. Connect an RDS database, 4. Create EBS snapshot policy, 5. To manage costs and avoid, 6. Once your instance is running, log into it from your local computer. Configure the connection. At the bottom, there are links for CloudShell, Feedback, Language, and cookie preferences.

Step 8: Launch the instance

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

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

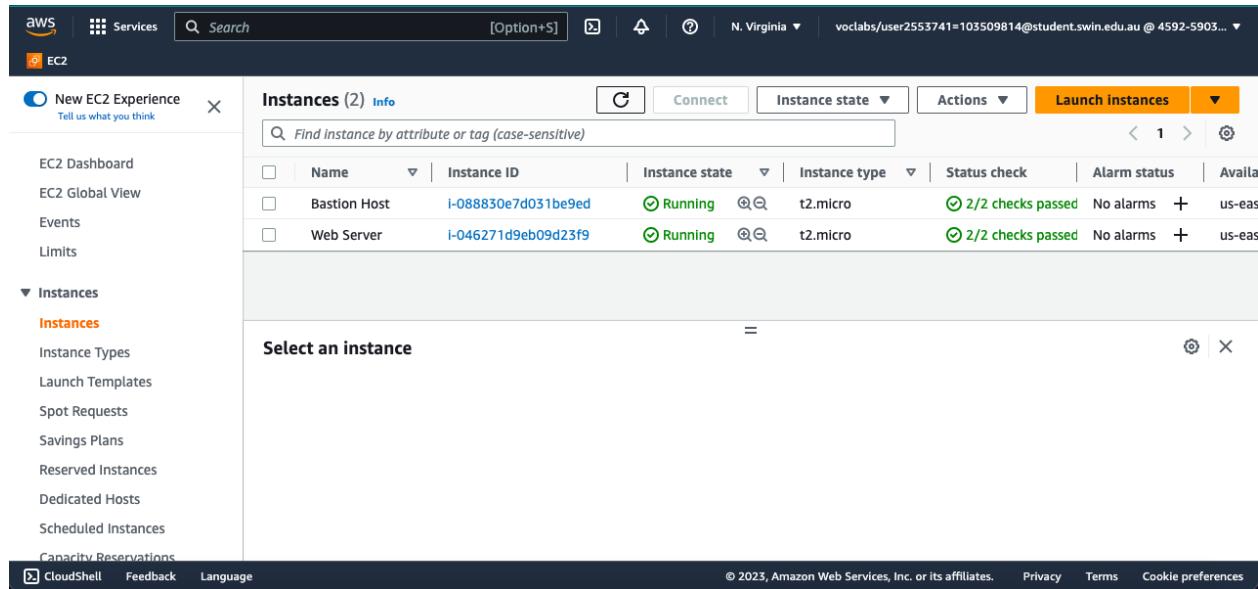
The instance is assigned a *Public IPv4 DNS* that you can use to contact the instance from the Internet.

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*.

21. Wait for your instance to display the following:

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



The screenshot shows the AWS EC2 Instances page. The left sidebar has 'New EC2 Experience' selected under 'Instances'. The main table lists two instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Available
Bastion Host	i-088830e7d031be9ed	Running	t2.micro	2/2 checks passed	No alarms	us-eas
Web Server	i-046271d9eb09d23f9	Running	t2.micro	2/2 checks passed	No alarms	us-eas

A modal window titled 'Select an instance' is open at the bottom.

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

Task 2: Monitor Your Instance

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

22. Choose the **Status checks** tab.

With instance status monitoring, you can quickly determine whether Amazon EC2 has detected any problems that might prevent your instances from running applications. Amazon EC2 performs automated checks on every running EC2 instance to identify hardware and software issues.

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

Instances (1/2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Available
Bastion Host	i-088830e7d031be9ed	Running	t2.micro	2/2 checks passed	No alarms	+ us-eas
Web Server	i-046271d9eb09d23f9	Running	t2.micro	2/2 checks passed	No alarms	+ us-eas

Instance: i-046271d9eb09d23f9 (Web Server)

Status checks Info

Status checks detect problems that may impair i-046271d9eb09d23f9 (Web Server) from running your applications.

System status checks	Instance status checks
System reachability check passed	Instance reachability check passed

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

Actions

23. Choose the Monitoring tab.

This tab displays Amazon CloudWatch metrics for your instance. Currently, there are not many metrics to display because the instance was recently launched. You can choose the three dots icon in any graph and select **Enlarge** to see an expanded view of the chosen metric.

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

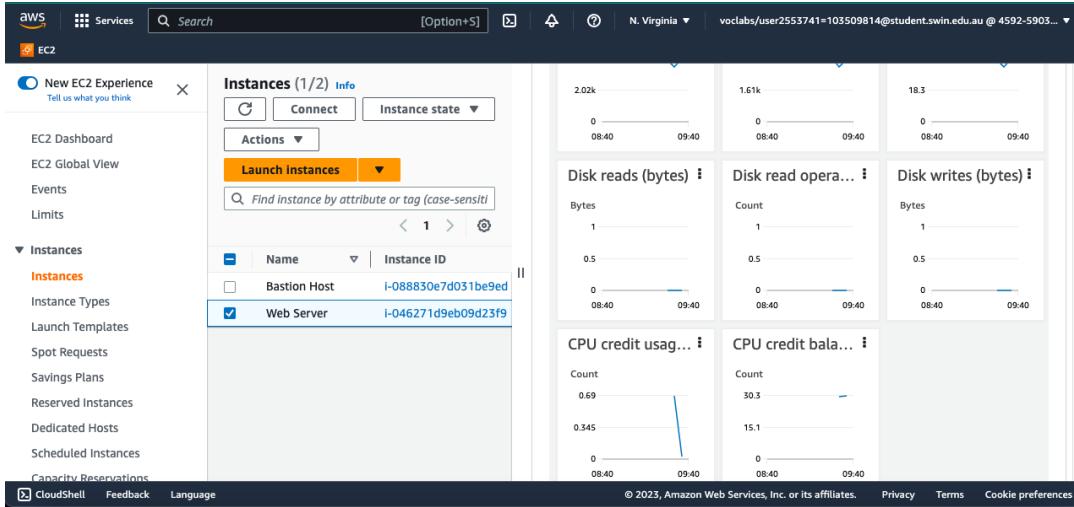
Instances (1/2) Info

Instance: i-046271d9eb09d23f9 (Web Server)

Monitoring

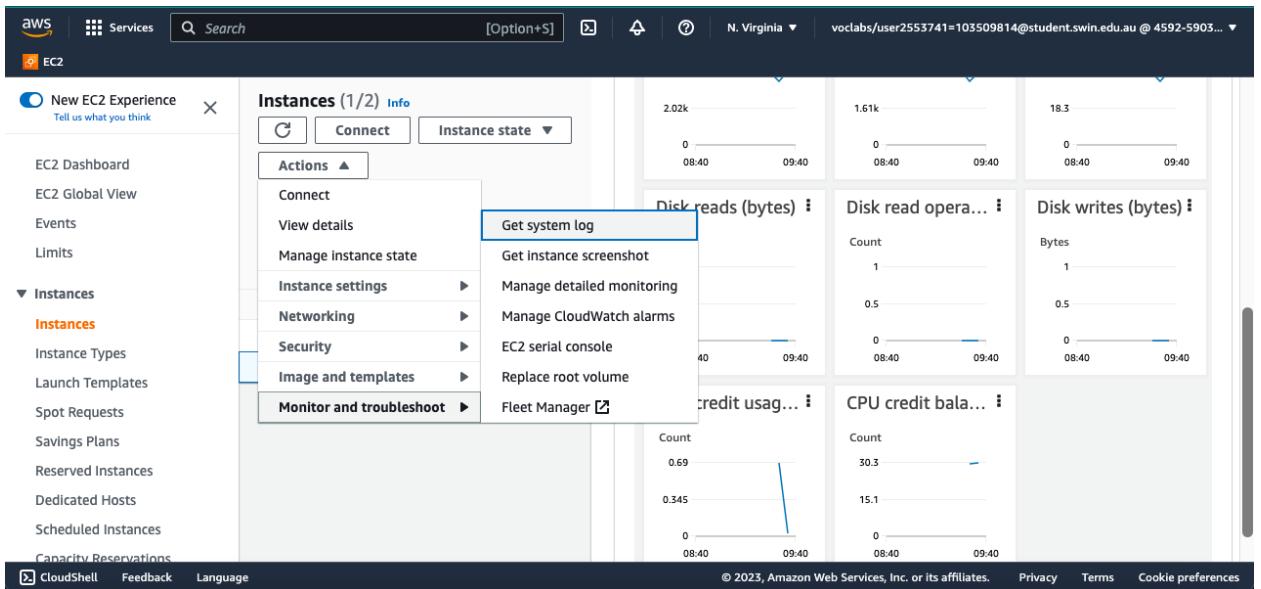
1h	3h	12h	1d	3d	1w	Custom
0.498	0.249	0	0.5	0	0.5	08:40 09:40
Percent	Count					

Network in (bytes)	Network out (bytes)	Network packets
Bytes	Bytes	Count
4.03k	3.22k	36.6



24. In the Actions menu towards the top of the console, select **Monitor and troubleshoot Get system log**.

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



25. 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 AWS EC2 console. A warning icon is displayed at the top left. The main area shows a terminal window displaying the output of a command, likely related to instance configuration or logs. The terminal output includes several lines of text starting with brackets and numbers, followed by package names and versions.

```
[ 27.77427] cloud-init[2079]: Verifying . apr_dctt-1.0.5-1.amzn2023.0.1.x86_64
[ 27.767537] cloud-init[2079]: Verifying : mod_http2-2.0.11-2.amzn2023.x86_64
[ 27.775497] cloud-init[2079]: Verifying : httpd-tools-2.4.56-1.amzn2023.x86_64
[ 27.827437] cloud-init[2079]: Verifying : mod_lua-2.4.56-1.amzn2023.x86_64
[ 27.848291] cloud-init[2079]: Verifying : mailcap-2.1.49-3.amzn2023.0.3.noarch
[ 27.854965] cloud-init[2079]: Verifying : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch
[ 27.989212] cloud-init[2079]: Verifying : httpd-filesystem-2.4.56-1.amzn2023.noarch
[ 28.001952] cloud-init[2079]: Installed: [ 28.024181] cloud-init[2079]: apr-1.7.2-2.amzn2023.0.2.x86_64
[ 28.029300] cloud-init[2079]: apr-util-1.6.3-1.amzn2023.0.1.x86_64
[ 28.047576] cloud-init[2079]: apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64
[ 28.060117] cloud-init[2079]: generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch
[ 28.071146] cloud-init[2079]: httpd-2.4.56-1.amzn2023.x86_64
[ 28.076977] cloud-init[2079]: httpd-core-2.4.56-1.amzn2023.x86_64
[ 28.107502] cloud-init[2079]: httpd-filesystem-2.4.56-1.amzn2023.noarch
[ 28.112553] cloud-init[2079]: httpd-tools-2.4.56-1.amzn2023.x86_64
[ 28.117505] cloud-init[2079]: libbrotli-1.0.9-4.amzn2023.0.2.x86_64
[ 28.137410] cloud-init[2079]: mailcap-2.1.49-3.amzn2023.0.3.noarch
[ 28.148156] cloud-init[2079]: mod_http2-2.0.11-2.amzn2023.x86_64
[ 28.151336] cloud-init[2079]: mod_lua-2.4.56-1.amzn2023.x86_64
[ 28.154537] cloud-init[2079]: Complete!
```

26. Choose Cancel.

The screenshot shows the AWS EC2 console after a command has been run. The terminal output displays SSH host key fingerprints and a message indicating the cloud-init process has finished. A callout box provides troubleshooting instructions for boot or networking issues, and a 'Connect' button is available to start a serial console session.

```
ci-info: | ssh-rsa | 43:18:40:49:69:99:f4:f8:9e:01:c7:fe:9c:85:e2:a6:61:07:96:7b:21:ff:24:f3:7a:21:db:13:3a
ci-info: +-----+
<14-May 19 09:26:36 cloud-init: #####-----#####
<14-May 19 09:26:36 cloud-init: ----BEGIN SSH HOST KEY FINGERPRINTS-----
<14-May 19 09:26:36 cloud-init: 256 SHA256:QQQsAwvoZIJk6yzAkJXwyUEIMBtvEdiE/z0V4ubI71o root@ip-10-0-2-202.e
<14-May 19 09:26:36 cloud-init: 256 SHA256:r7v05ujYEkt1NxR3p7nE5Be8fv7r4J1gGKa0NLXRLTio root@ip-10-0-2-202.e
<14-May 19 09:26:36 cloud-init: -----END SSH HOST KEY FINGERPRINTS-----
<14-May 19 09:26:36 cloud-init: #####-----#####
-----BEGIN SSH HOST KEY KEYS-----
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmLzdHAyNTYAAAIBmlzdHAyNTYAAABBL2ehwazB6b0CtkmYjcVP/e0gcF6BoxtBPs
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBLKoEhjhMac01uFr3gaQ+leC+CFiJoulgpVIwx7AA4N root@ip-10-0-2-202.ec2.int
-----END SSH HOST KEY KEYS-----
[ 29.677986] cloud-init[2079]: Cloud-init v. 22.2.2 finished at Fri, 19 May 2023 09:26:36 +0000. Datasour
```

For boot or networking issues, use the EC2 serial console for troubleshooting. Choose the **Connect button to start a session.**

Cancel

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

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



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

The screenshot shows the AWS EC2 Instance Screenshot interface. At the top, there's a navigation bar with the AWS logo, Services, a search bar, and account information. Below the navigation bar, the title "Instance screenshot" is displayed, followed by the instance ID and timestamp: "i-046271d9eb09d23f9 (Web Server) on 2023-05-19 at T16:49:20.708 +07:00". On the left, there's a sidebar with a "CloudShell" button. The main area contains a terminal window showing a log message from an Amazon Linux 2023 instance:

```
Amazon Linux 2023
Kernel 6.1.25-37.47.amzn2023.x86_64 on an x86_64 (-)

[ 28.695965] systemd-sysv-generator[3500]: SysV service '/etc/rc.d/init.d/cfn-hup' lacks a native systemd unit file. Automatically generating a unit file for compatibility. Please update package to include a native systemd unit file, in order to make it more safe and robust.
[ 28.695965] systemd-sysv-generator[3500]: SysV service '/etc/rc.d/init.d/cfn-hup' lacks a native systemd unit file. Automatically generating a unit file for compatibility. Please update package to include a native systemd unit file, in order to make it more safe and robust.
-
```

At the bottom of the terminal window, there are "CloudShell", "Feedback", and "Language" buttons. To the right, there are links for "© 2023, Amazon Web Services, Inc. or its affiliates.", "Privacy", "Terms", and "Cookie preferences".

28. Choose Cancel.

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

The screenshot shows the AWS EC2 Serial Console interface. At the top, there's a navigation bar with the AWS logo, Services, a search bar, and account information. Below the navigation bar, the title "Serial console" is displayed, followed by the instance ID and timestamp: "i-046271d9eb09d23f9 (Web Server) on 2023-05-19 at T16:49:20.708 +07:00". On the left, there's a sidebar with a "CloudShell" button. The main area contains a terminal window showing a log message from an Amazon Linux 2023 instance:

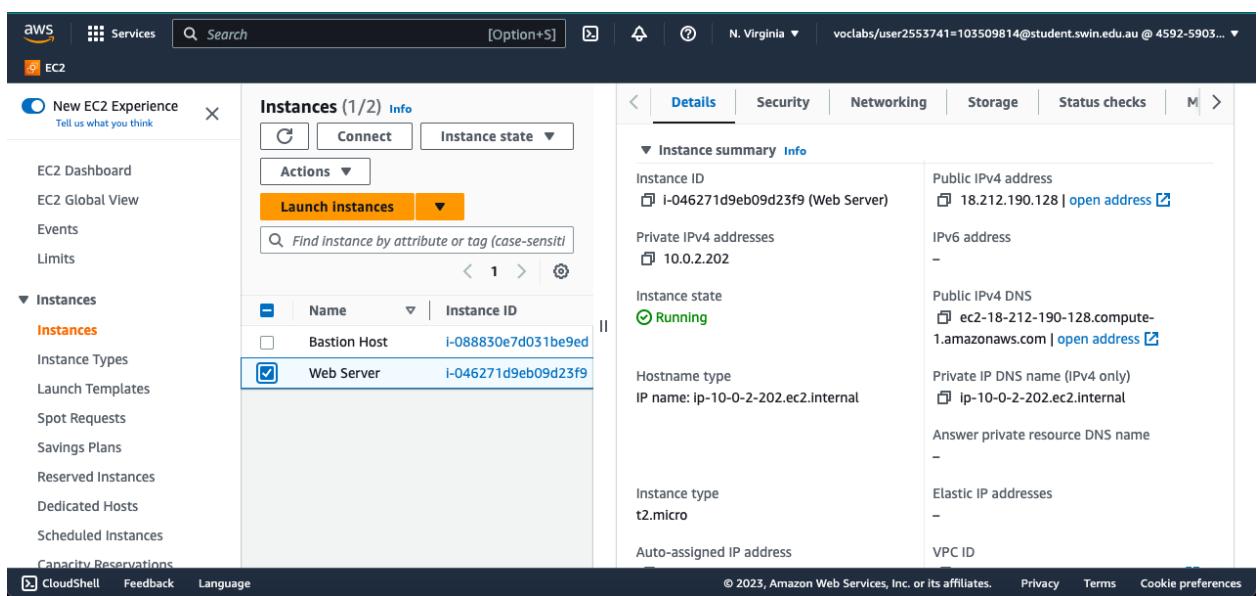
```
[ 28.695965] systemd-sysv-generator[3500]: SysV service '/etc/rc.d/init.d/cfn-hup' lacks a native systemd unit file. Automatically generating a unit file for compatibility. Please update package to include a native systemd unit file, in order to make it more safe and robust.
-
```

Below the terminal window, there's a callout box with the text: "For boot or networking issues, use the EC2 serial console for troubleshooting. Choose the Connect button to start a session." A "Connect" button is located next to the callout box. At the bottom right, there's a "Cancel" button. At the very bottom, there are "CloudShell", "Feedback", and "Language" buttons, along with copyright and legal links.

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.

29. Ensure **Web Server** is still selected. Choose the **Details** tab.



The screenshot shows the AWS EC2 Instances page. On the left, the navigation pane is visible with options like EC2 Dashboard, EC2 Global View, Events, Limits, Instances, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, CloudShell, Feedback, and Language. The main area displays two instances: 'Bastion Host' (Instance ID: i-088830e7d031be9ed) and 'Web Server' (Instance ID: i-046271d9eb09d23f9). The 'Web Server' instance is selected. The right side shows the 'Details' tab of the instance summary. Key details include:

Attribute	Value
Instance ID	i-046271d9eb09d23f9 (Web Server)
Private IPv4 address	10.0.2.202
Instance state	Running
Hostname type	IP name: ip-10-0-2-202.ec2.internal
Instance type	t2.micro
Auto-assigned IP address	-
Public IPv4 address	18.212.190.128 open address
Public IPv4 DNS	ec2-18-212-190-128.compute-1.amazonaws.com open address
Private IP DNS name (IPv4 only)	ip-10-0-2-202.ec2.internal
Answer private resource DNS name	-
Elastic IP addresses	-
VPC ID	-

30. Copy the **Public IPv4 address** of your instance to your clipboard.

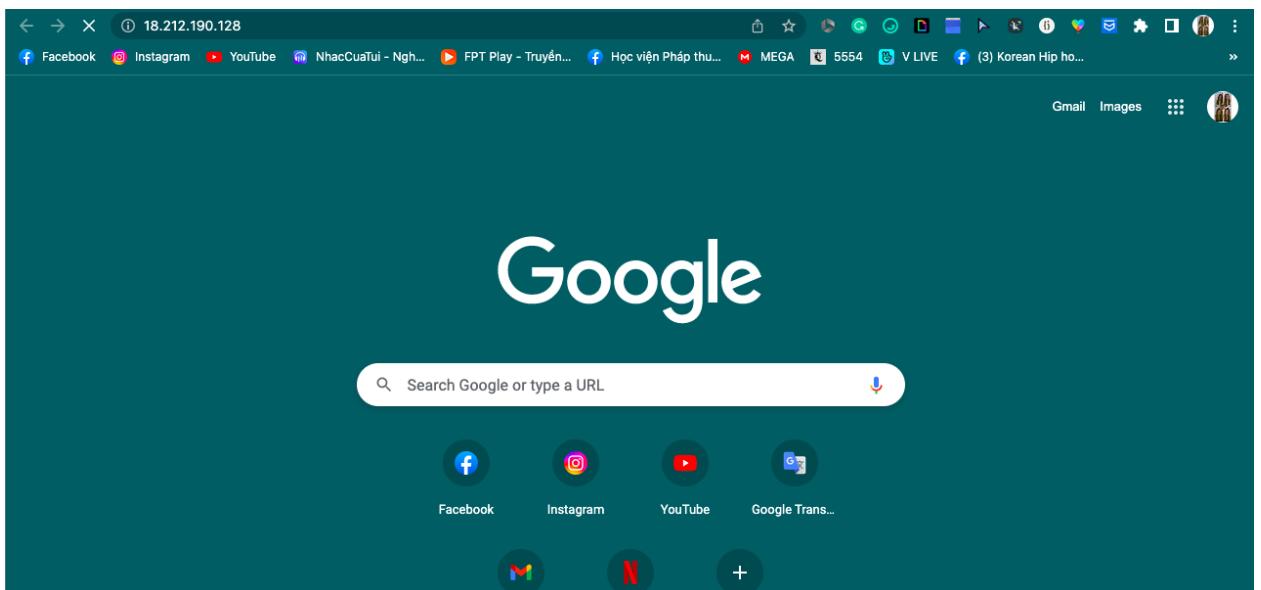
The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with options like EC2 Dashboard, EC2 Global View, Events, Limits, Instances, and more. The main area shows 'Instances (1/2) Info' with a table containing one row: 'Bastion Host' (Instance ID: i-088830e7d031be9ed) and 'Web Server' (Instance ID: i-046271d9eb09d23f9, which is selected). To the right, the 'Details' tab is active, displaying instance details such as Instance ID (i-046271d9eb09d23f9), Instance state (Running), Hostname type (IP name: ip-10-0-2-202.ec2.internal), and Instance type (t2.micro). A green callout box highlights the 'Public IPv4 address copied' message above the instance summary. The copied address is 18.212.190.128.

31. 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.



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

The screenshot shows the AWS EC2 Instances page. On the left, the navigation pane includes links like EC2 Dashboard, EC2 Global View, Events, Limits, Instances (selected), Instances Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, CloudShell, Feedback, and Language. The main content area displays 'Instances (1/2) Info' for a single instance named 'Web Server' (Instance ID: i-046271d9eb09d23f9). The 'Details' tab is selected, showing details such as Public IPv4 address (18.212.190.128), Instance state (Running), Hostname type (IP name: ip-10-0-2-202.ec2.internal), and Instance type (t2.micro). A green note indicates 'Public IPv4 address copied'. Other tabs include Security, Networking, Storage, and Status checks.

33. In the left navigation pane, choose **Security Groups**.

The screenshot shows the AWS Security Groups page. The left navigation pane includes links for Snapshots, Lifecycle Manager, Network & Security (selected), Security Groups (selected), Elastic IPs, Placement Groups, Key Pairs, Network Interfaces, Load Balancing, Load Balancers, Target Groups, Auto Scaling, Launch Configurations, and Auto Scaling Groups. The main content area displays 'Security Groups (5) Info' with a table listing five security groups: default (sg-047eedcdee603fc15), default (sg-040078406d817e7f8), default (sg-061c737acf569ad4), default (sg-0e8cce1479f2cc6a2), and Web Server security gr... (sg-0f369c7a981e67d94). The table columns are Name, Security group ID, Security group name, VPC ID, and Description. A 'Create security group' button is visible at the top right. Other tabs include Actions, Export security groups to CSV, and a help icon.

34. Select Web Server security group.

The screenshot shows the AWS EC2 Security Groups page. On the left sidebar, under 'Network & Security', 'Security Groups' is selected. In the main content area, a table lists five security groups. The fifth row, 'sg-0e8cce1479f2cc6a2 - Web Server security group', has a checked checkbox in the first column and is highlighted with a blue border. The table columns are: Name, Security group ID, Security group name, VPC ID, and Description. The 'Description' column for the selected group shows 'Security group f'. Below the table, a modal window titled 'sg-0e8cce1479f2cc6a2 - Web Server security group' is open, showing the 'Details' tab. At the bottom of the modal, there is a message: 'You can now check network connectivity with Reachability Analyzer' and a button 'Run Reachability Analyzer'.

35. Choose the Inbound rules tab.

The security group currently has no inbound rules.

The screenshot shows the AWS EC2 Security Groups page. The 'Inbound rules' tab is selected in the navigation bar. A message at the top of the table area says 'No security group rules found'. The table columns are: Name, Security group rule..., IP version, Type, and Protocol. The table is currently empty.

36. Choose Edit inbound rules, select Add rule and then configure:

- **Type: HTTP**
- **Source: Anywhere-IPv4**

- Choose Save rules

The screenshot shows the AWS Management Console interface for managing security groups. The user is on the 'Edit inbound rules' page for a specific security group. A new rule is being configured with the following parameters:

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
-	HTTP	TCP	80	Anywhere	0.0.0.0/0

At the bottom right of the form, there are three buttons: 'Cancel', 'Preview changes', and a prominent orange 'Save rules' button.

37. 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.

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 runtime charge for a stopped EC2 instance, but the storage charge for attached Amazon EBS volumes remains.

38. On the **EC2 Management Console**, in the left navigation pane, choose **Instances**.

Web Server should already be selected.

The screenshot shows the AWS EC2 Management Console interface. The left sidebar has 'Instances' selected. The main area displays a table of instances:

Name	Instance ID	Instance state	Instance type	Status
Bastion Host	I-088830e7d031be9ed	Running	t2.micro	2/2
Web Server	I-046271d9eb09d23f9	Running	t2.micro	2/2

The 'Web Server' instance is selected. The right panel shows the 'Details' tab for the selected instance, with the following information:

- Instance summary:
 - Instance ID: I-046271d9eb09d23f9 (Web Server)
 - Public IPv4 address: 18.212.190.128 [open address]
 - Private IPv4 addresses: 10.0.2.202
 - IPv6 address: -
 - Instance state: Running
 - Public IPv4 DNS: ec2-18-212-190-

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

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with options like EC2 Dashboard, EC2 Global View, Events, Limits, and Instances (selected). Under Instances, 'Instances' is also selected. The main area shows a table of instances with two rows: 'Bastion Host' and 'Web Server'. The 'Actions' menu is open over the 'Web Server' row, with 'Stop instance' highlighted. To the right, a detailed view of the 'Web Server' instance is shown, including its summary, security settings, and network information.

40. Choose Stop

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

41. Wait for the **Instance state** to display: *Stopped*.

The screenshot shows the AWS EC2 Instances page after stopping the 'Web Server' instance. A green success message at the top says 'Successfully stopped i-046271d9eb09d23f9'. The main table now shows the 'Web Server' instance with its status as 'Stopping'. The detailed view on the right remains the same, showing the instance summary and security settings.

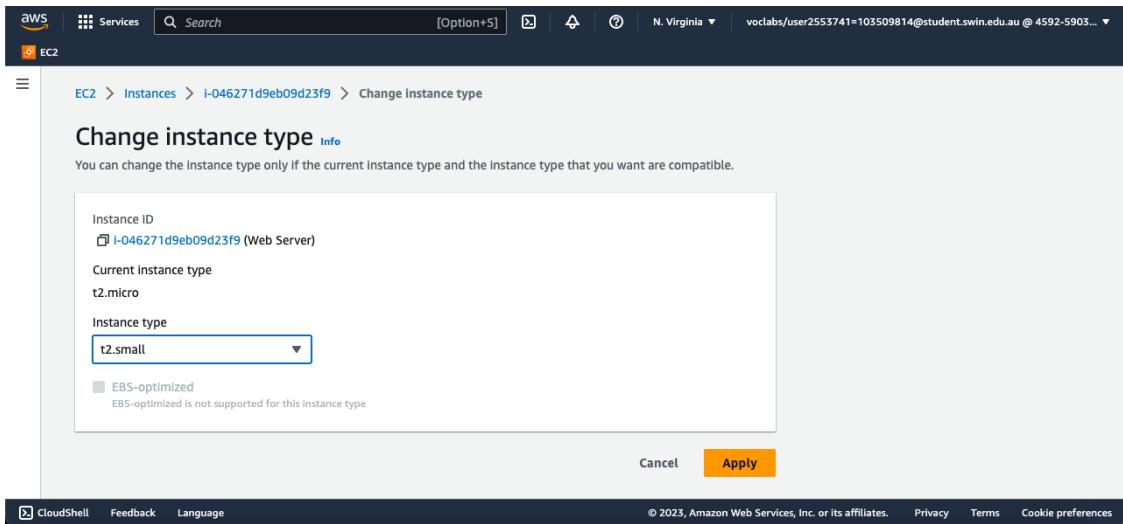
Change The Instance Type

42. In the Actions menu, select **Instance settings Change instance type**, then configure:

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

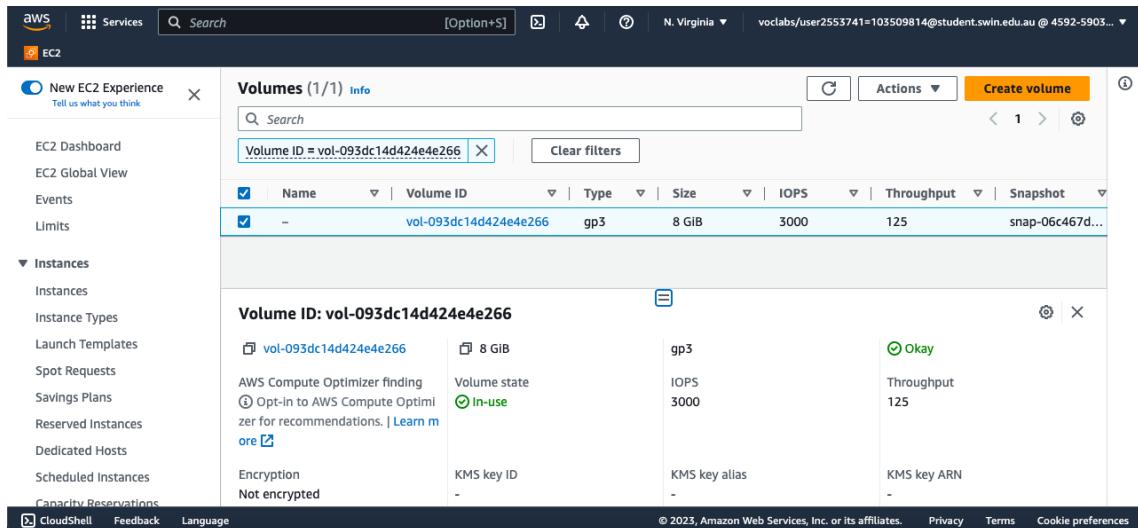
- Choose Apply

When the instance is started again it will run as 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.



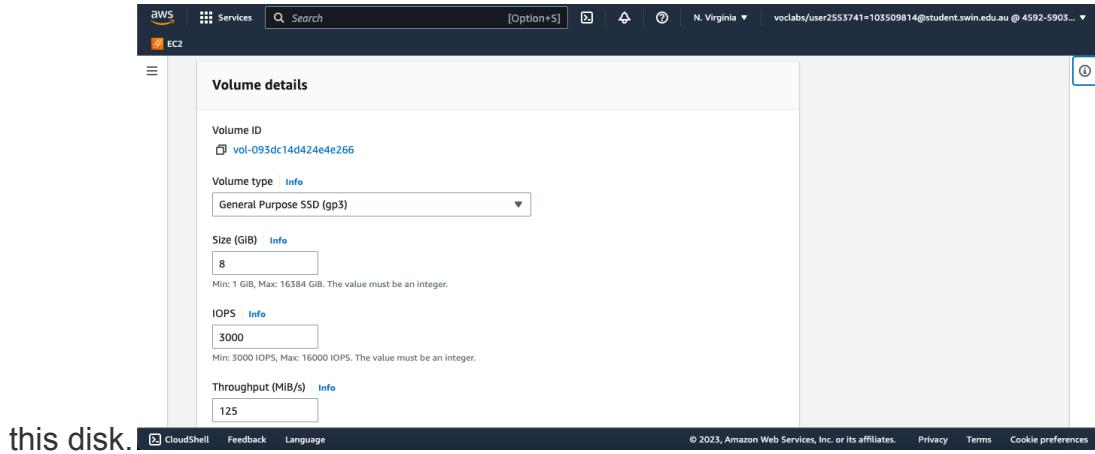
Resize the EBS Volume

43. With the Web Server instance still selected, choose the **Storage** tab, select the name of the Volume ID, then select the checkbox next to the volume that displays.

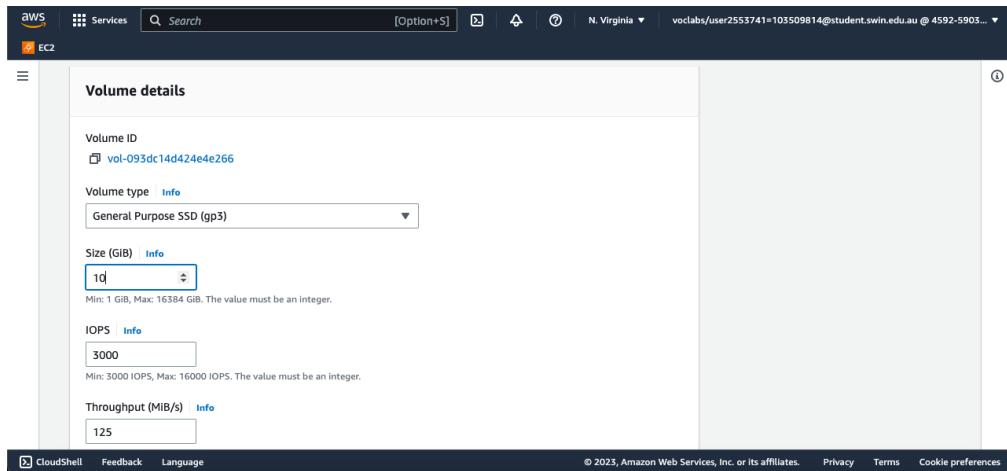


44. In the Actions menu, select **Modify volume**.

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

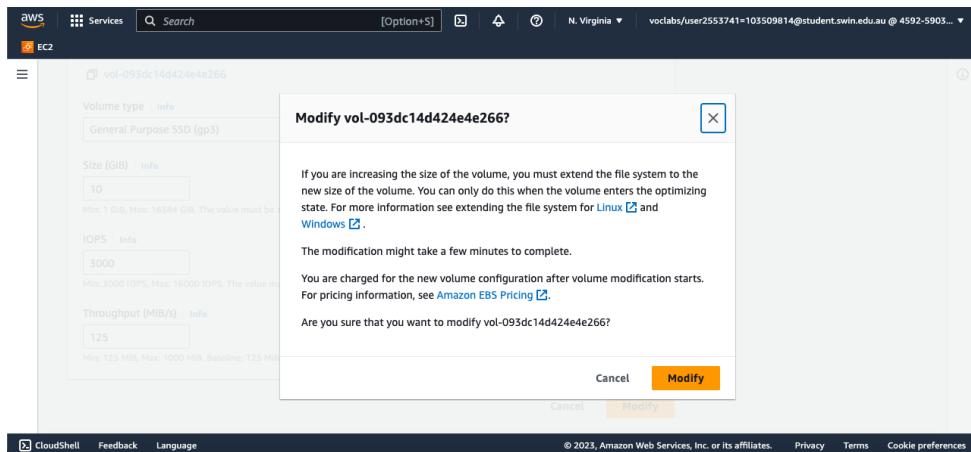


45. Change the size to: **10** **NOTE:** You may be restricted from creating large Amazon EBS volumes in this lab.



46. Choose Modify

47. Choose Modify again to confirm and increase the size of the volume.

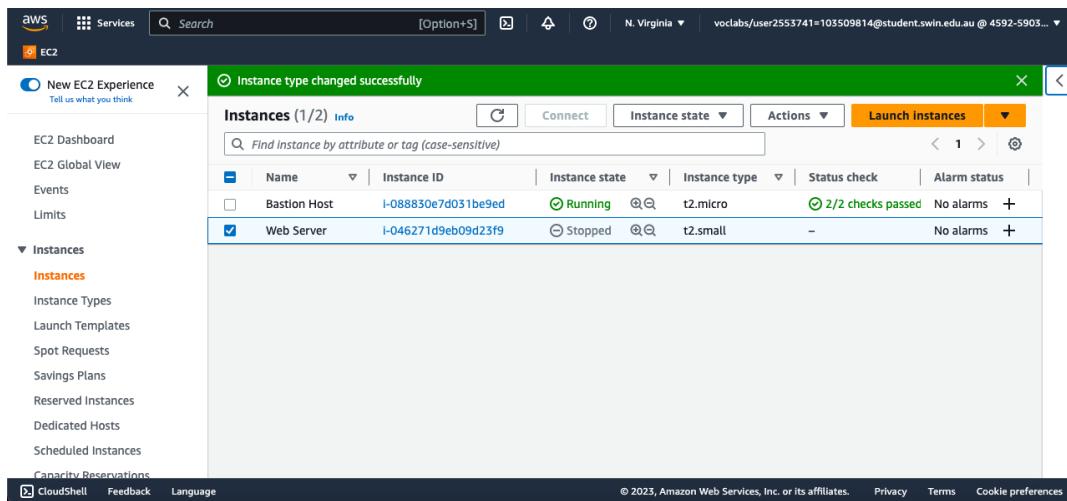


Start the Resized Instance

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

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

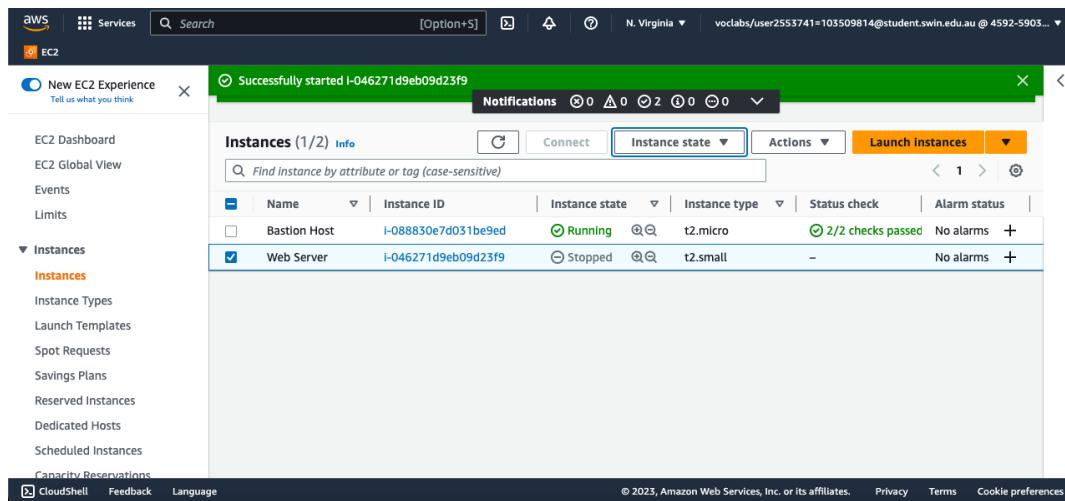
50. Select the **Web Server** instance.



The screenshot shows the AWS EC2 Instances page. A green notification bar at the top says "Instance type changed successfully". The main table has a header: "Instances (1/2) Info". Columns include Name, Instance ID, Instance state, Instance type, Status check, and Alarm status. There are two rows: "Bastion Host" (Running, t2.micro, 2/2 checks passed, No alarms) and "Web Server" (Stopped, t2.small, -). The "Web Server" row is selected, indicated by a checked checkbox in the first column. The left sidebar shows navigation options like EC2 Dashboard, EC2 Global View, Events, Limits, and Instances (selected).

51. In the Instance state menu, select **Start instance**.

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.



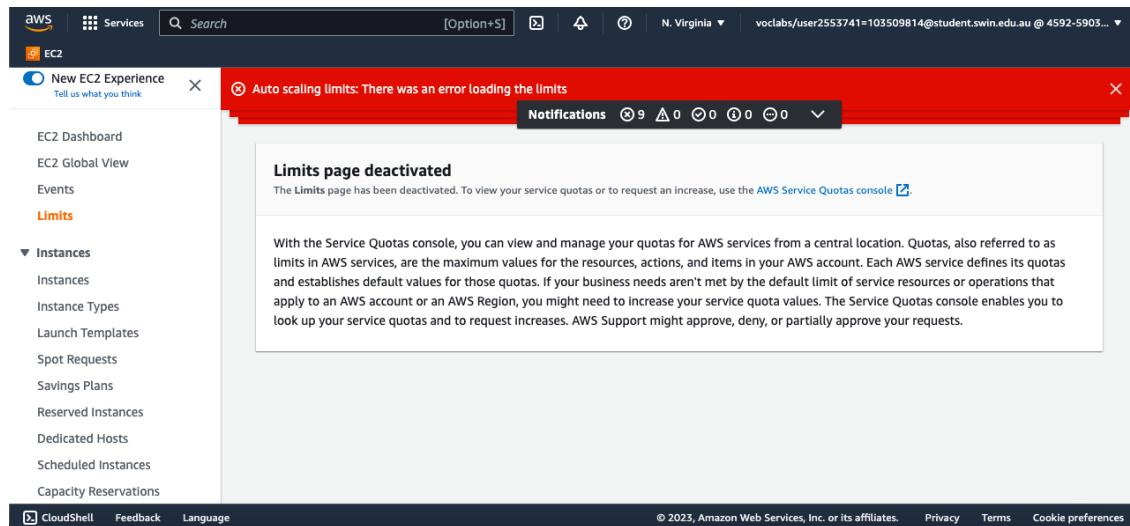
The screenshot shows the AWS EC2 Instances page after starting the instance. A green notification bar at the top says "Successfully started i-046271d9eb09d23f9". The main table shows the "Web Server" instance is now "Running". The left sidebar shows navigation options like EC2 Dashboard, EC2 Global View, Events, Limits, and Instances (selected).

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.

52. In the left navigation pane, choose **Limits**.

Note: You may see some banner messages indicating that you cannot load some limits. You can safely ignore these messages.



53. From the **All limits** drop down list, choose **Running instances**.

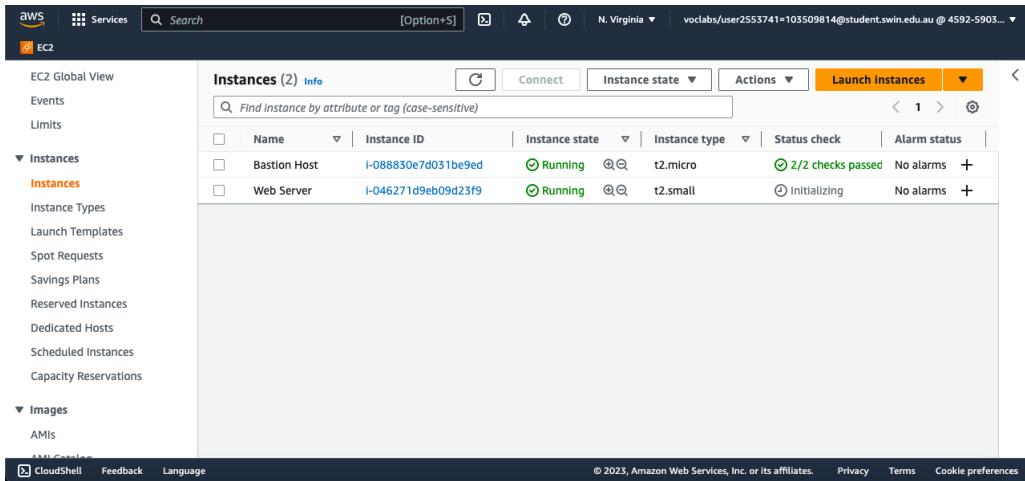
Notice that there are limits on the number and types of instances that can run in a region. For example, there is a limit on the number of *Running On-Demand Standard*... instances that you can launch in this region. When launching instances, the request must not cause your usage to exceed the instance limits currently defined 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*.

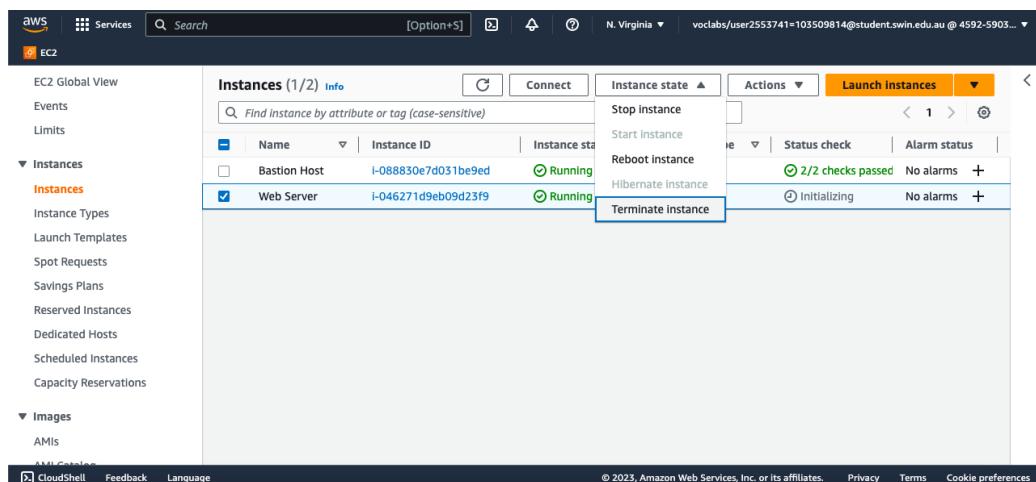
54. In left navigation pane, choose **Instances**.



The screenshot shows the AWS EC2 Instances page. The left sidebar has 'Instances' expanded, with 'Instances' selected. The main table lists two instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
Bastion Host	i-088830e7d031be9ed	Running	t2.micro	2/2 checks passed	No alarms
Web Server	i-046271d9eb09d23f9	Running	t2.small	Initializing	No alarms

55. Select the **Web Server** instance and in the Instance state menu, select **Terminate instance**.



The screenshot shows the AWS EC2 Instances page. The 'Actions' dropdown menu for the selected 'Web Server' instance has 'Terminate instance' highlighted.

56. 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.

The screenshot shows the AWS EC2 Instances page. A red error message at the top states: "Failed to terminate an instance: The Instance i-046271d9eb09d23f9' may not be terminated. Modify its 'disableApiTermination' instance attribute and try again." Below this, the "Instances (1/2) Info" table lists two instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
Bastion Host	i-088830e7d031be9ed	Running	t2.micro	2/2 checks passed	No alarms
Web Server	i-046271d9eb09d23f9	Running	t2.small	Initializing	No alarms

57. In the Actions menu, select **Instance settings Change termination protection**.

The screenshot shows the "Change termination protection" dialog box. It contains the following information:

- A message: "To prevent your instance from being accidentally terminated, you can enable termination protection for the instance. [Learn more](#)"
- An "Instance ID" field: "i-046271d9eb09d23f9 (Web Server)"
- A "Termination protection" section with a checked checkbox labeled "Enable".
- Buttons: "Cancel" and "Save" (highlighted in orange).

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

59. Choose **Save**

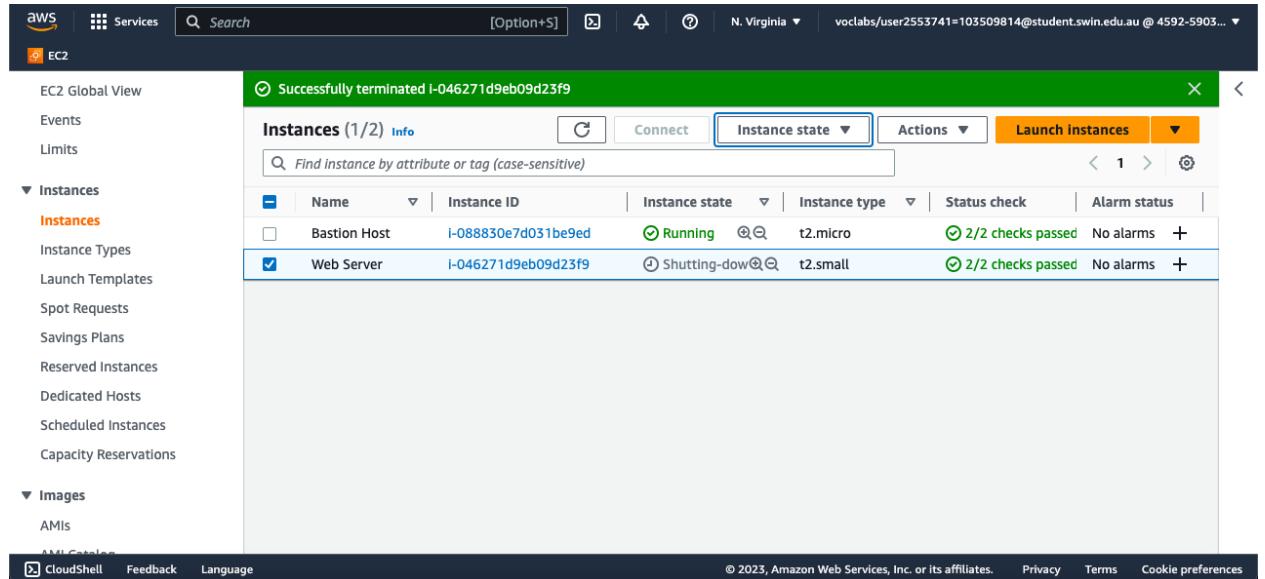
You can now terminate the instance.

The screenshot shows the AWS EC2 Instances page. A green success message at the top states: "Successfully removed termination protection for instance i-046271d9eb09d23f9. The instance can be terminated." Below this, the "Instances (1/2) Info" table lists the same two instances as before.

60. Select the **Web Server** instance again and in the Instance state menu, select **Terminate instance**.

61. Choose Terminate

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



The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with options like EC2 Global View, Events, Limits, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, and Capacity Reservations. Below that is another sidebar for Images and AMIs. The main content area has a green header bar with the message "Successfully terminated i-046271d9eb09d23f9". Below it is a table titled "Instances (1/2) Info" with columns: Name, Instance ID, Instance state, Instance type, Status check, and Alarm status. The table contains two rows: "Bastion Host" (Instance ID: i-088830e7d031be9ed, State: Running, Type: t2.micro, Checks: 2/2 passed, Alarms: None) and "Web Server" (Instance ID: i-046271d9eb09d23f9, State: Shutting-down, Type: t2.small, Checks: 2/2 passed, Alarms: None). The "Instance state" dropdown in the header is highlighted with a blue border. There are also "Actions" and "Launch instances" buttons.

Lab Complete

Congratulations! You have completed the lab.

62. Choose End Lab at the top of this page and then choose Yes to confirm that you want to end the lab.

An End Lab panel will appear, indicating that "You may close this message box now."

The screenshot shows the AWS Academy interface. On the left is a sidebar with icons for Account, Dashboard, Courses, Calendar, Inbox, History, and Help. The main area shows a navigation path: ACFv2EN... > Modules > Module 6 ... > Lab 3 - Introduction to Amazon EC2. A modal dialog is open in the center, asking "Are you sure you want to end the lab?". Below the modal, the lab content continues with steps 57, 58, and 59. Step 57 says: "In the Actions menu, select **Instance settings** **Change termination protection**". Step 58 says: "Remove the check next to **Enable**". Step 59 says: "Choose Save". At the top of the main area, there are buttons for Details, AWS, Start Lab, End Lab, 0:32, Instructions, and Actions. A "Source" button is also visible.

63. Choose the X in the top right corner to close the panel.

The screenshot shows the same AWS Academy interface as the previous one, but the modal dialog from step 63 has been closed. The "End Lab" panel is now visible, containing information about the lab's region, ID, creation time, and a message stating "You may close this message box now. Lab resources are terminating ...". The "X" button in the top right corner of the panel is highlighted with a red box. The rest of the interface remains the same, including the sidebar, navigation path, and lab steps 57, 58, and 59.

Additional Resources

- [Launch Your Instance](#)
- [Amazon EC2 Instance Types](#)
- [Amazon Machine Images \(AMI\)](#)
- [Amazon EC2 - User Data and Shell Scripts](#)
- [Amazon EC2 Root Device Volume](#)

- [Tagging Your Amazon EC2 Resources](#)
- [Security Groups](#)
- [Amazon EC2 Key Pairs](#)
- [Status Checks for Your Instances](#)
- [Getting Console Output and Rebooting Instances](#)
- [Amazon EC2 Metrics and Dimensions](#)
- [Resizing Your Instance](#)
- [Stop and Start Your Instance](#)
- [Amazon EC2 Service Limits](#)
- [Terminate Your Instance](#)
- [Termination Protection for an Instance](#)

© 2022, Amazon Web Services, Inc. and its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.