



COS20019

Cloud Computing Architecture

Assignement 1 – Part A
Creating and Deploying a Web Page

Truong Ngoc Gia Hieu
105565520

Due date: This assignment will be assessed by your tutor in your tutorial in **Week 4**. No submission is required. ***You must attend this demonstration to have your assignment assessed and be eligible for future assignments.***

Weighting: 5%

Preparation:

- ACF Labs 2 & 3.
- You will also need to create your own key pair and be able to access your EC2 instance via SSH using utilities like PuTTY and/or WinSCP. For more details, see *Remote Access to an EC2.pdf* file.

All supporting materials mentioned in this document can be found in the corresponding assignment page on Canvas

Objectives

This assignment has the following objectives:

1. Get familiar with the AWS management console.
2. Launch your own EC2 instance.
3. Deploy your first PHP web page (PhotoAlbum) on Apache web server on your EC2 instance.
4. Make cost-efficient use of your budget. Terminate any unnecessary extra resources that you created

AWS Accounts

You have a choice of accounts/environments you can use to complete the assignments in this unit.

1. **AWS Academy Learner Lab (recommended):** accessible through AWS Canvas. Note that this is NOT the sandbox in ACA/ACF courses that you use for your weekly labs. This is a managed environment that allows your tutor to gain access to your AWS console so your work can be marked/troubleshooted. This class gives you **US\$100 credit**. **Use it carefully.** This account is deleted at the end of the semester.
2. **Regular AWS account (NOT recommended):** new AWS accounts are eligible for a free tier. This gives you more freedom, but you need to be careful as you will be charged for the services if you go outside the free tier offering. Make sure to keep track of your AWS services usage (using Billing & Cost Management Dashboard) throughout the semester to avoid paying fees. This account is on-going, but some services are no longer free after 12 months. If you choose this option, you will need to create a (read-only) IAM user and provide its credentials to your tutor so they can mark the assignment

A. TASK 1 – Launch your own Linux EC2 instance

- First and foremost, opening the Learner Lab and then wait until the circle next to the AWS is green.

AWS  Used \$0 of \$50 03:59  Start Lab

Figure 1: Launching the AWS Console Home

- After launching the AWS Console Home successfully, search and open the EC2 main homepage to create own key pair.

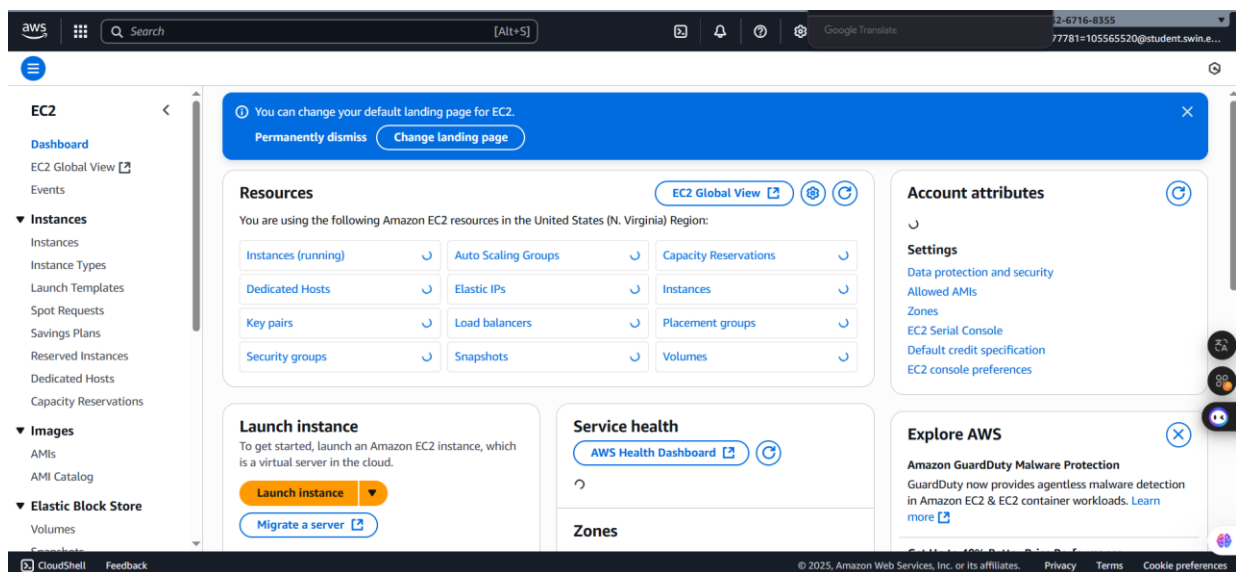


Figure 2: EC2 main homepage

- Then, configure settings for own key pair including:
 - + Name: Assignment1a
 - + Key pair type: RSA
 - + Private key file format: .pem

Create key pair [Info](#)

Key pair
A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type [Info](#)
☒ RSA ☐ ED25519

Private key file format
☒ .pem
For use with OpenSSH
☐ .ppk
For use with PuTTY

Figure 3: Key pair configuration

- As I expect, the own key pair named “Assignment1a” is successfully created key pair and the key pair “Assignment1a” has downloaded as “Assignment1a.pem”

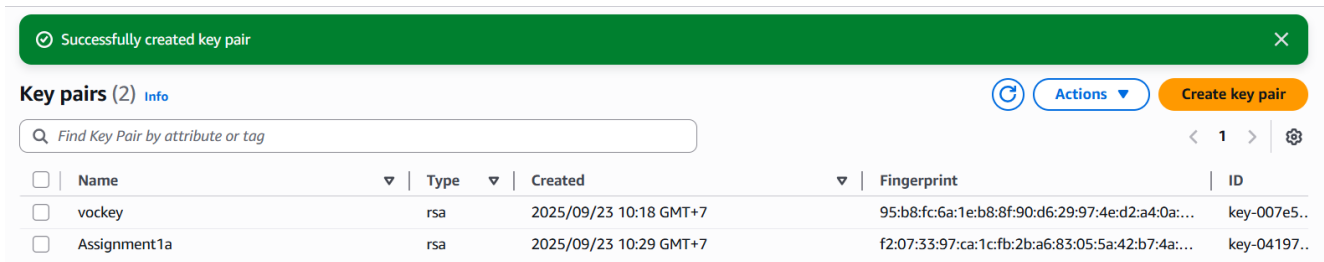


Figure 4: Successfully created key pair

- Then, I open the PuTTY Key Generator which convert file format from .pem to .ppk

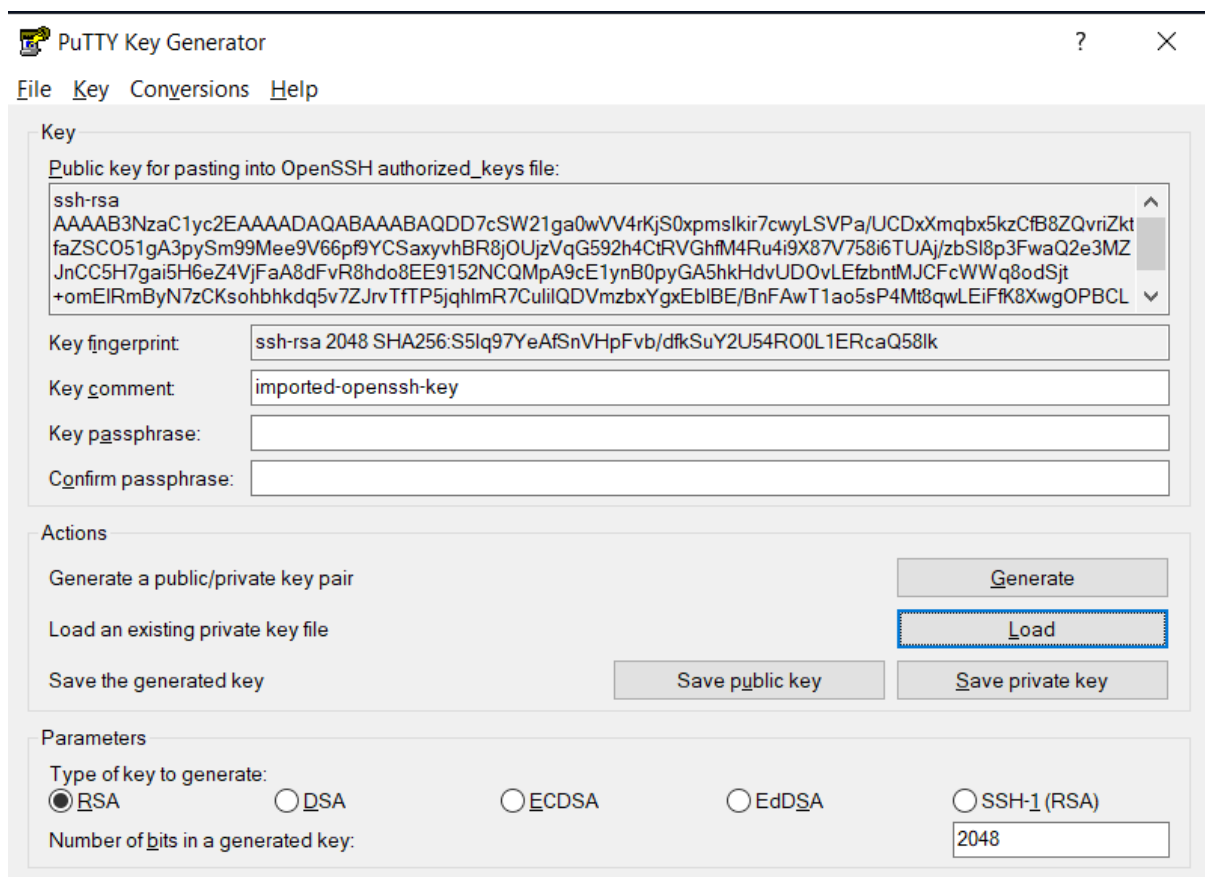


Figure 5: Convert from .pem to .ppk

- After that, the file is successfully converted from .pem to .ppk and stored in the folder named “Assignment1a”

> This PC > DATA (D:) > University > Sep_2025 > Cloud_Computing_Technology_COS20019 > Assignments > Assignment 1a

Name	Date modified	Type	Size
Assingment1a-WebsiteFiles	9/20/2025 10:17 AM	File folder	
Assignment requirements	9/16/2025 2:32 PM	Microsoft Edge PD...	467 KB
Assignment1a.pem	9/23/2025 10:29 AM	PEM File	2 KB
Assignment1a.ppk	9/23/2025 10:56 AM	PPK File	2 KB

Figure 6: Converting successfully

- Next, after setting up important feature, I decide to launch the EC2 instance with following settings:

- + Amazon Machine Image (AMI): Amazon Linux 2023 AMI
- + Instance type: t2.micro
- + Key Pair: Assignment1a
- + Security group named: "WebServer-SG"

Name

Assignment1a

Add additional tags

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose **Browse more AMIs**.

Q

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

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE

Debian

debian

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI

ami-08982f1c5bf93d976 (64-bit (x86), uefi-preferred) / ami-039f81f5ce6752b10 (64-bit (Arm), uefi)

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Figure 7: Name and AMI configuration

5

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

☐ All generations[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login) [Info](#)

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

Key pair name - *required*

Assignment1a

[Create new key pair](#)**Figure 8: Instance type and Key pair configuration**Security group name - *required*

WebServer-SG

Type	Protocol	Port range
ssh	TCP	22
Source type	Source	Description - <i>optional</i>
Anywhere	<input type="text" value="0.0.0.0/0"/>	e.g. SSH for admin desktop
▼ Security group rule 2 (TCP, 443, 0.0.0.0/0) Remove		
HTTPS	TCP	443
Source type	Source	Description - <i>optional</i>
Anywhere	<input type="text" value="0.0.0.0/0"/>	e.g. SSH for admin desktop
▼ Security group rule 3 (TCP, 80, 0.0.0.0/0) Remove		
HTTP	TCP	80

Figure 9: Security group configuration

User data - optional | Info

Upload a file with your user data or enter it in the field.

 Choose file

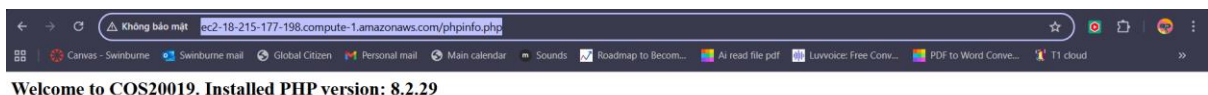
```
#!/bin/bash
PHP_VERSION=8.2
dnf update -y
dnf install -y httpd wget php${PHP_VERSION}-fpm php${PHP_VERSION}-mysqlnd
php${PHP_VERSION} php${PHP_VERSION}-devel
dnf install -y mariadb105-server
sed -i "s/upload_max_filesize = 2M/upload_max_filesize = 10M/g" /etc/php.ini
systemctl start httpd
systemctl enable httpd
usermod -a -G apache ec2-user
chown -R ec2-user:apache /var/www
chmod 2775 /var/www
find /var/www -type d -exec sudo chmod 2775 {} \;
find /var/www -type f -exec sudo chmod 0664 {} \;
echo "<?php echo '<h2>Welcome to COS20019. Installed PHP version: ' . phpversion() .
```

☐ User data has already been base64 encoded**Figure 10: User Data Script****- After configuring, the EC2 instance has successfully launched**

Instances (1/2) Info									
Find Instance by attribute or tag (case-sensitive)				All states					
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP	
<input type="checkbox"/>	Assignment1a	i-0c1bb00b56e0a9959	Terminated	t2.micro	-	View alarms +	us-east-1a		
<input checked="" type="checkbox"/>	Assign1a	i-0c6ecc7988428d131	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-18-215-177-198.compute-1.amazonaws.com	

Figure 11: EC2 instance successfully launched

- According to the requirement, after waiting the instance launch successfully, visit the [link http://ec2-18-215-177-198.compute-1.amazonaws.com/phpinfo.php](http://ec2-18-215-177-198.compute-1.amazonaws.com/phpinfo.php) and picture below is the result.



B. TASK 2 – Create a PHP website (Photo Album)

- First and foremost, I configure these following settings to access the WinSCP:

+ Host Name: **ec2-18-215-177-198.compute-1.amazonaws.com**

+ User Name: **ec2-user**

+ **Advanced => SSH => Authentication:**

Then, upload the file “Assignment1a.ppk” to the Private Key Field:

- As a result, the WinSCP has been activated

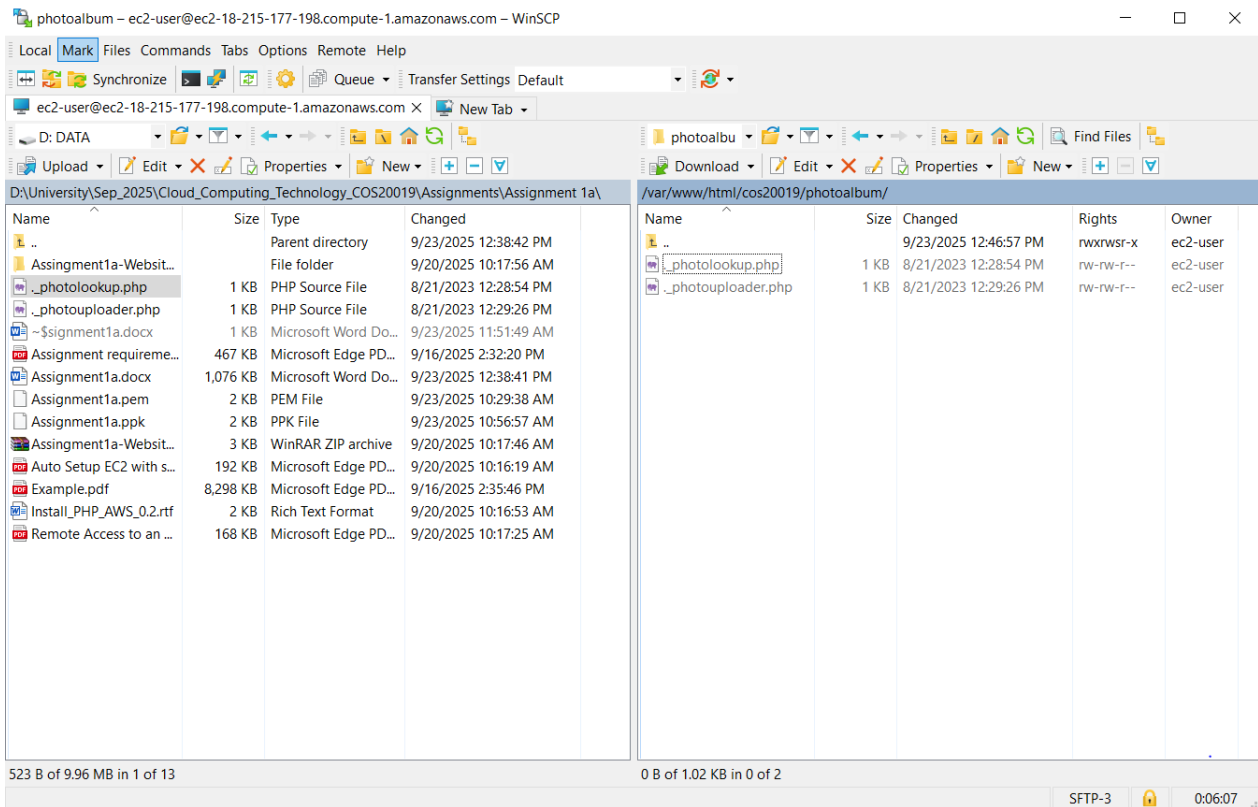


Figure 12: WinSCP

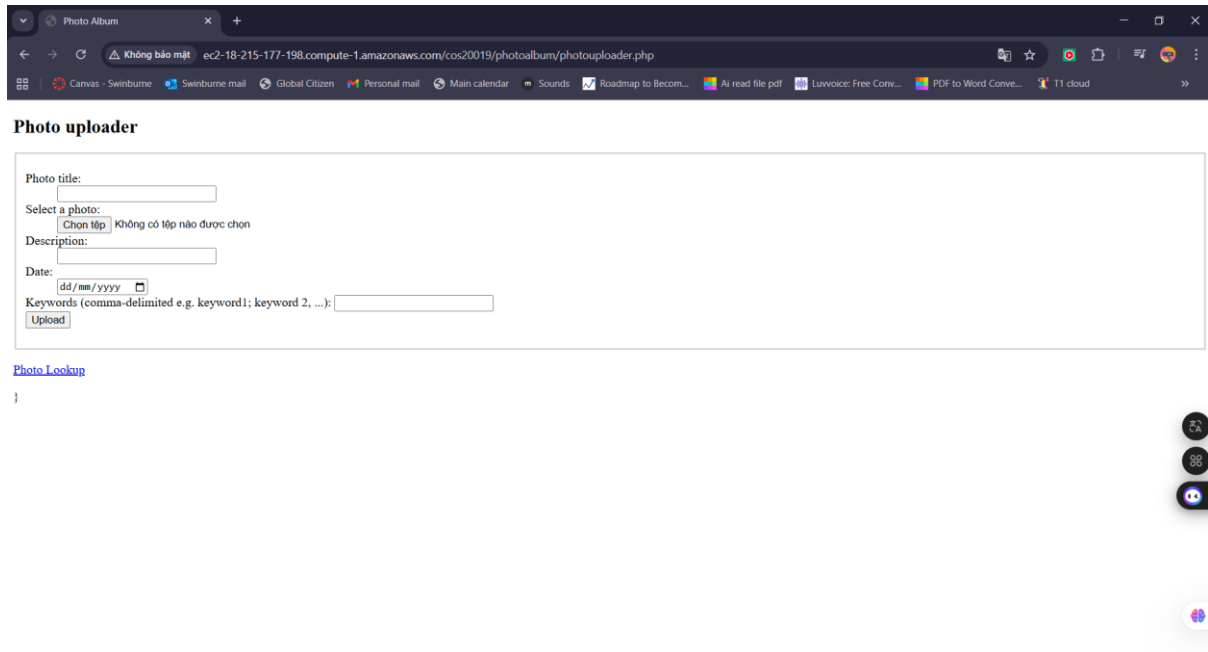


Figure 13: “photouploader.php” file

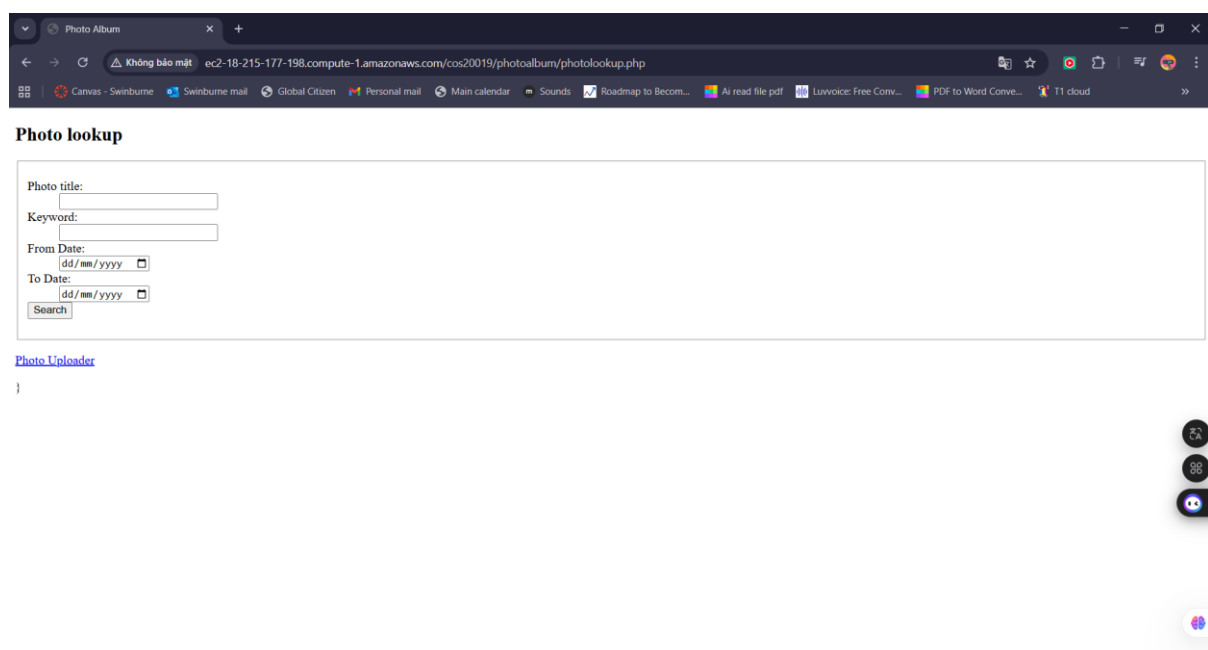


Figure 14: “photouplookup.php” file

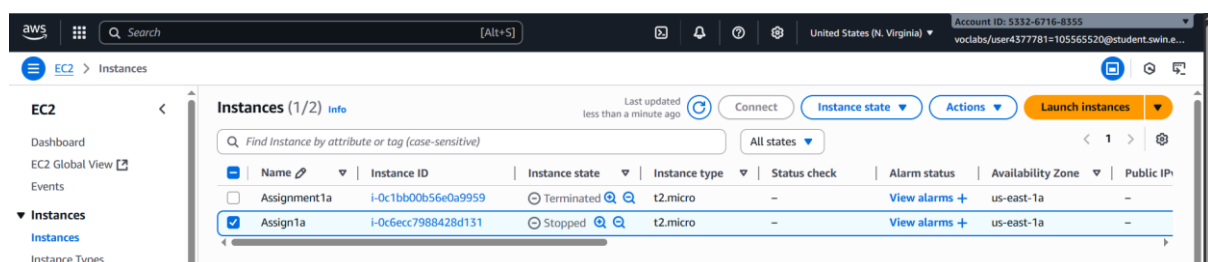


Figure 15: Stop the Assign1a instance