


## Introduction

- This guide is applicable to all students on the Network and Information Security Module (NISM). It describes how to set up a target website that can be used as the target of security scans and to allow students to potentially compromise and exploit it. With this in mind, it is important that students do NOT include any personally identifiable information or commonly used passwords on the site.
- On the module students will be assigned to a team/group to carry out the assignment – each team will also create a target site following the instructions in this guide. This target site will be used by one of the other teams to carry out their exercises. It is recommended that the assignment of sites be reciprocal, that is that a pair of teams test each other's target site. **A word of warning: these instructions utilise the 'free tier' provision of AWS. Hence, it is NOT recommended to leave the web sites running all day every day as this will result in all your free credits being consumed prematurely.** It is recommended that teams agree 'test periods' when web sites will be up and running and available for testing.
- This guide will cover:
  - how to set up a free AWS account,
  - how to set up security groups and keys,
  - how to obtain and upload the demo application,
  - how to modify security groups for optimum testing,
  - how to check and assign Elastic IP addresses,
  - how to check access, and
  - how to review, monitor and backup the application using the EB console.


## Sign up for AWS Educate

This first section will describe how to sign up for a free AWS Educate account using your **Essex University email account**.

[Content](#) [Classrooms & Credits](#) [Professional Resources](#) [AWS Account](#) [Profile](#)



### How to access AWS Services



Choose an option to get started!

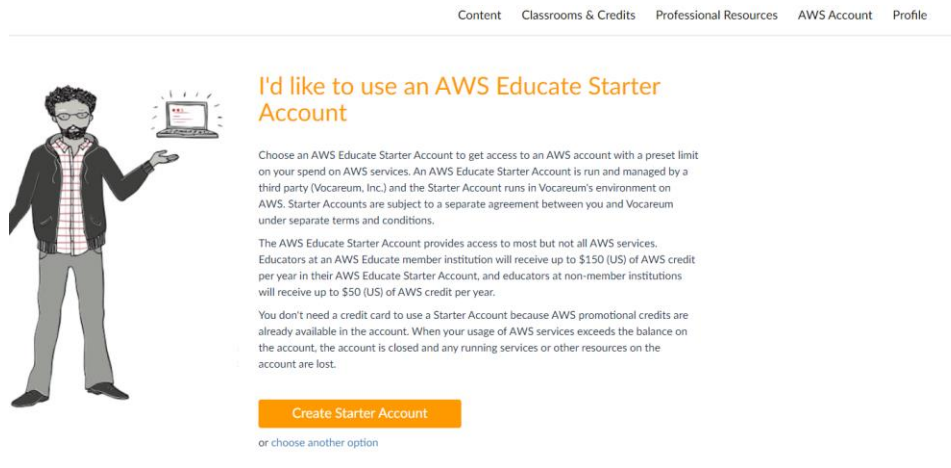
☐ I would like to use a personal AWS Account

☐ I would like to use an AWS Educate Starter Account

[Get Started](#)

1. Go to the AWS Educate account at <https://aws.amazon.com/education/awseducate/>

2. Choose the I would like to use an AWS Educate button
3. Click the Get Started button shown above.
4. On the first screen displayed, click on the Create Starter Account button - as shown below.



5. The screen below is then displayed:

The screenshot shows the AWS Educate registration page, Step 2/3: Tell us about yourself. The page has a blue header with the text 'Apply to join AWS Educate' and 'Step 2/3: Tell us about yourself'. Below the header, there is a form with several fields: School or Institution Name, Country, First Name, Last Name, Email, Graduation Month, Graduation Year, Birth Month, Birth Year, and Promo Code (optional). There is also a reCAPTCHA 'I'm not a robot' checkbox and a 'Frequently Asked Questions' link. At the bottom, there is a note about the terms and conditions.

6. Complete **all** the boxes with your details using your Essex University details - **specify the 'University of Essex' as the institution and use your Essex email address**. Click on the "I'm not a robot" captcha and then click on the Next button
7. On the next page, read and agree to the end user agreement and then click submit.

Please read the terms and conditions shown below and click on the "I agree" button at the bottom of this page to continue.

#### Terms and Conditions

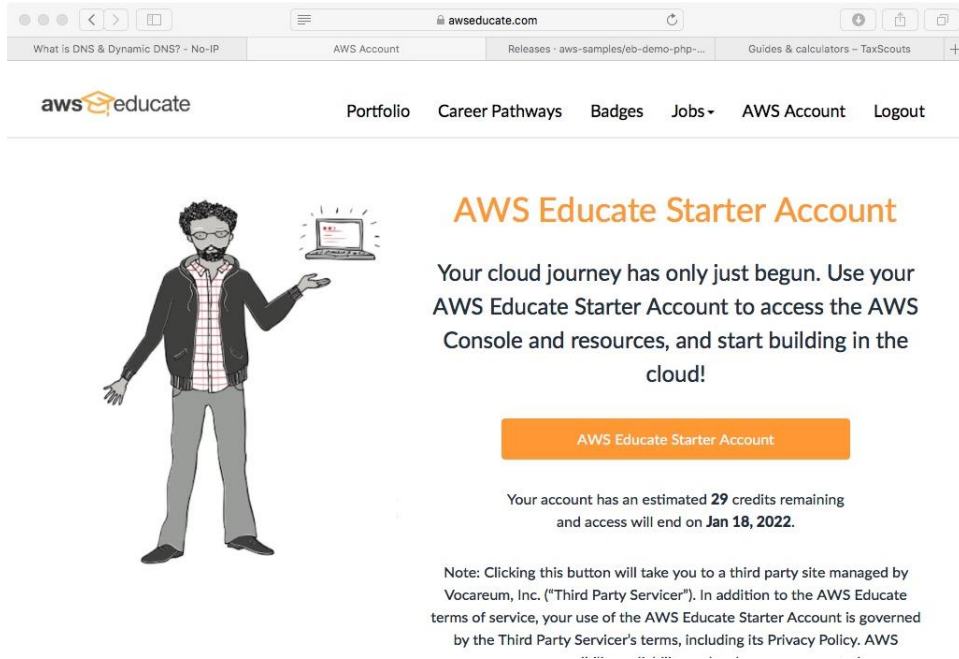
Welcome to the Vocareum, Inc. ("Vocareum") website located at [www.vocareum.com](http://www.vocareum.com) (the "Site"). Please read these Terms of Service (the "Terms") and our Privacy Policy ( <http://www.vocareum.com/privacy-policy/> ) carefully because they govern your use of our Site and our web-based education and learning platform. To make these Terms easier to read, the Site and our platform are collectively called the "Services."

8. The web site will then send you an email. Click on the link to confirm your email address and activate your AWS Educate account.

### Log in via the AWS Educate page

1. You will receive an email confirming your AWS Educate application has been approved. You will then have to set up a password for your account.
2. The email link will take you directly to the AWS Educate login page, but generally you can access your account from the main url: <https://aws.amazon.com/education/awseducate/>
3. This time click on the sign into AWS Educate link (below the main button)
4. The screen below is displayed:

5. Enter your university email and your password.
6. The next screen displayed provides access to a number of AWS courses, allows you to upload your CV/create a portfolio and look for jobs related to AWS
7. On the menu bar at the top of the screen, click on the AWS account option, the screen below is displayed or you will be asked to choose an account – please choose the AWS Educate Starter Account:



awseducate.com

What is DNS & Dynamic DNS? ~ No-IP | AWS Account | Releases ~ aws-samples/eb-demo-php... | Guides & calculators ~ TaxScouts

awseducate Portfolio Career Pathways Badges Jobs AWS Account Logout

## AWS Educate Starter Account

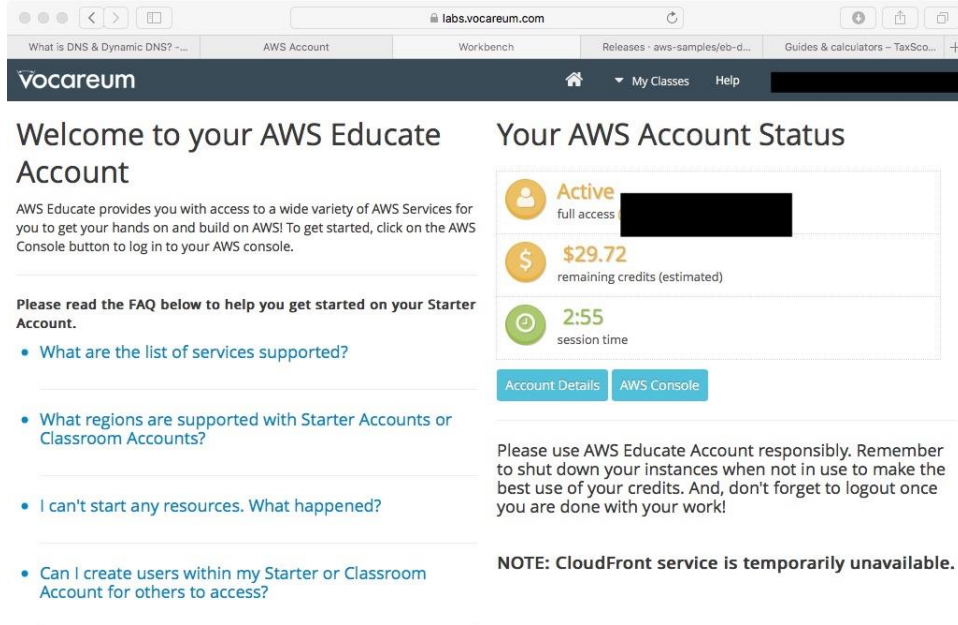
Your cloud journey has only just begun. Use your AWS Educate Starter Account to access the AWS Console and resources, and start building in the cloud!

**AWS Educate Starter Account**

Your account has an estimated **29** credits remaining and access will end on **Jan 18, 2022**.

Note: Clicking this button will take you to a third party site managed by Vocareum, Inc. ("Third Party Servicer"). In addition to the AWS Educate terms of service, your use of the AWS Educate Starter Account is governed by the Third Party Servicer's terms, including its Privacy Policy. AWS

8. Click on the button named AWS Educate starter account, the screen below is displayed:



labs.vocareum.com

What is DNS & Dynamic DNS? ~... | AWS Account | Workbench | Releases ~ aws-samples/eb-d... | Guides & calculators ~ TaxSco... +

vocareum My Classes Help

## Welcome to your AWS Educate Account

AWS Educate provides you with access to a wide variety of AWS Services for you to get your hands on and build on AWS! To get started, click on the AWS Console button to log in to your AWS console.

Please read the FAQ below to help you get started on your Starter Account.

- What are the list of services supported?
- What regions are supported with Starter Accounts or Classroom Accounts?
- I can't start any resources. What happened?
- Can I create users within my Starter or Classroom Account for others to access?

## Your AWS Account Status

**Active**  
full access

**\$29.72**  
remaining credits (estimated)

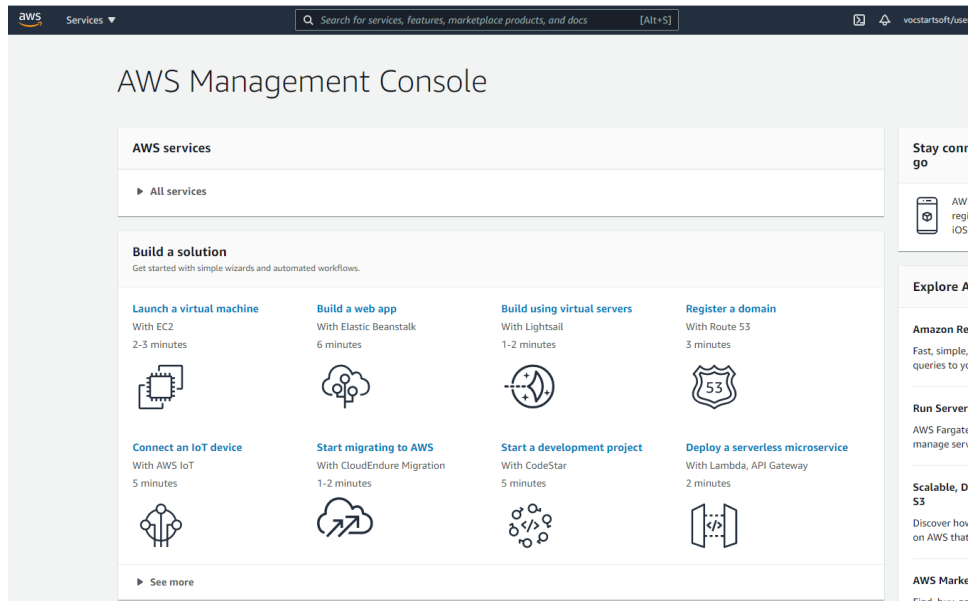
**2:55**  
session time

Account Details AWS Console

Please use AWS Educate Account responsibly. Remember to shut down your instances when not in use to make the best use of your credits. And, don't forget to logout once you are done with your work!

**NOTE: CloudFront service is temporarily unavailable.**

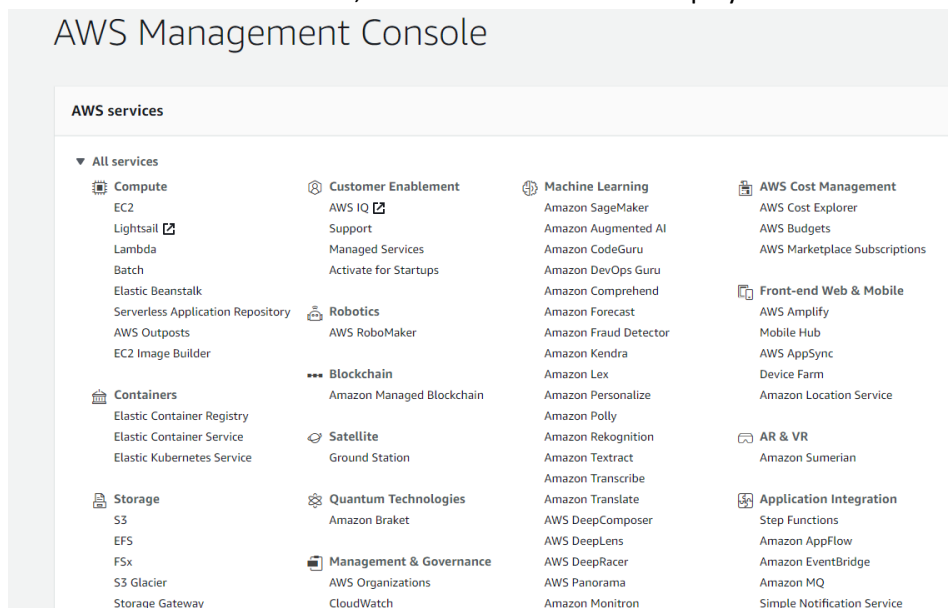
9. Click on the **AWS console** button to access the main account screen, shown below:



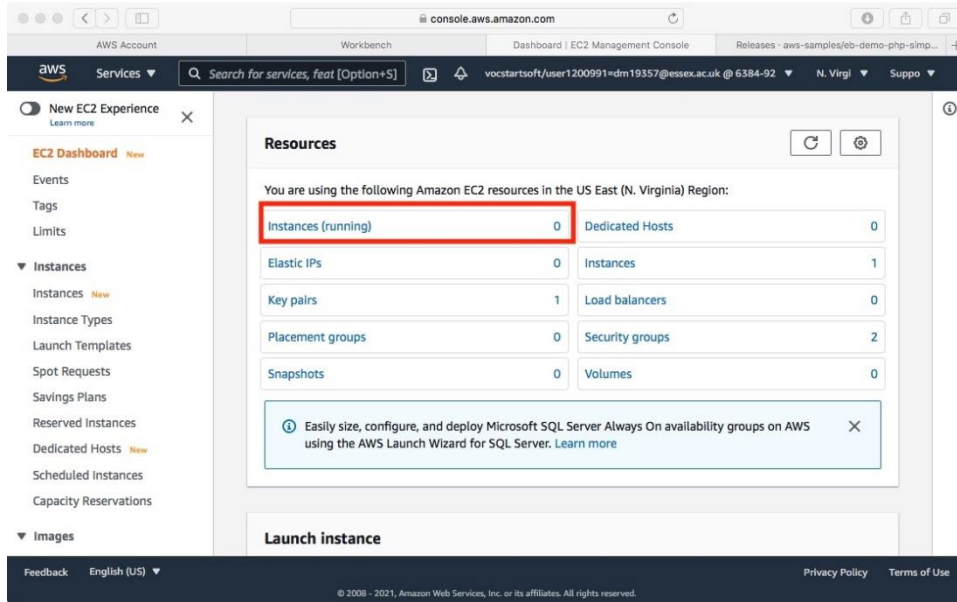
10. From this screen, there are a couple of housekeeping tasks that need to be done, which will be covered in the next section.

## Initial Set Up

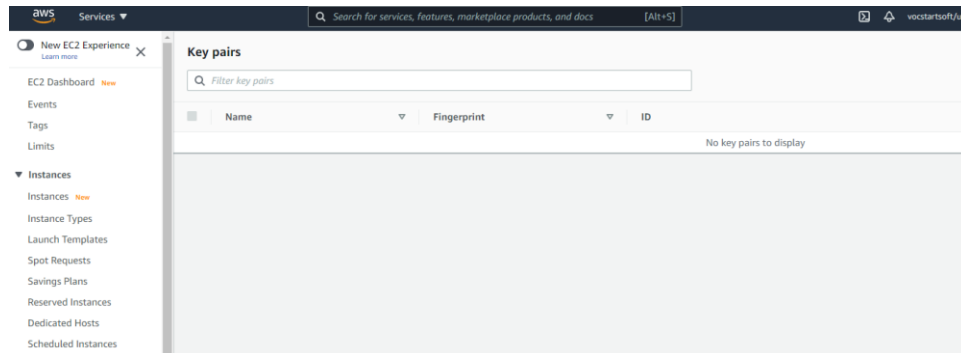
1. The first task is to set up keys for remote, secure access. Select the **EC2** option from the dropdown menu on AWS Services, and the screen below is displayed:



2. Initially the numbers should be "0" next to all the options. This is a crucial screen that you should refer to regularly as it tells you how many resources you have and, **most importantly**, how many are actually running (the **Instances running** button).



3. To set up your secure access keys, click on the **Key pairs** button and the screen below is displayed:



4. Click on the **Create key pair** button in the top right corner, the screen below is displayed:

**Create 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**

NISMtest

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

**File format**

☒ pem  
For use with OpenSSH

☐ ppk  
For use with PuTTY

**Tags (Optional)**

No tags associated with the resource.

[Add tag](#)

You can add 50 more tags.

5. Name your key pair `NISMtest` and select the file format. If you are going to use a Unix/ MacOS machine to access the cloud, choose `PEM`. If you are going to use a Windows machine, then chose `PPK`. It will also give you the option to download your keys. If it does this, make sure to save them somewhere safe.

## Create a security group

1. Return to the EC2 dashboard (there is a link in the left-hand column). The dashboard screen (shown below) should be displayed:

**EC2 Dashboard**

Events  
Tags  
Limits

▼ **Instances**

Instances  
Instance Types  
Launch Templates  
Spot Requests  
Savings Plans  
Reserved Instances  
Dedicated Hosts  
Scheduled Instances  
Capacity Reservations

▼ **Images**

**Welcome to the new EC2 console**

We're redesigning the EC2 console to make it easier to use and improve performance. We'll release new screens periodically. We encourage you to try them and let us know where we can improve. To see the new console and the new EC2 Experience toggle.

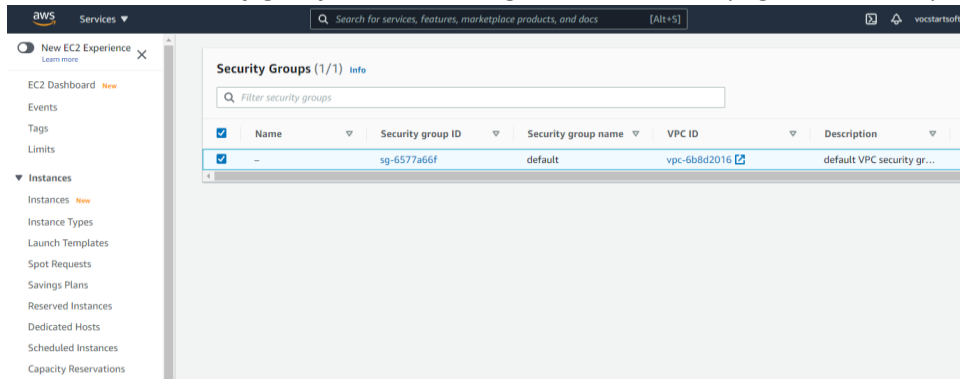
**Resources**

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

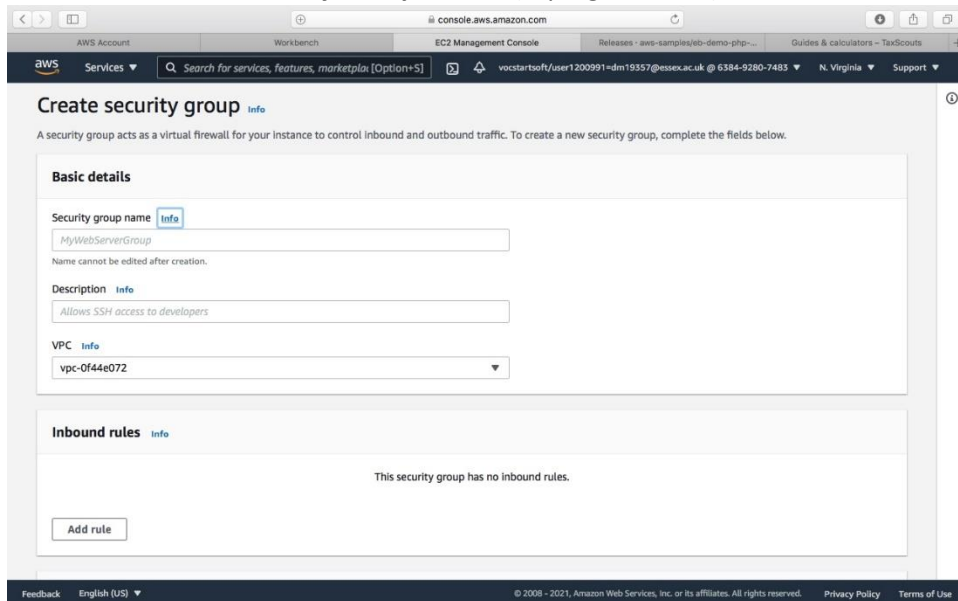
Instances (running)	0	Dedicated Hosts	0	Elastic IPs	0
Instances	0	Key pairs	1	Load balancers	0
Placement groups	0	Security groups	1	Snapshots	0
Volumes	0				

[Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more](#)

- Click on the **Security groups** link on the right-hand side, the page below is displayed:



- Click on the **Create Security Group** button (top right corner) - the screen below will be displayed:



- In the security group name box enter 'Main' and the description should be 'Allows HTTP, HTTPS and SSH access'. No other changes are needed in this section.
- Then click on the **Add rule** button (you may need to scroll down to access it).



6. The screen below will be displayed:

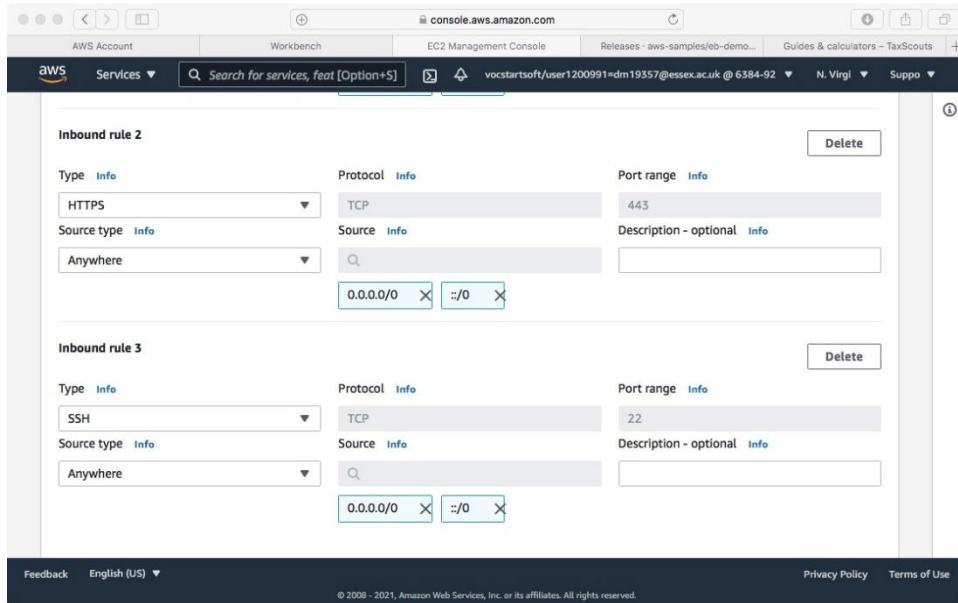
The screenshot shows the AWS Management Console interface for configuring a security group rule. The top navigation bar includes the AWS logo, account information, and a search bar. The main content area is titled 'Inbound rules' and shows a configuration for 'Inbound rule 1'. The 'Type' dropdown is set to 'HTTP', which automatically sets the 'Protocol' to 'TCP' and the 'Port range' to '80'. The 'Source type' is set to 'Anywhere', and the 'Source' field displays '0.0.0.0/0' and '::/0'. An 'Add rule' button is located at the bottom of the configuration section.

7. In the type dropdown choose 'HTTP', it will fill in 'TCP' and '80' automatically.
8. Choose source type from the pulldown menu, and select 'Anywhere' (as shown) - it will automatically insert the source address/ mask.
9. Click Add Rule and the screen below is shown:

This screenshot is identical to the one above, showing the 'Inbound rules' configuration for 'Inbound rule 1'. The settings are: Type: HTTP, Protocol: TCP, Port range: 80, Source type: Anywhere, and Source: 0.0.0.0/0, ::/0. The 'Add rule' button is visible at the bottom.

10. Repeat for rule 2, but use HTTPS instead of HTTP.
11. For Rule 3, chose SSH.

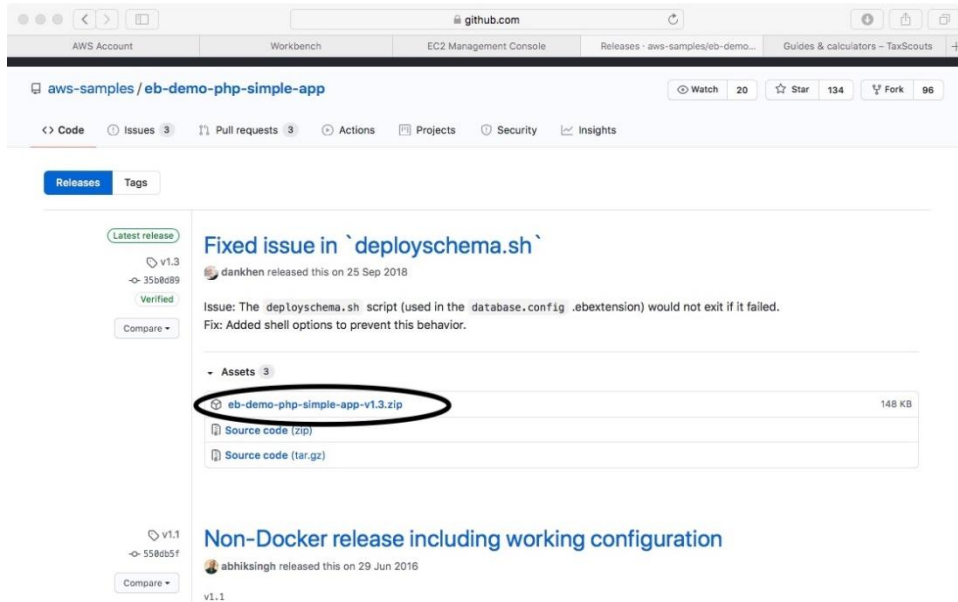
12. The two new rules should look as in the screenshot below:



13. Click **Create Security Group** (you may need to scroll down to find the button).

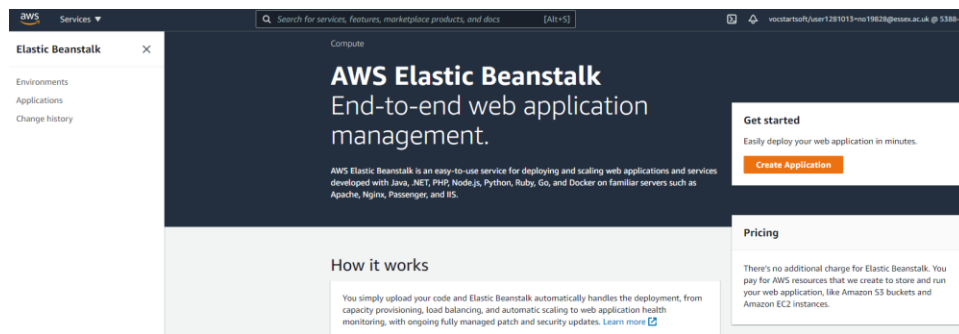
14. Now you are ready to start creating your application.

15. First, download the demo app from <https://github.com/aws-samples/eb-demo-php-simple-app/releases> (At the time of writing the latest version was v1.3 as shown below):

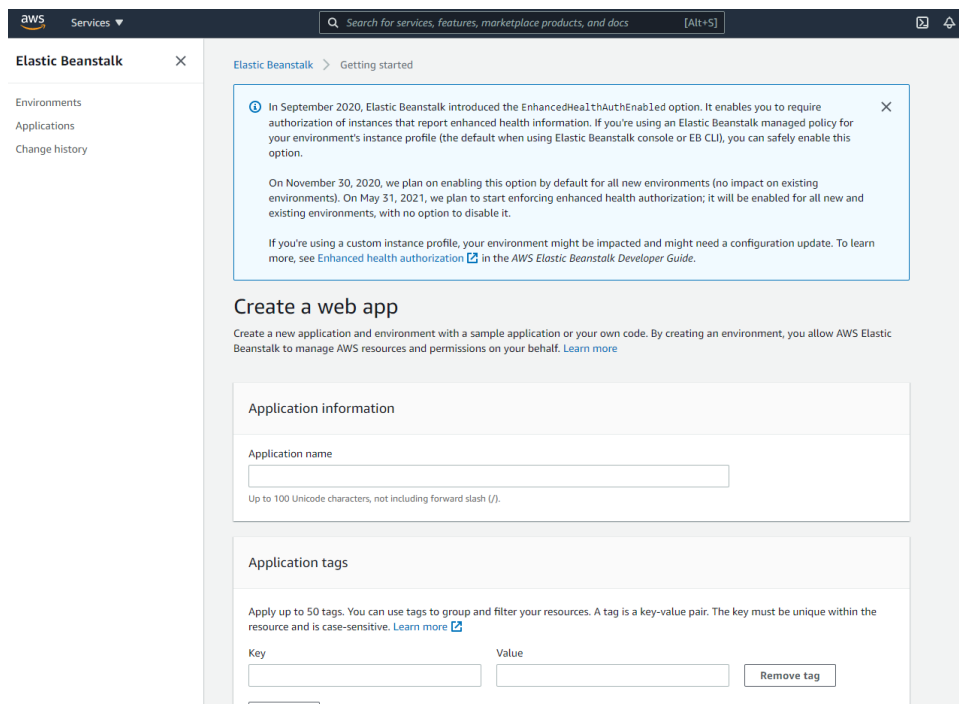


## Create the Application in Elastic Beanstalk

1. In the AWS console (from the dropdown menu on the **Services** button, top left-hand corner), choose the Elastic Beanstalk option.

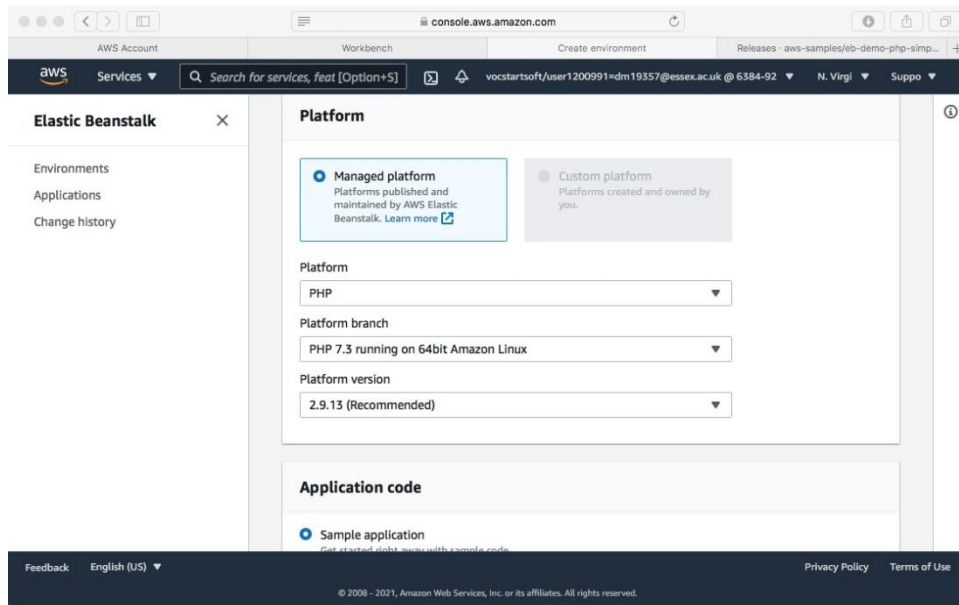


2. Click on the Create Application button shown above.



3. In the application name box type 'NISMPHP' and press enter.
4. Scroll down and check that the environment name box says 'Nismphp-env' (it should have entered that automatically).
5. Scroll down to the platform box, ensure that the 'Managed Platform' box is selected.
6. From the platform dropdown choose PHP – leave the version as default. Ensure you are running PHP 7.3 on 64 bit Amazon Linux (NOT Linux 2).

7. Your screen should now be as shown below:



8. The next section is where you upload the demo code.

**Application code**

☐ Sample application  
Get started right away with sample code.

☒ Upload your code  
Upload a source bundle from your computer or copy one from Amazon S3.

**Source code origin**

Version label  
Unique name for this version of your application code.

Source code origin  
Maximum size 512 MB

☒ Local file

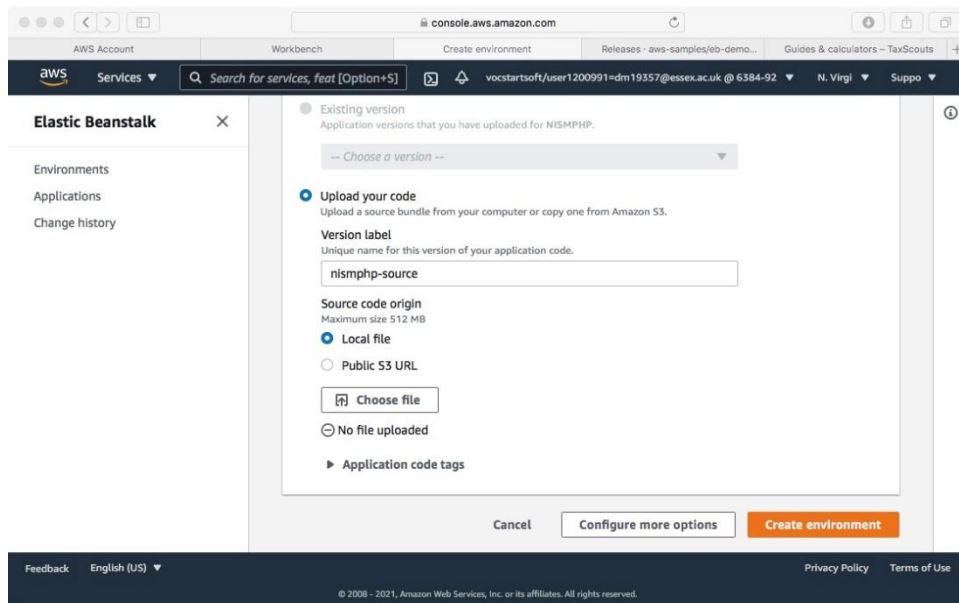
☐ Public S3 URL

☒ No file uploaded

► Application code tags

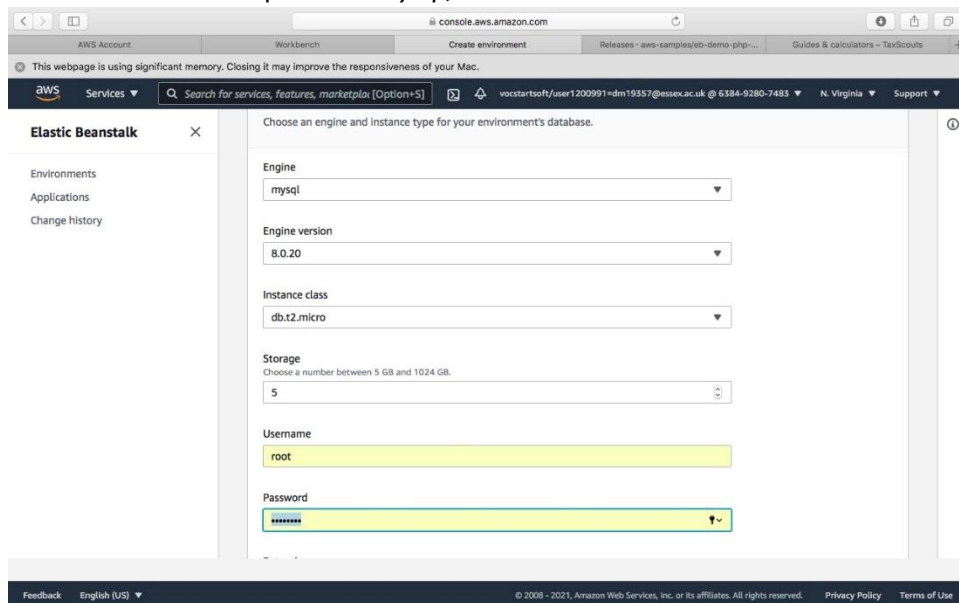
9. Click on upload your code, it should populate the version label automatically.

10. Under source code origin make sure that local file is selected then click choose file as shown in the screenshot below:



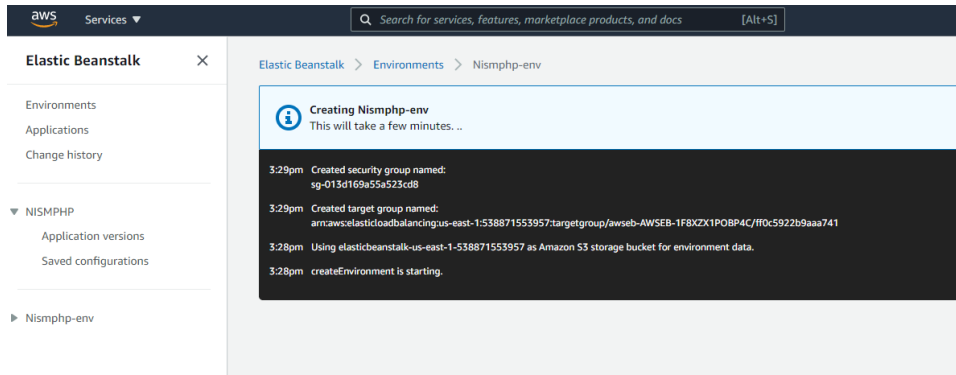
The screenshot shows the AWS Elastic Beanstalk console. On the left, the 'Elastic Beanstalk' sidebar is visible with options for 'Environments', 'Applications', and 'Change history'. The main panel is titled 'Existing version' and shows 'Application versions that you have uploaded for NISMPHP'. Under the 'Upload your code' section, the 'Source code origin' is set to 'Local file'. A 'Choose file' button is present. At the bottom, there are 'Cancel', 'Configure more options', and 'Create environment' buttons.

11. From the file dialogue, select the demo app you downloaded previously and click choose.  
12. Click on **Configure more option (before Creating the app)**, on the screen displayed select **Database** and click **Edit** (you may need to scroll down to find the database option).  
13. Confirm the default options of **mysql**, the version and instance as shown below:

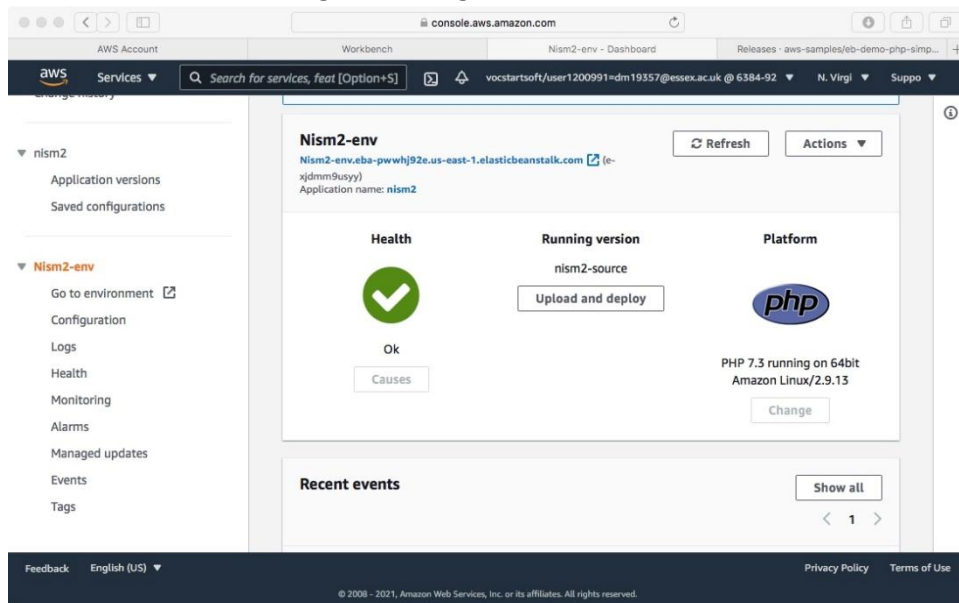


The screenshot shows the AWS Elastic Beanstalk console. The main panel is titled 'Choose an engine and instance type for your environment's database'. It contains several dropdown menus: 'Engine' (mysql), 'Engine version' (8.0.20), and 'Instance class' (db.t2.micro). Below these, there is a 'Storage' section with a value of 5. The 'Username' field is highlighted in yellow and contains the text 'root'. The 'Password' field is also highlighted in yellow and contains a masked password. At the bottom, there are 'Feedback', 'English (US)', and copyright information.

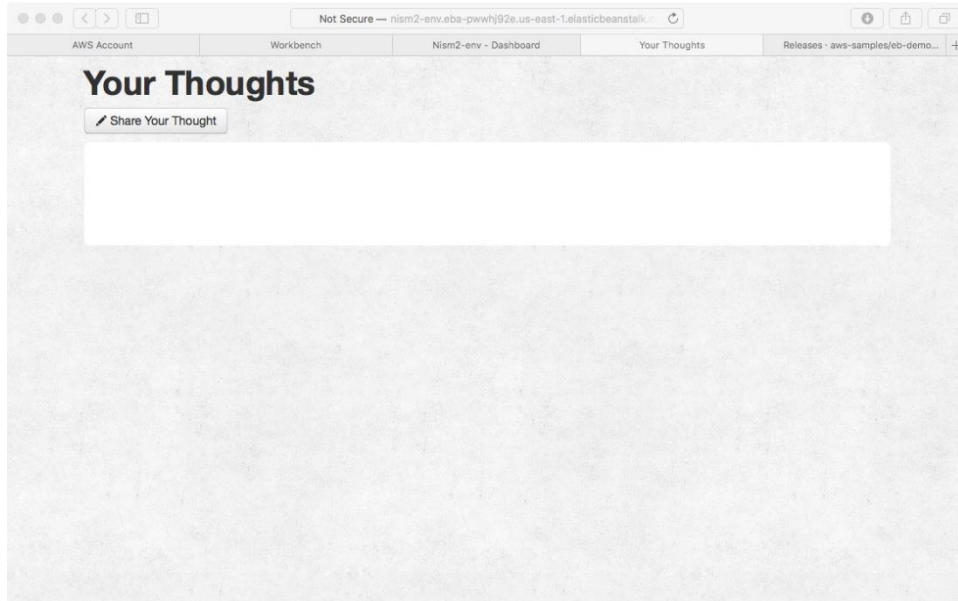
14. In the highlighted boxes enter root and enter a password, minimum length is 8 characters.  
15. Scroll down and click save.  
16. On the previous screen click **Create Environment**.



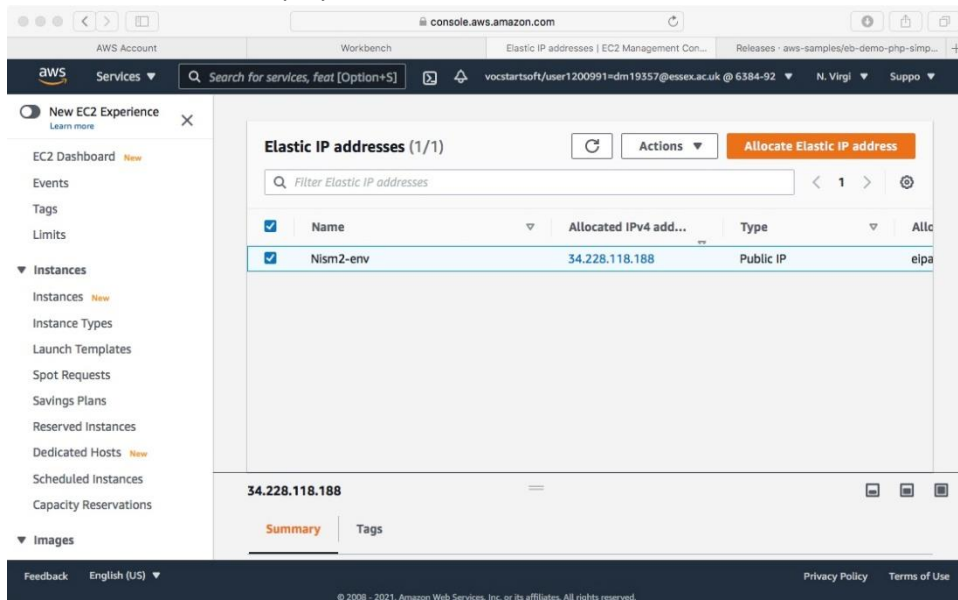
17. AWS will now create and upload the application for you – this will take several minutes. A typical update screen is shown above. You can monitor progress from the EB Console page – a screenshot of the running version is given below:



18. In the screenshot above the environment is called Nism2-env, and below the name is a link that launches the website. Click on the link and the web app is displayed – as shown below:

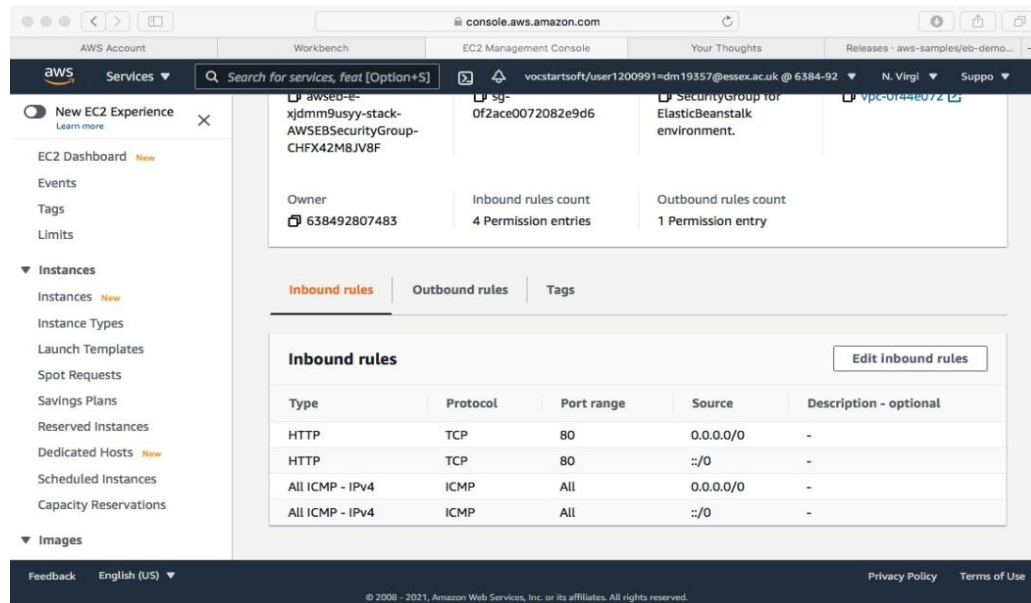


19. Assuming that this screen is displayed you can add a comment (thought) and a name – both will be written to the database running in the background.
20. The IP address (known as Elastic IP or EIP in AWS terminology) can be found from the EIP page (go back to the EC Console page and click on the **Elastic IP** link).
21. The screen below is displayed:

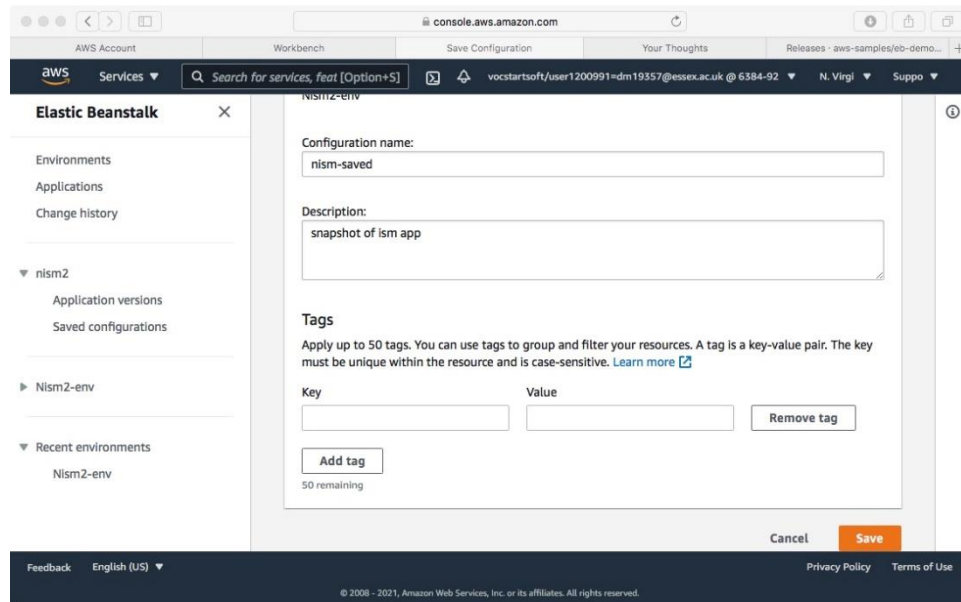


22. The IP is shown next to the environment name. In this example, it is **34.228.118.188**
23. Note the IP address may change every time the environment is restarted. So, be sure to check the page above and let the other group members know the new address.
24. You should also change the security group to allow ICMP access to the website. Use the instructions provided previously to add a new rule to the 'Main' group you created earlier; it

should look like the screenshot below:

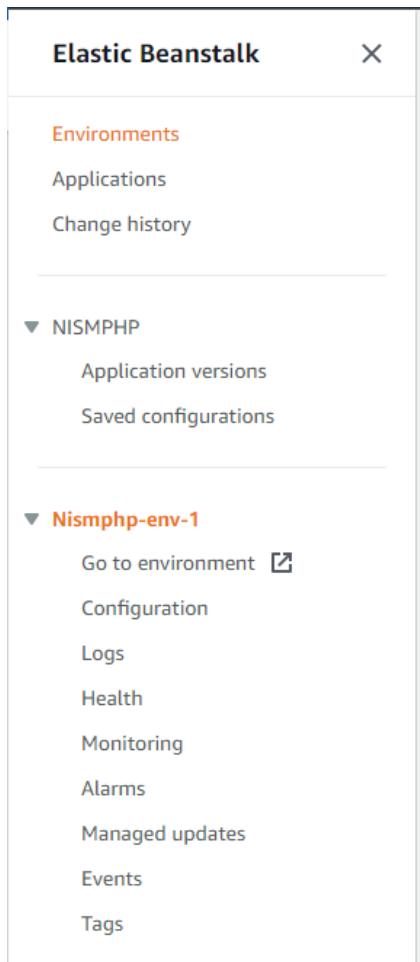


25. You should also save the current configuration to make restoring the application easier when required.
26. Access the Elastic Beanstalk (EB) console again and click on the Environment you have created. Then click Actions and **save configuration**. The screen below will then be displayed:

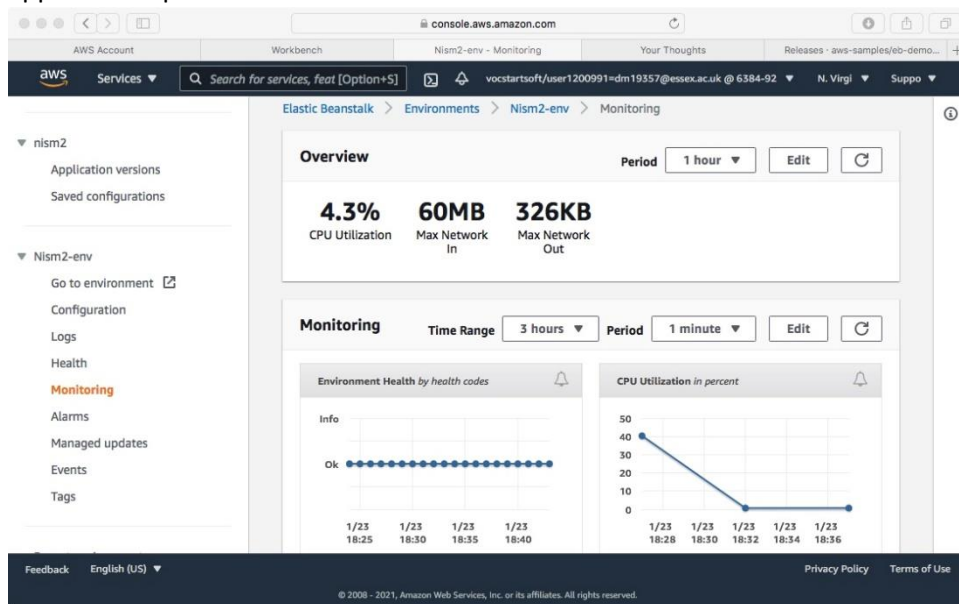


27. In the configuration name box enter nism-saved. Add a description such as 'snapshot of the app'. Then click save.
28. This will make it easier to restore the application later, when required.
29. The EB-console also lets you check the configuration. Go back to the Environments list and click on your environment for this set of options to come up:



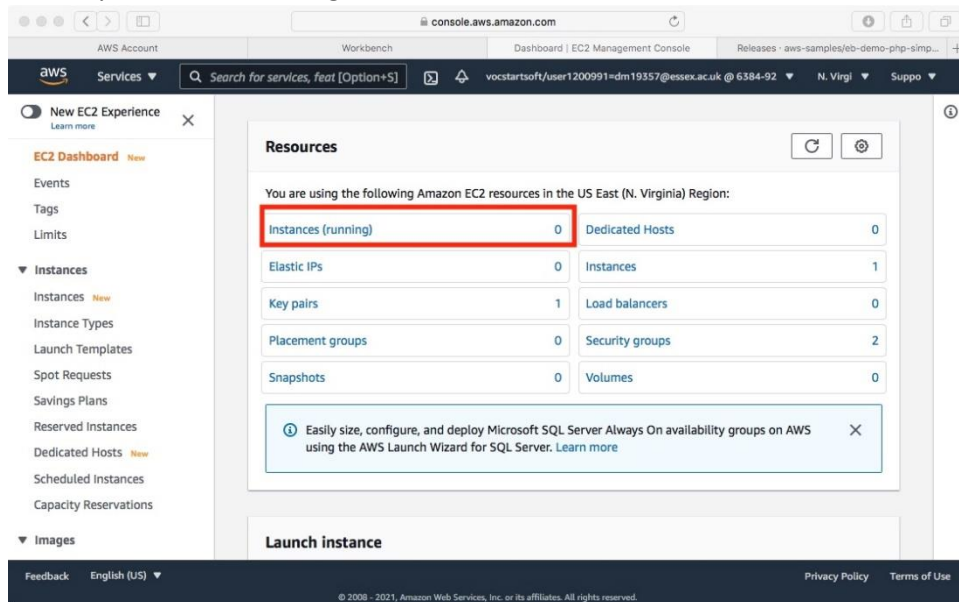


30. The screenshot below shows the monitor screen which displays useful data about the application operation:



## Housekeeping

1. The AWS free tier provides 750 hours per month of EC2 instances, among other resources. Therefore, if we leave the app running all the time, we will soon consume all our free credits. We recommend that the groups liaise and schedule sessions when the web app can be left running so that scans and exploits can be tested.
2. Applications can be quickly restored from the saved configuration you created previously.
3. From the EB-Console, click on environments, select your environment and click on the actions pull down.
4. From the actions menu, choose **load configuration**.
5. Click on the configuration you saved (it should be called nism-saved if you followed instructions).
6. Click on load and it will reload your saved configuration.
7. Remember to terminate your environment when the agreed test period has completed to save your credits.
8. From the environments screen, click on your running environment, click on the actions menu and choose 'terminate environment'.
9. After the EB-console informs you that the environment has terminated, check the EC console to ensure you have no running instances. It should look like the screenshot below:



10. Finally, during these instructions, I have made a few common (and hopefully fairly obvious) security *faux pas* that you should be able to pick up, and you should include them in your **individual** e-portfolio.