



Assignment 1

AWS Basics and EC2 Instance

Cloud Infrastructure Services (CIS443)

Prepared By

Yazeed AlKhalaf
202211123

Submitted To

Prof. Mohammad Mehedi Hassan

January 27, 2025

Contents

1 Part A: Creating an AWS account and Setup Zero Spend Budget plan	1
2 Part B: Secure Your AWS Account	2
3 Part C: Create IAM Account	3
4 Part D: Create EC2 Instance and Security Groups	4
4.1 Launch EC2 Instance	4
4.2 Create Security Groups	6
4.3 Configure Elastic IP	7
5 Part E: Install a LAMP web server on Amazon Linux 2023	9
6 Part F: Connect to EC2 Linux Instance using Termius on Mac or Windows	11

List of Figures

1	AWS Account Creation and Zero Spend Budget Configuration	1
2	AWS Account Security Configuration	2
3	IAM Account Creation and Setup	3
4	EC2 Instance Launch Configuration - Instance Type Selection	4
5	EC2 Instance Launch Configuration - Network Settings	4
6	EC2 Instance Launch Configuration - Successfully Launched	5
7	Security Group Configuration - Inbound Rules Addition	6
8	Security Group Configuration - Outbound Rules Verification	6
9	Elastic IP Configuration - Allocation	7
10	Elastic IP Configuration - Association	7
11	Elastic IP Configuration - Verification	8
12	LAMP Web Server - Successfully Installed	9
13	LAMP Web Server - Adding ec2-user to apache group with other security practices	9
14	LAMP Web Server - PHP Info Page	10
15	LAMP Web Server - MariaDB Secure Setup	10
16	Termius SSH Connection Configuration	11
17	Termius SSH Connected - Saying Hello to Professor	12

1 Part A: Creating an AWS account and Setup Zero Spend Budget plan

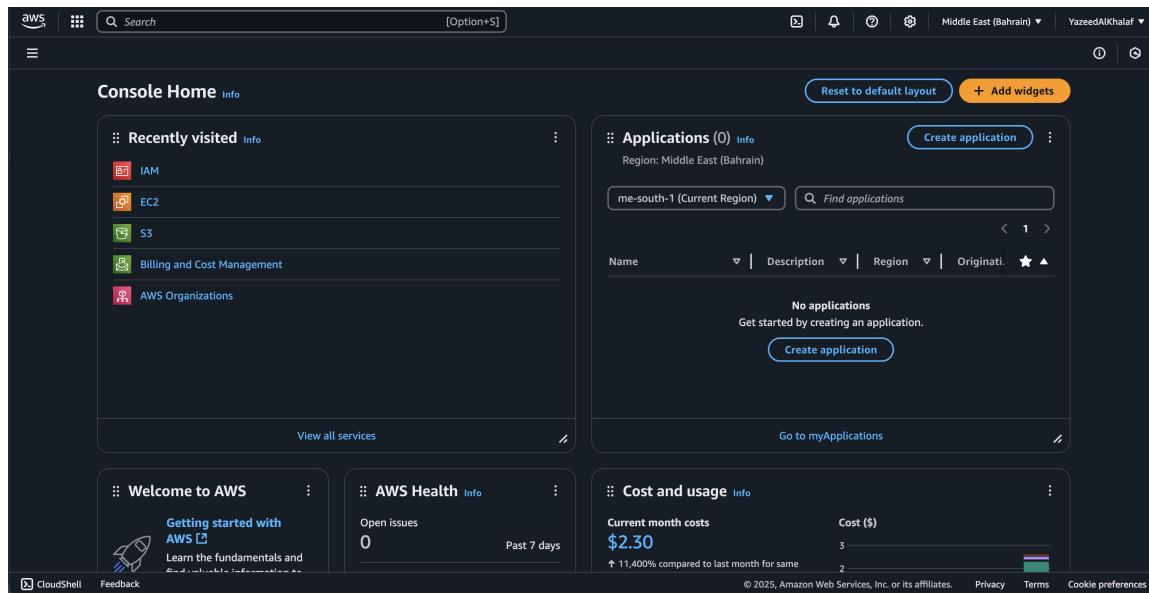


Figure 1: AWS Account Creation and Zero Spend Budget Configuration

2 Part B: Secure Your AWS Account

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar lists navigation options: Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management), Access reports (Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity, Service control policies), and CloudShell Feedback.

The main content area includes:

- Security recommendations**:
 - Root user has MFA (Having multi-factor authentication (MFA) for the root user improves security for this account.)
 - Root user has no active access keys (Using access keys attached to an IAM user instead of the root user improves security.)
- IAM resources**:

User groups	Users	Roles	Policies	Identity providers
0	3	12	0	0
- What's new**:
 - Introducing resource control policies (RCPs) to centrally restrict access to AWS resources. 2 months ago
 - AWS IAM now supports PrivateLink in the AWS GovCloud (US) Regions. 3 months ago
 - Streamline automation of policy management workflows with service reference information. 4 months ago
 - Amazon S3 Access Grants introduce the ListCallerAccessGrants API. 5 months ago
- AWS Account**:
 - Account ID: [REDACTED]
 - Account Alias: Create
 - Sign-in URL for IAM users in this account: https://[REDACTED].signin.aws.amazon.com/console
- Quick Links**: My security credentials (Manage your access keys, multi-factor authentication (MFA) and other credentials).
- Tools**: Policy simulator (The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.)

At the bottom, there are links for CloudShell, Feedback, © 2025, Amazon Web Services, Inc. or its affiliates, Privacy, Terms, and Cookie preferences.

Figure 2: AWS Account Security Configuration

3 Part C: Create IAM Account

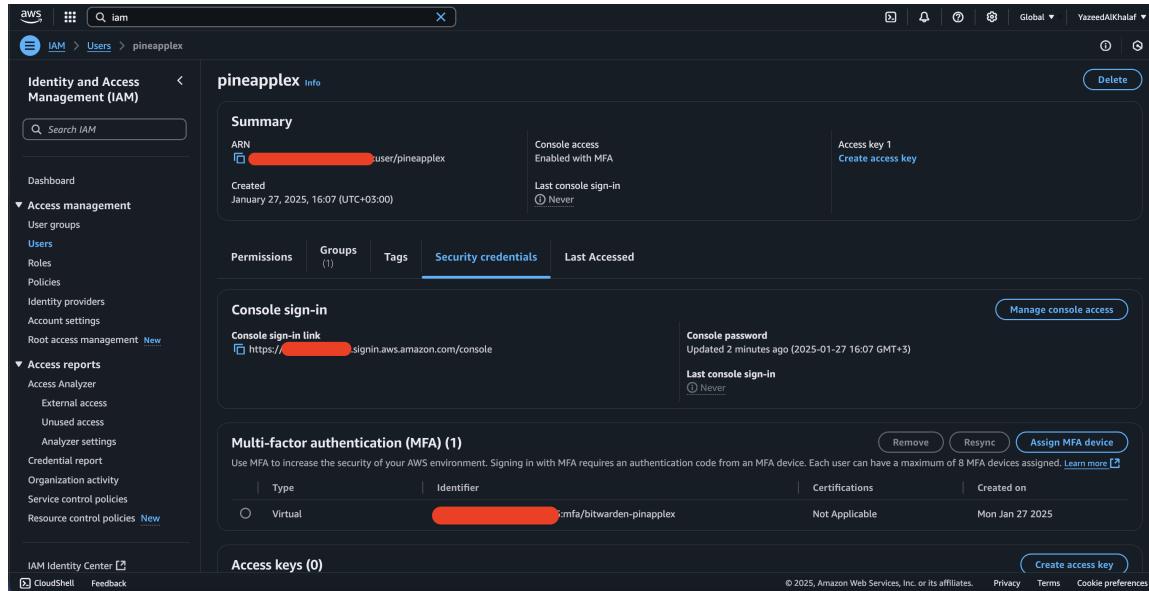


Figure 3: IAM Account Creation and Setup

4 Part D: Create EC2 Instance and Security Groups

4.1 Launch EC2 Instance

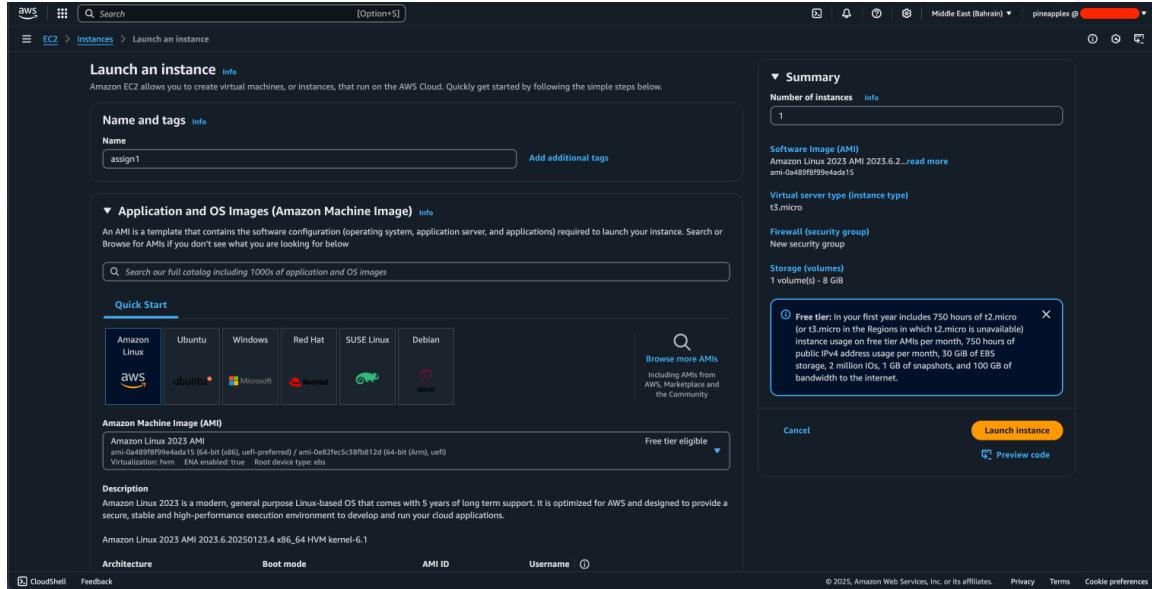


Figure 4: EC2 Instance Launch Configuration - Instance Type Selection

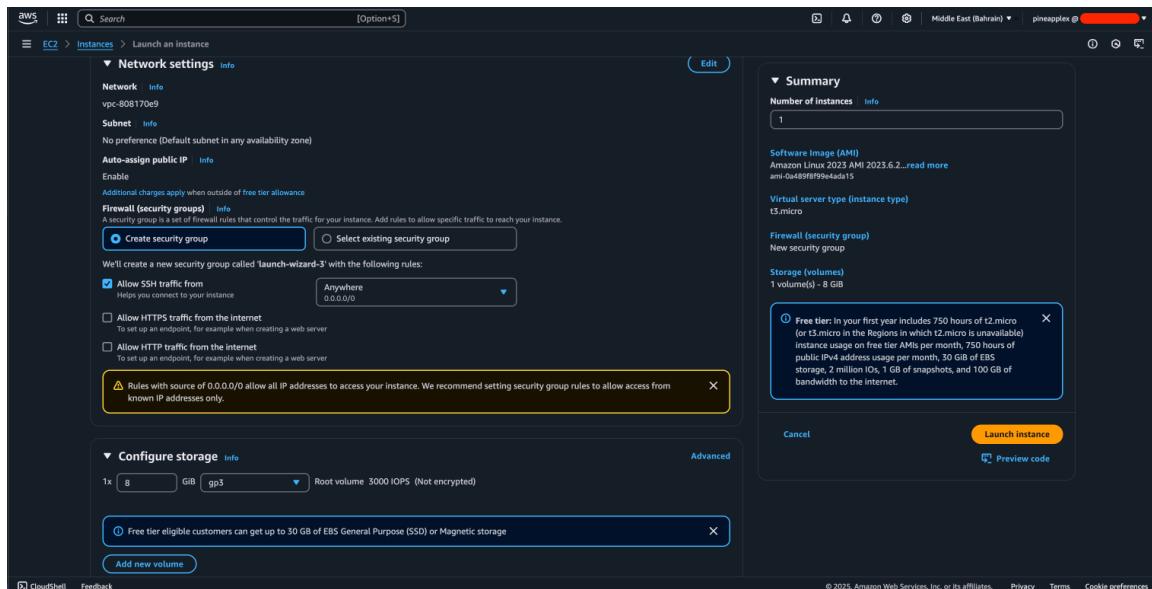


Figure 5: EC2 Instance Launch Configuration - Network Settings

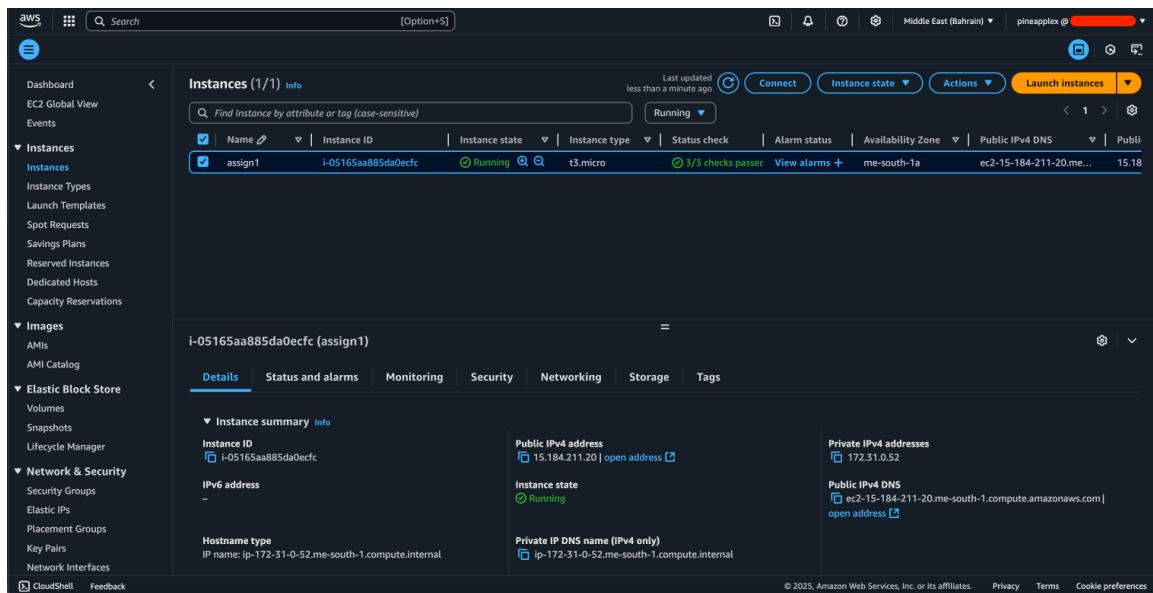


Figure 6: EC2 Instance Launch Configuration - Successfully Launched

4.2 Create Security Groups

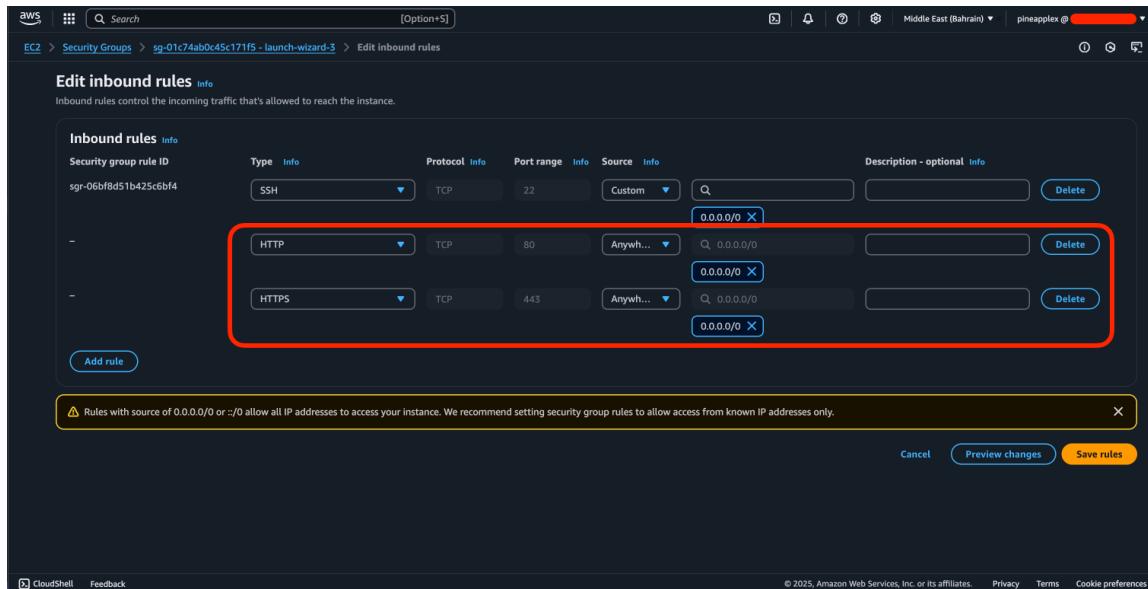


Figure 7: Security Group Configuration - Inbound Rules Addition

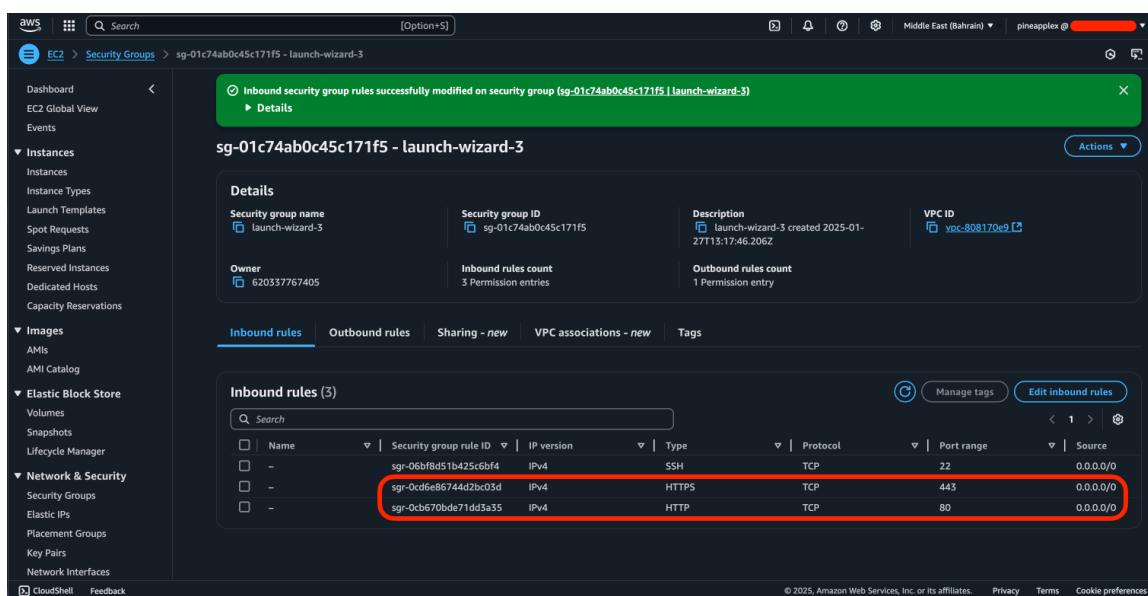


Figure 8: Security Group Configuration - Outbound Rules Verification

4.3 Configure Elastic IP

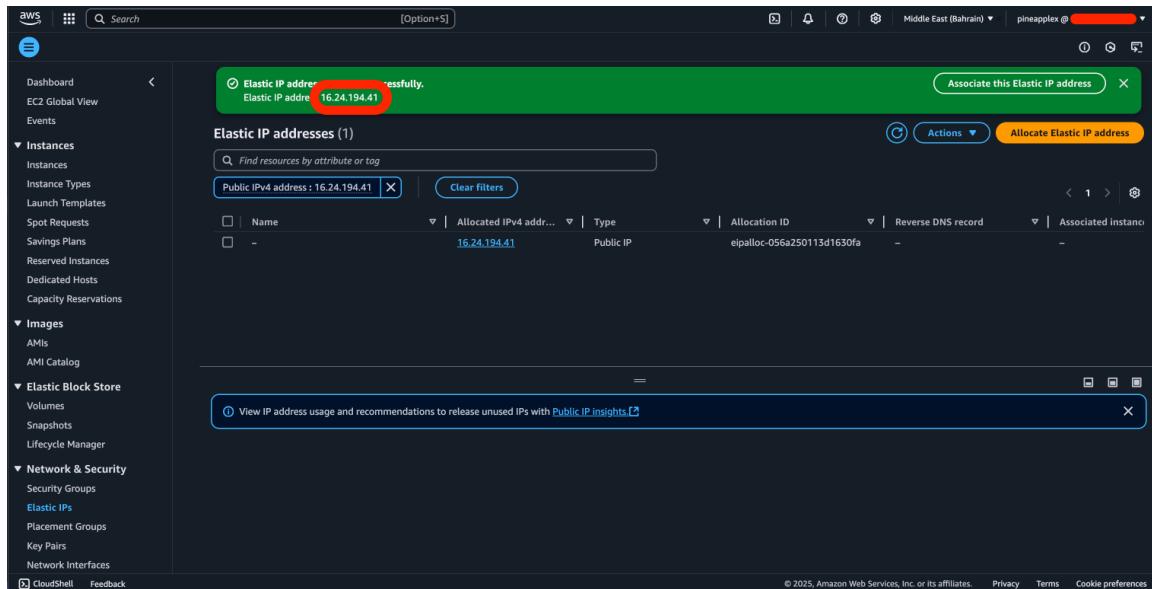


Figure 9: Elastic IP Configuration - Allocation

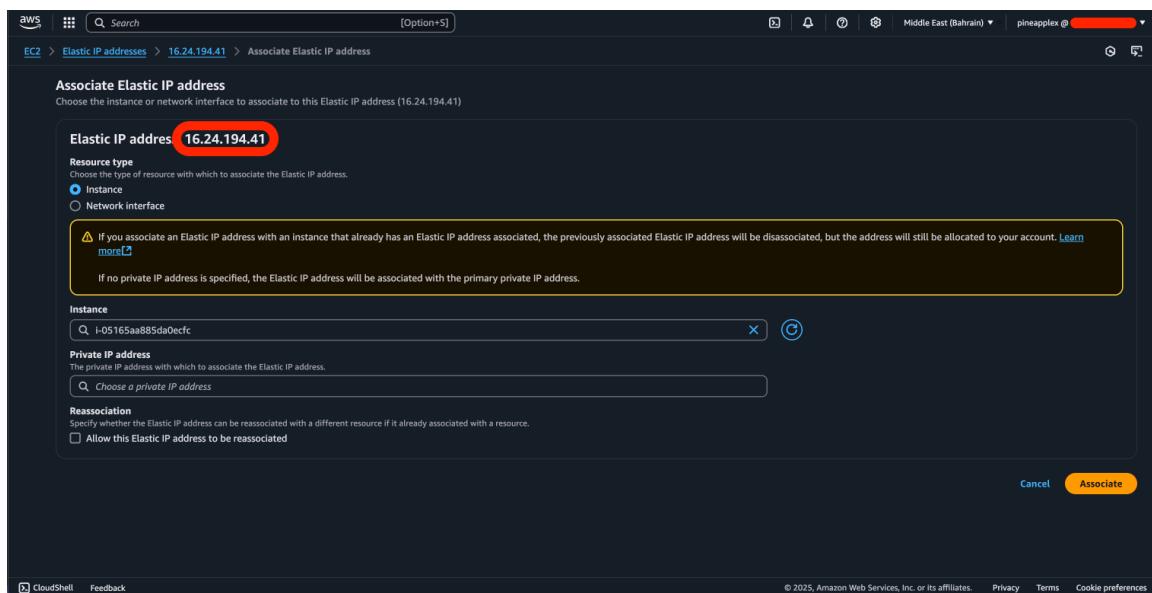


Figure 10: Elastic IP Configuration - Association

The screenshot shows the AWS EC2 Instances page. In the top navigation bar, the path is EC2 > Elastic IP addresses > 16.24.194.41. The main table lists one instance, 'assign1', which is running and has an 't3.micro' instance type. The 'Elastic IP' column shows '16.24.194.41'. Two red boxes highlight this value and the public IP '16.24.194.41' in the 'Public IPv4 DNS' column. Below the table, the 'Details' tab of the instance's configuration page is visible, showing various network details including the assigned elastic IP.

Figure 11: Elastic IP Configuration - Verification

5 Part E: Install a LAMP web server on Amazon Linux 2023

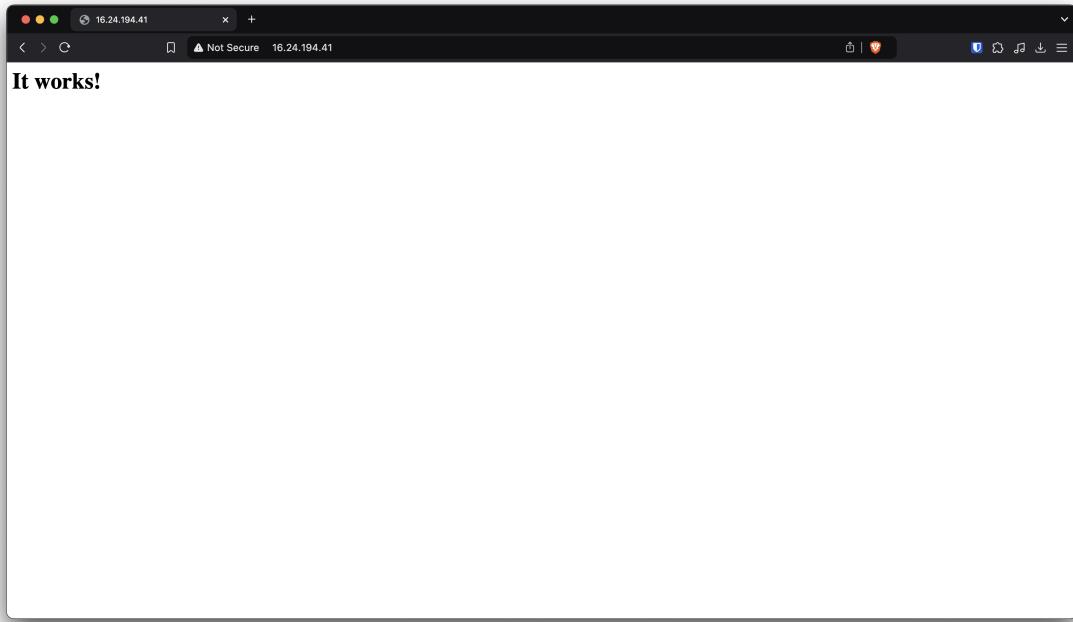


Figure 12: LAMP Web Server - Successfully Installed

A screenshot of a terminal window. The session starts with the command 'groups' which shows the user is part of the adm, wheel, apache, and systemd-journal groups. It then uses 'sudo chown' to change ownership of the /var/www directory to the apache user. Following this, it uses 'sudo chmod' to set the directory permission to 2775. The command 'find /var/www -type d -exec sudo chmod 2775 {} +' is run. Finally, it runs 'find /var/www -type f -exec sudo chmod 0664 {} +' to change the permissions of all files in the directory to 0664. The terminal window also shows tabs for 'Vaults' and 'SFTP'.

Figure 13: LAMP Web Server - Adding ec2-user to apache group with other security practices

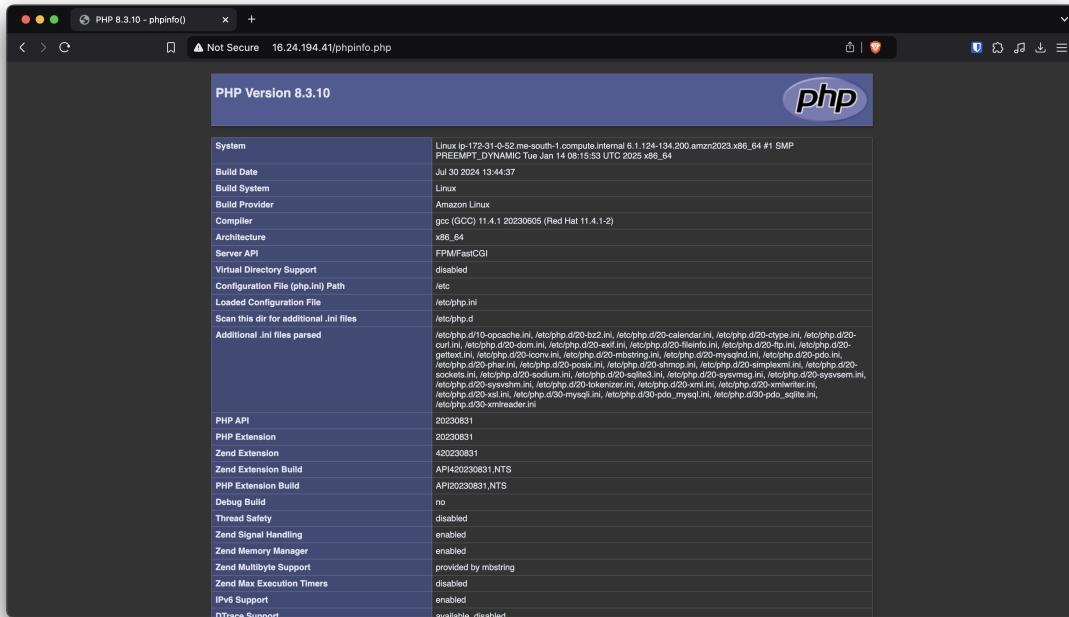


Figure 14: LAMP Web Server - PHP Info Page

```

... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] Y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] Y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
[ec2-user@ip-172-31-0-52 ~]$ sudo systemctl stop mariadb
[ec2-user@ip-172-31-0-52 ~]$ 

```

Figure 15: LAMP Web Server - MariaDB Secure Setup

6 Part F: Connect to EC2 Linux Instance using Termius on Mac or Windows

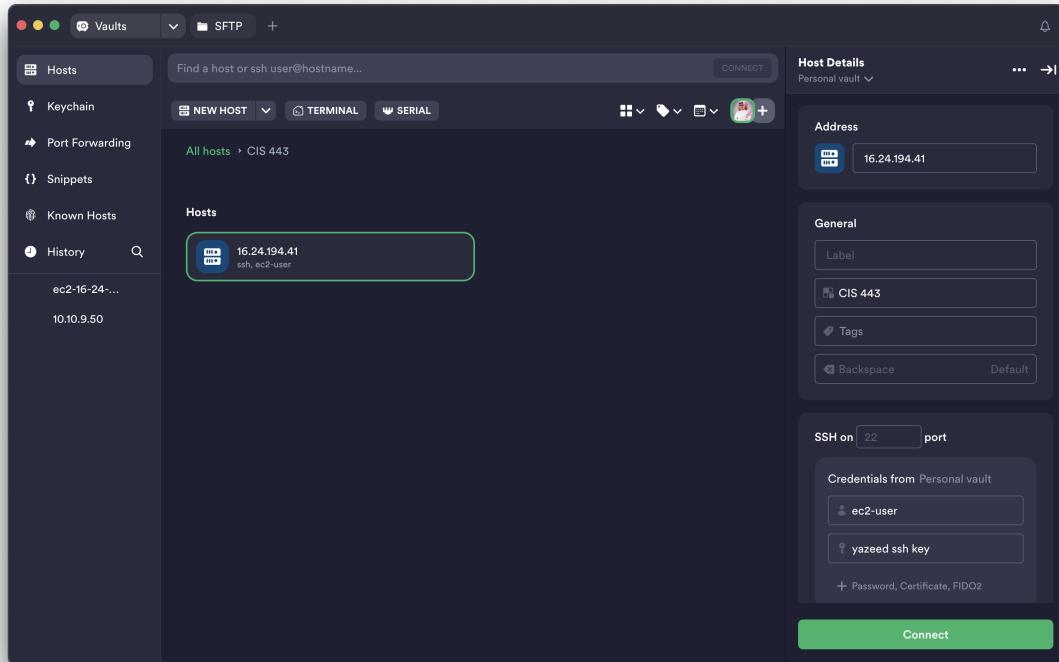


Figure 16: Termius SSH Connection Configuration

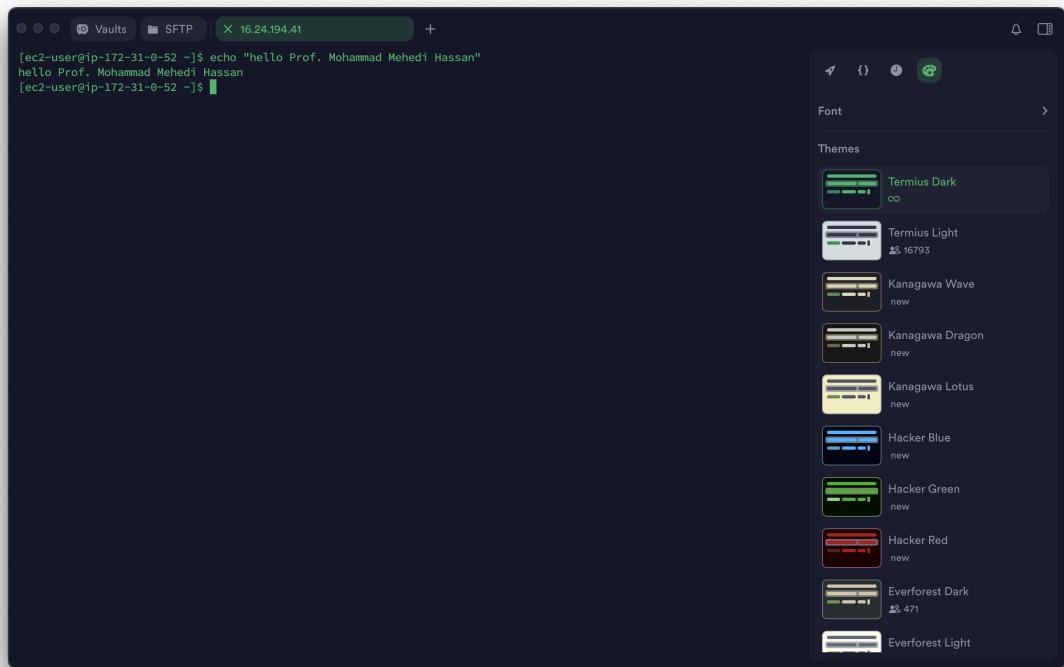


Figure 17: Termius SSH Connected - Saying Hello to Professor