**Lab 1: Create EC2 Instance and Configure a Web Server**

Adam Livingston

University of Arizona

NETV 379 SUM22 101-104 201-202: Cloud Computing

Professor Henry Werchan

12 June 2022

**Intro and Background**

In this lab, students were assigned to create an Amazon Web Services (AWS) account. In that account, they were instructed to create an Amazon Elastic Compute Cloud (EC2) instance and configure a web server. This lab requires some basic proficiency in Windows CLI and the Ubuntu Linux distribution. The steps annotated are for Windows 10 users. After instructions are given to type information, it is implied that the user presses the Enter key afterwards.

**Create EC2 Instance**

**Note**: that these steps are annotated by **not** using the new AWS interface. After successful login to AWS account, you will be at the AWS Management Console. Click on the “EC2” icon or “Launch a virtual machine With EC2”. Click on orange icon that says “Launch Instance” then click on “Launch Instance”. Top of screen now reads “Step 1: Choose an Amazon Machine Image (AMI)”. On left-hand side of screen, check the “Free tier only” box. Locate “Ubuntu Server [version #] LTS (HVM), SSD Volume Type”. Ensure that underneath the red Ubuntu logo there is a black box that says “Free tier eligible”. Pick the latest version, indicated by the higher/most recent [version #]. On right-hand side of screen, select “64-bit (x86)”. Click the blue “Select” icon. Top of screen now reads “Step 2: Choose an Instance Type”.

On left-hand side of screen, locate white square check boxes. When an instance type is selected, the check box will fill with a blue square. Ensure that the instance with the following parameters is selected: Family: t2; Type: t2.micro (with green box below t2.micro that says “Free tier eligible”. This is the only instance option that is free tier eligible. At bottom-right corner of screen, click grey box that says “Next: Configure Instance”. Top of screen will now read “Step 3: Configure Instance Details”.

Do not change anything on this screen (Step 3: Configure Instance Details). At bottom-right corner of screen, click grey box that says “Next: Add Storage”. Top of screen will now read “Step 4: Add Storage”. Do not change anything on this screen. At bottom-right corner of screen, click grey box that says “Next: Add Tags”. Top of screen will now read “Step 5: Add Tags”. Do not change anything on this screen. At bottom-right corner of screen, click grey box that says “Next: Configure Security Group”. Top of screen will now read “Step 6: Configure Security Group”.

Locate the yellow “Warning” box near bottom of screen. Above the warning box on left-hand side of screen, locate the grey box that says “Add Rule” and click on it. A new line will appear that has a pull-down menu under the “Type” column of the table. Click on the pull-down menu of the second row under the “Type” column (pull-down menu will read “Custom TCP Rule”). Under the pull-down menu that you just clicked, select the “HTTP” option. Ensure that there are two rules, one being “HTTP” that you just added and the other being “SSH” that was on the screen prior to clicking on “Add Rule”. At bottom-right corner of screen, click blue box that says “Next: Review and Launch”. Top of screen will now read “Step 7: Review Instance Launch”. At bottom-right corner of screen, click blue box that says “Launch”.

A window will pop up that says “Select an existing key pair or create a new key pair”. Click the pull-down menu that says “Choose an existing key pair” and select “Create a new key pair”. Key pair type defaults to RSA. Ensure RSA is selected. In the box under “Key pair name”, type out a name for your key pair then click grey box “Download Key Pair”. The file name will be downloaded as [KeyPairNameYouChose].pem. Take note of the download location. Click blue icon “Launch Instances”. Top of screen will say “Launch Status”. At bottom-right of screen, click blue icon “View Instances”. In the table called “Instances”, once column “Status Check” states “2/2 checks passed”, column “Instance State” will read “Running” with a green check mark to its left. The EC2 instance is now running.

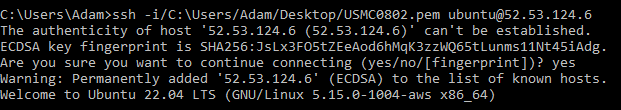
**Configure Web Server**

Following previous steps, you will be at your AWS account’s “Instances” page. Next to column labeled “Name”, click on the white square in the row of your EC2 instance to view details. Locate the .pem file when you downloaded your key pair. Right click and select “Properties”. Click “Security” tab. Click “Advanced”. Locate your Windows username (names are under column “Principal”). Ensure that your username has Full Control under the “Access” column. If your username already has administrator privileges, then it should already have Full Control Access.

On your Windows taskbar (the bar that defaults to the bottom of your screen), click on “Type here to search”. Type “cmd” and hit the “Enter” key. The command prompt will now appear. Type the following command: “ssh -i/[pathtokeyfile]/[key.pem] ubuntu@[aws\_ip]”. Insert the following information in the respective brackets (ensure to remove brackets after typing in the info. Example in *Fig.1*):

* [pathtokeyfile]: This will be the path to your .pem file
* [key.pem]: This is the filename of the .pem file
* [aws\_ip]: On the AWS instance dashboard after bringing up your EC2 instance details, under “Instance Summary”, this is the Public IPv4 address.

You will be prompted, “Are you sure you want to continue connecting (yes/no/[fingerprint])?”. Type “yes”. You are now connected to your AWS EC2 instance via your computer.



*Fig.1*

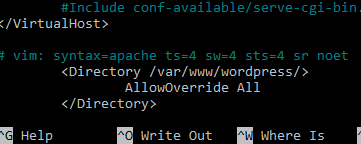
You now need to install updates on the EC2 instance. Type “sudo apt update”. Once updates are complete, install Apache HTTP server. Type “sudo apt install apache2”. You will be prompted with “Do you want to continue? [Y/n]”. Type “y”. Updates and Apache install is now complete.

We now need to install a firewall. Type “sudo ufw app list”. This will list available applications for Uncomplicated Firewalls (UFW) (Listed apps are Apache, Apache Full, Apache Secure, and OpenSSH). Type “sudo ufw app info Apache Full”. This lists the information about the Apache Full application. Type “sudo ufw allow in “Apache Full””. This updates the UFW rules and Apache is now running.

Type “sudo apt install mysql-server”. You will be prompted with “Do you want to continue? [Y/n]”. Type “y”. This installs MySQL server, a database management system. Once the download and install are complete, type “sudo apt install php libapache2-mod-php php-mysql”. You will be prompted with “Do you want to continue? [Y/n]”. Type “y”. This installs PHP, a programming language for web development. We now need to configure the MySQL server.

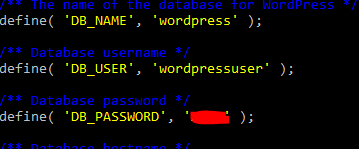
Type “sudo mysql -u root -p”. You will be prompted with “Enter Password:”. Press Enter. The line you can enter information on is now prefaced with “mysql>”, indicating that you are now in the MySQL server. Type “CREATE DATABASE wordpress;”. Type “CREATE USER ‘wordpressuser’@’localhost’ IDENTIFIED BY ‘[password]’;” where [password] is replaced with your choice of password. Press Enter. (**Note:** the single quotations are apostrophes, not the symbol above the tilde key). Type “GRANT ALL ON wordpress.\* TO ‘wordpressuser’@’localhost’;” . Type “FLUSH PRIVILEGES;”. Type “EXIT;”. MySQL Server is now configured.

Install updates again (“sudo apt update”). Type “sudo apt install php-curl php-gd php-mbstring php-xml php-xmlrpc php-soap php-intl php-zip”. Type “Y” to continue. New software is now installed. Type “sudo systemctl restart apache2”. The server has restarted. Type “sudo nano /etc/apache2/sites-available/000-default.conf”. Using arrow keys, navigate to “DocumentRoot /var/www/html” and change to “DocumentRoot /var/www/wordpress”. Using arrow keys, navigate down to end and type in the information located on *Fig.2*. Press Ctrl+X. Press Y. Press Enter.



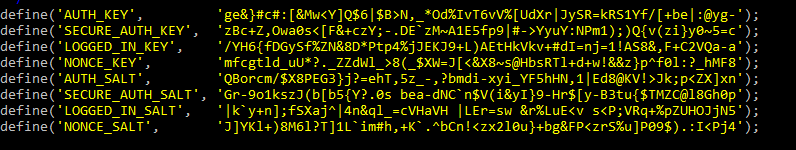
*Fig.2*

Type “sudo a2enmod rewrite”. Test the configuration by typing “sudo apache2ctl configtest”. Restart the server by typing “sudo systemctl restart apache2”. Type “cd /tmp”. Type “wget https://wordpress.org/latest.tar.gz”. Wordpress file is now saved in the tmp folder. Type “tar xzvf latest.tar.gz”. Type “touch wordpress/.htaccess”. Type “cp wordpress/wp-config-sample.php wordpress/wp-config.php”. Type “mkdir wordpress/wp-content/upgrade”. Type “sudo cp -a /tmp/wordpress/. /var/www/wordpress”. Type “sudo chown -R www-data:www-data /var/www/wordpress”. Type “sudo find /var/www/wordpress/ -type d -exec chmod 750 {} \;”. Type sudo find /var/www/wordpress/ -type f -exec chmod 640 {} \;”. Type “sudo nano /var/www/wordpress/wp-config.php”. This opens the wordpress php file for editing wordpress credentials. Using same process as before when editing 000-default.conf, edit the document according to *Fig.3* and entering the password when creating MySQL Server. DO NOT EXIT YET.



*Fig.3*

Using a web browser, go to <https://api.wordpress.org/secret-key/1.1/salt> and copy all information. Go back to the command prompt and scroll down to location referenced in *Fig.4* and paste the information over the existing info. Now you can exit.



*Fig.4*

Using a web browser, go to http**://[EC2IPv4AddressHere]**/php-admin/install.php. Select language. Enter in information of your choosing, check “Discourage search engines from indexing this site” box, then click “Install WordPress”. Click “Log In” then enter your login information. Click “Posts” on left hand side of screen. Click “Add New”. Type in something over the “Add title” area then click “Publish” in upper-right corner of screen.

