Proof of Concept Technical Solution

for the *Marconi Law Firm, LLC*.

(WordPress Website)

Project Background: Assume that you are an entrepreneur and that you own your own Information Technology (IT) consulting firm. You have recently acquired a new client called "Marconi Law Firm". As part of your client's contract agreement, you are to deliver full documentation for their upcoming WordPress Website Hosting project implementation. This documentation includes a Proof-of-Concept Technical Solution which documents all software, hardware, and network configuration details. Assume that the finished document will be used in-house by the Marconi Law Firm and will be referenced by their in-house IT department---after the project has been successfully completed.

Ydali Hernandez

Palm Beach Network Corporation

Preface

This document will serve as proof of concept to Mr. Marconi for creating his WordPress website for his law firm and as audit documentation.

The purpose of audit documentation is to provide a comprehensive record of the organization's information technology infrastructure and security controls and processes. It plays a crucial role in providing transparency, accountability, and QA/QC regarding an organization's cybersecurity controls and practices. It enables organizations to demonstrate compliance, identify areas for improvement, and make informed decisions to strengthen their overall organizational cybersecurity.

Audit documentation serves several important purposes:

- **Compliance**: Evidence that an organization has undergone a thorough examination of its systems. It helps validate that the organization has implemented appropriate controls to protect its information systems and sensitive data.

- **Validation**: Verification of the effectiveness and adequacy of cybersecurity controls. It provides detailed information about the design, implementation, and operation of these controls, enabling reviewers to assess their reliability and identify any gaps or weaknesses.

- **Records Maintenance**: Historical record of cybersecurity audits conducted over time. It enables organizations to track their progress, identify trends, and evaluate the effectiveness actions taken. It also serves as reference for future audits and allows auditors to understand the current cybersecurity implemented and facilitates a more targeted approach to future cybersecurity updates and audits.

- **Decision-making Support**: Valuable insights and information that can support decision-making processes. It allows management to make informed decisions about allocating resources, prioritizing cybersecurity investments, and addressing identified risks and vulnerabilities.

Table of Contents

Inventory 7

Custom Network 7

IDs and Passwords 7

Network Topology Diagram 8

Node.js Application (Ghost) on Docker 8

Show screenshot of your CentOS 7 Console in VE 9

Update CentOS 10

Install EPEL Packages 11

Install Nano Editor 12

Docker CE 13

Install required packages 13

Set up stable repository 14

Install Docker CE 15

Verify docker version 16

Initialize Docker 17

Start Docker 17

Enable Docker 18

Test Docker (hello-world) 19

Disable SELinux 20

Reboot VM 21

Test SELinux 22

Confirm SELinux Status 23

Install Ghost Docker Container 24

Test Ghost 25

Ghost Container ID 25

NginX Reverse Proxy 26

Show screenshot of your Rocky 8 Console in VE 26

Update Rocky 8 27

Install EPEL Packages 28

Install Nano Editor 29

Disable SELinux 30

Reboot VM 31

Test SELinux **32**

Confirm SELinux Status **33**

Rocky Firewall **34**
Stop Firewall 34
Disable Firewall 35

NginX **36**
Install NginX 36
Start NginX 37
Enable NginX 38
Test NginX 39

Reverse Proxy for Ghost Site **40**
Edit NginX configuration file 40
Reload NginX service 41
Terminate Docker 42
Delete Ghost Container 43
Create New Ghost Container 44
Browse to Ghost 45

WordPress on Ubuntu - LAMP Stack ***46***

Show screenshot of your Ubuntu Console in VE **47**

Update Ubuntu **47**

Upgrade Ubuntu **49**

Install Nano Editor **49**

Install Git **50**

Install Apache2 ..... **51**
Open Firewall Ports 80 and 443 52
Browse to Apache2 Ubuntu Default Page 53

Install MySQL **54**
Alter root user password 55
Flush Privileges 56
Quit MySQL 57

Install PHP **58**
Edit Sources.list File 58
Update Ubuntu (refreshes the repolist) 59
Install Required PHP Libraries 60
Install Required MySQL Libraries 61
Enable URL Rewrites (clean URLs) 62
Restart Apache Service 63
Create a test.php Web Page 64
Test the test.php Web Page 65

Database Configuration in MySQL Log into MySQL Database **66**
Create WordPress Database in MySQL 68

Create WordPress User for MySQL Database ... 69
Grant Privileges to this New WordPress User ... 70
Flush Privileges ... 71
Quit MySQL ... 72

Install WordPress ... 73
Grant Permission to html Directory to WordPress User ... 73
Delete Files from html Directory ... 74
Verify html Directory is Empty ... 75

Clone WordPress to html Directory ... 76
Verify html Directory Contains WordPress Files ... 77
Verify Permissions on html Directory ... 78

Edit Ownership ... 79
Edit Ownership of Contents of html Directory ... 79
Edit Ownership of the html Directory Itself ... 80

Edit the apache2.conf File ... 81
Override All Default Apache Directives ... 82

Create a .htaccess File in the /var/www/html/.git/ Directory ... 83

Restart the Apache Service ... 84

WordPress Configuration ... 84

Configure WordPress ... 85
WordPress Configuration Selections ... 85
Run Installation ... 86
Create an Admin WordPress User ... 87
WordPress Site Selections ... 88
Test WordPress ... 90

WordPress Security Settings and Configurations ... 92

WordPress Security Summary ... 92

Defense-in-depth ... 92

File Permissions ... 93
Vulnerability ... 93
Configuration ... 94
Validation ... 94

Securing wp-config.php ... 94
Vulnerability ... 96
Configuration ... 97
Validation ... 97

Firewall (Shield) ... 97
Vulnerability ... 100
Configuration ... 101
Validation ... 101

Conclusion *103*

Appendix A *103*

NginX Config File ..... Error! Bookmark not defined.

Appendix B *104*

NginX Access Log File ..... Error! Bookmark not defined.

NginX Error Log File **104**

Inventory

EQUIPMENT	OPERATIING SYSTEM	ADDITIONAL INFO	IP ADDRESS
Router/Custom Network	-	-	10.10.229.1
Docker	CentOS 7	Ghost Container	10.10.229.11
NginX Reverse Proxy	Rocky 8	Reverse Proxy	10.10.229.10
WordPress	Ubuntu	LAMP Stack running WordPress	10.10.229.12

Custom Network

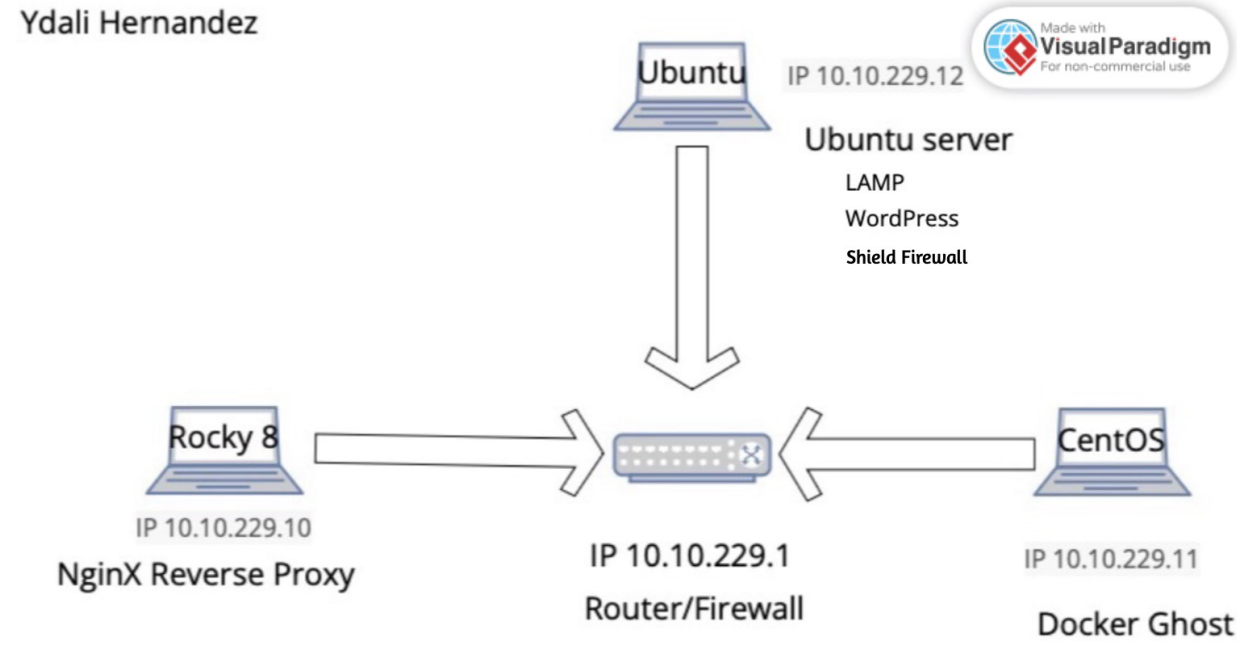
NETWORK NAME	SUBNET IP	SUBNET MASK	DNS	GATEWAY
ITE229	10.10.229.0	255.255.255.0	10.10.229.1	10.10.229.1

IDs and Passwords

ACCOUNT	USER ID	PASSWORD
CentOS 7 Root User	root	Fullsail1!
Rocky 8 Root User	root	Fullsail1!
MySQL Root User	root@localhost	VWqJReU17ak
MySQL WordPress User	WordPressUser	bLJvG8cddFyLgTv70oSp
WordPress Admin	admin	iHp1COMGwgD%4hhUU1

IMPORTANT: To earn full credit, ALL screenshots must include a “full view”, including your ProxMox title bar with your username showing.

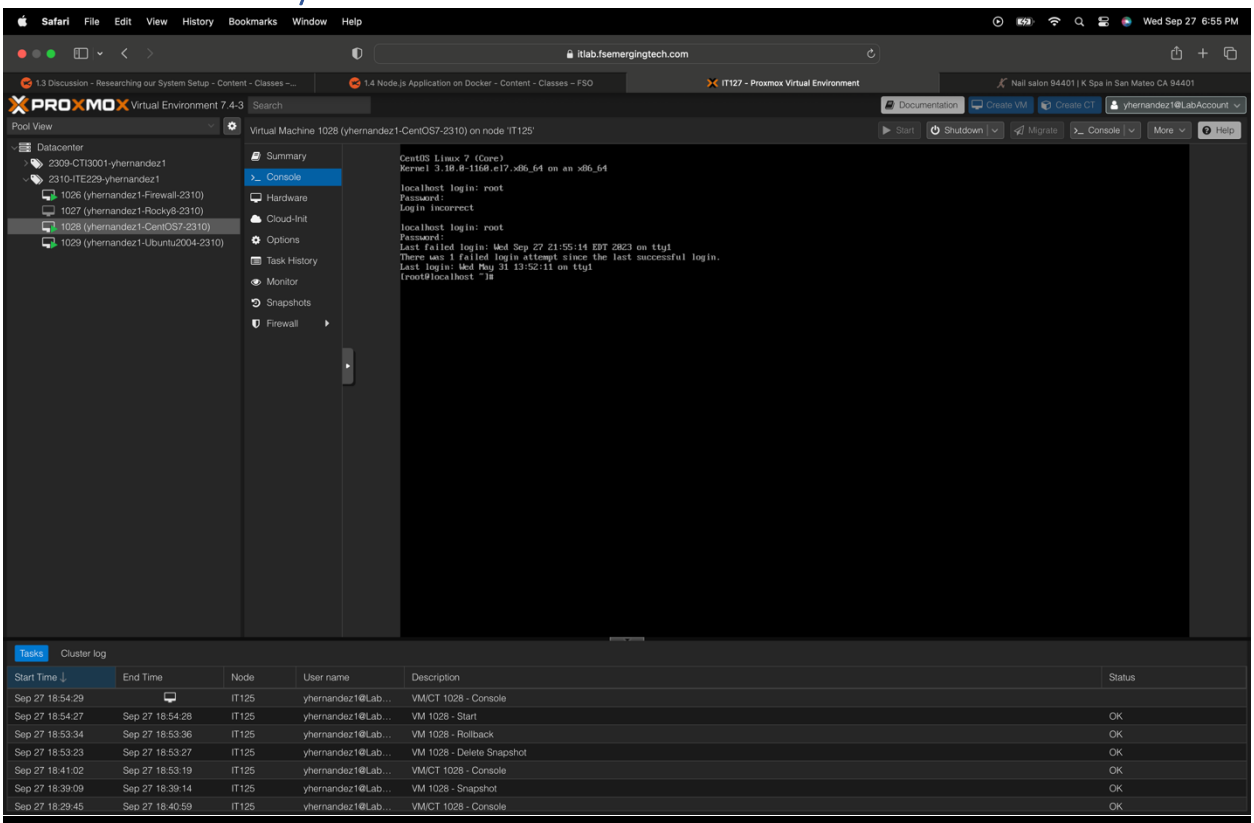
Network Topology Diagram

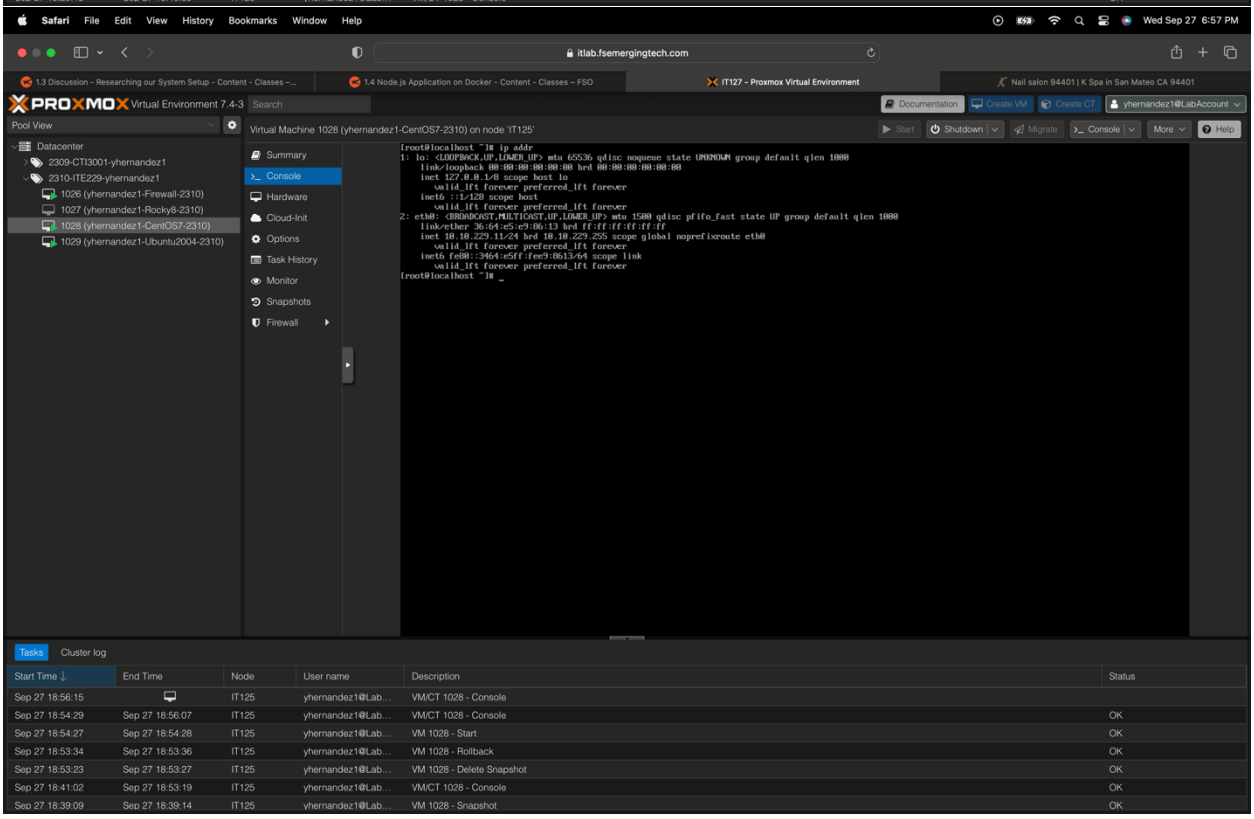


The Virtual machines communicate with each other through proper network configuration, which is internal networking. Each VM's firewall must be configured to allow incoming and outgoing traffic between VMs. Each VM should have a unique IP address within the same network segment. You can configure static IP addresses or use DHCP to assign IP addresses to VMs dynamically.

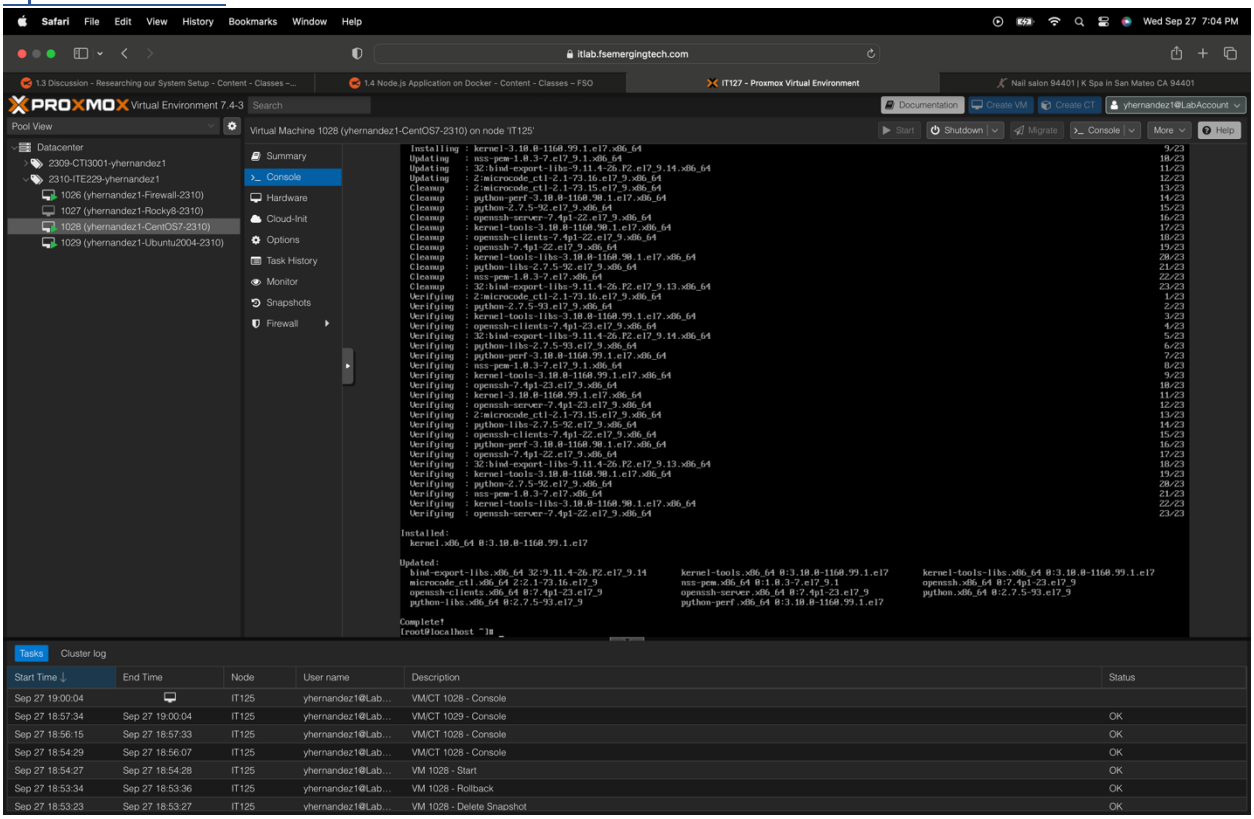
Node.js Application (Ghost) on Docker

Show screenshot of your CentOS 7 Console in VE



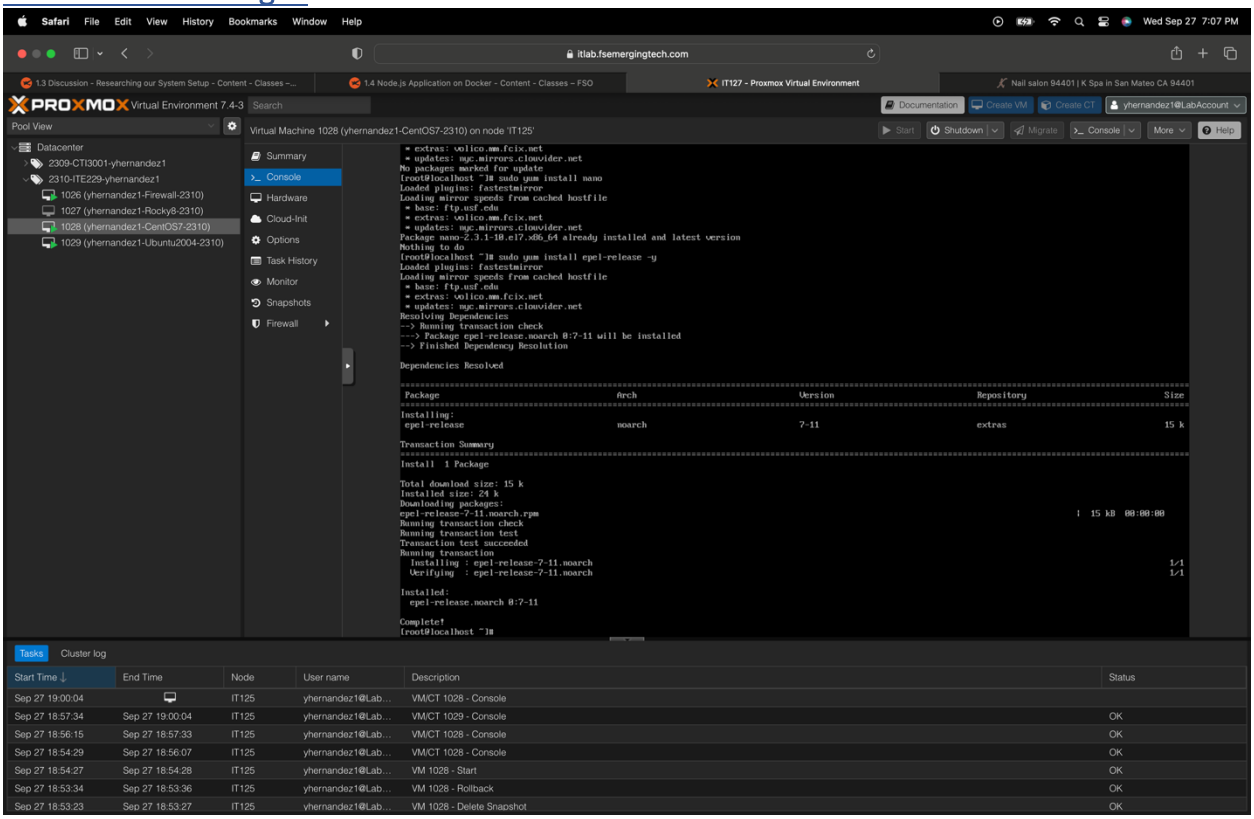


Update CentOS



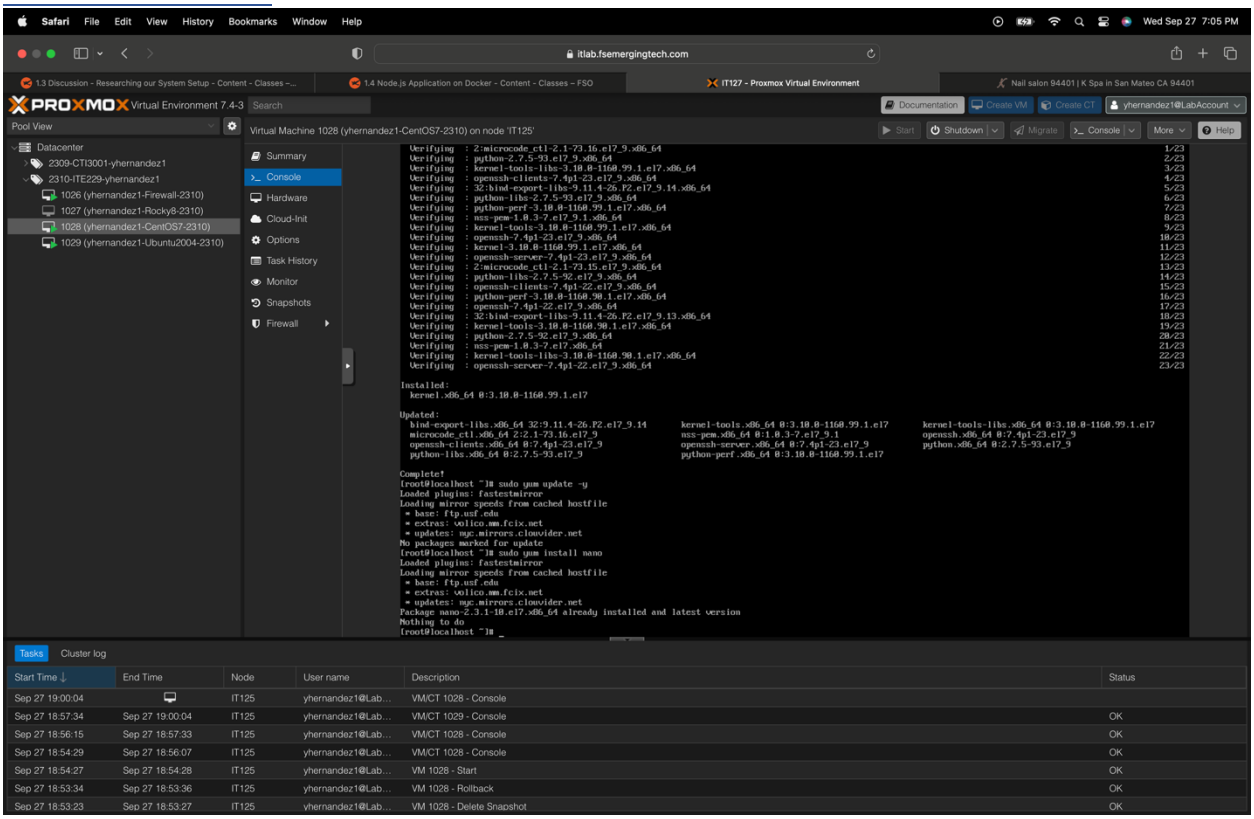
Type in **sudo yum update -y,** and the VM will automatically update CentOS.

Install EPEL Packages



Type in **sudo yum install epel-release -y,** and it will install automatically EPEL packages.

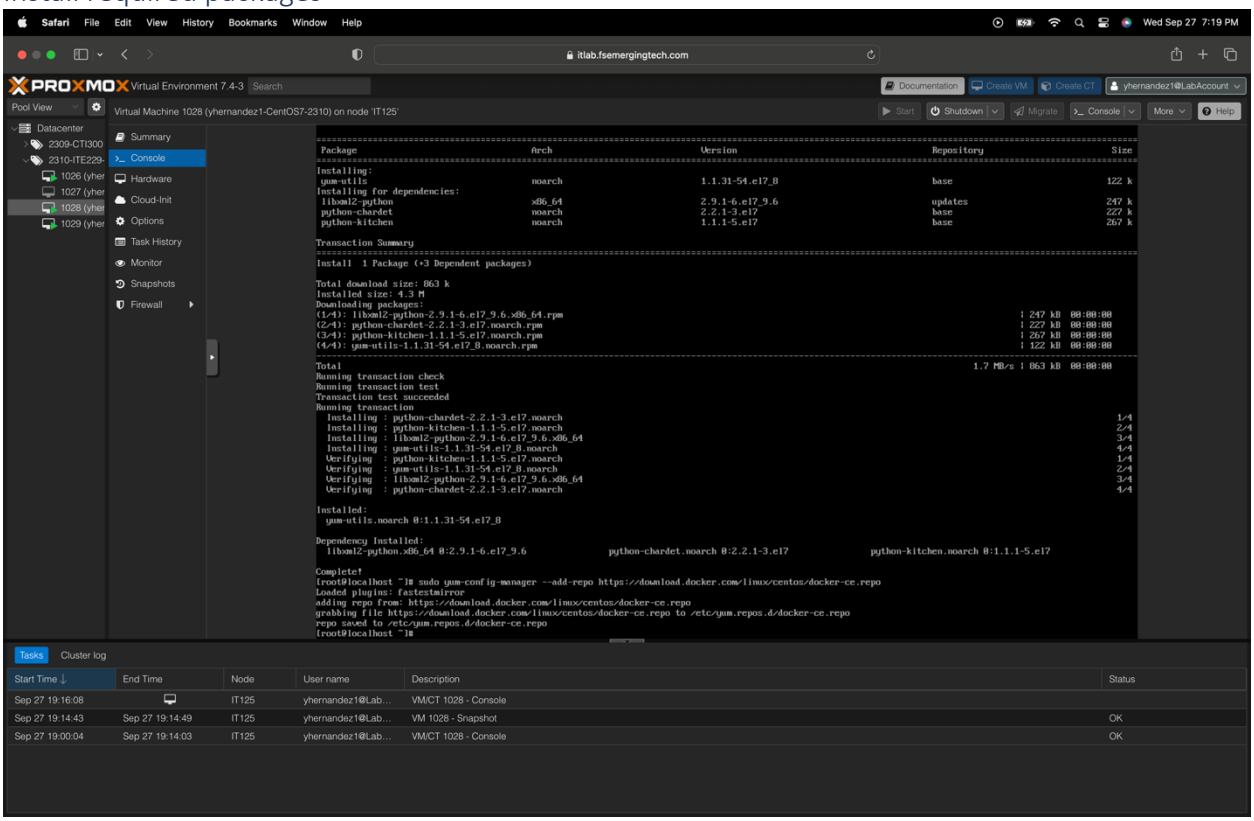
Install Nano Editor



Type in **sudo yum install nano,** and it will install nano.

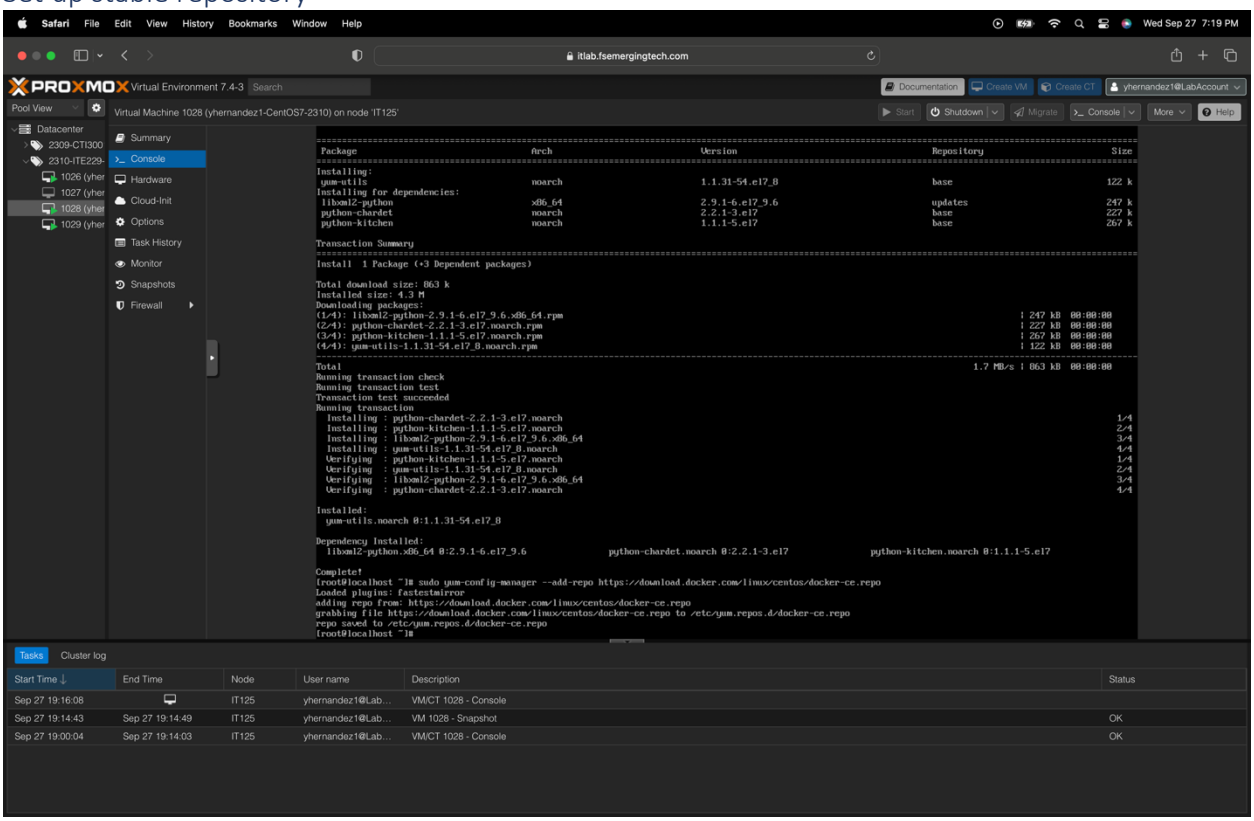
Docker CE

Install required packages



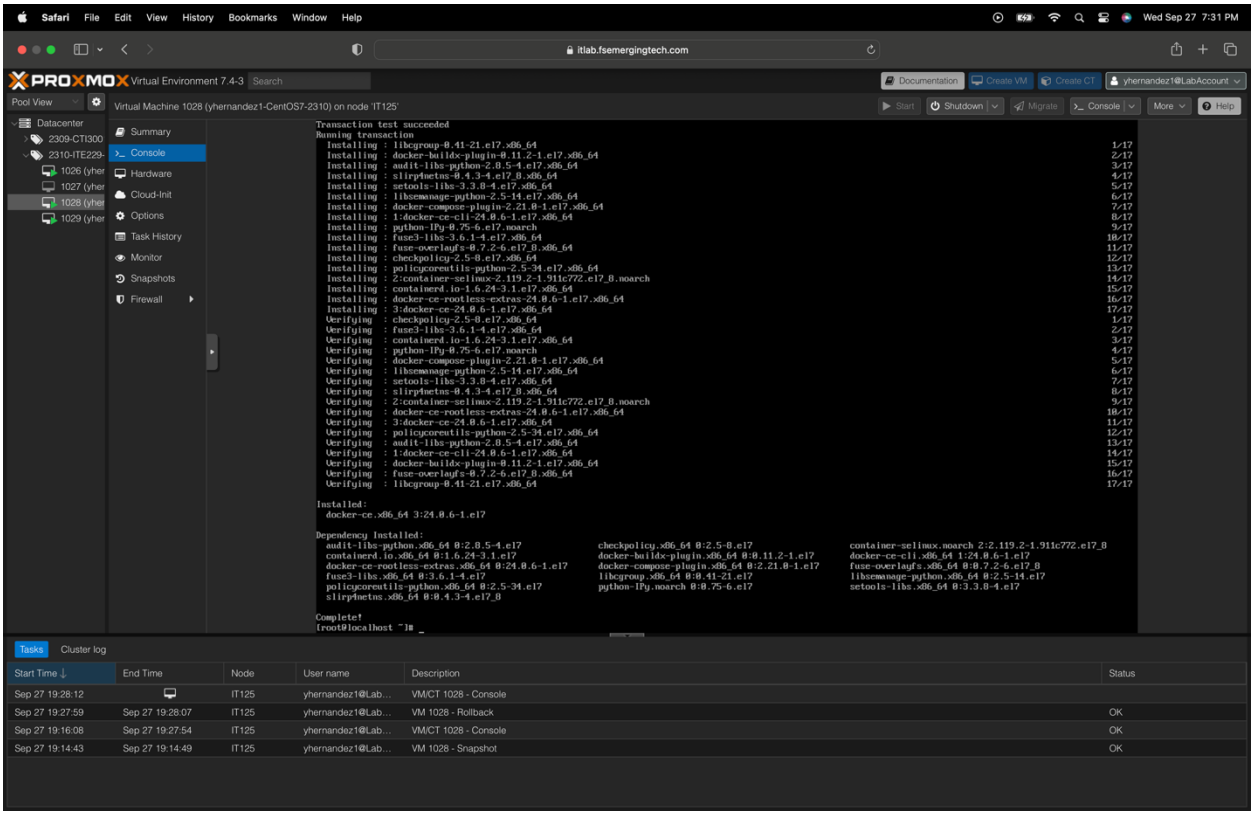
Type in **sudo yum install -y yum-utils,** and it will automatically install Docker packages.

Set up stable repository



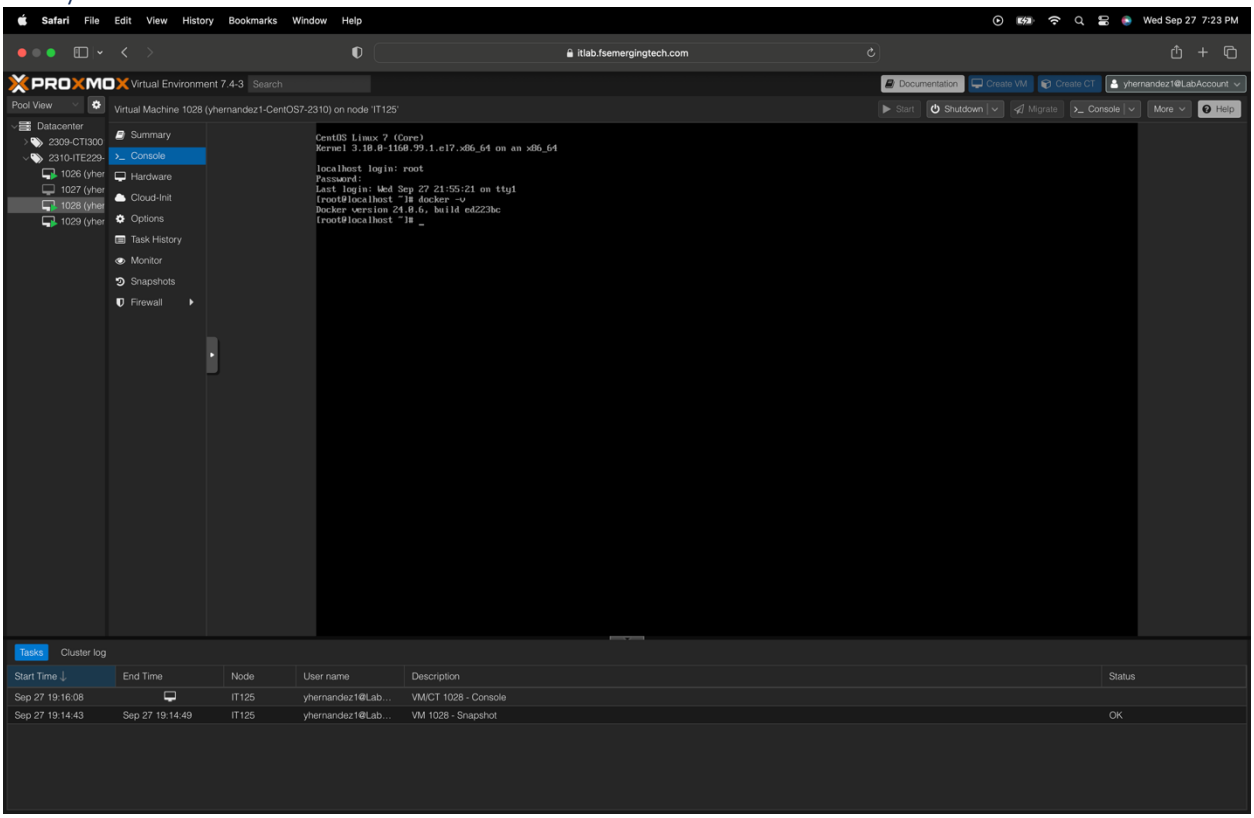
type in **sudo yum-config-manager --add-repo** **https://download.docker.com/linux/centos/docker-ce.repo** it will set up stable repository.

Install Docker CE



Type in **sudo yum install docker-ce,** and it will install Docker CE.

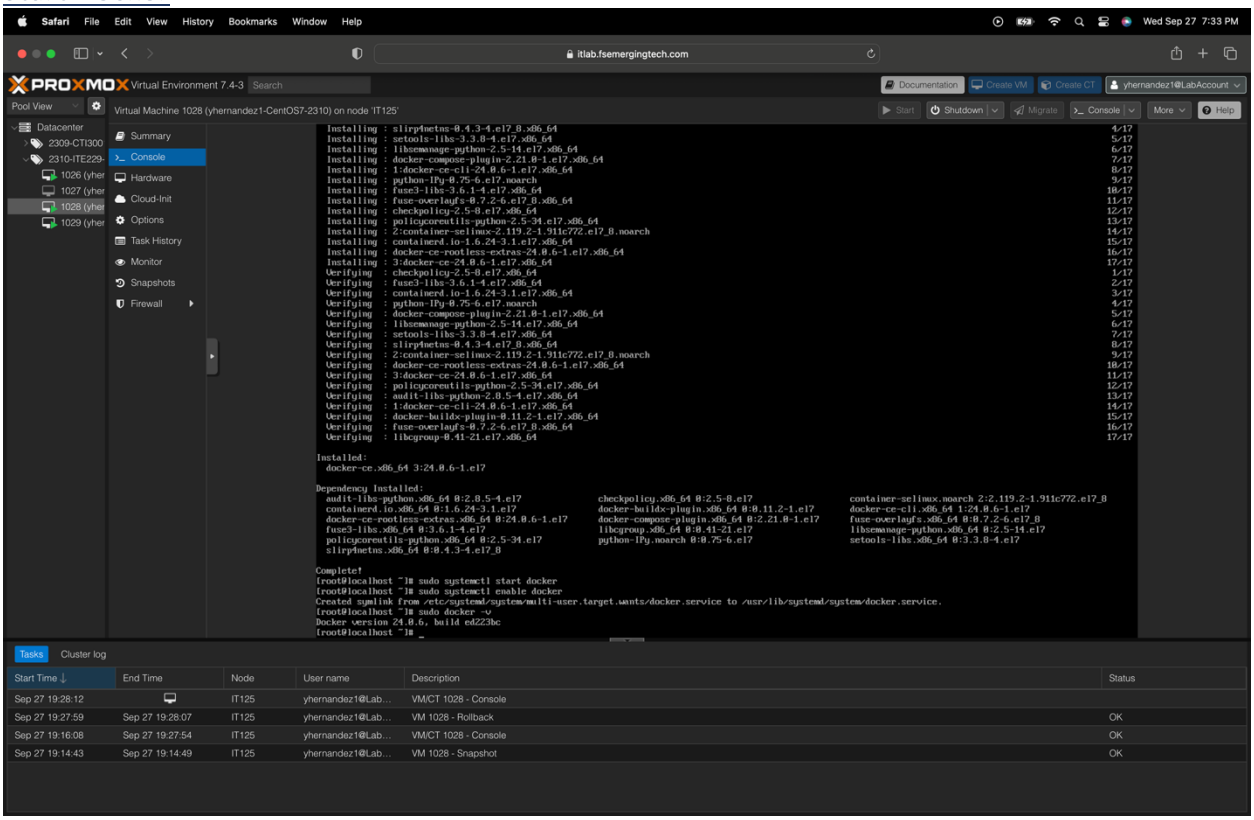
Verify docker version



Type in **sudo docker -v to** verify the docker version.

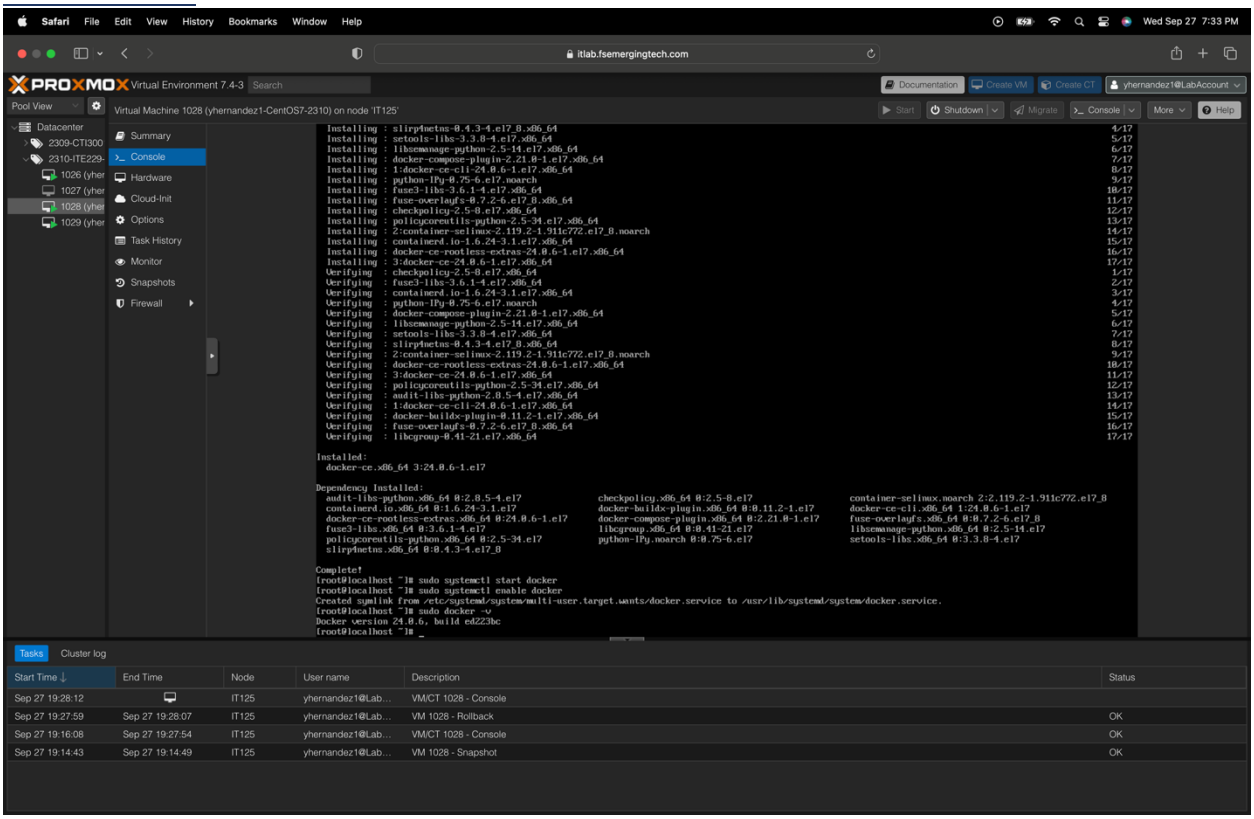
Initialize Docker

Start Docker



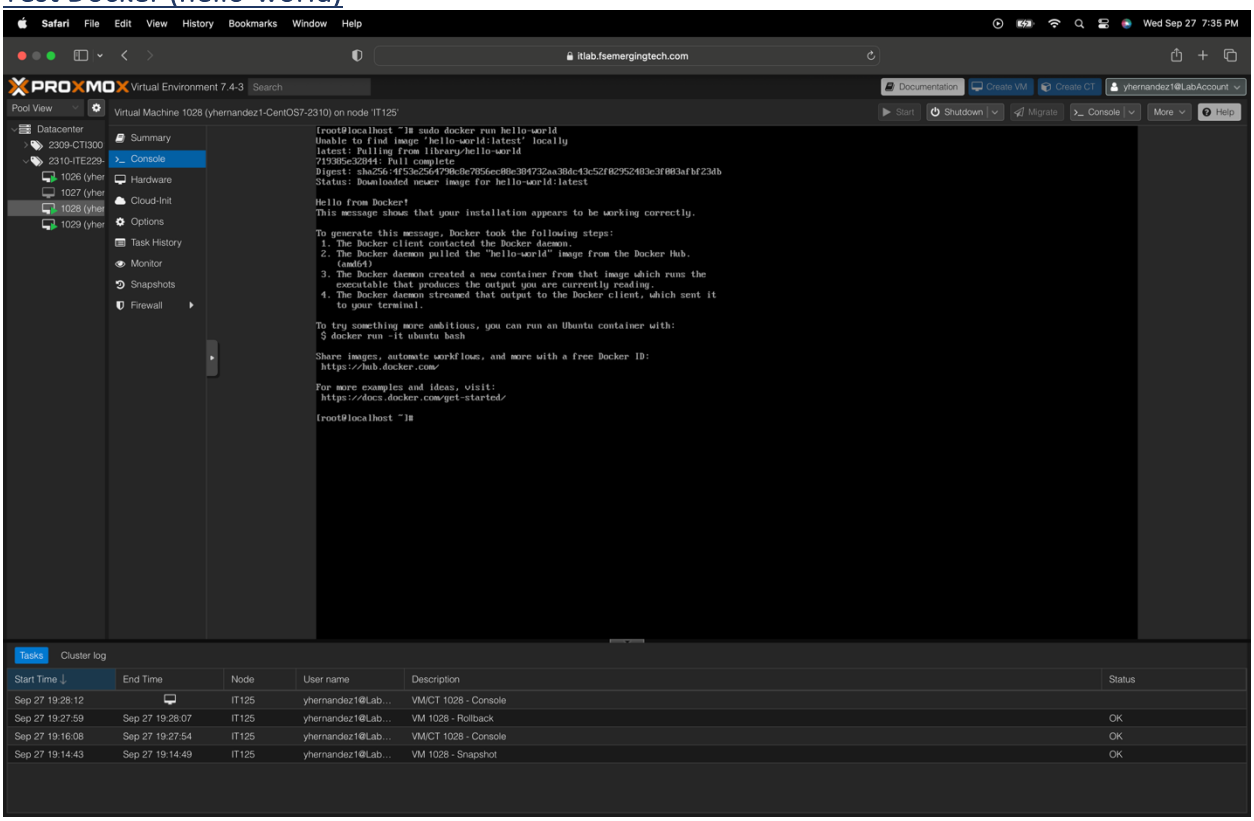
Type in **sudo systemctl start docker,** and it will initialize docker.

Enable Docker



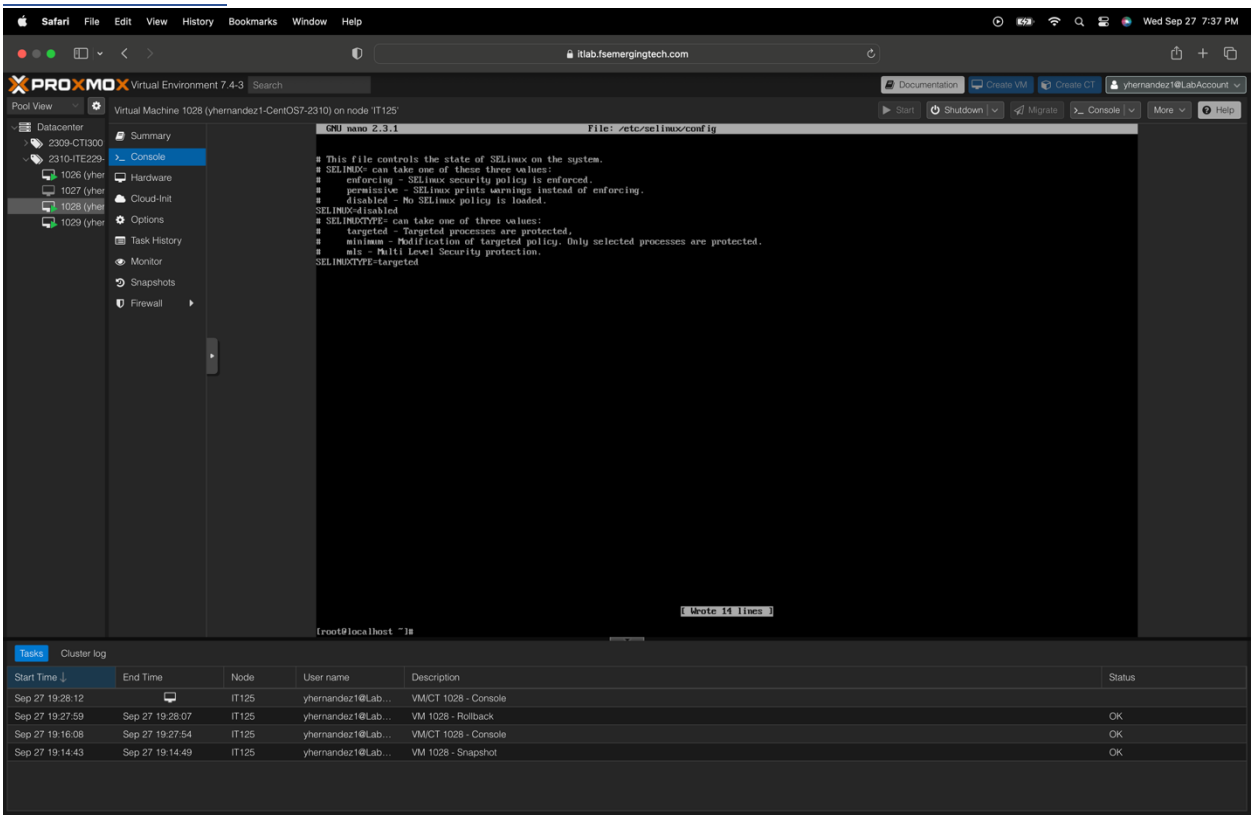
Type in **sudo systemctl enable docker,** and it will allow docker to use it.

Test Docker (hello-world)



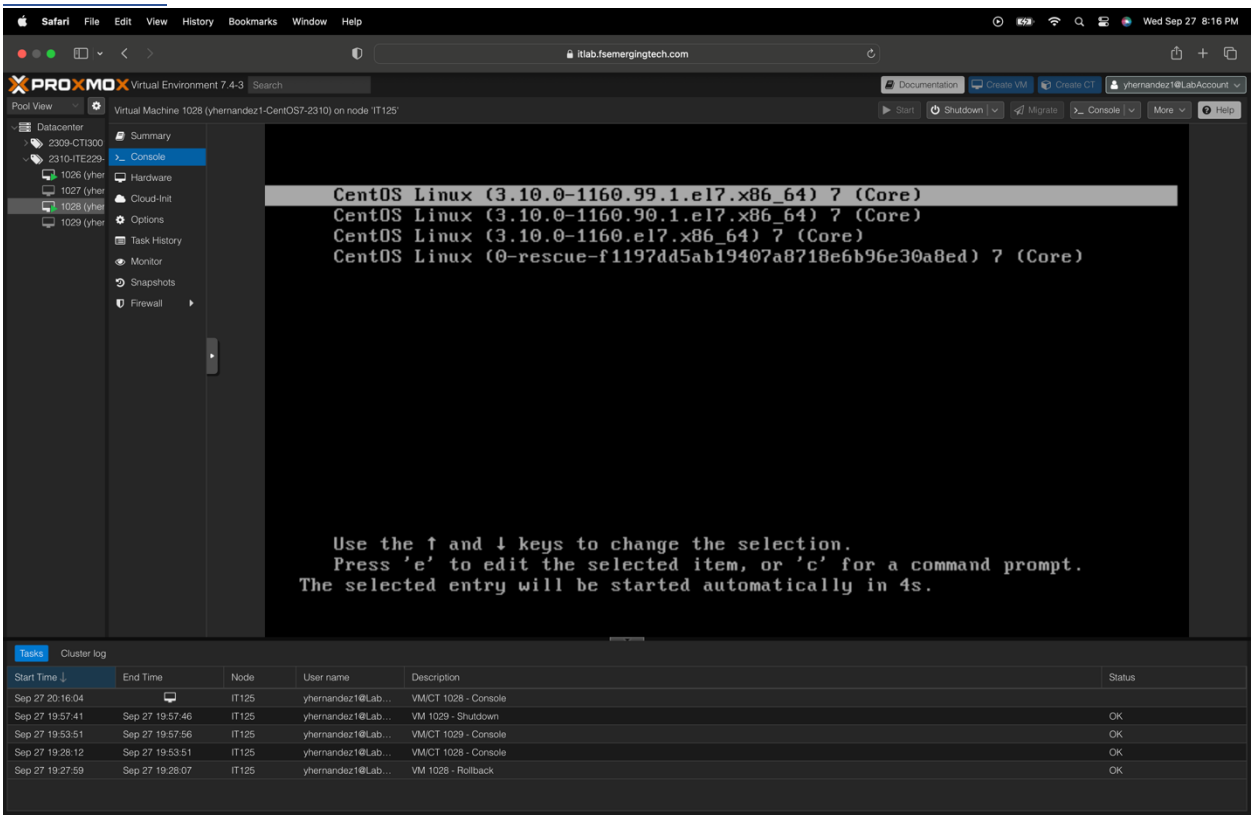
Type in **sudo docker run hello-world,** which will run the command and display a hello-world message.

Disable SELinux



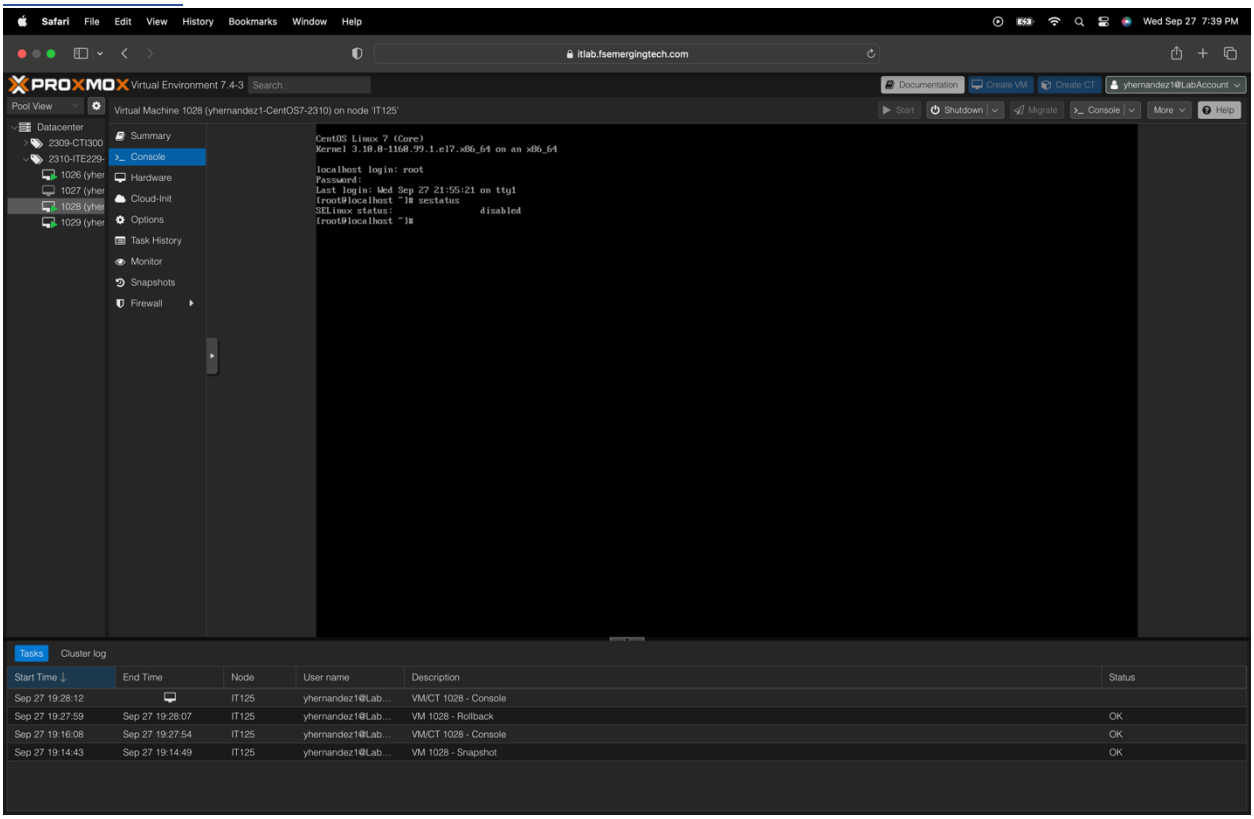
type in **sudo nano /etc/selinux/config.** Once in the configurations, go down to SELinux and delete enforcing to disabled, then press control x to save, press y when commanded, and enter to exit.

Reboot VM



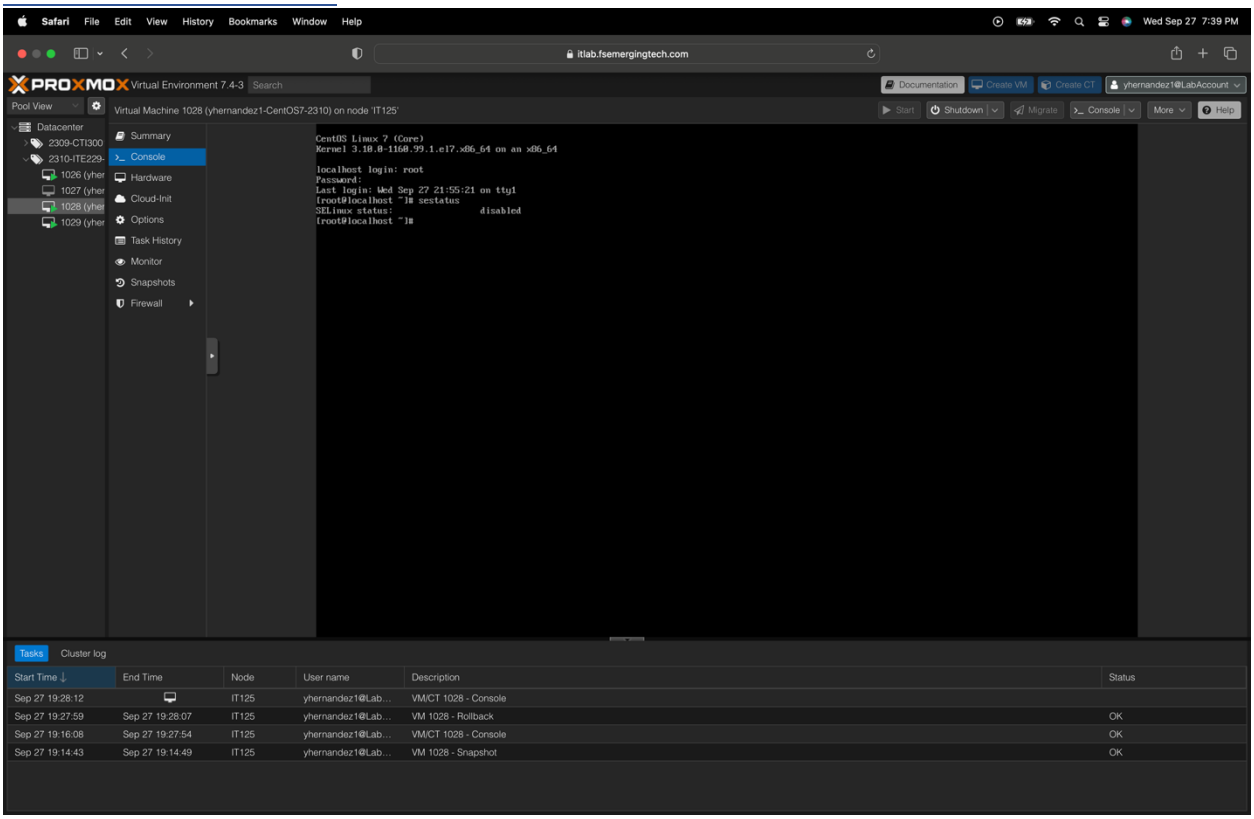
Type in **reboot,** and it will automatically reboot the system.

Test SELinux



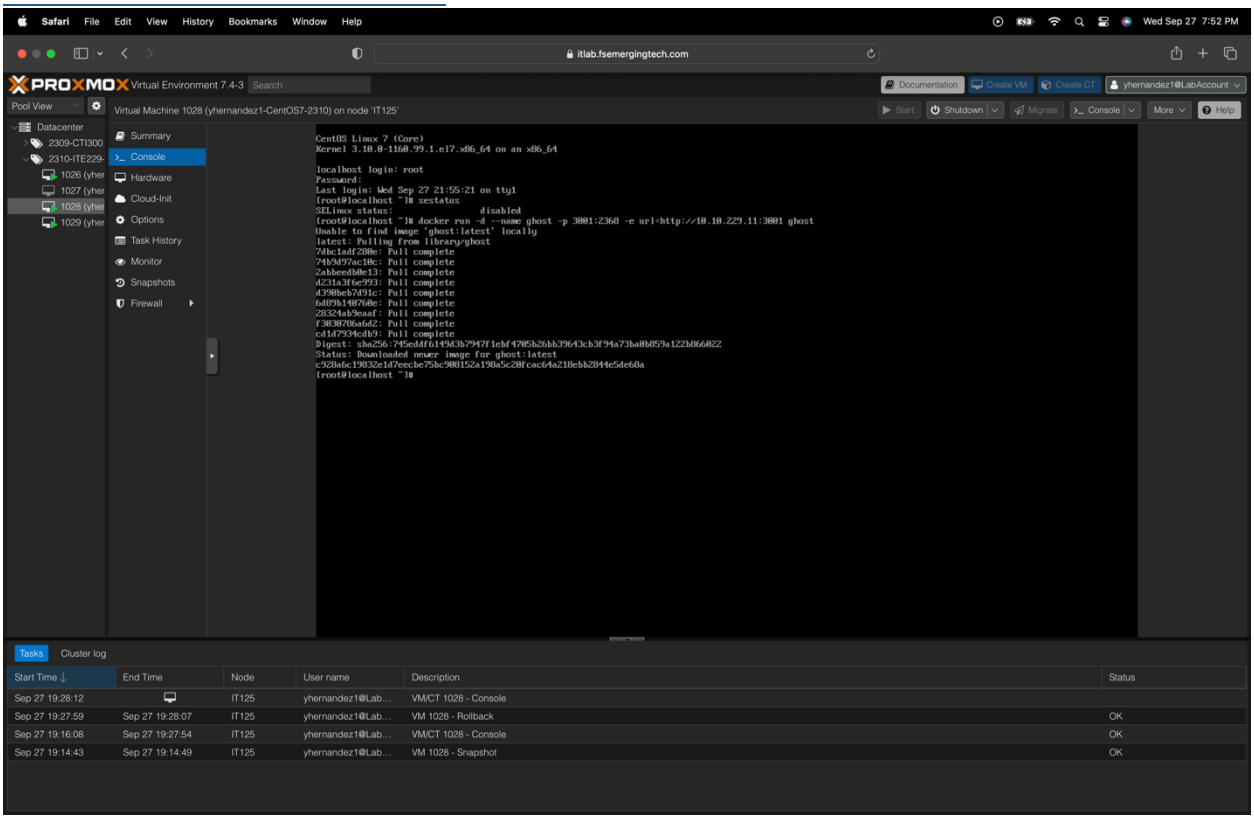
Type in **sestatus,** and this will test SELinux.

Confirm SELinux Status



Type in **sestatus** to confirm SELinux Status.

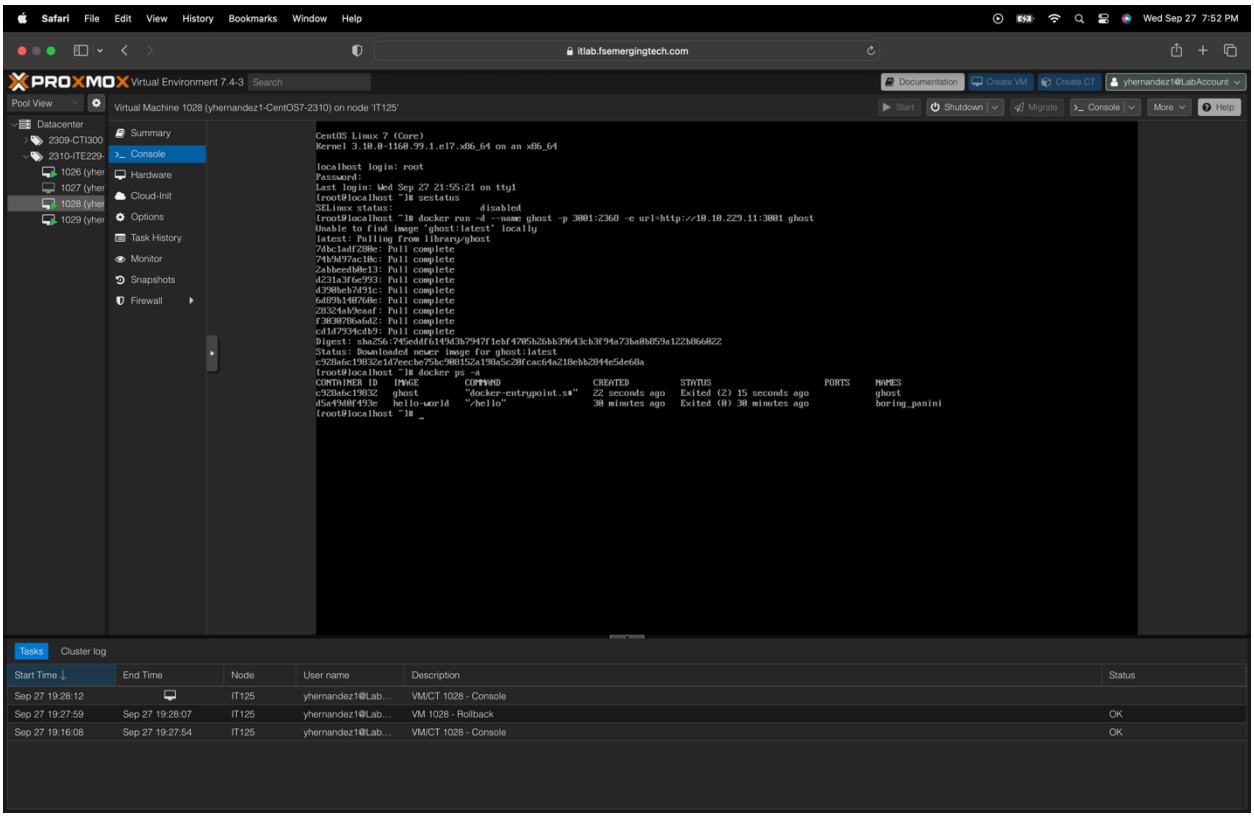
Install Ghost Docker Container



To install Ghost, type **docker run -d --name ghost -p 3001:2368 -e url=http://10.10.229.11:3001 ghost.** This will establish a ghost docker container.

Test Ghost

Ghost Container ID

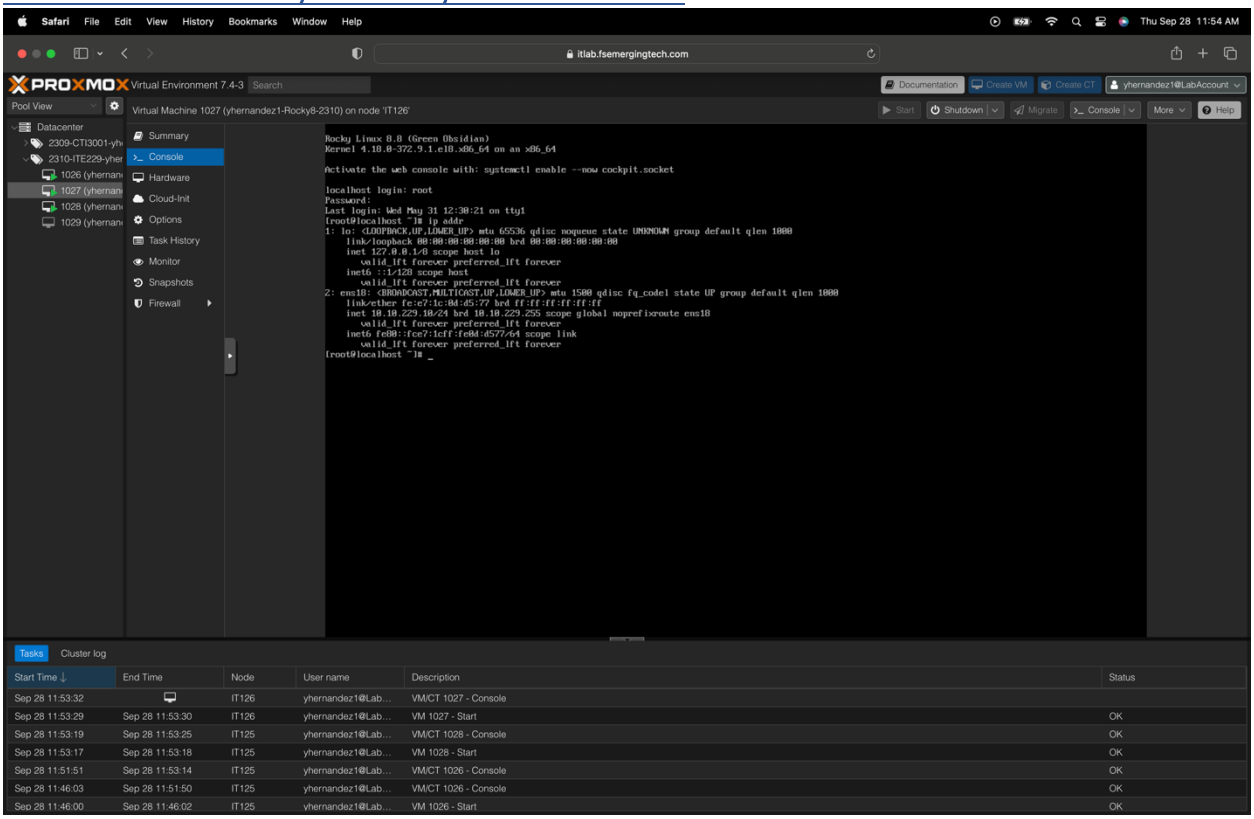


To test ghost container type in **docker ps -a,** this will display the containers created and give you the container ID.

IMPORTANT: To earn full credit, ALL screenshots must include a “full view”, including your ProxMox title bar with your username showing.

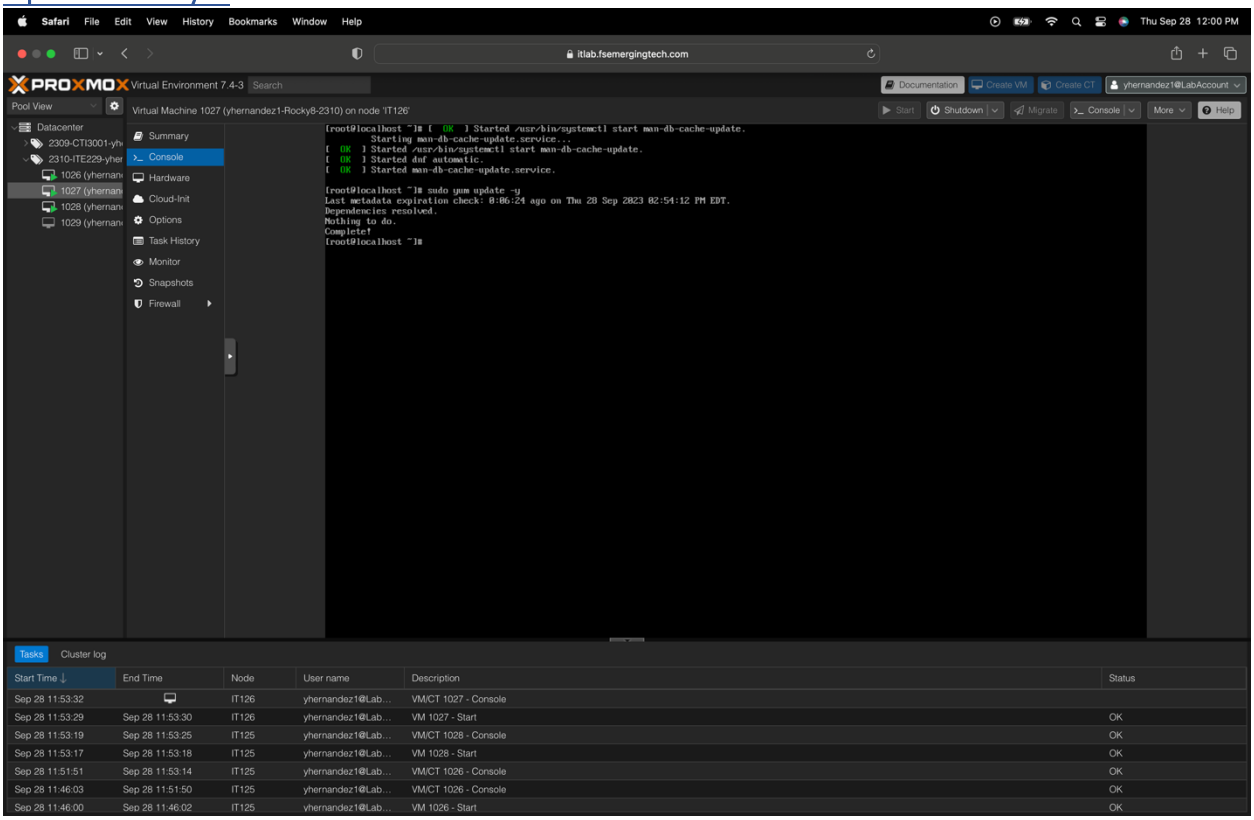
NginX Reverse Proxy

Show screenshot of your Rocky 8 Console in VE



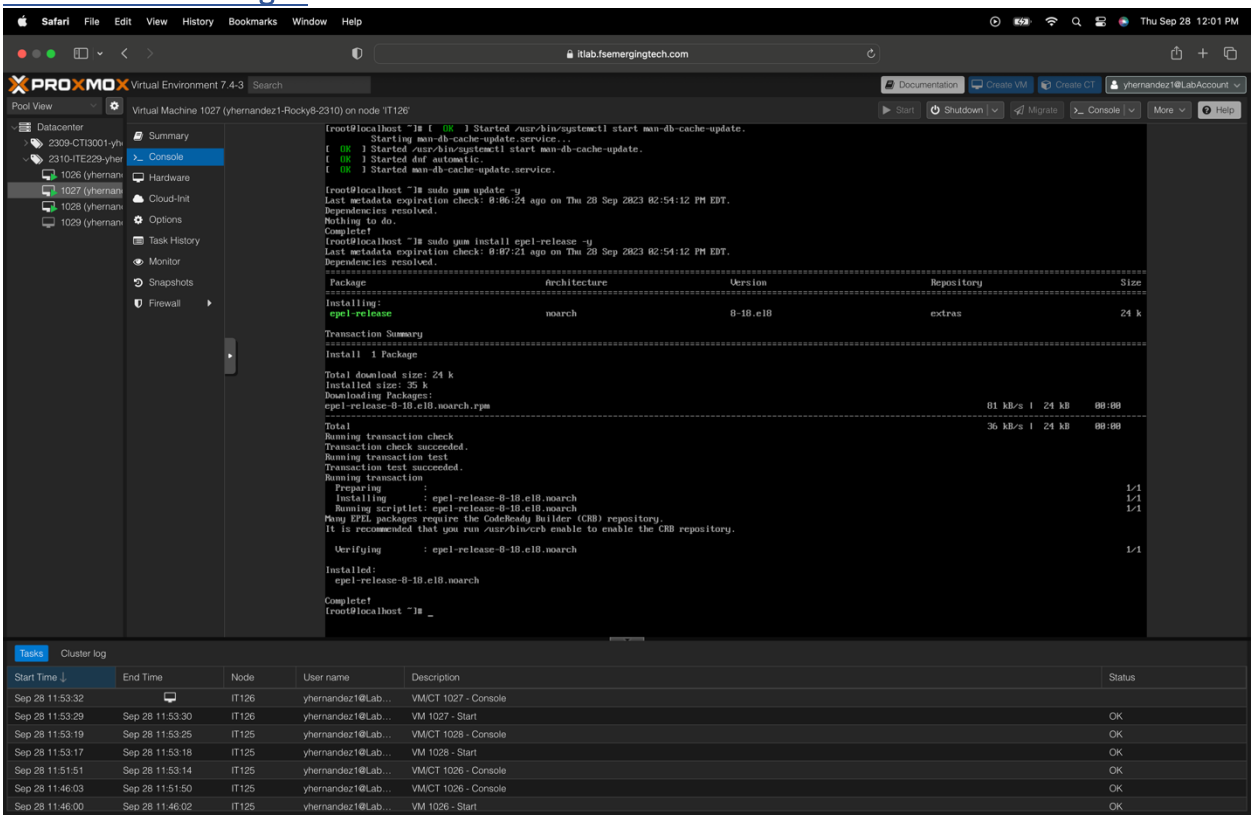
To access Rocky 8 Console, go to your proxmox environment, and on the left side of the screen, click on the firewall machine and start it up. Once completely loaded, click the Rocky 8 and start it up. Then, log in with credentials and verify the IP address on the command line—type in the **IP addr.**

Update Rocky 8



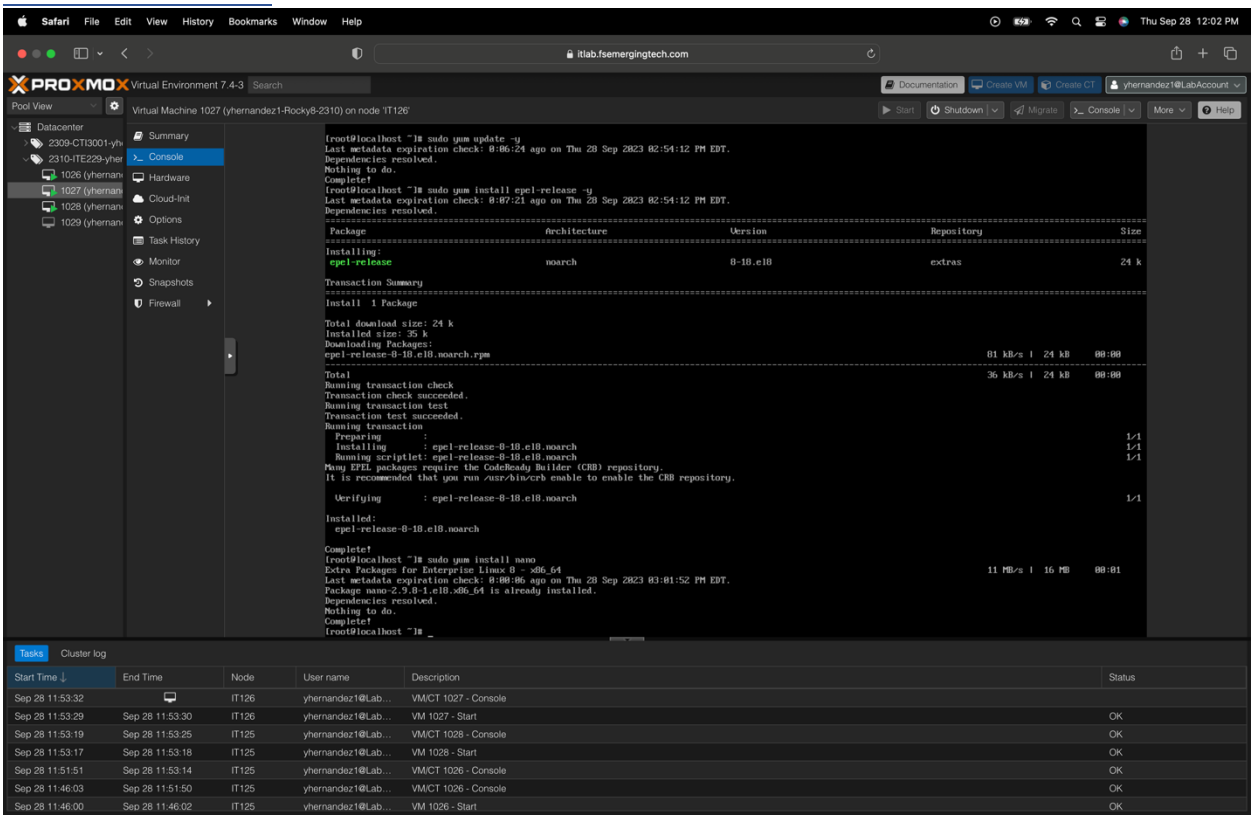
To update Rocky 8, type on the command line **sudo yum update -y,** which will update the machine to the latest updates.

Install EPEL Packages



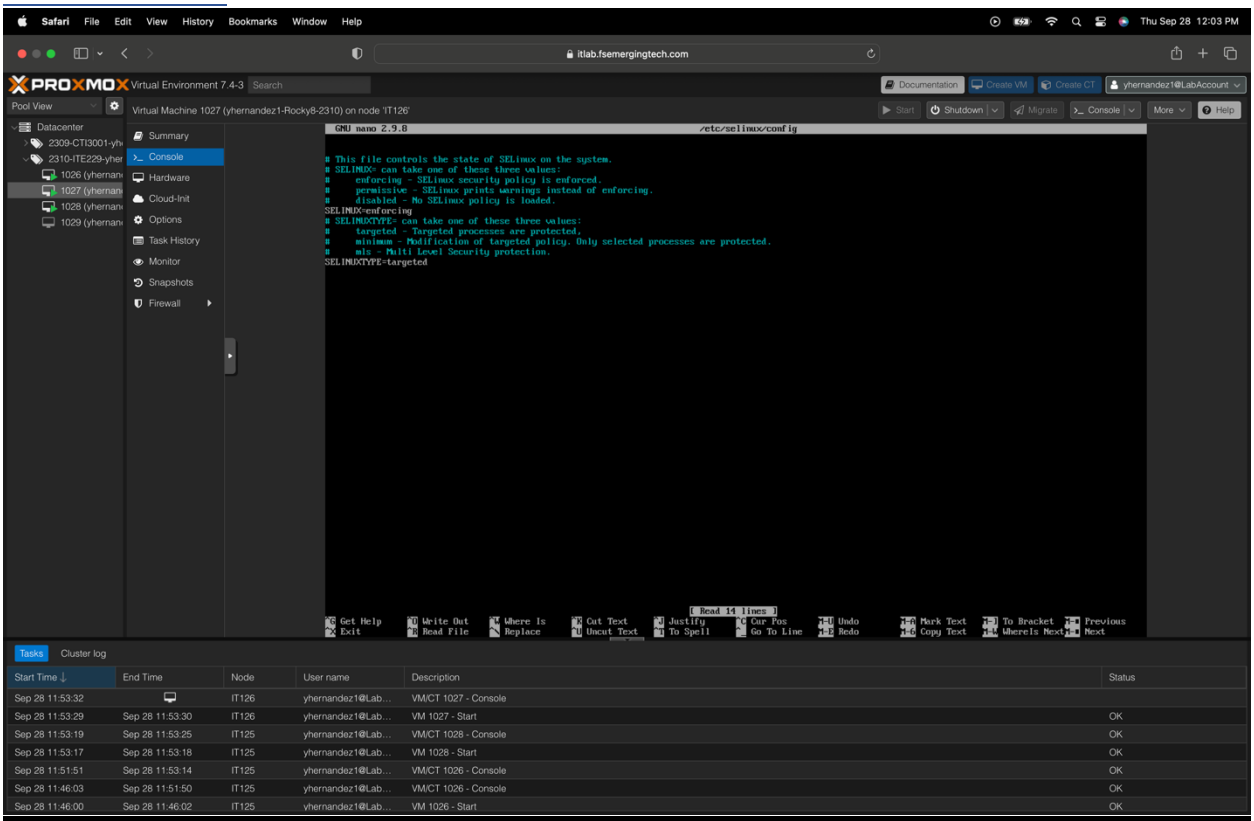
To install EPEL packages, type on the command line **sudo yum install epel-release -y.** This will install the packages for EPEL.

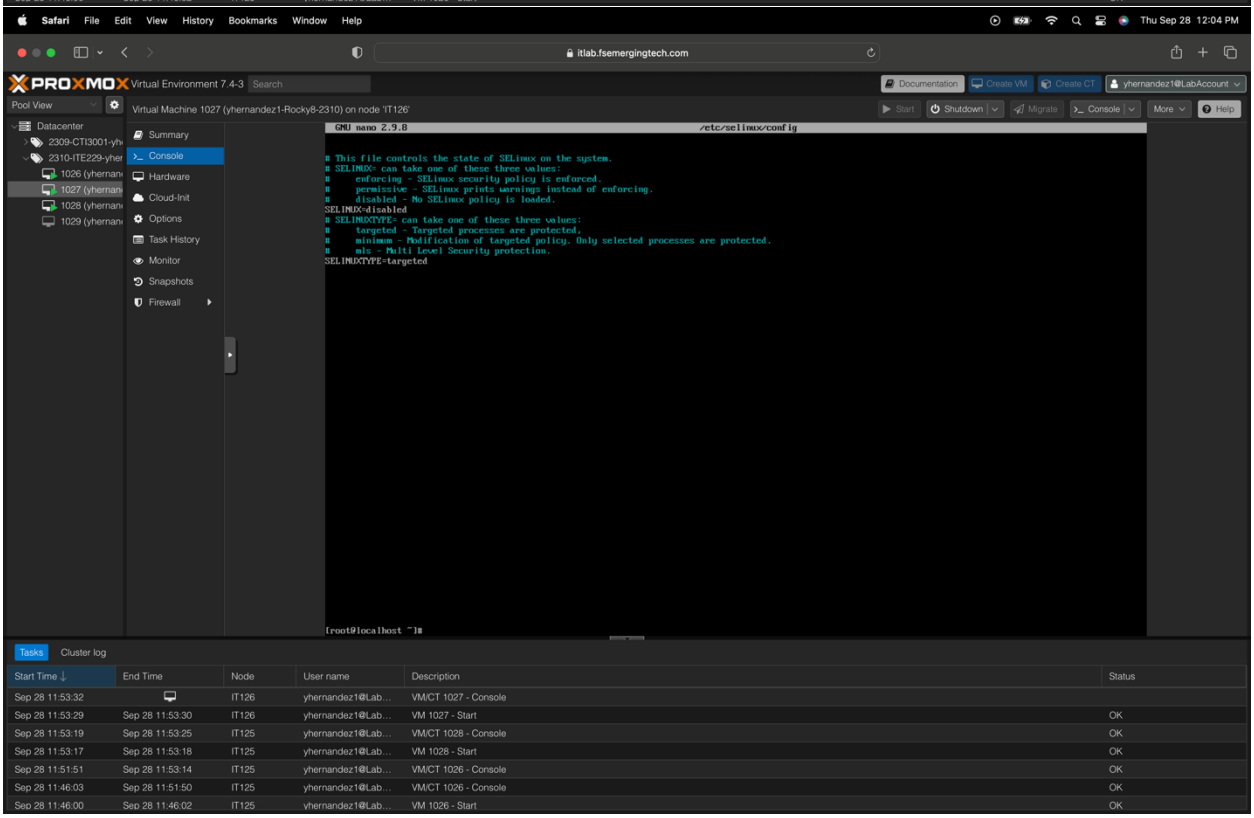
Install Nano Editor



To install nano, type on the command line **sudo yum install nano;** this will install nano to the machine.

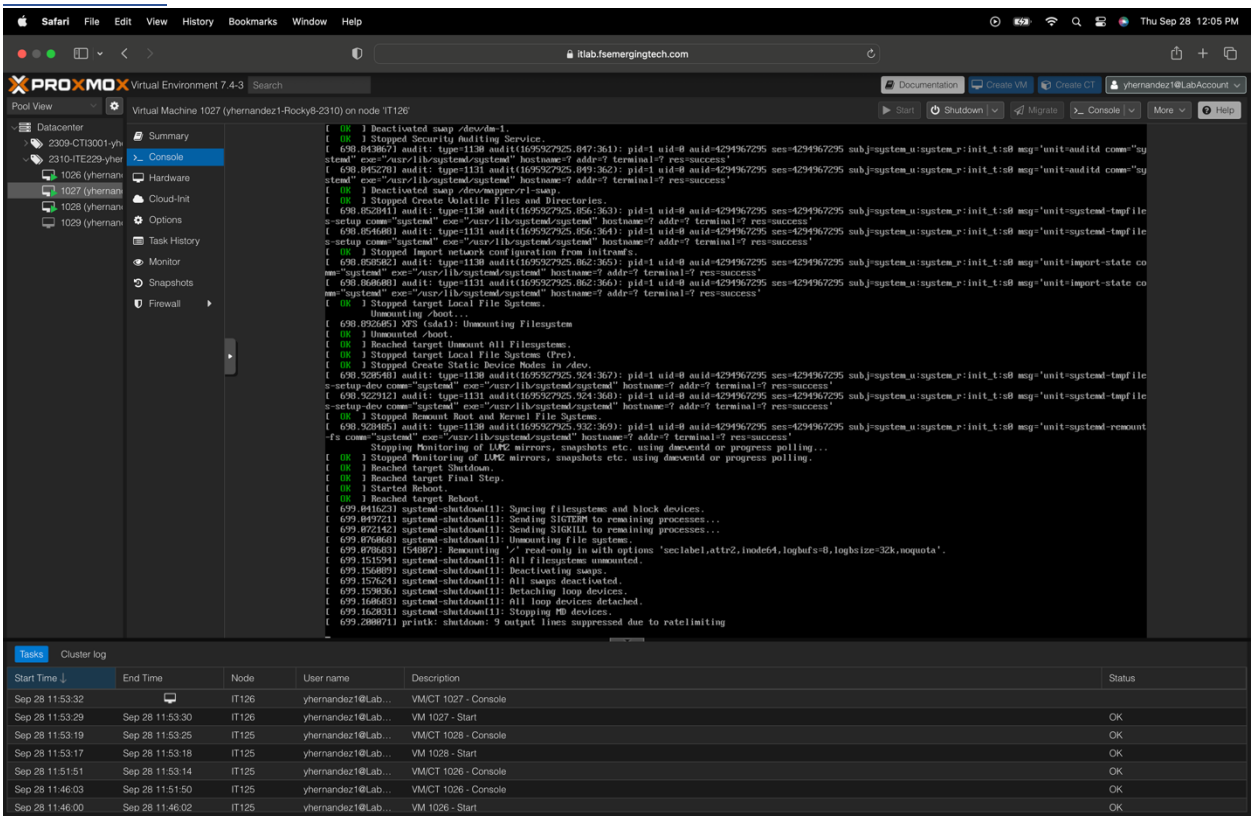
Disable SELinux





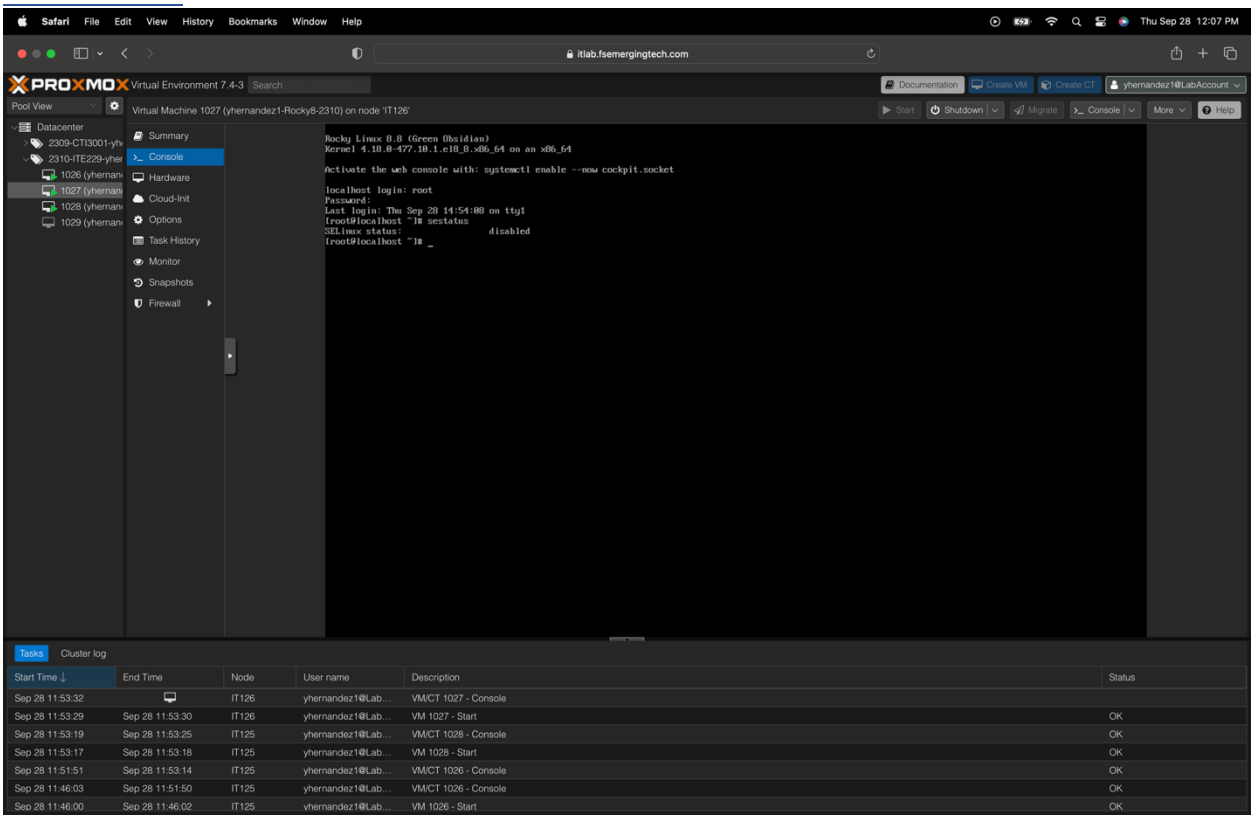
To disable SELinux on the command line, type **sudo nano /etc/selinux/config,** then scroll down to SELinux and remove enforcing and type in disabled, then press CONTROL X, and when prompted, press Y for YES then press enter, and it will take you back to the root.

Reboot VM



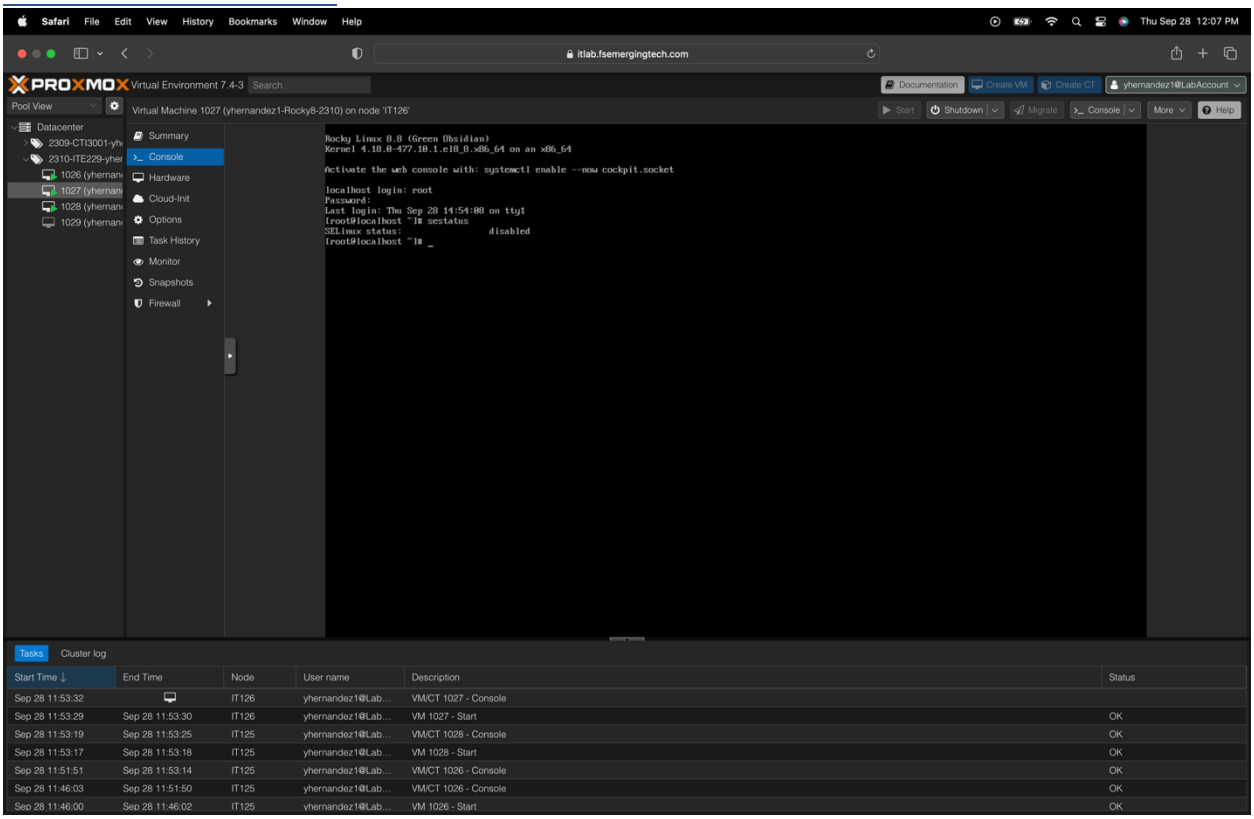
To reboot VM on the command line, type **reboot** and press enter. This will automatically reboot the system and log in with credentials again once fully rebooted.

Test SELinux



To test SELinux type on the command line **sestatus.**

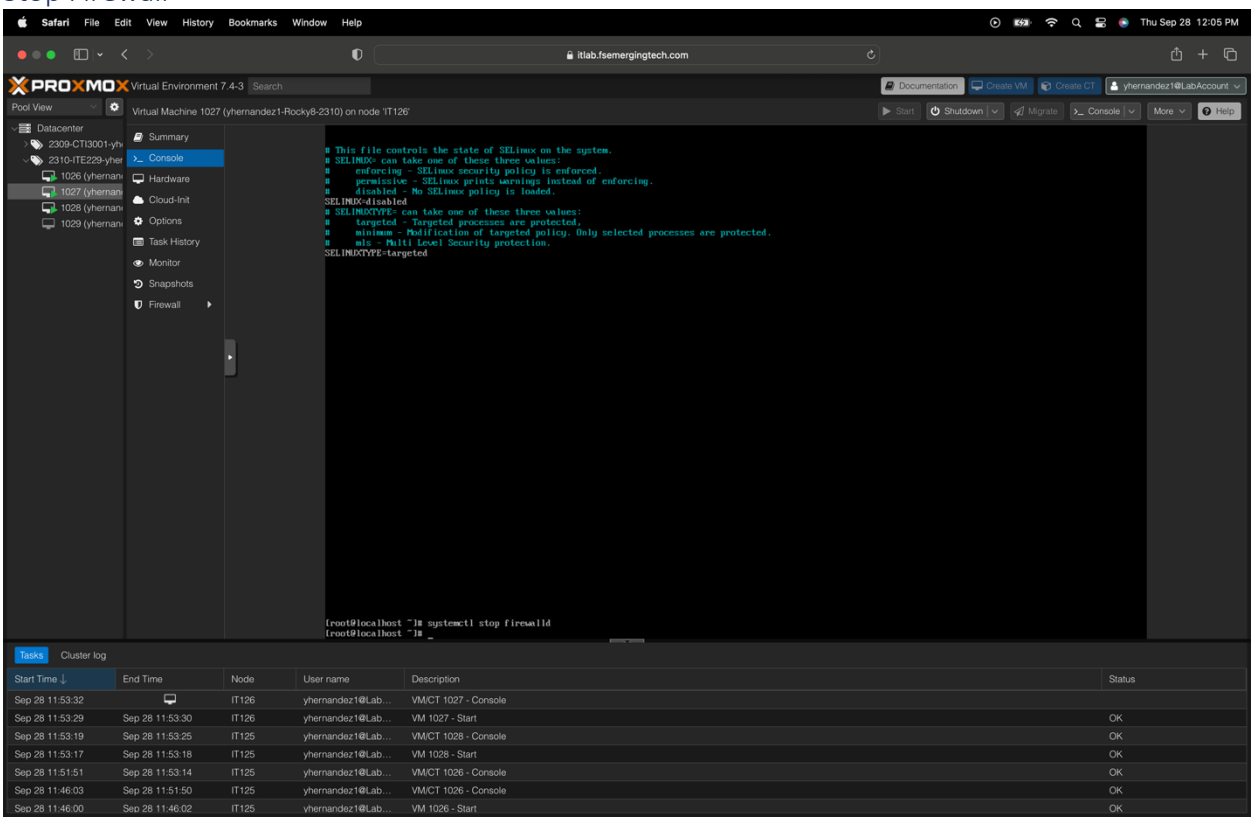
Confirm SELinux Status



To confirm SELinux status on the command line, type **sestatus.**

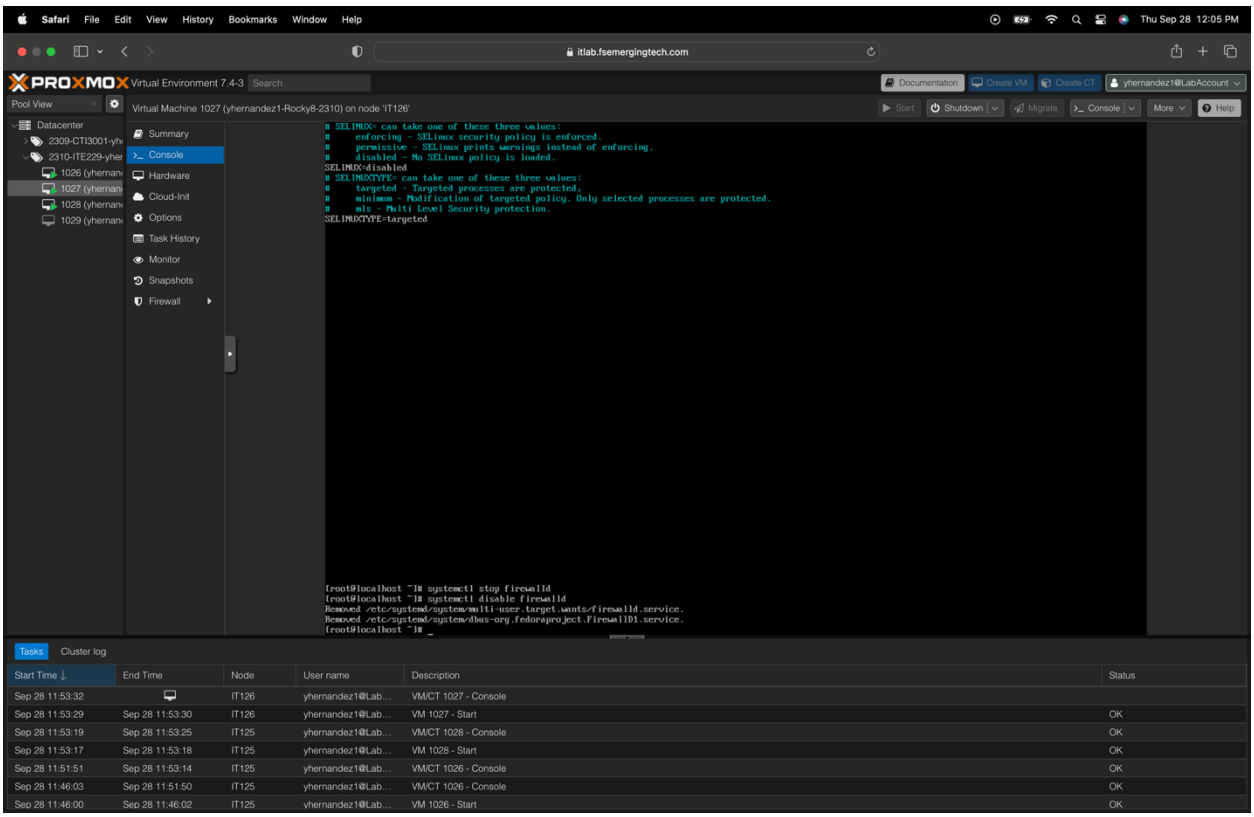
Rocky Firewall

Stop Firewall



To stop the Firewall on Rocky on the command line, type **systemctl stop firewalld,** then press enter.

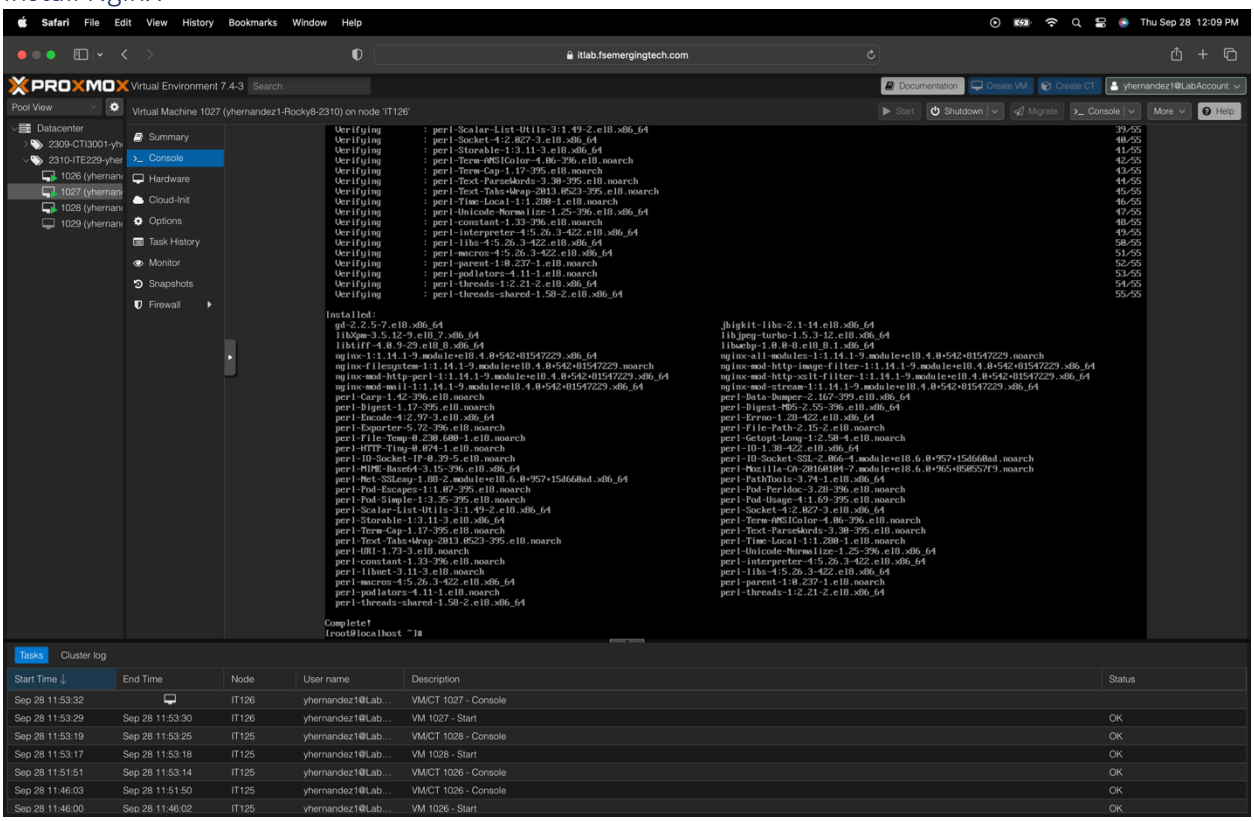
Disable Firewall



To disable the Firewall on the command line, type **systemctl disable firewalld.**

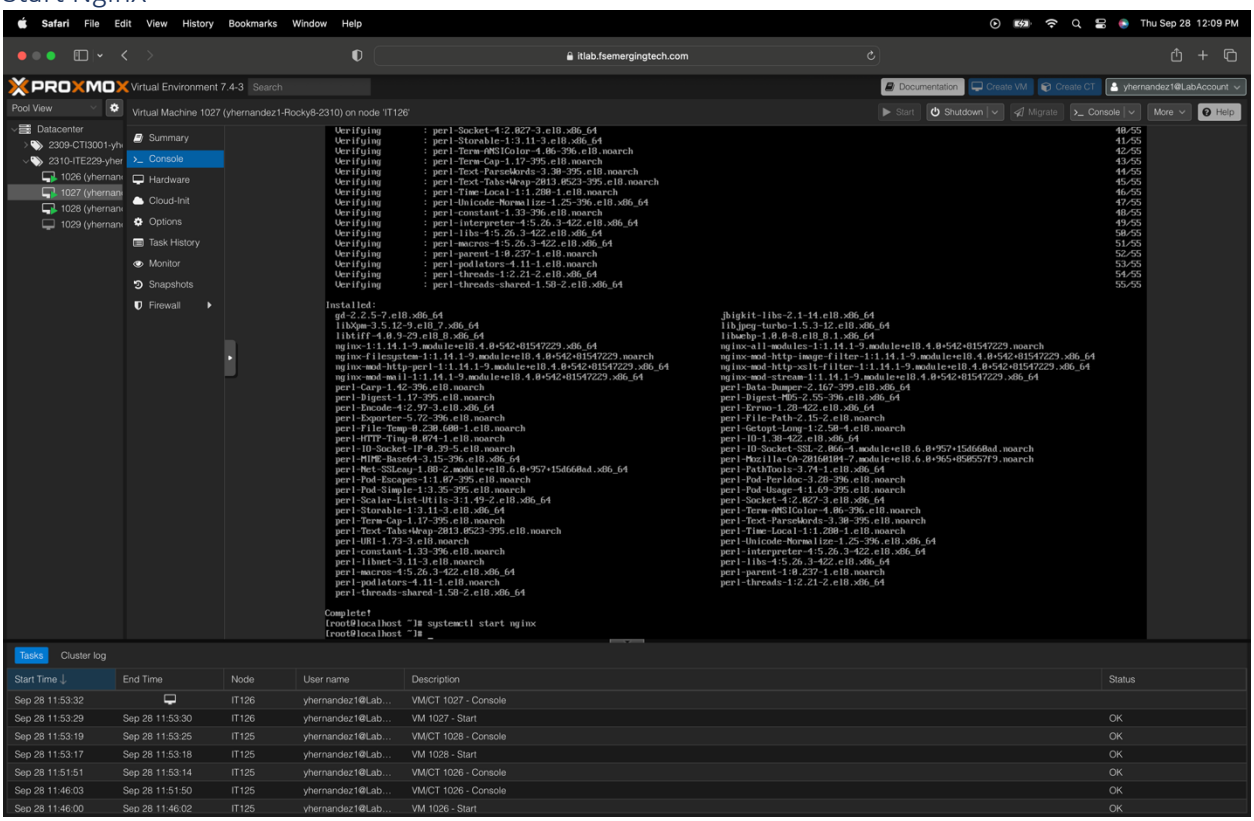
NginX

Install NginX



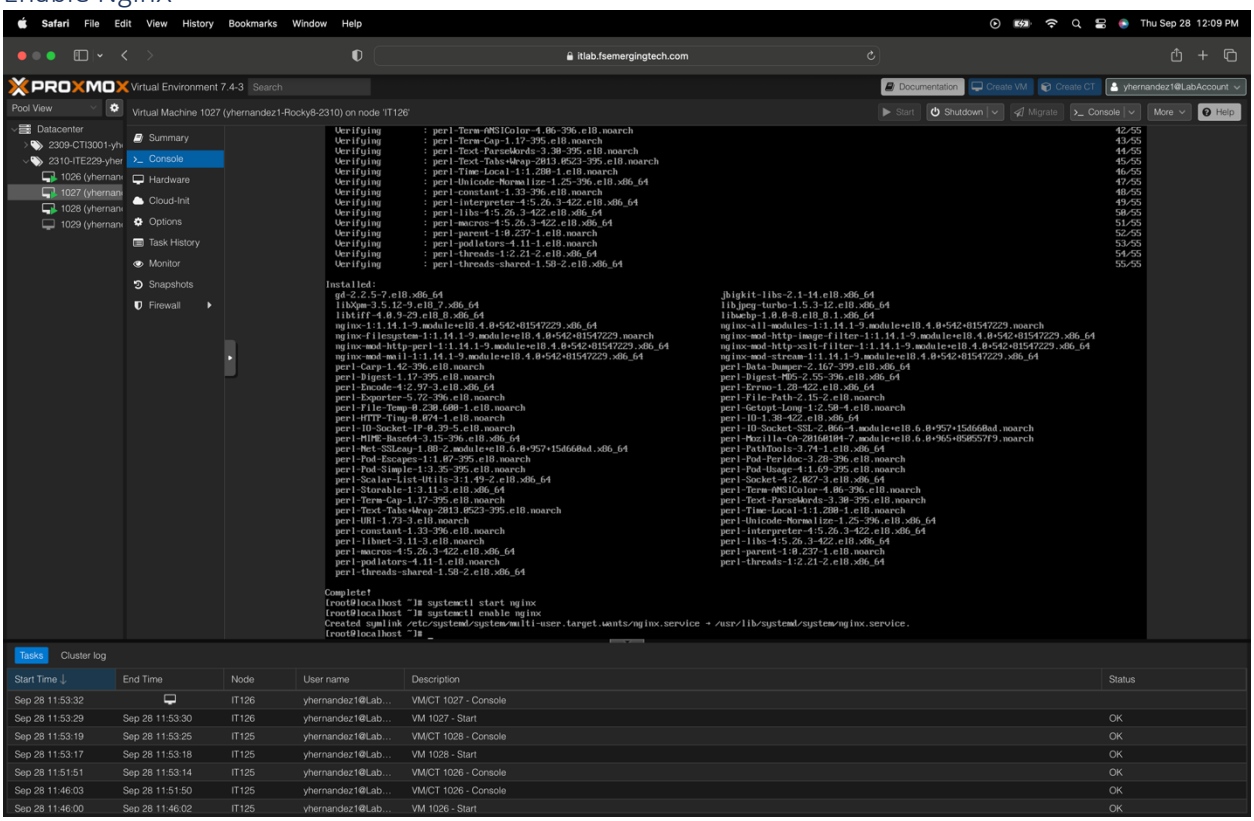
To install NginX, type **sudo yum install nginx -y** on the command line, which will automatically install NginX on your machine.

Start NginX



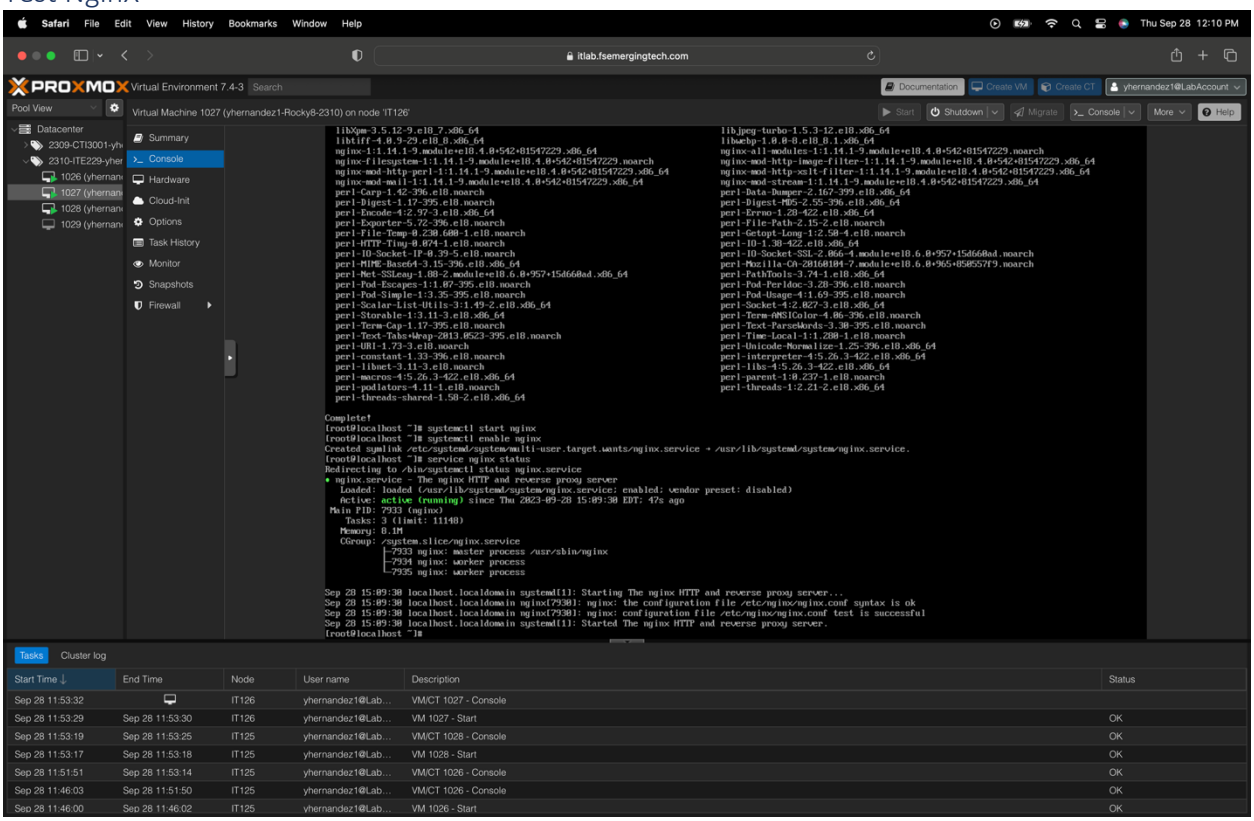
To start NginX on the command line, type **systemctl start nginx.**

Enable NginX



To enable NginX on the command line, type **systemctl enable nginx.**

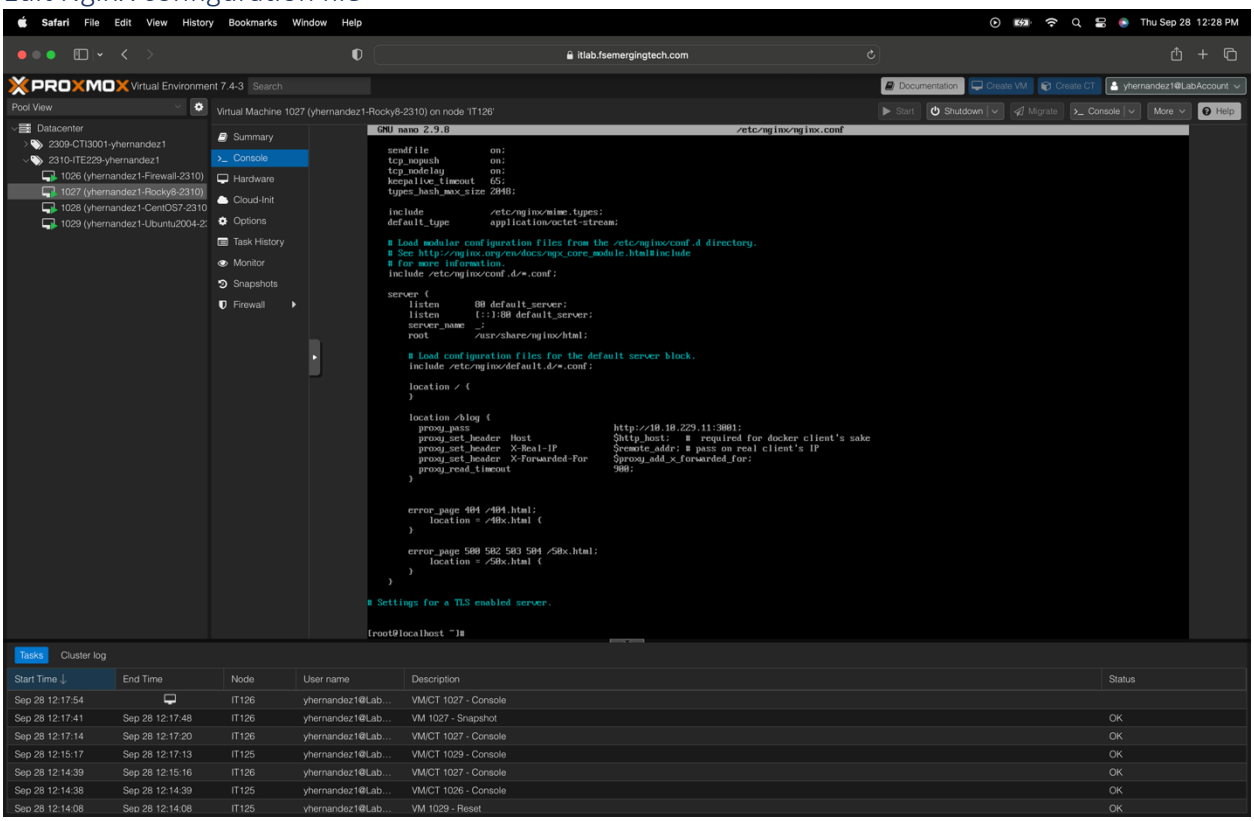
Test NginX



To test NginX on the command line, type **service nginx status.**

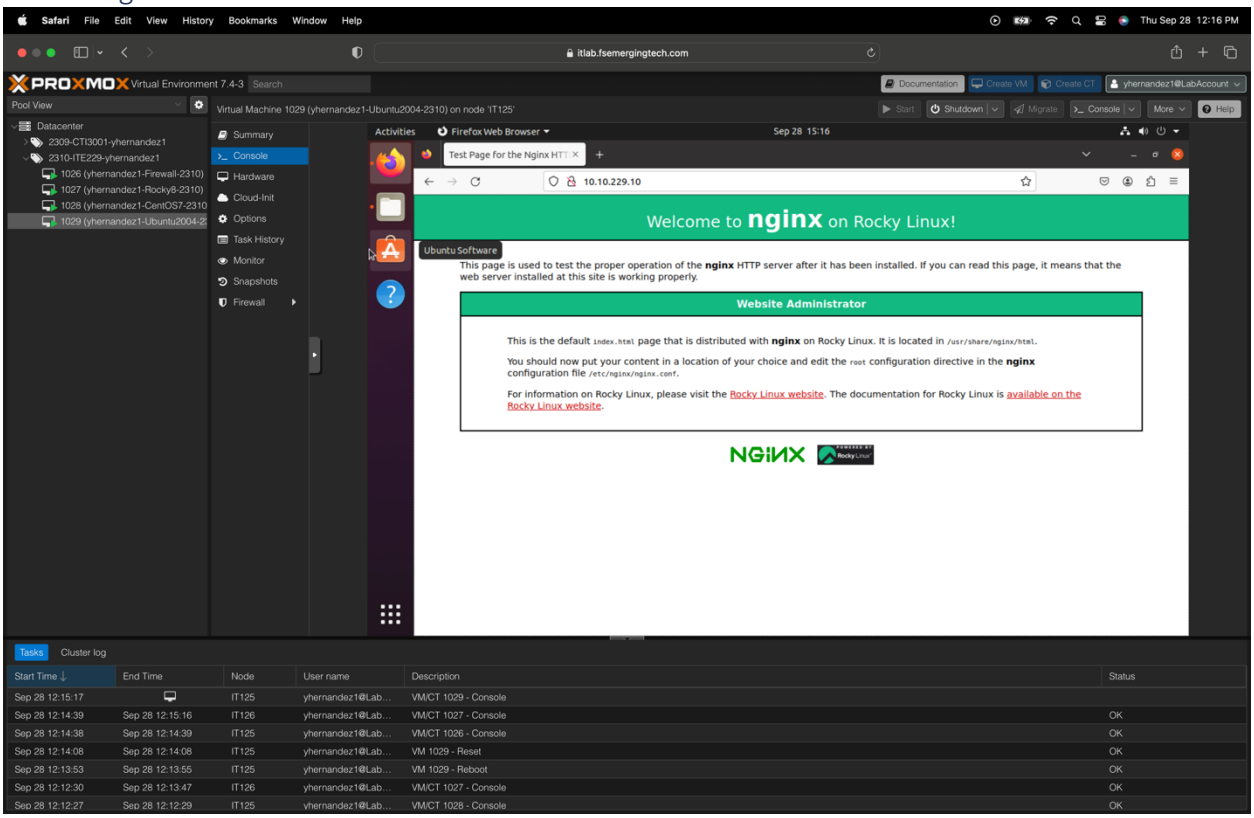
Reverse Proxy for Ghost Site

Edit NginX configuration file



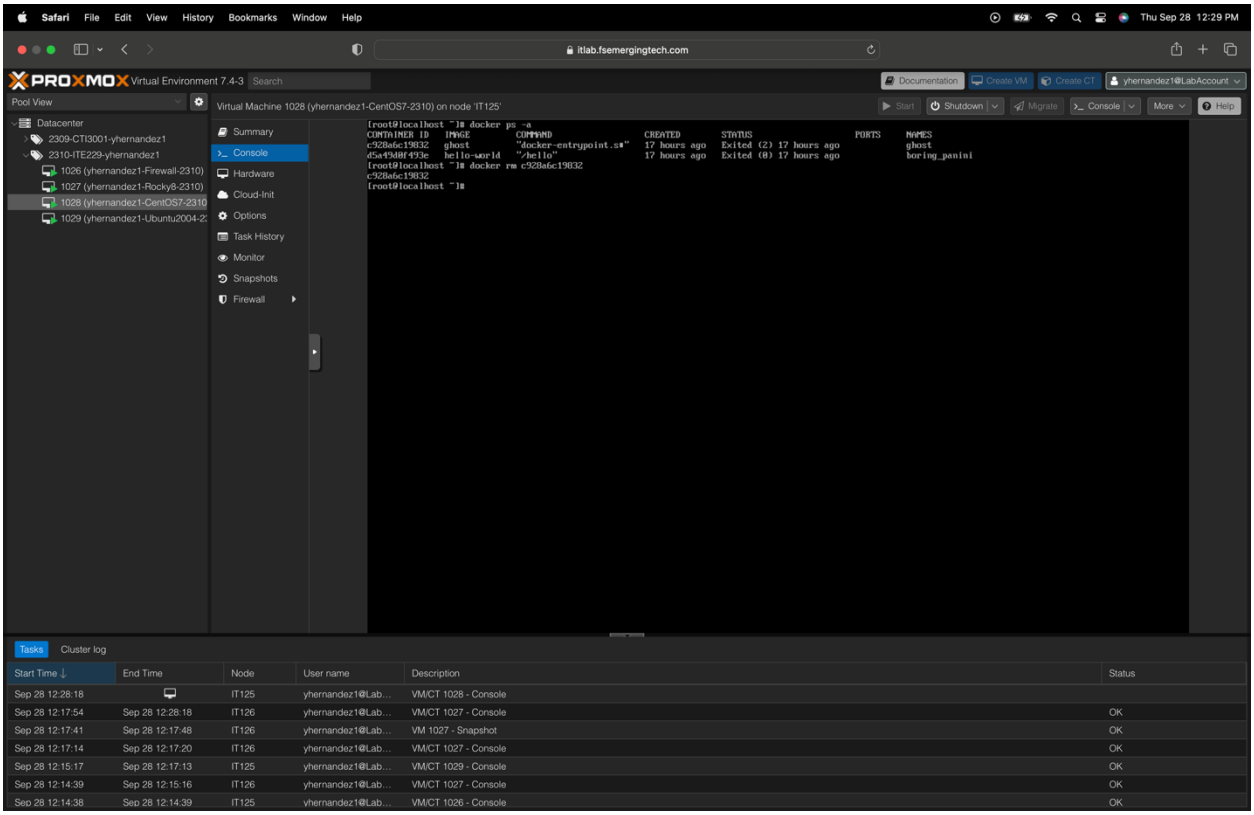
To edit the NginX configuration file on the command line, type **sudo nano /etc/nginx/nginx.conf.** This will take you to the GPU page, where you will scroll down until you find Location, and you will enter the needed reverse proxy code. Make sure everything is credited correctly.

Reload NginX service



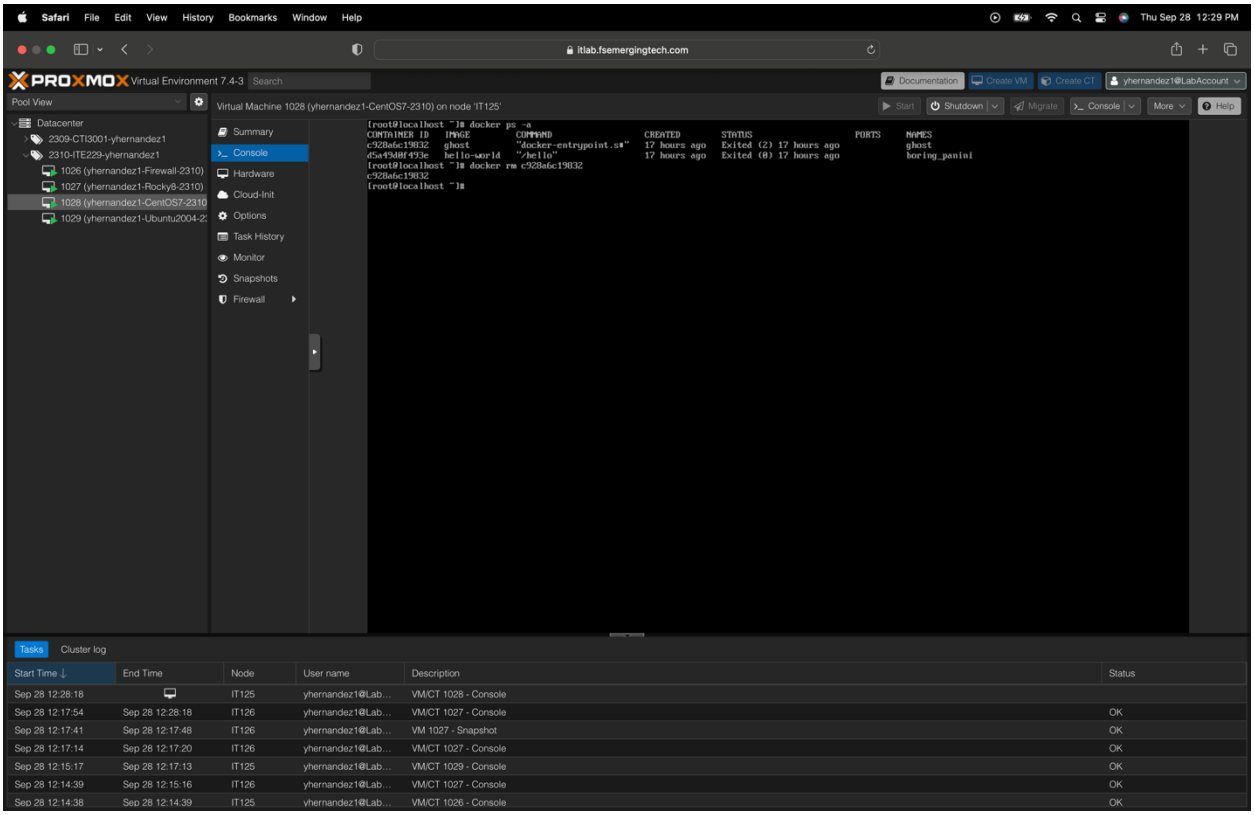
To reload the NginX service, go to the Ubuntu machine, open Firefox, and type in the address bar **10.10.229.10;** this will load the page.

Terminate Docker



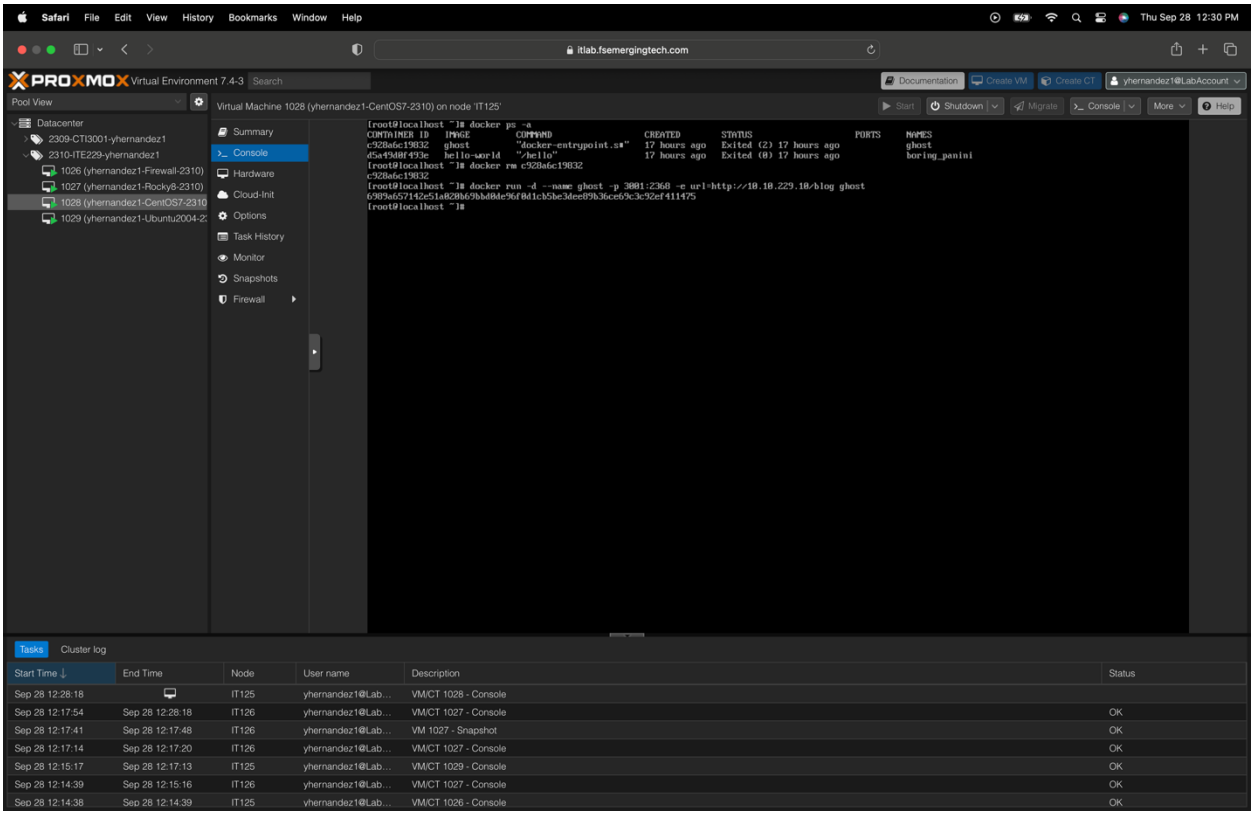
To terminate docker type in **docker rm.**

Delete Ghost Container



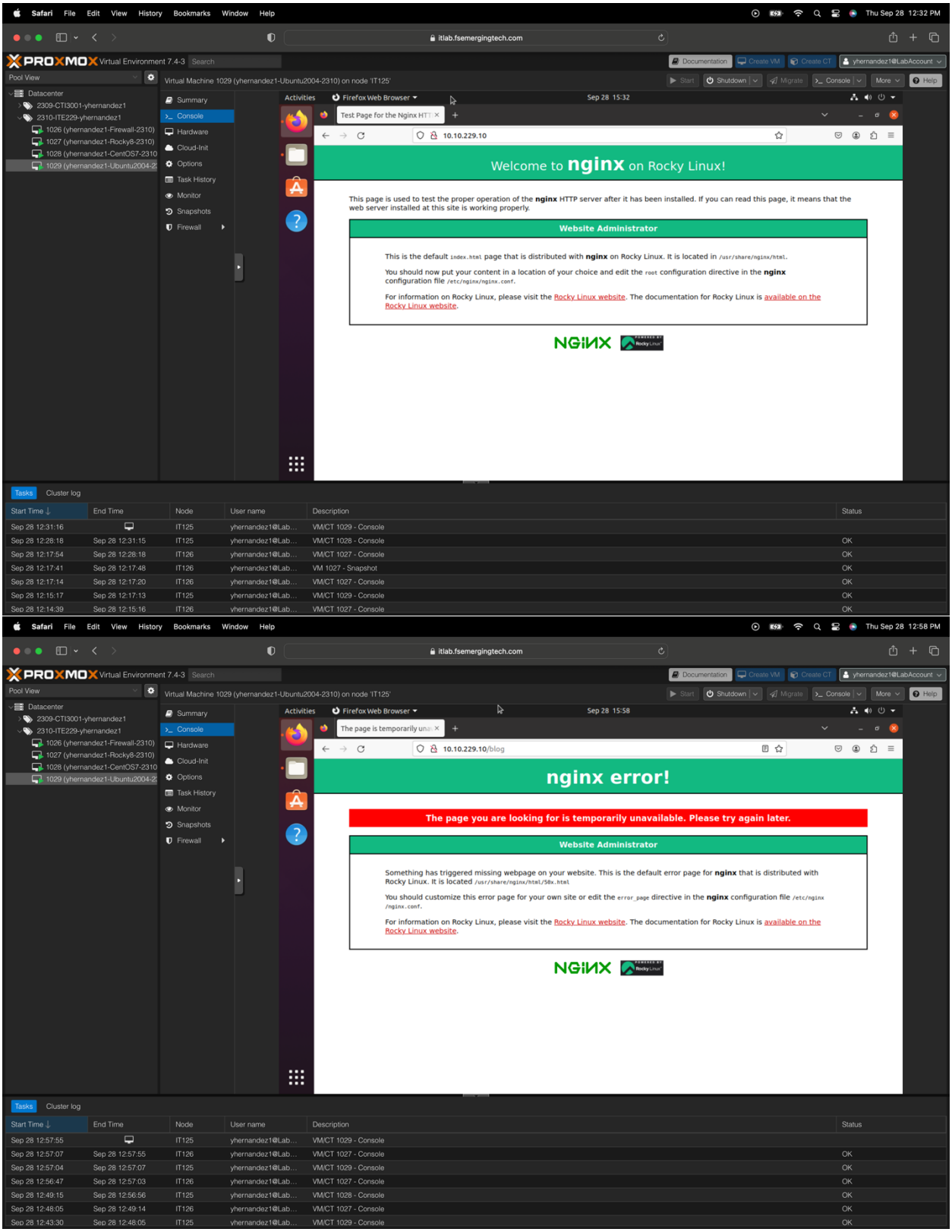
To delete the Ghost container on the command line, type **docker rm (container ID).**

Create New Ghost Container



To create a new Ghost container on the command line, type **docker run -d --name ghost 3001:2368 –e url=http://10.10.229.10/blog ghost.**

Browse to Ghost

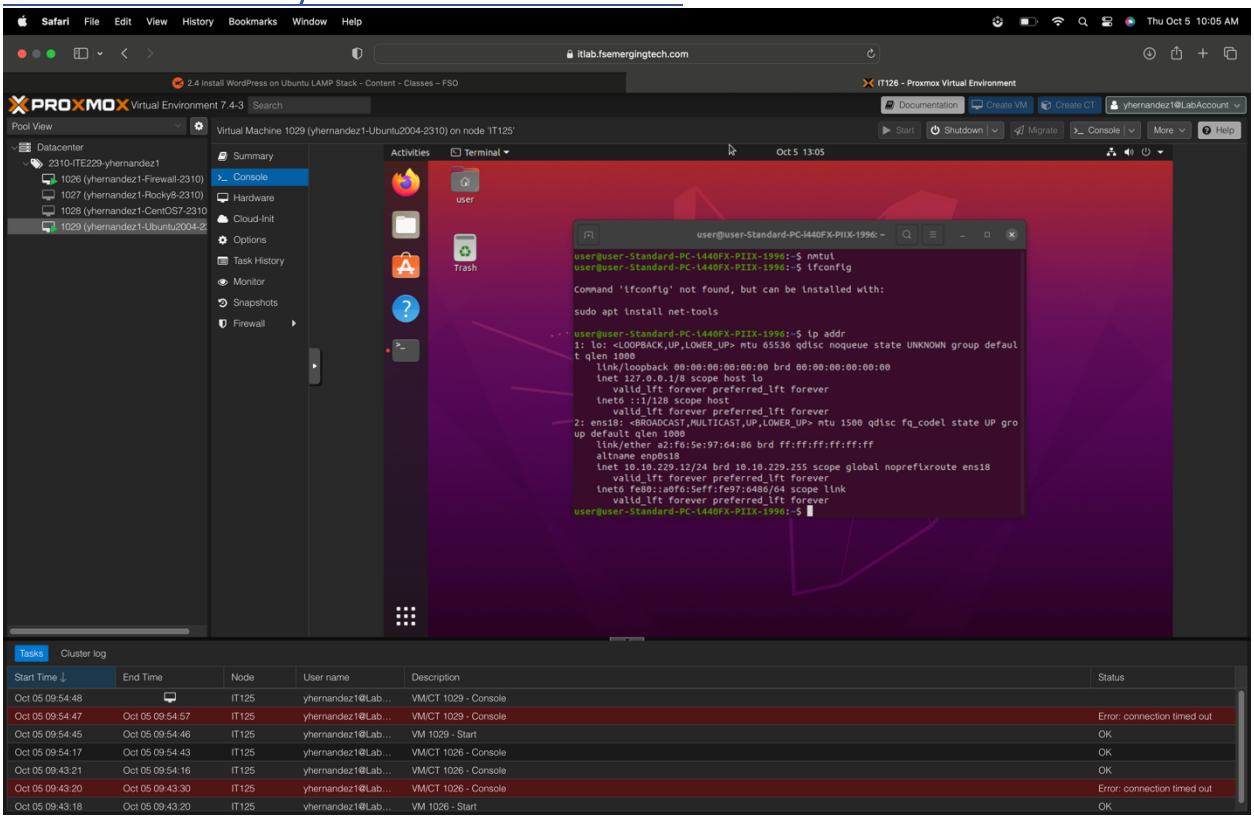


To browse to ghost log in to the Ubuntu machine, open up Firefox and type on the address bar **http://10.10.229.10,** then press enter, and once it loads, type on the address bar **http://10.10.229.10/blog.**

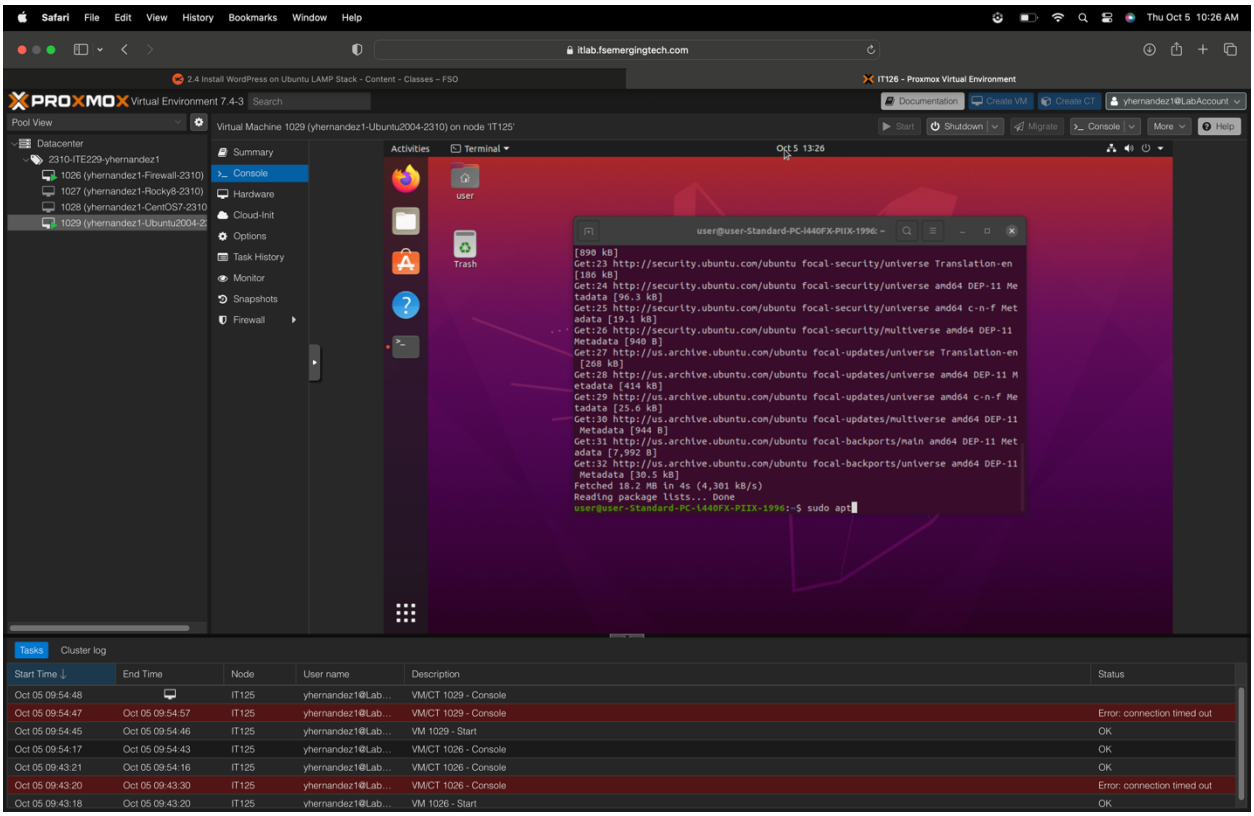
IMPORTANT: To earn full credit, ALL screenshots must include a “full view”, including your ProxMox title bar with your username showing.

WordPress on Ubuntu - LAMP Stack

Show screenshot of your Ubuntu Console in VE

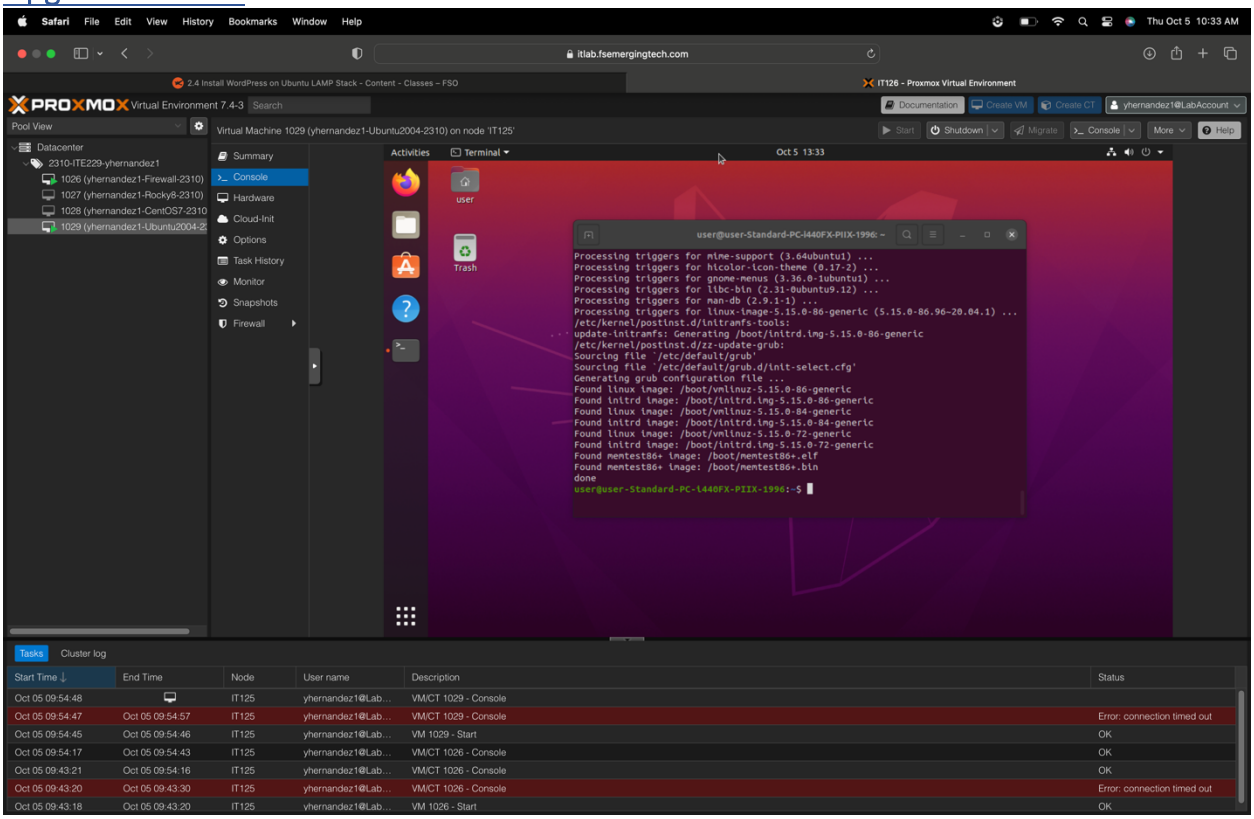


Update Ubuntu



To update Ubuntu, you type on the terminal **sudo apt-get update,** and then it will update.

Upgrade Ubuntu

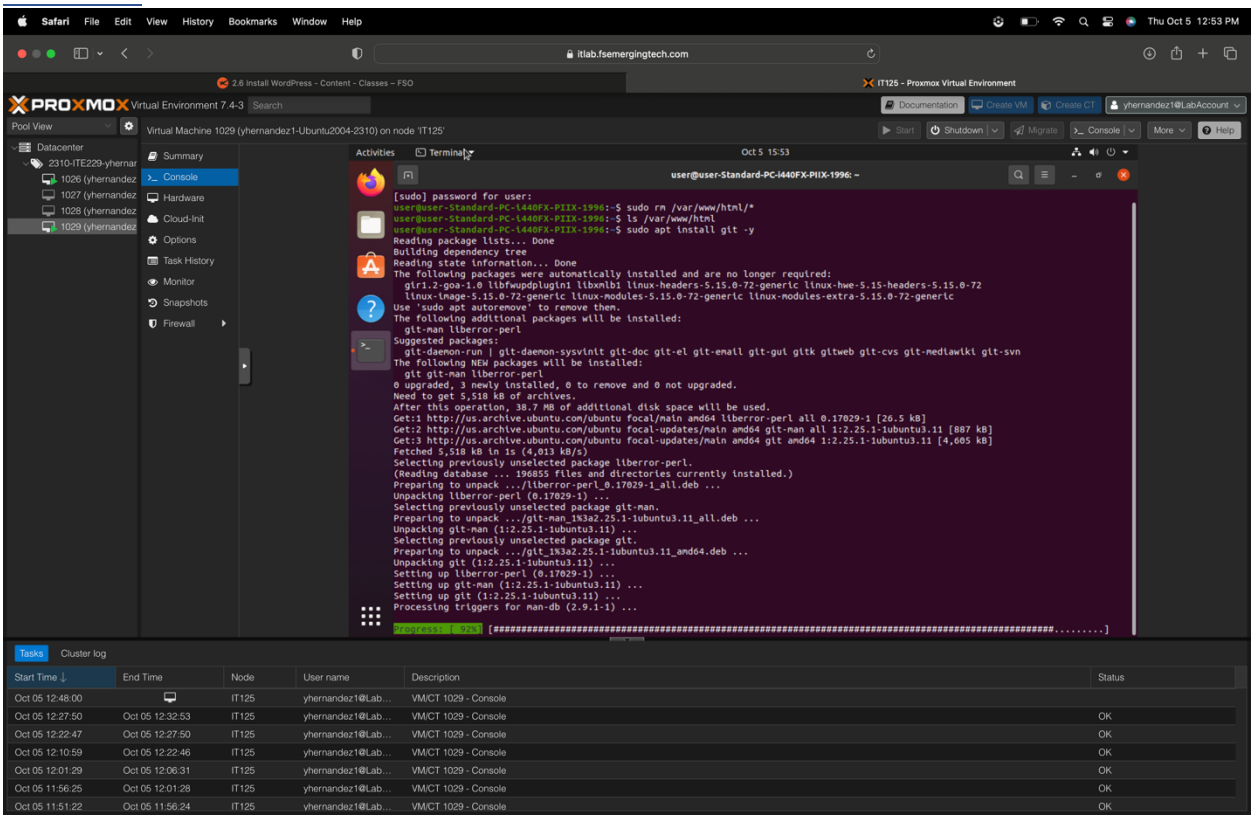


To upgrade Ubuntu on the terminal, you type **sudo apt upgrade,** then press enter, and it will upgrade.

Install Nano Editor

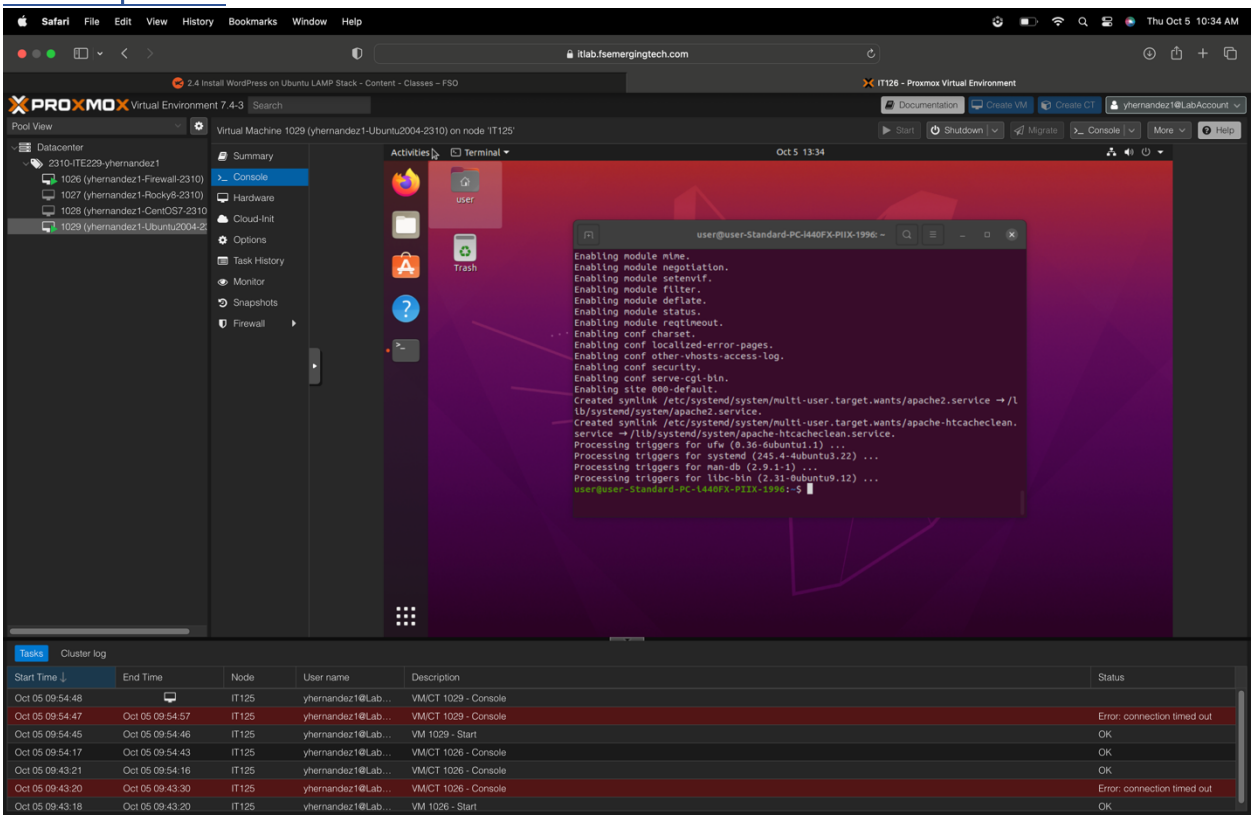
Nano was installed already.

Install Git



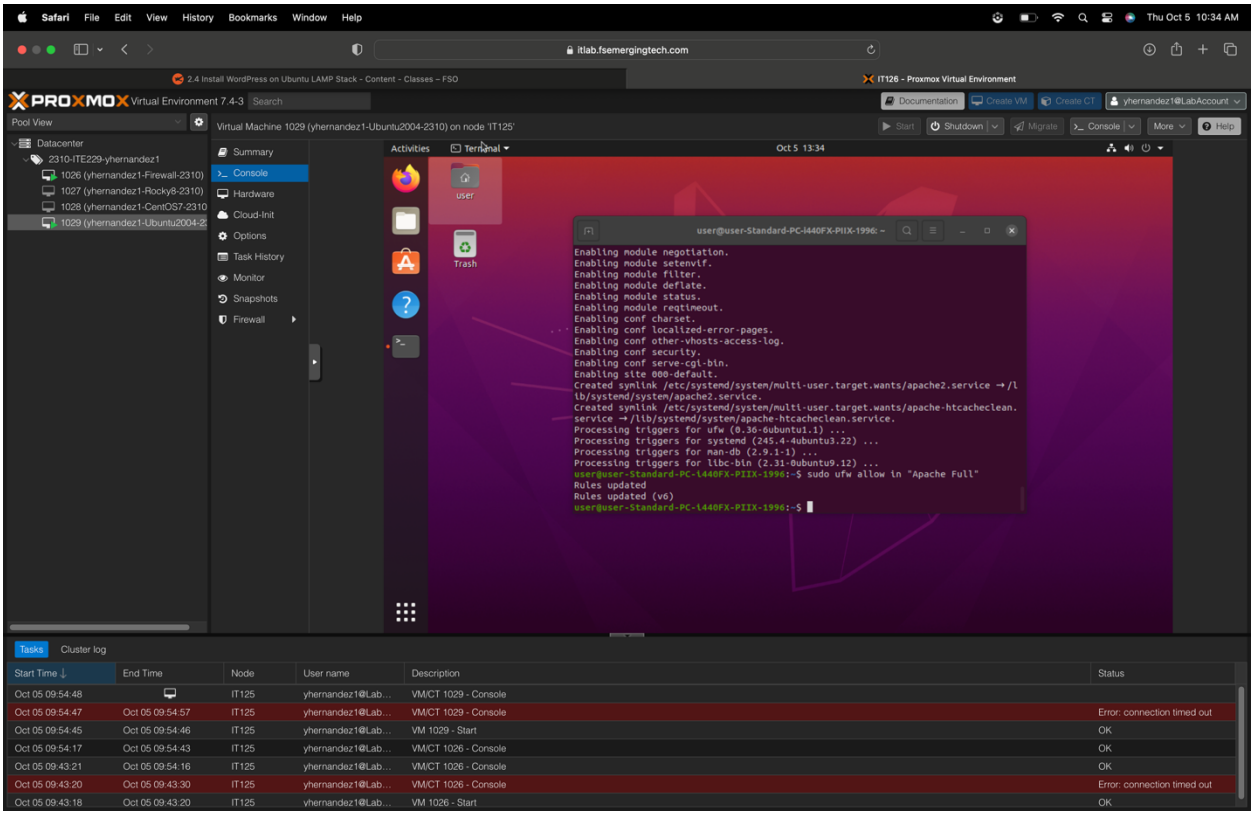
To install Git, you type **sudo apt install git -y;** this will automatically install Git.

Install Apache2



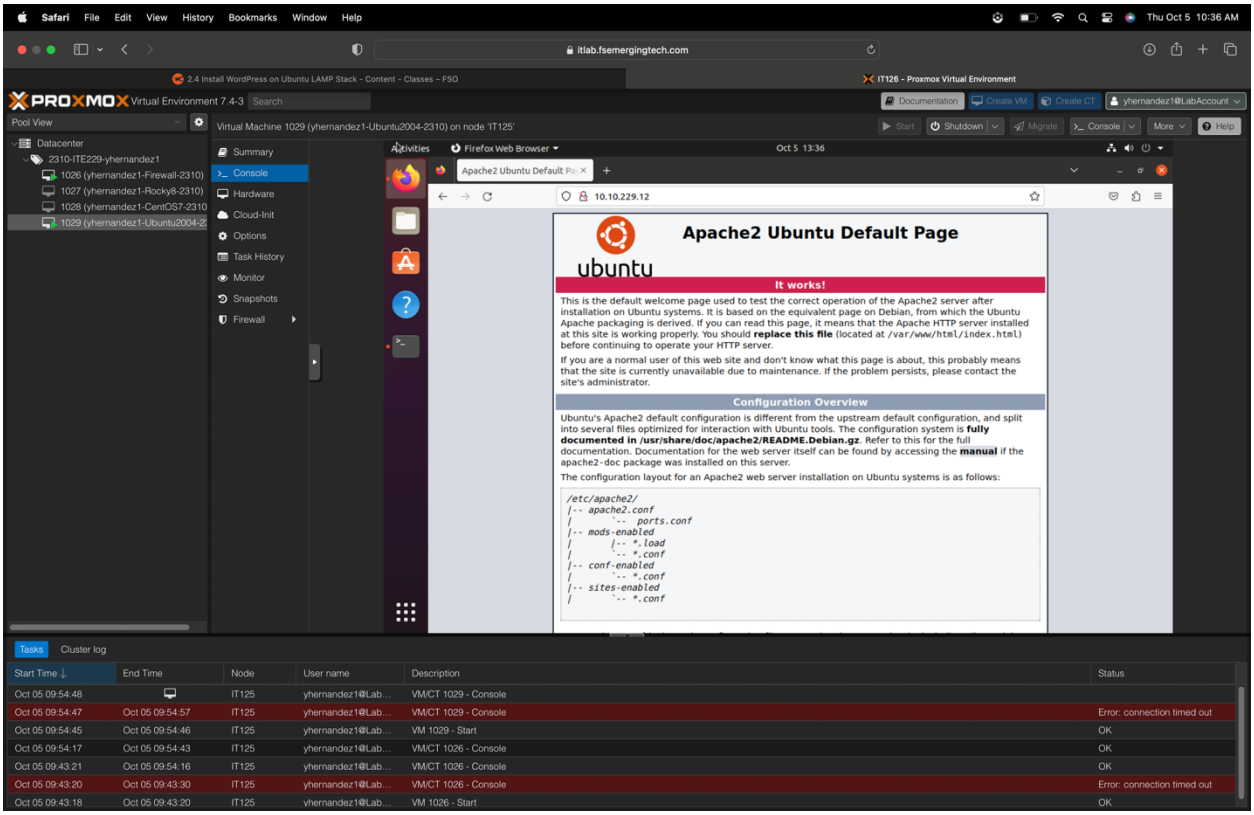
To install Apache2 on the terminal, type **sudo apt install apache2,** then press enter.

Open Firewall Ports 80 and 443



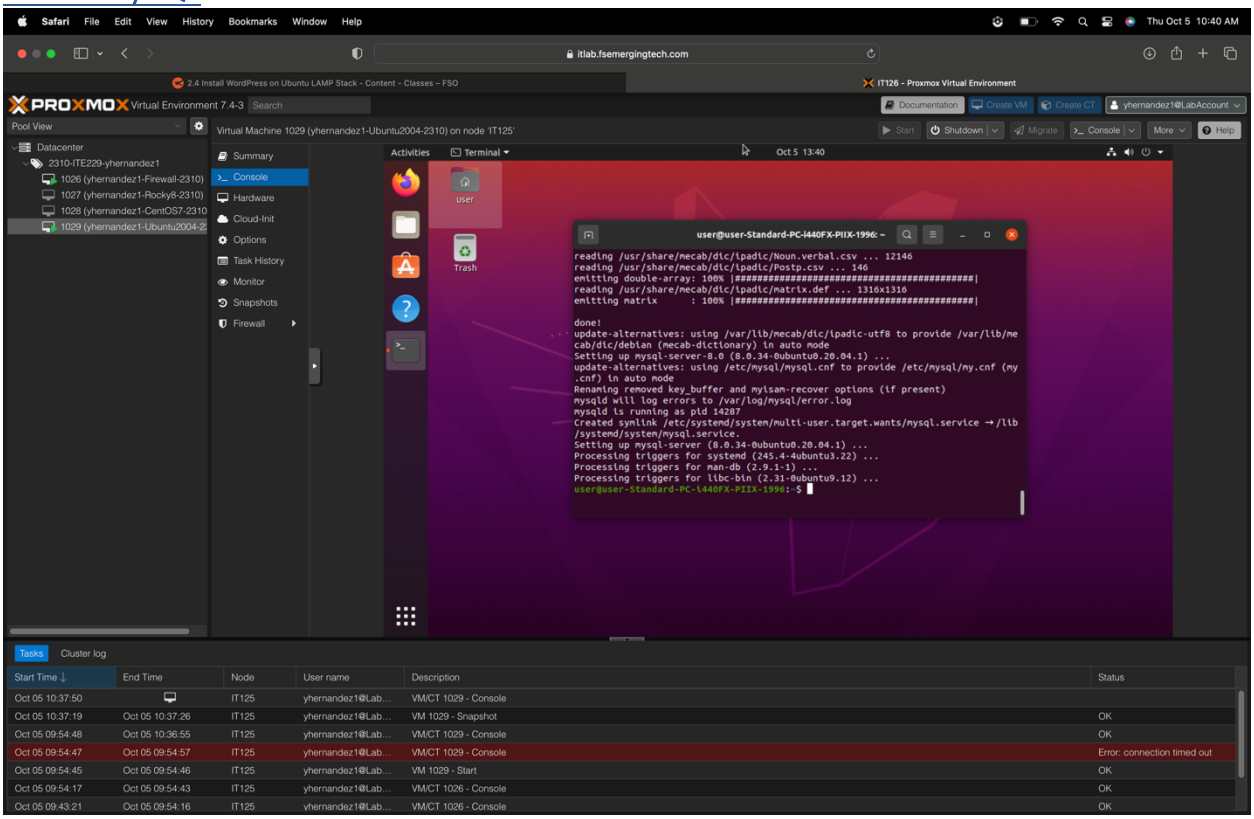
To open Firewall Ports 80 and 443 on the terminal, type **sudo ufw allow in “Apache Full”** then press enter to ensure it's correctly spelled with quotations and uppercase included.

Browse to Apache2 Ubuntu Default Page



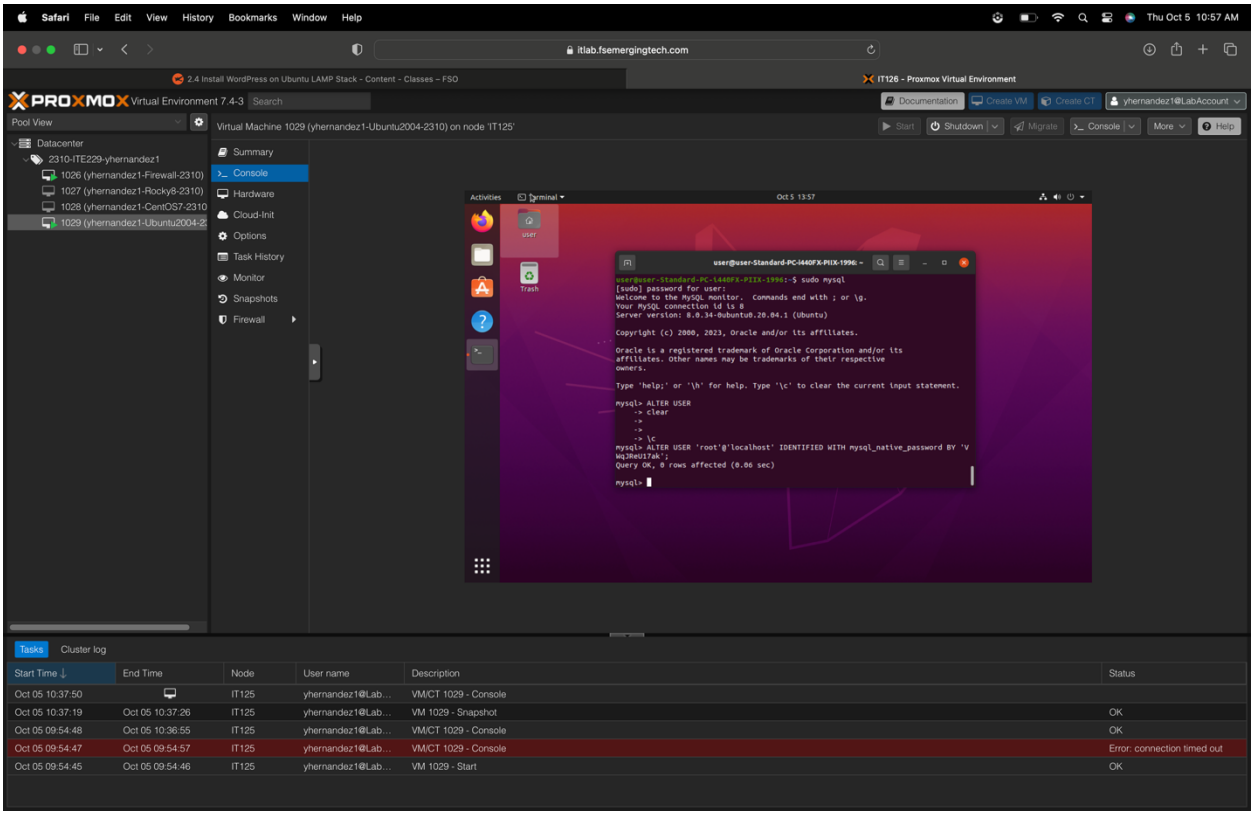
To browse the Apache2 Ubuntu Default Page, click on Firefox browser, and on the address bar, type **http://10.10.229.12.** Press enter, and it will take you to the default page.

Install MySQL



To install MySQL, we type **sudo apt install mysql-server** on the terminal and type enter.

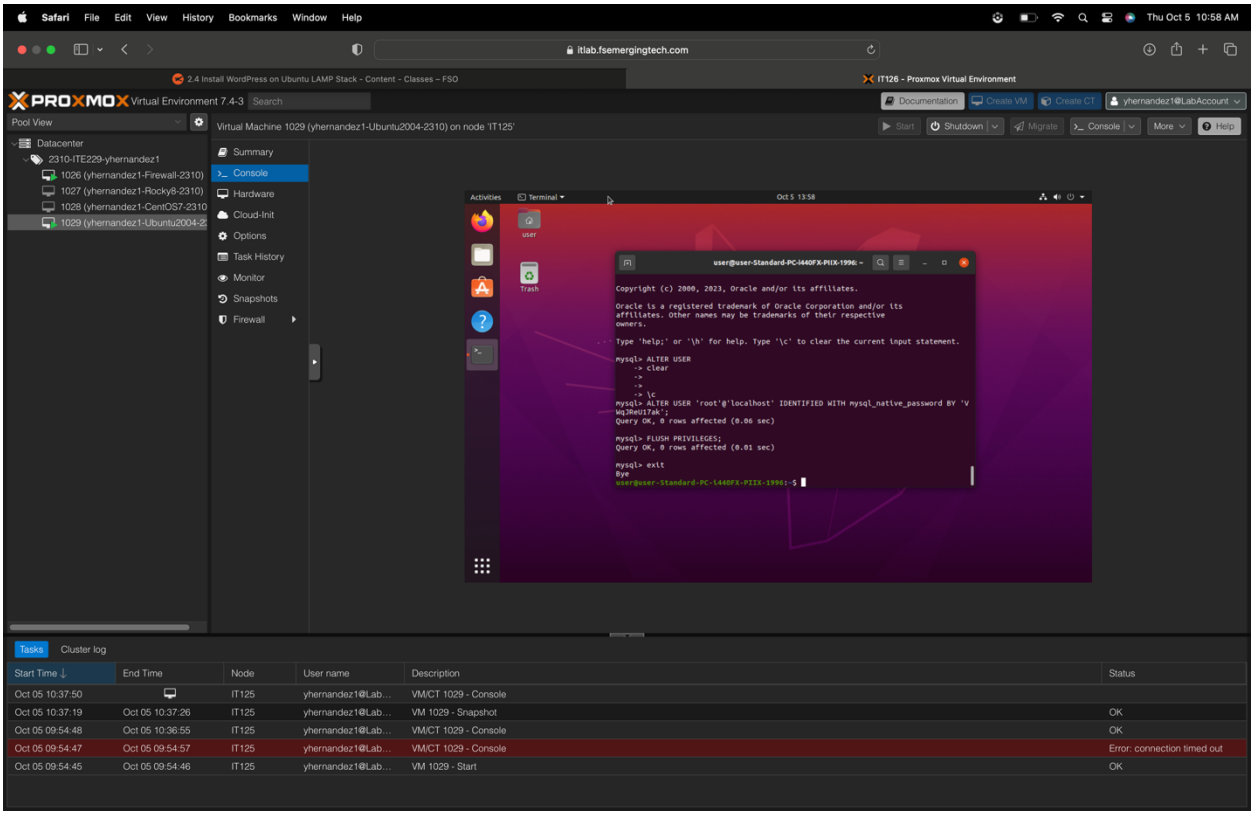
Alter root user password



To alter the root user password, you must load the MySQL CLI; therefore, you type **sudo mysql,** then press enter MySQL will show up. By this time, we had created a password through a website or on our own. Then we will type **ALTER USER** (in uppercase) **'root'@'localhost' IDENTIFIED WITH** (in uppercase) **mysql_native_password BY '**[add password]**';** then press enter.

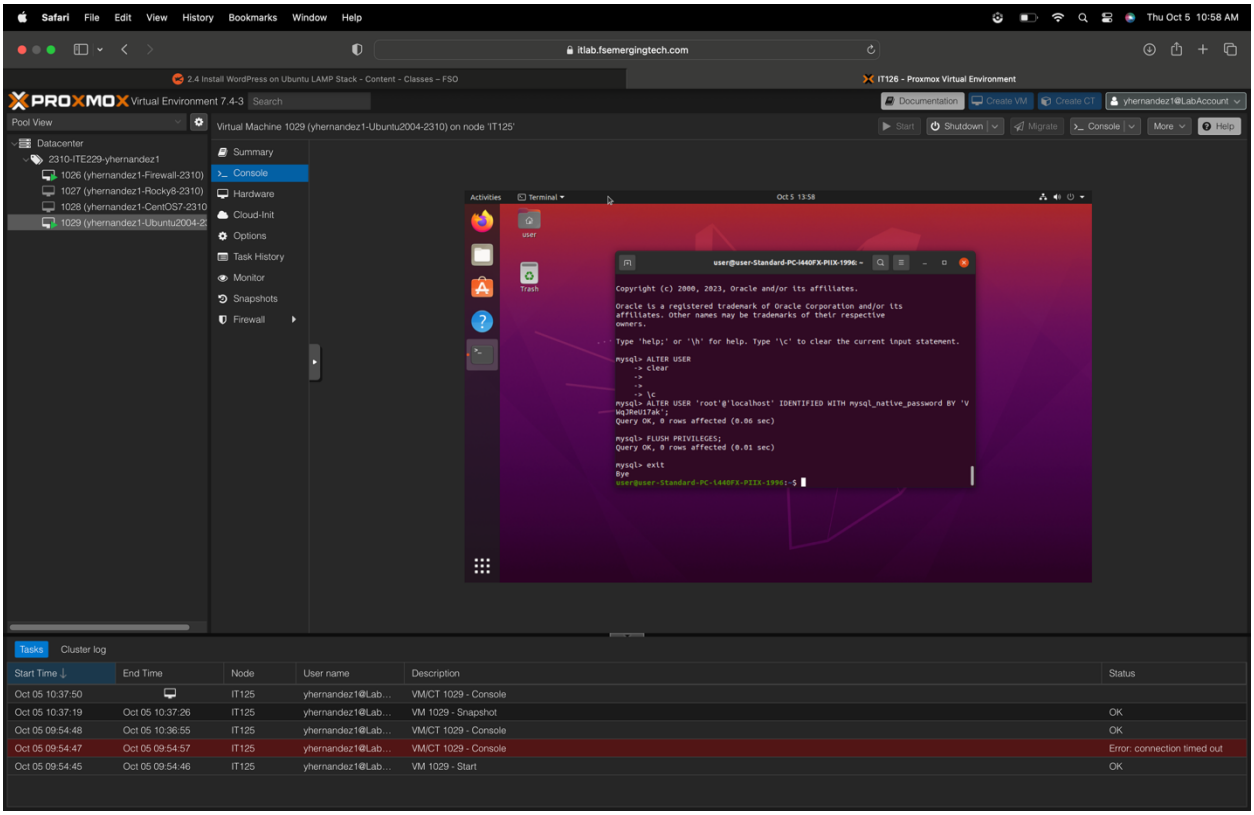
NOTE: Document root user password in table at top of document.

Flush Privileges



To flush privileges, type **FLUSH PRIVILEGES** on the command line**,** then enter.

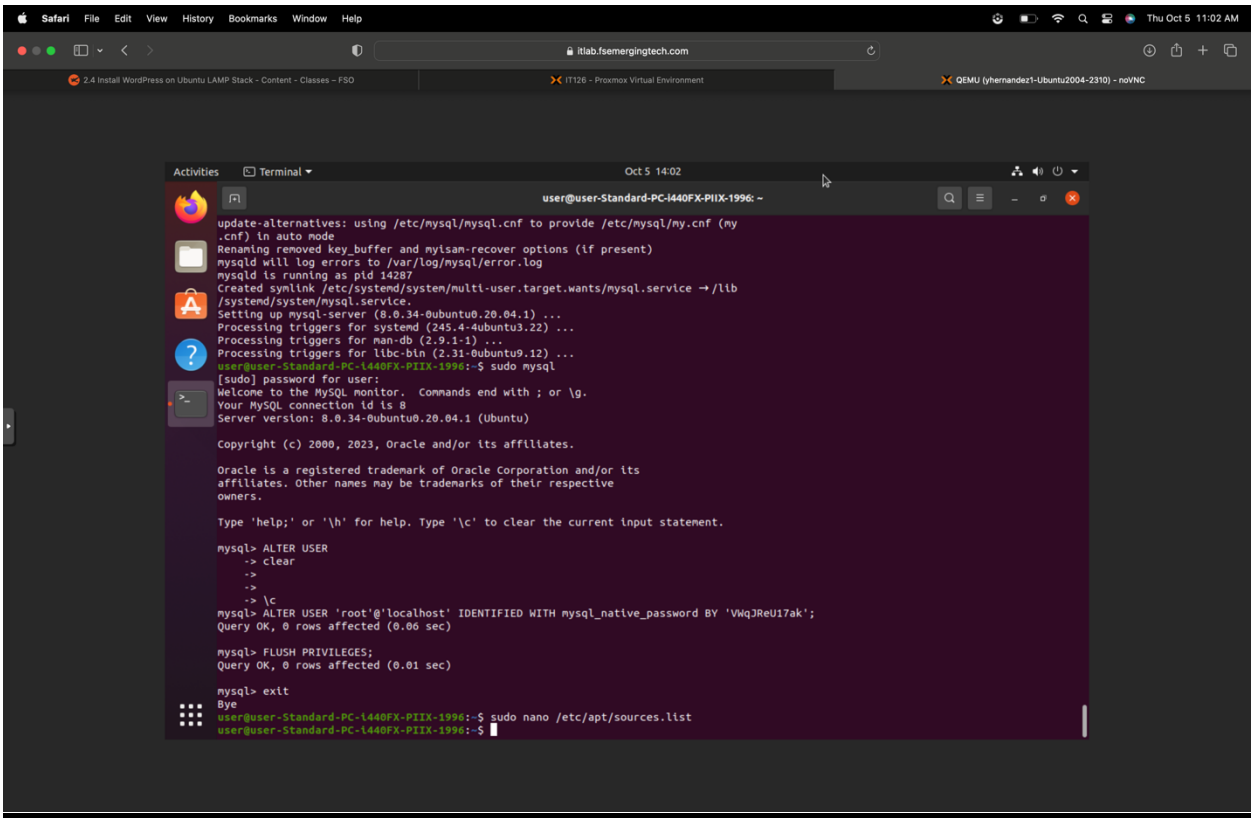
Quit MySQL

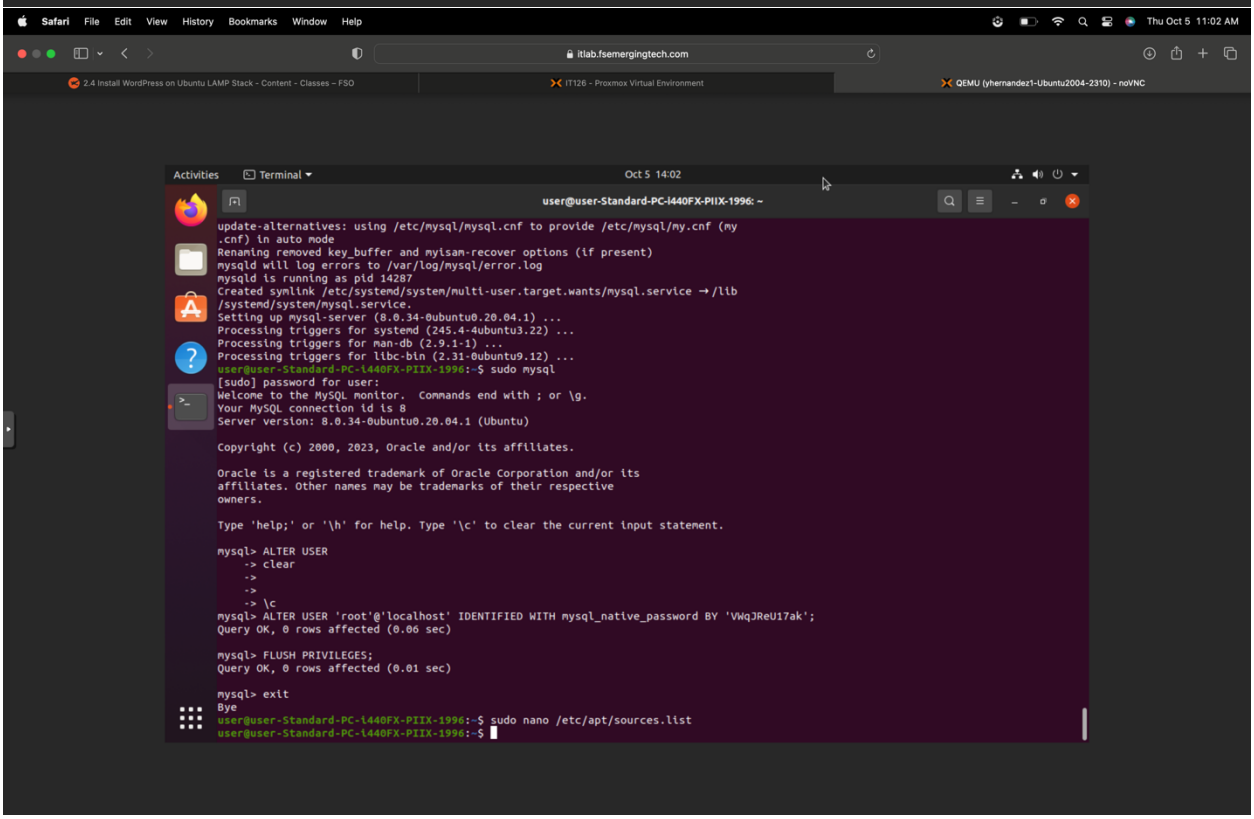


To quit MySQL, you type **exit** and then enter. This will exit you out of MySQL.

Install PHP

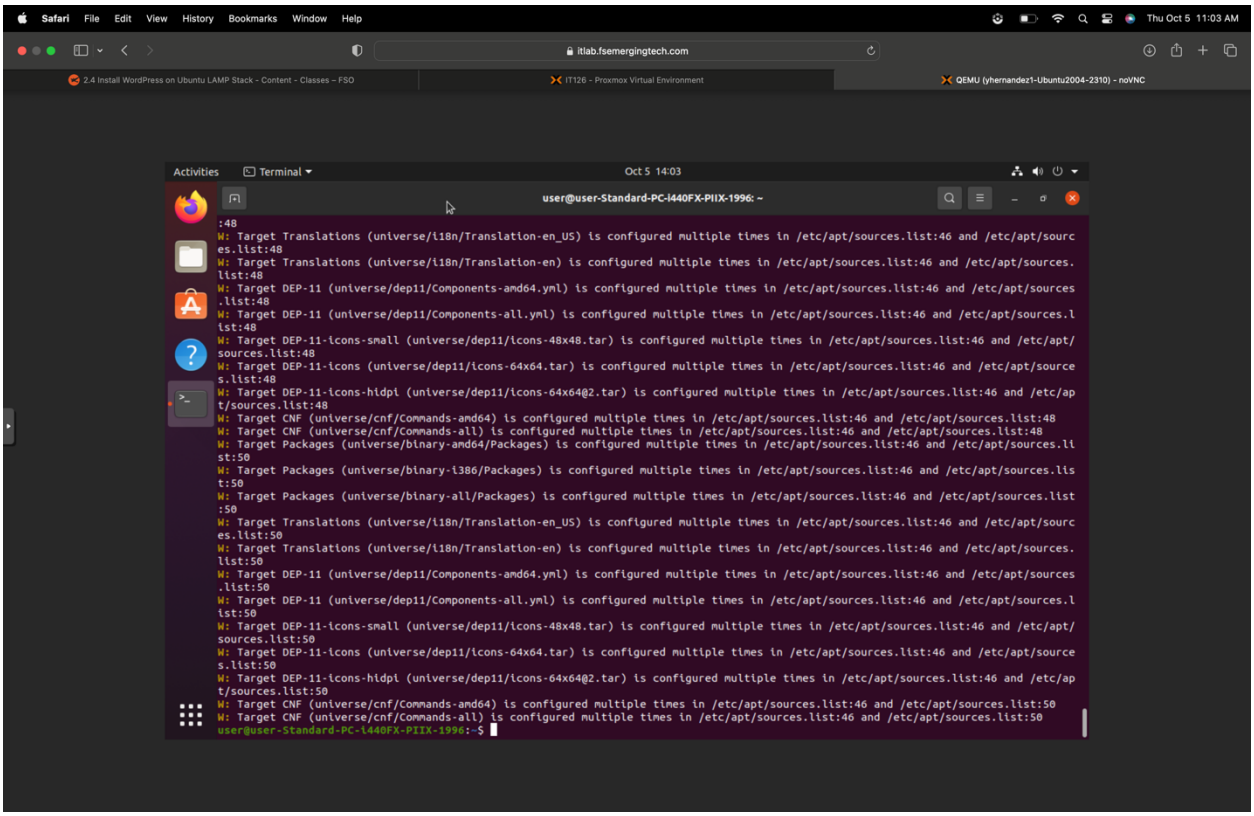
Edit Sources.list File





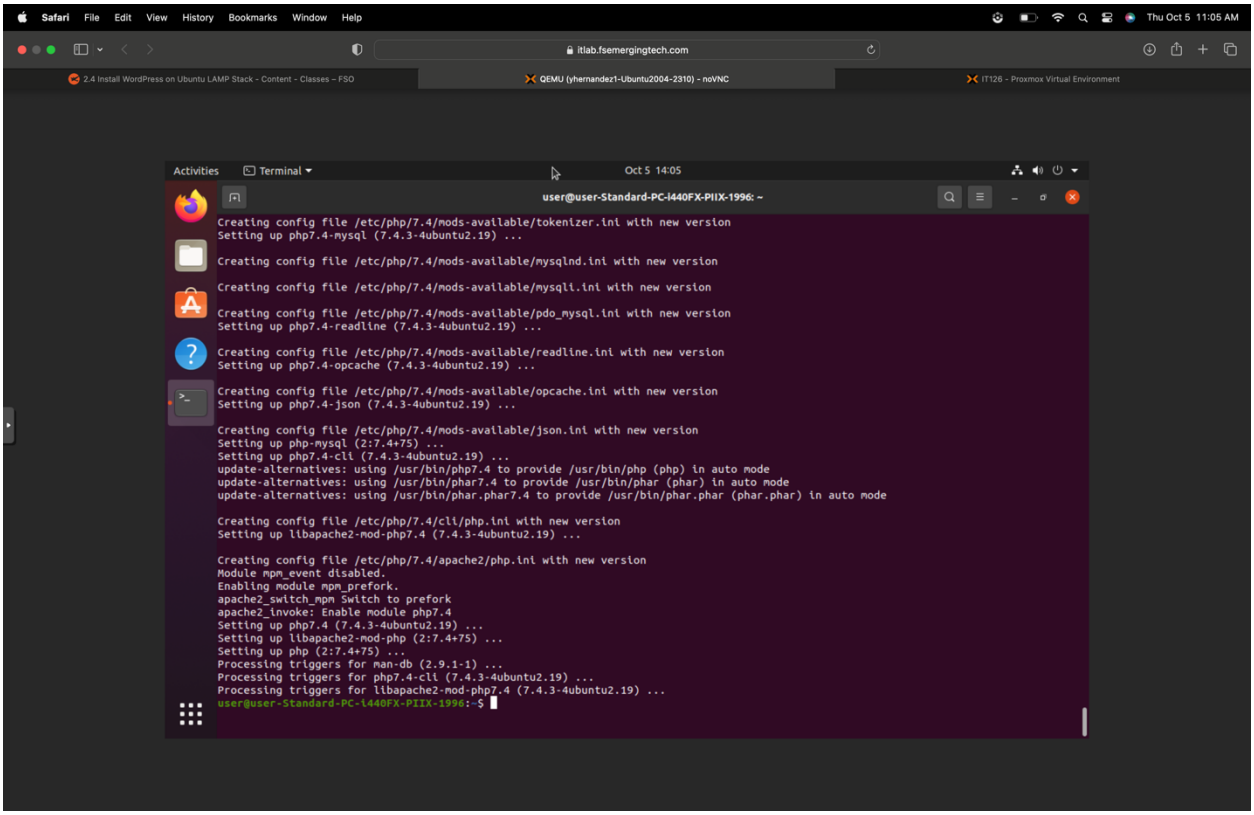
Add “universe” to all URLs

Update Ubuntu (refreshes the repolist)



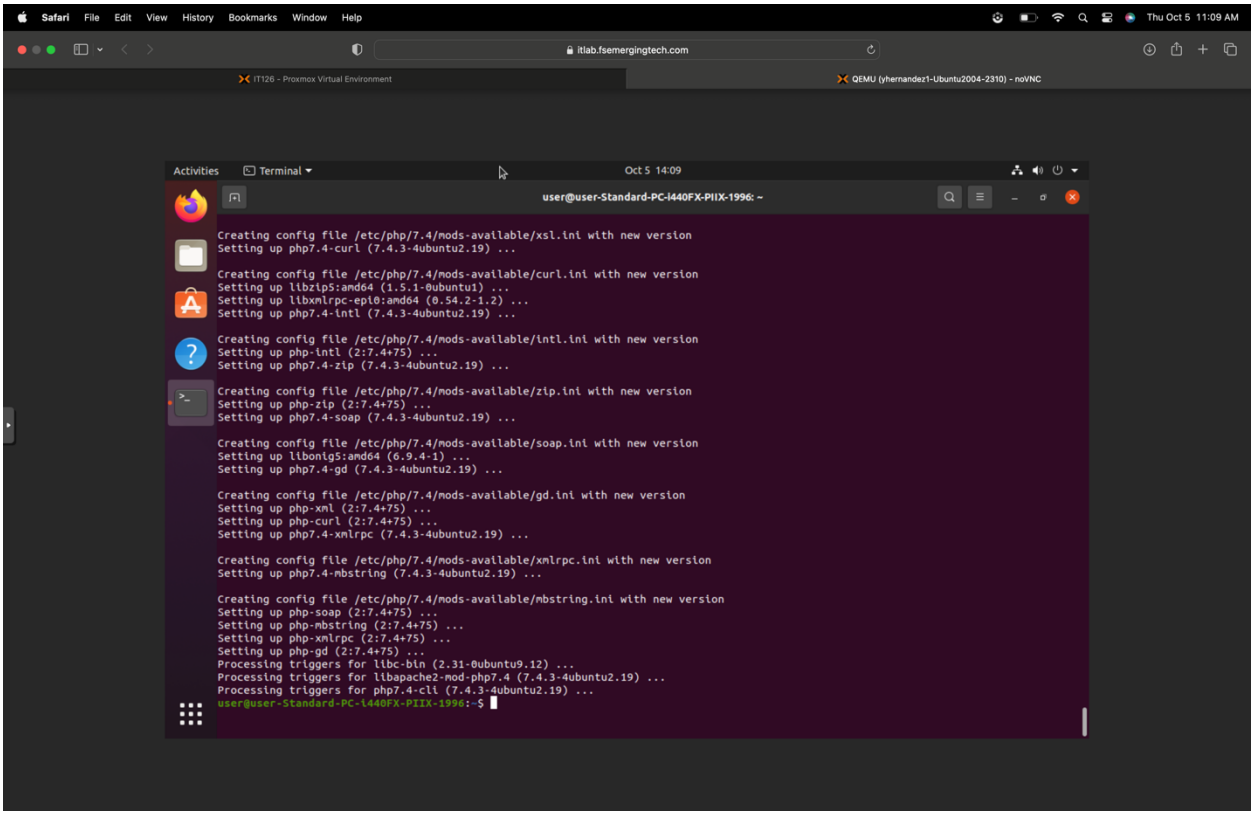
To update Ubuntu, you type **sudo apt update,** then press enter.

Install Required PHP Libraries



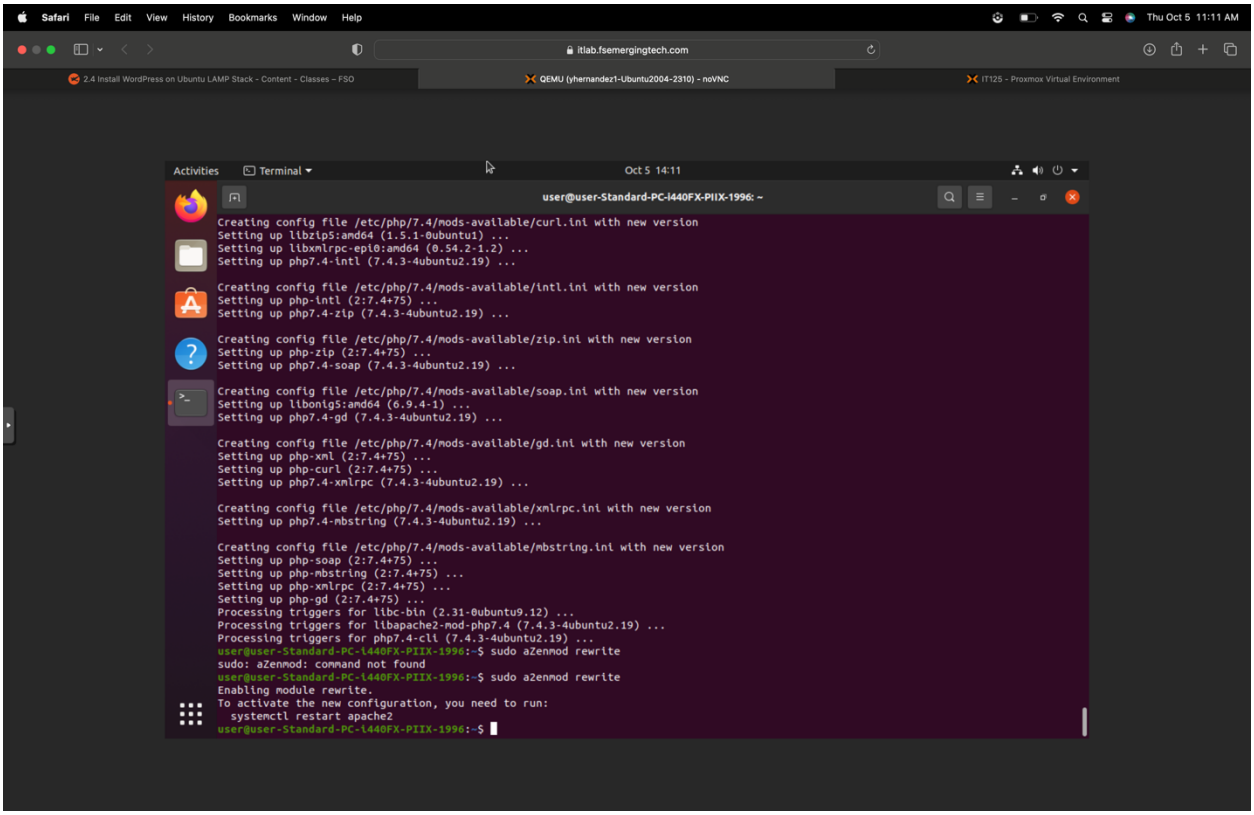
To install required PHP libraries, you type **sudo apt install php libapache2-mod-php php-mysql,** then press enter.

Install Required MySQL Libraries



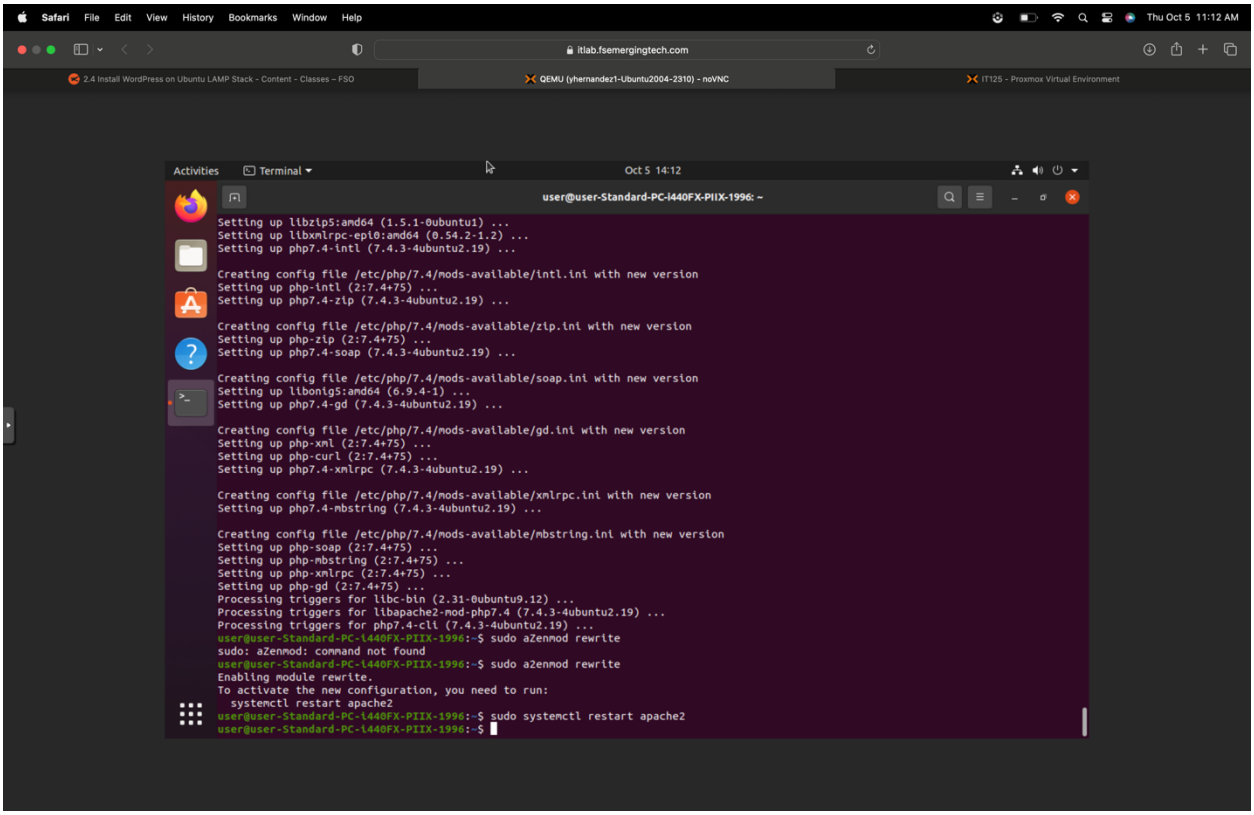
To install required MySQL libraries, you type on the terminal **sudo apt install php-curl php-gd php-xml php-mbstring php-xmlrpc php-zip php-soap php-intl** then press enter.

Enable URL Rewrites (clean URLs)



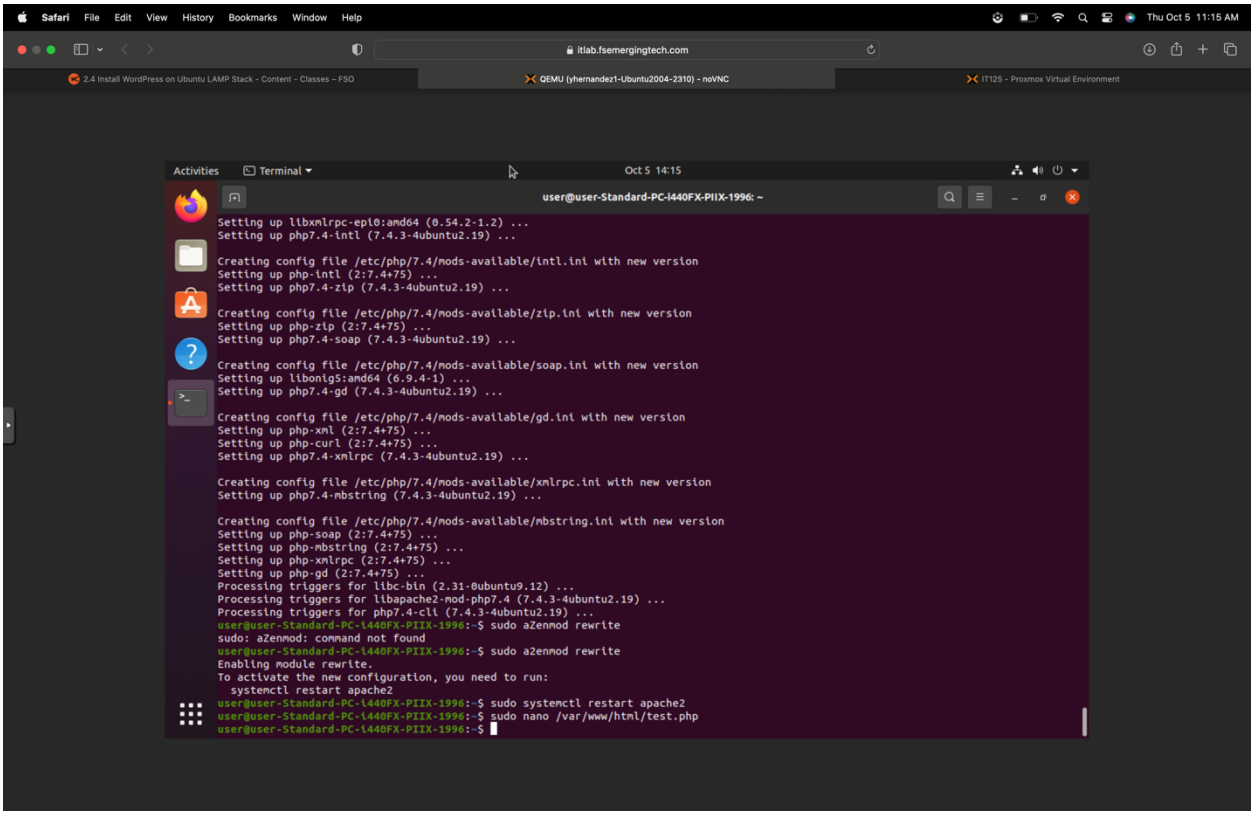
To enable URL Rewrites, type **sudo a2enmod rewrite,** then press enter.

Restart Apache Service



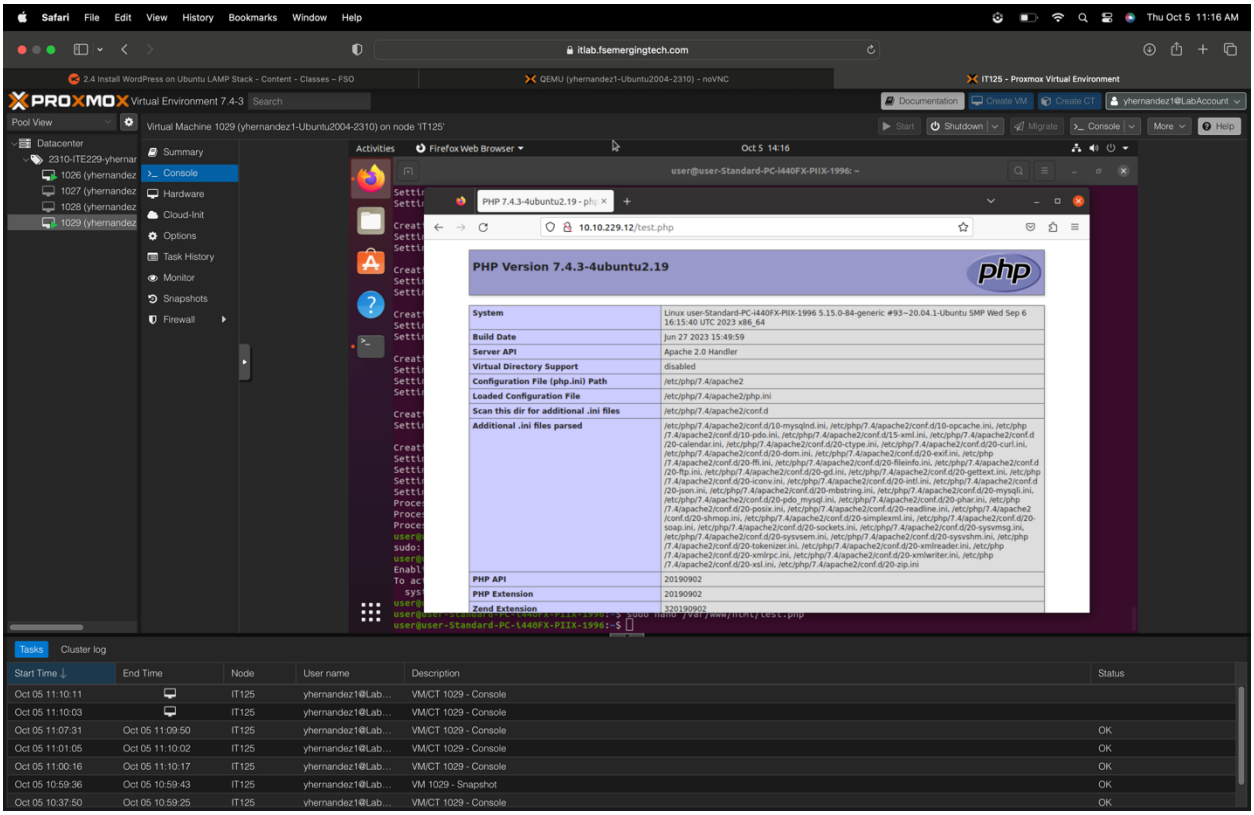
To restart Apache, you type **sudo systemctl restart apache2.**

Create a test.php Web Page



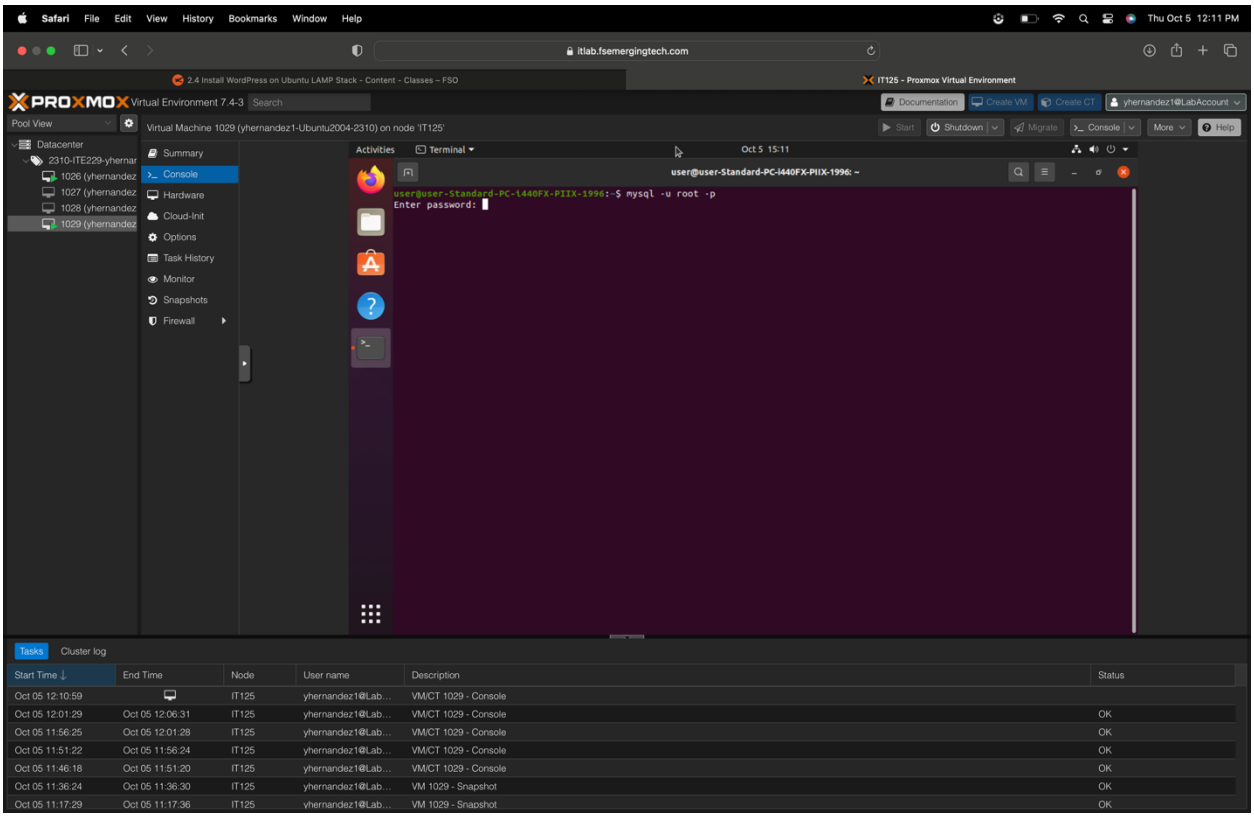
To create a test.php web page, type **sudo nano /var/www/html/test.php,** then enter. When the nano page comes up, you will order **<?php phpinfo(); ?>,** then you will save it by pressing (Control ^ and X) and exit by pressing enter.

Test the test.php Web Page



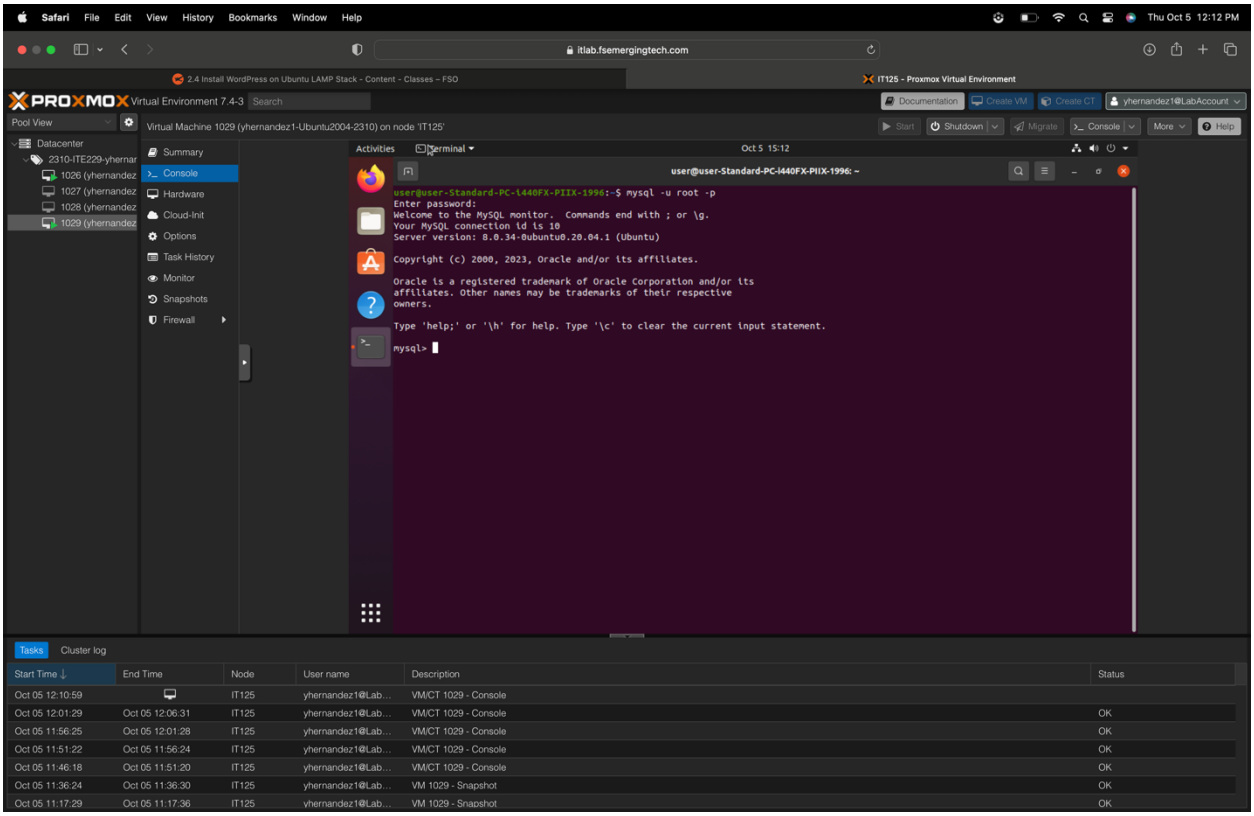
To test the test.php web page, go to a Firefox web browser, and on the address bar, type **10.10.229.12/test.php.** Then you press enter, and you will get the PHP Version page.

Database Configuration in MySQL



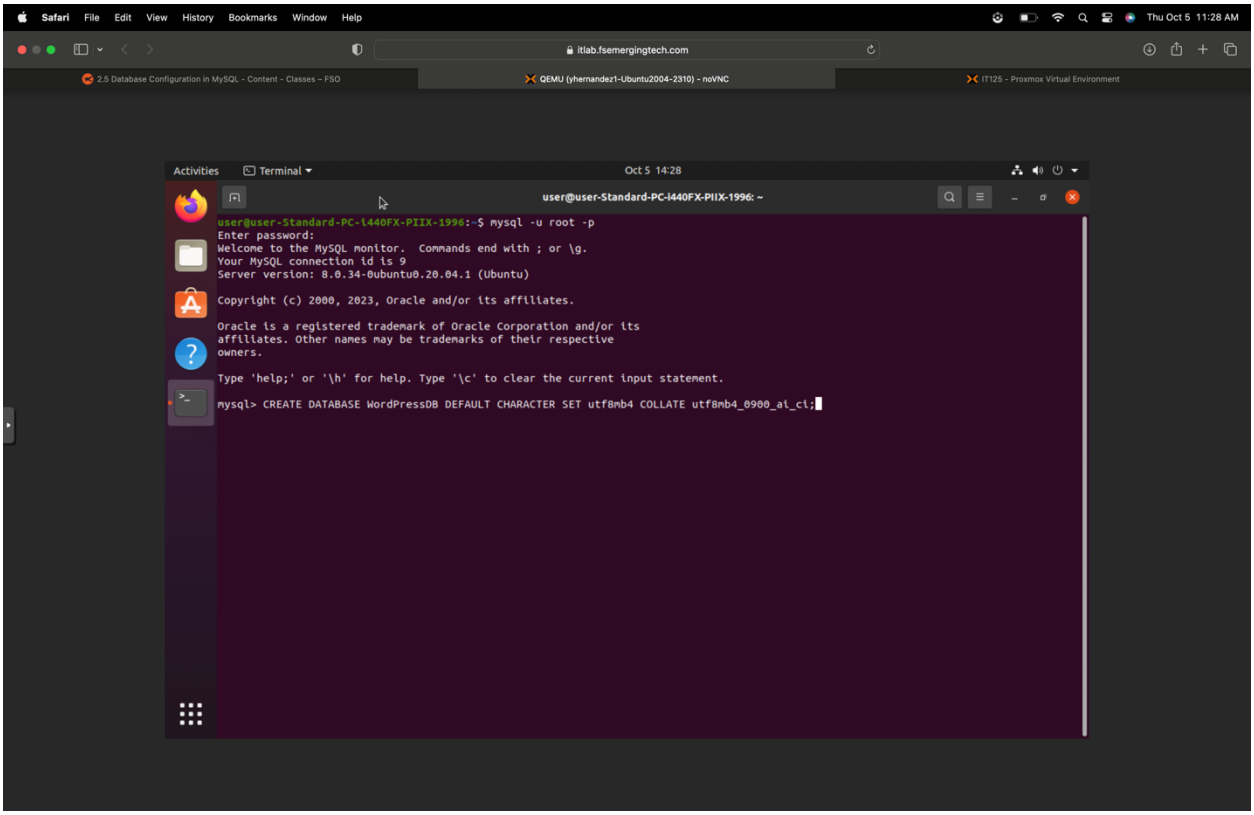
To log in to the Database Configuration in MySQL on the command line, type **mysql -u root -p,** then press enter.

Log into MySQL Database



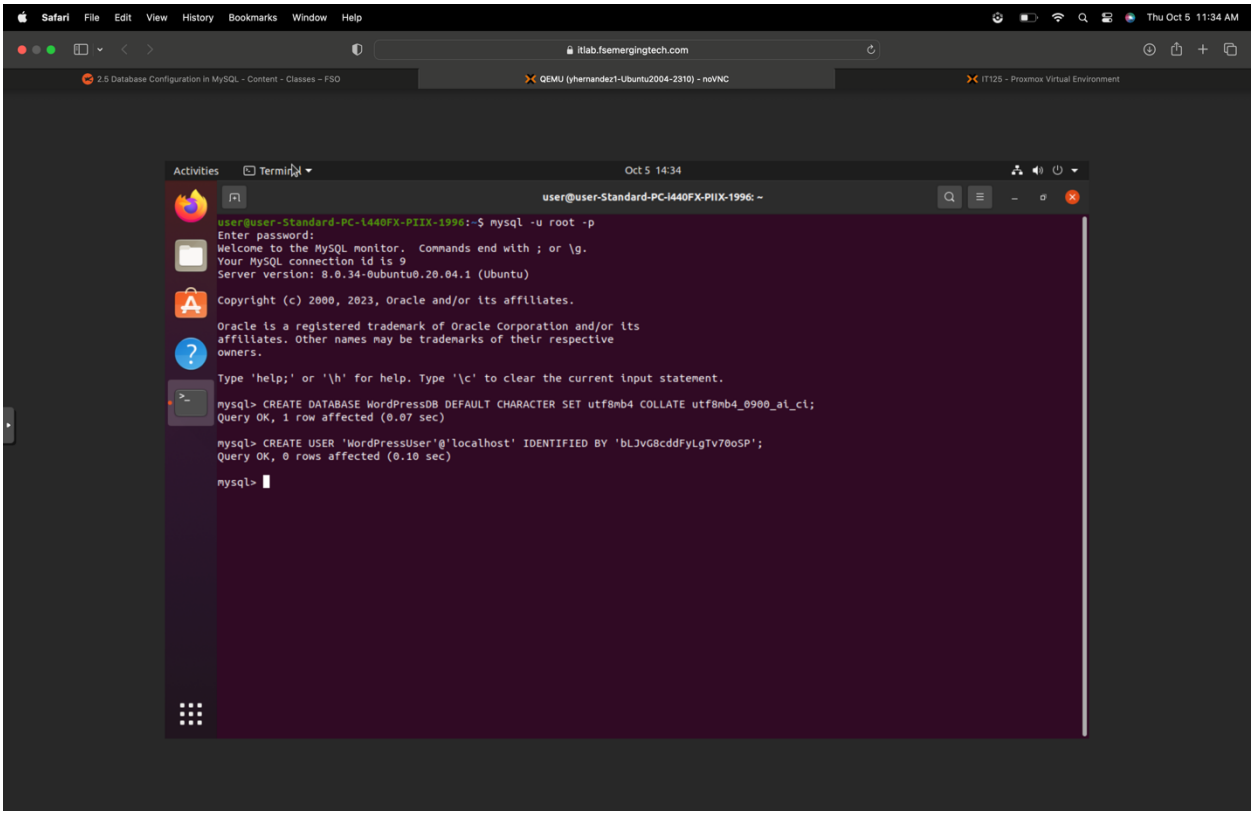
To log in to MySQL, you have to type in your password.

Create WordPress Database in MySQL



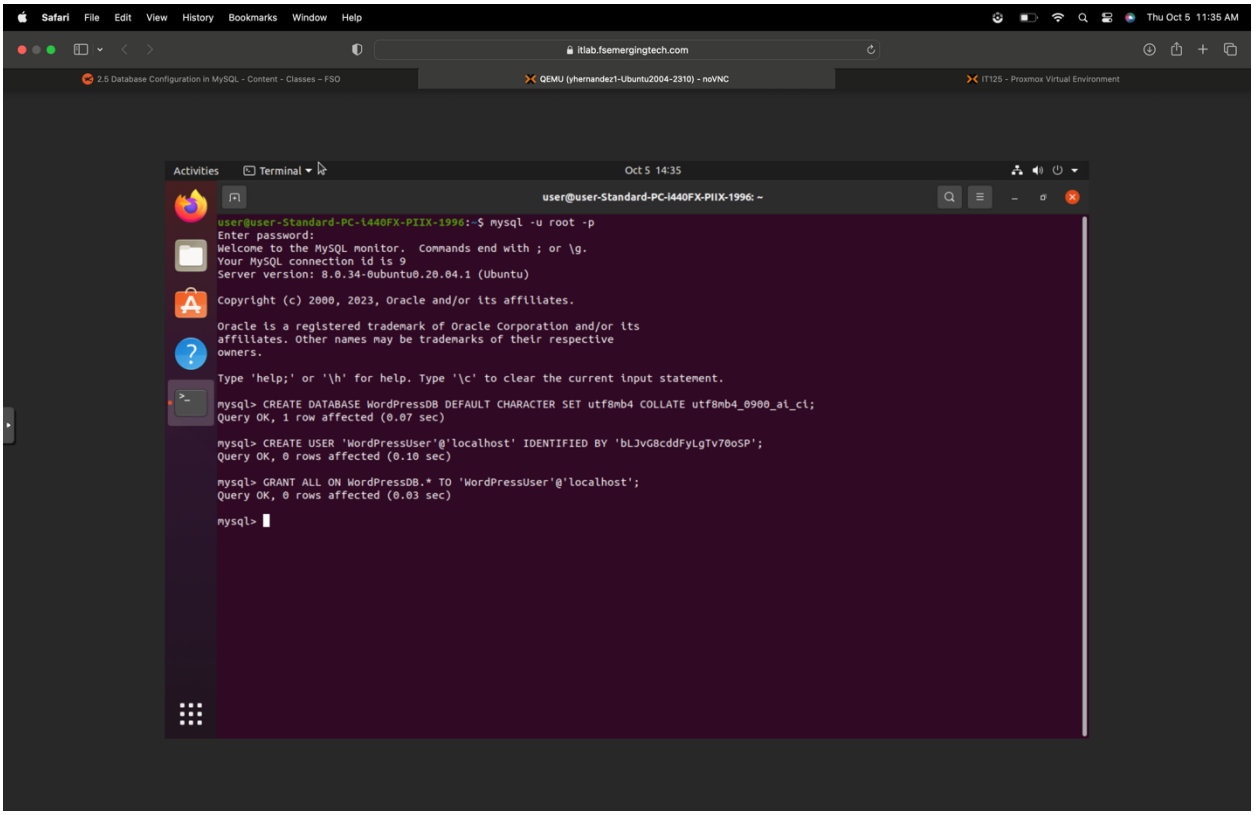
To create y Database on the command line, type **CREATE DATABASE WordPressDB DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4_0900_ai_ci;** then enter.

Create WordPress User for MySQL Database



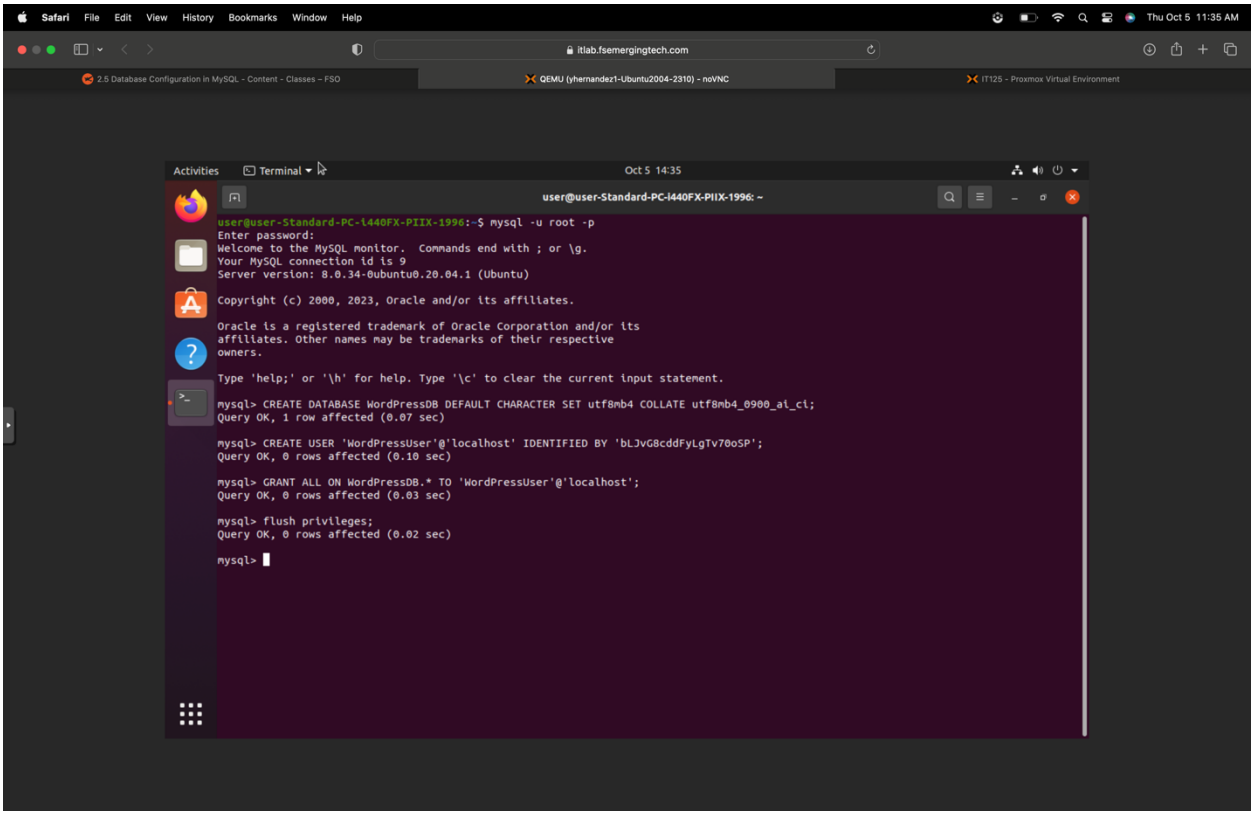
To create a WordPress User on the command line, type **CREATE USER 'WordPressUser'@'localhost' IDENTIFIED BY '**[add password]**';** then press enter.

Grant Privileges to this New WordPress User



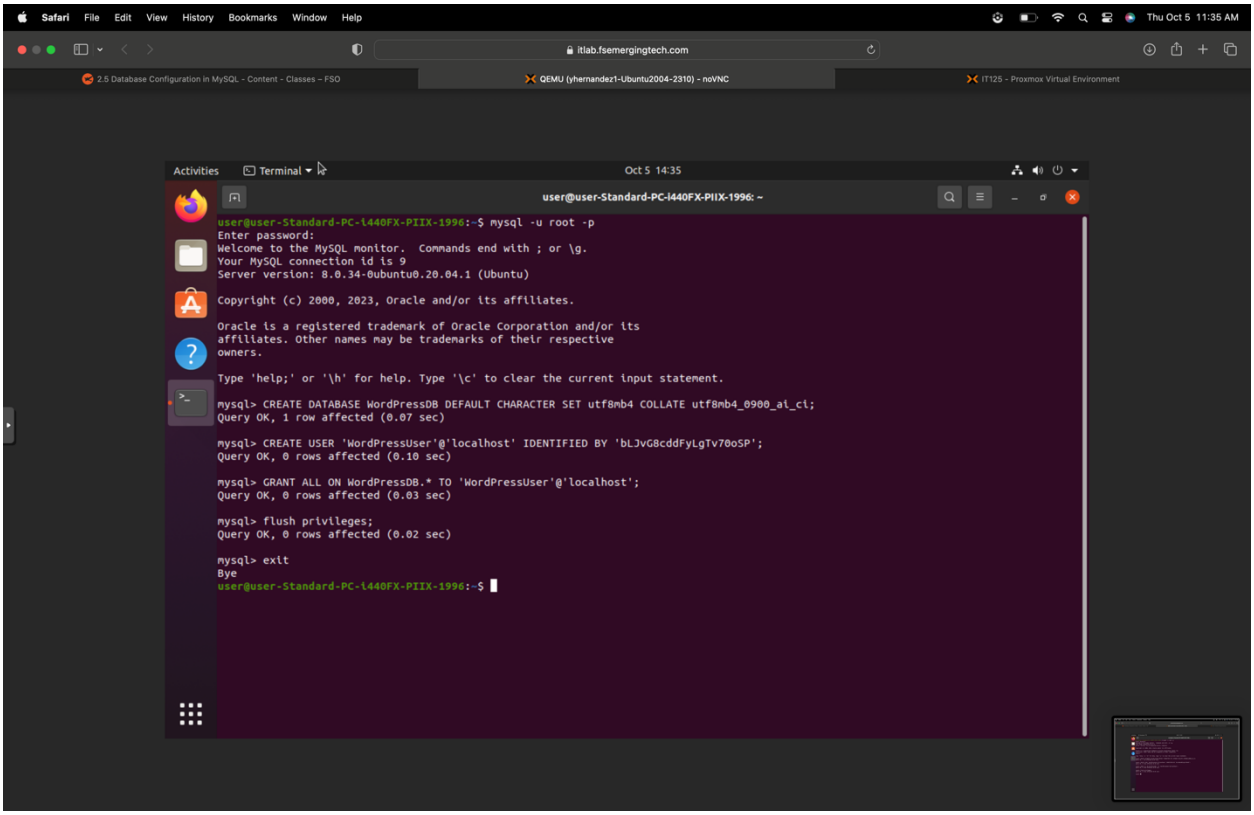
To grant privileges on the command line, type **GRANT ALL ON WordPressDB.* TO 'WordPressUser'@'localhost';** then press enter.

Flush Privileges



To flush privileges, you type **flush privileges** on the command line, then press enter.

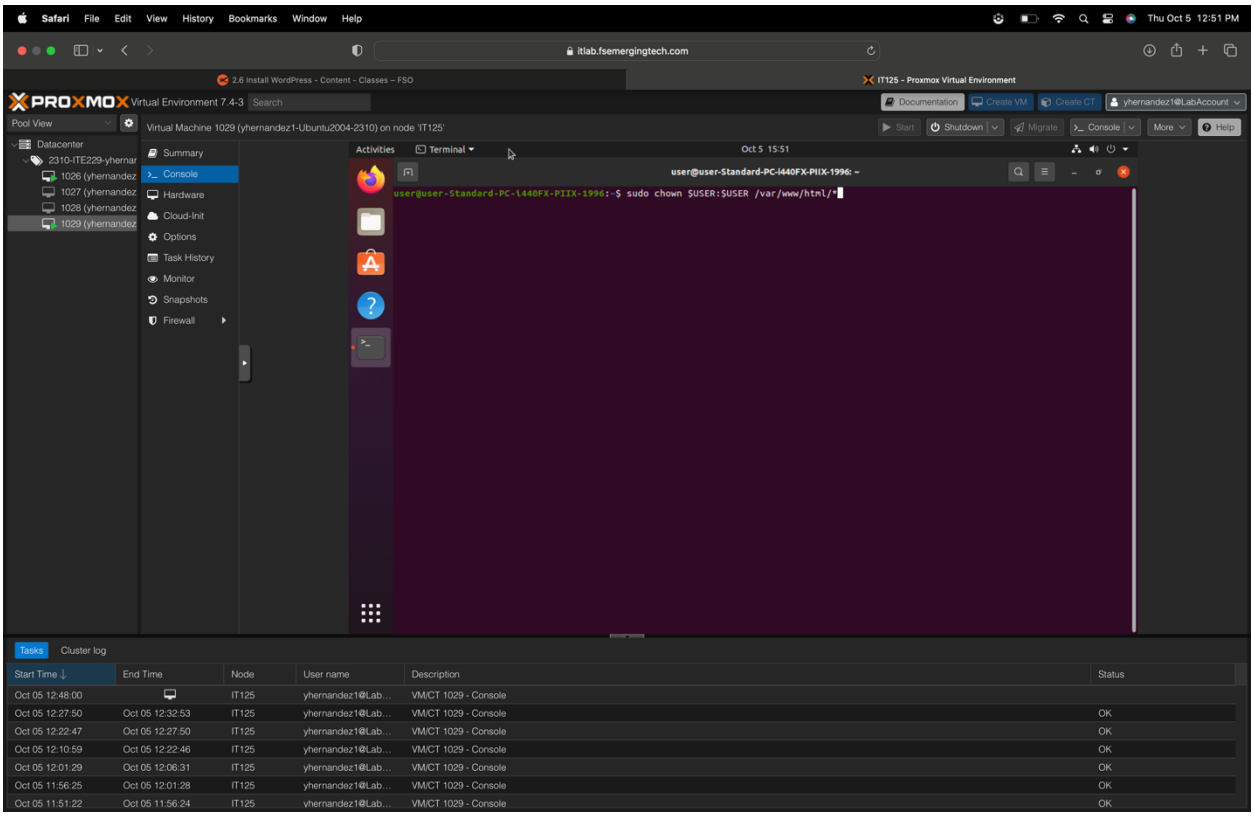
Quit MySQL



To quit MySQL, you type **exit** on the command line and press enter.

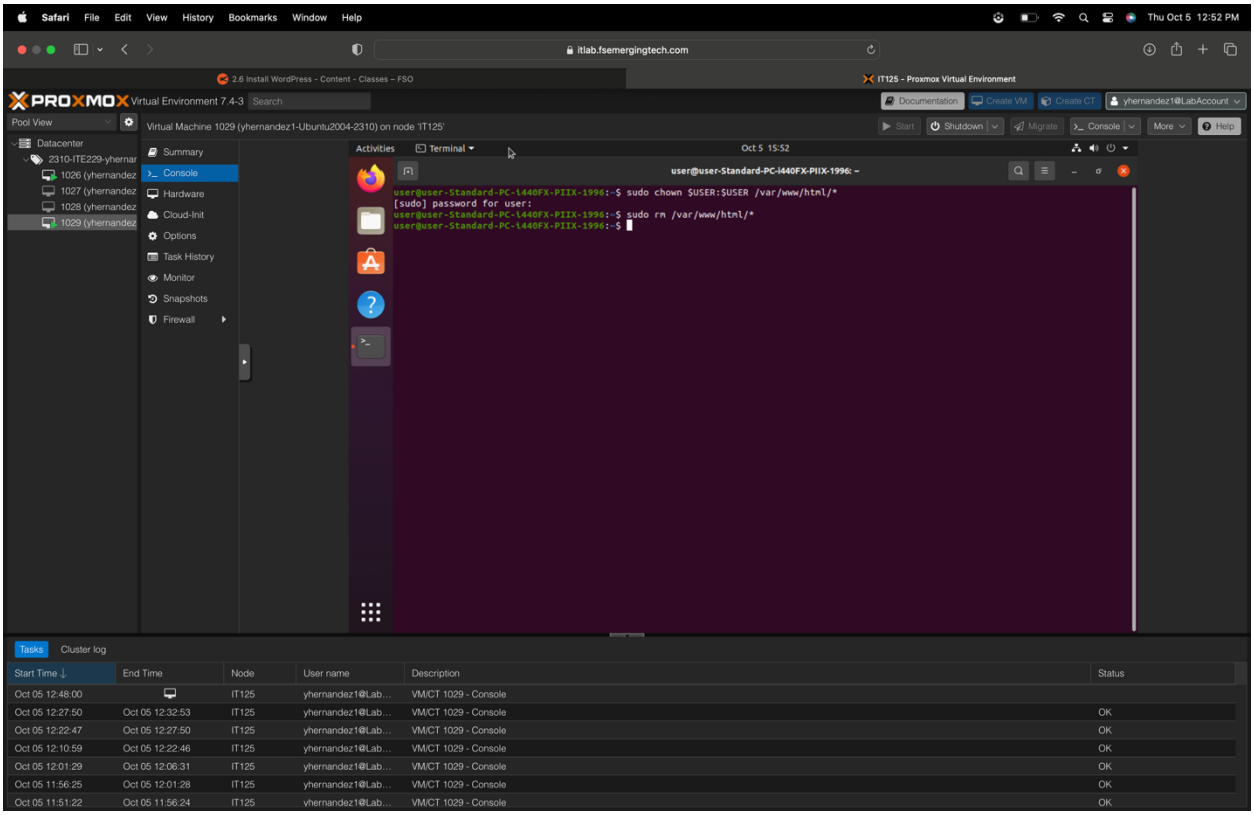
Install WordPress

Grant Permission to html Directory to WordPress User



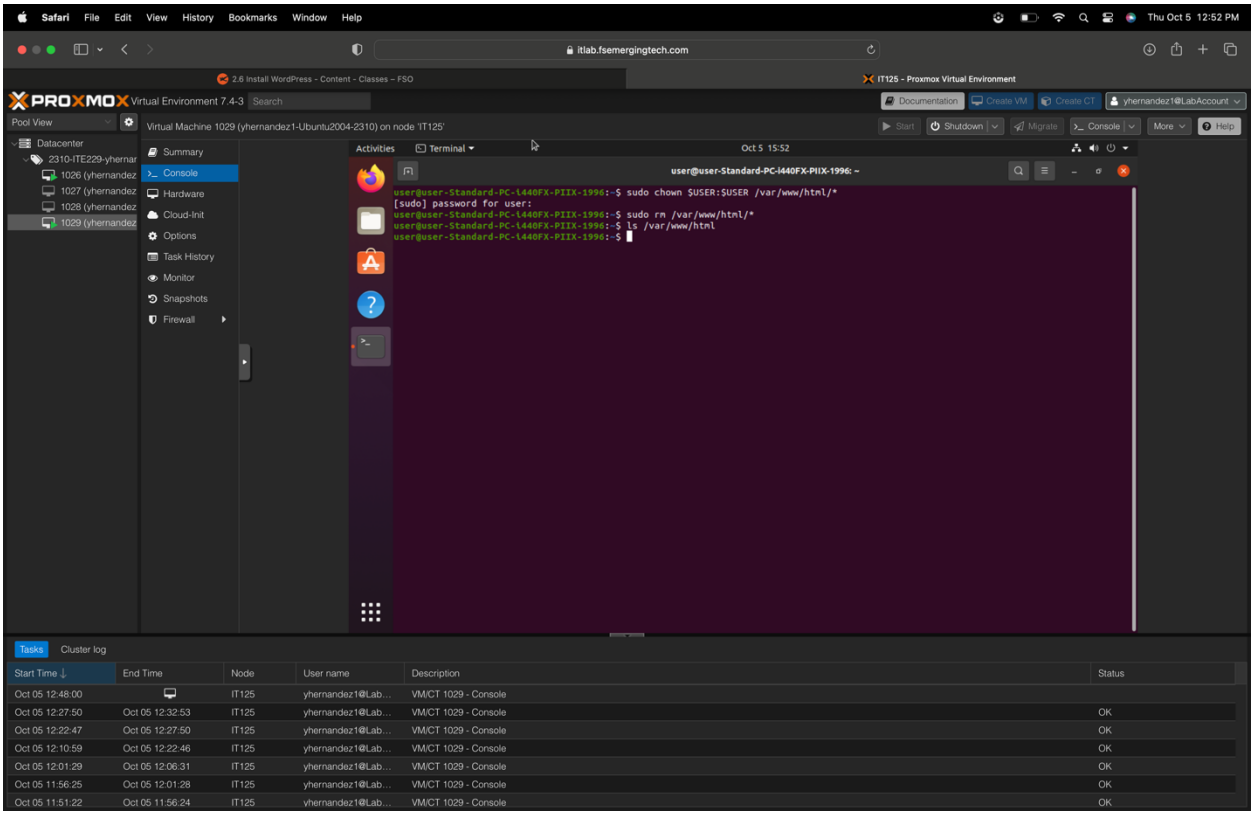
To grant permissions to the html directory on the command line, type **sudo chown $User:$User /var/www/html/*,** then press enter.

Delete Files from html Directory



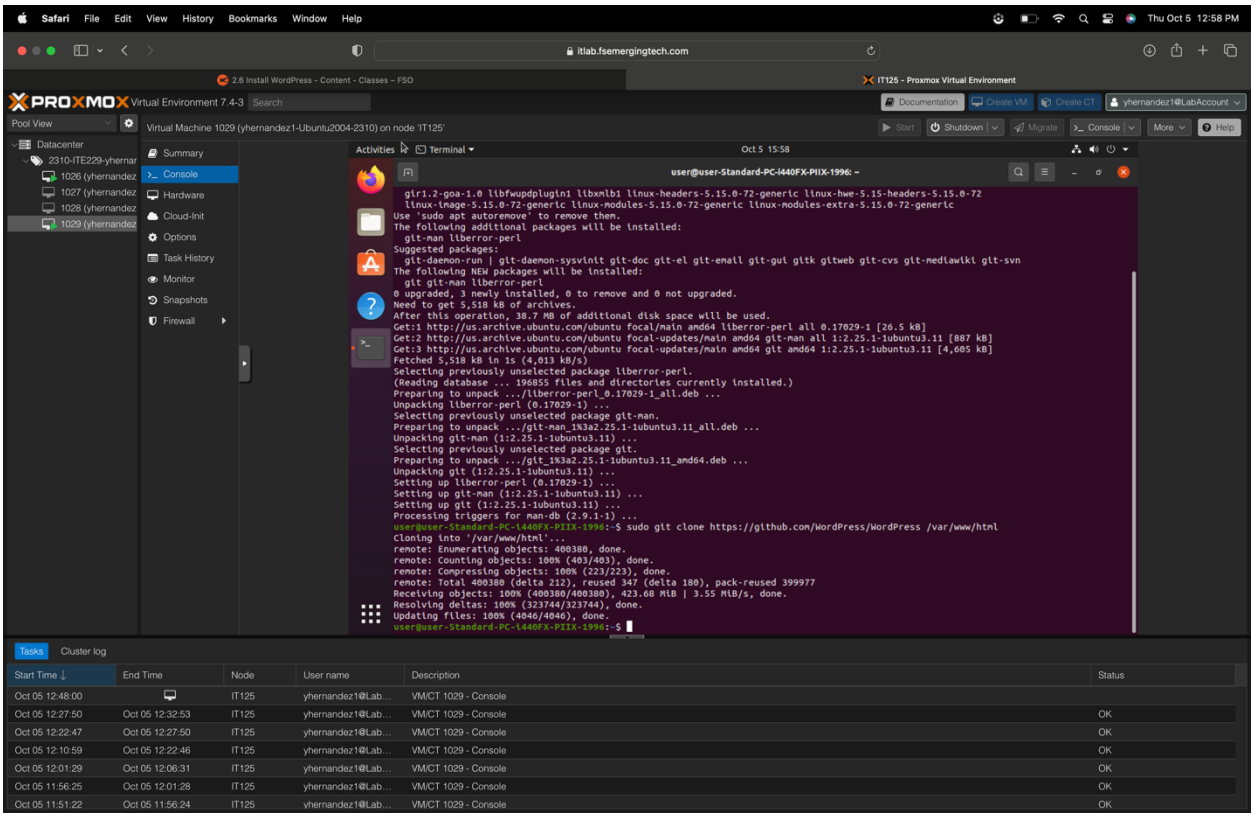
To delete files from the html directory on the command line, type **sudo rm /var/www/html/*,** then press enter.

Verify html Directory is Empty



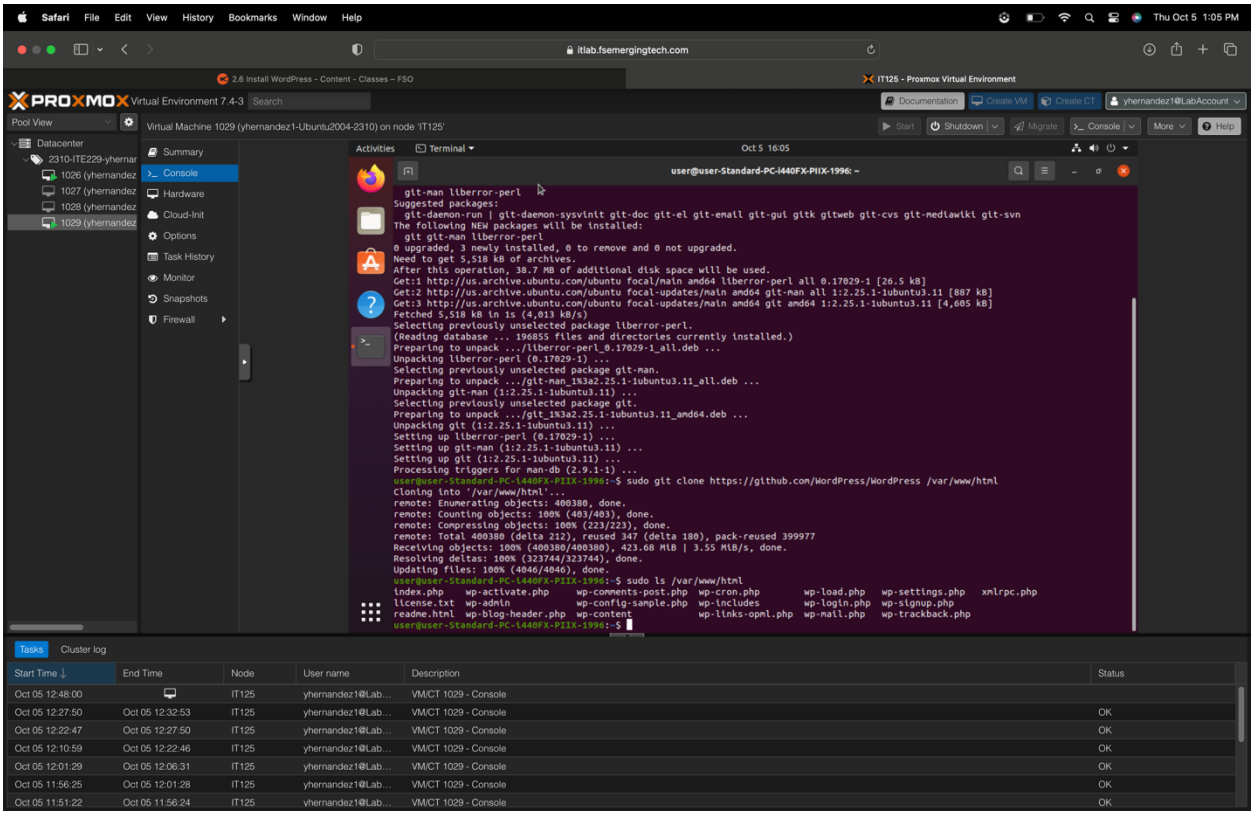
To verify the empty html directory, type **ls /var/www/html** on the command line, then press enter.

Clone WordPress to html Directory



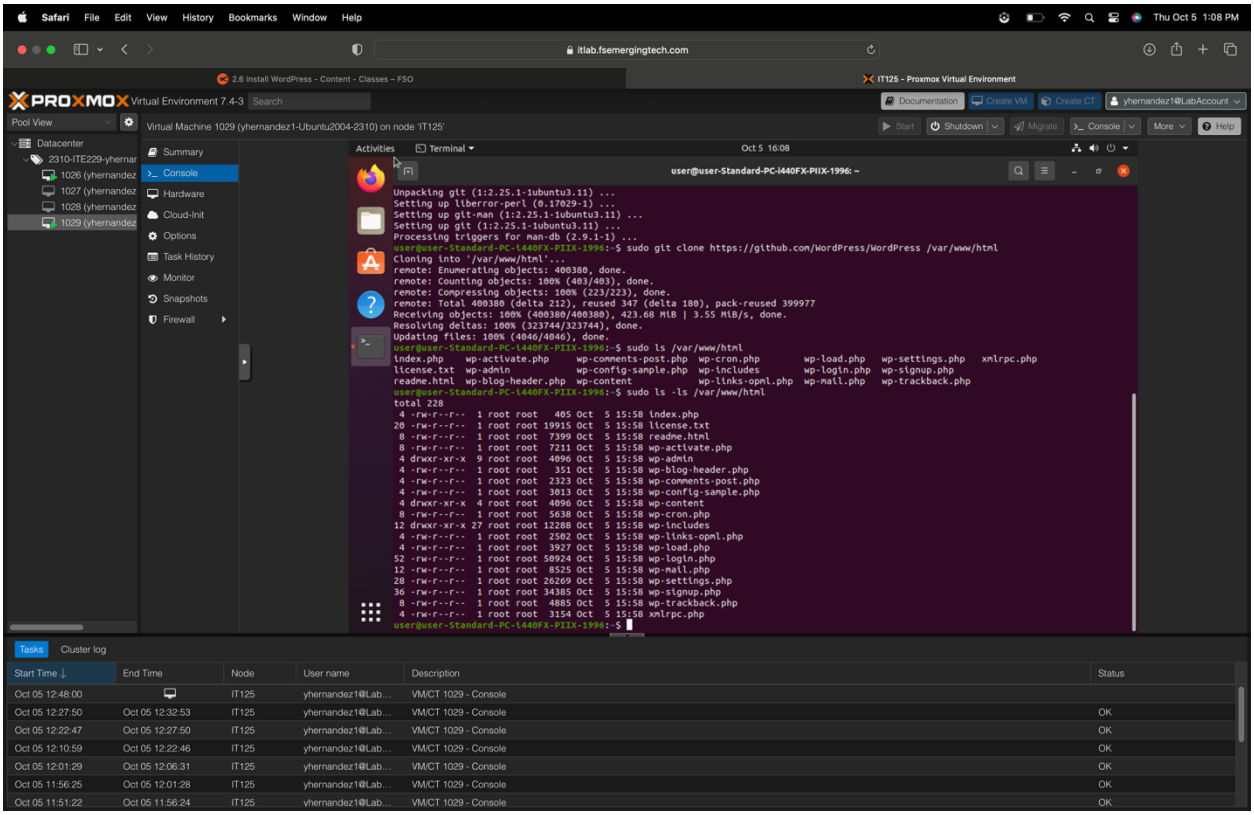
To clone WordPress, type **sudo git clone https://github.com/WordPress/WordPress /var/www/html/** on the command line, then press enter.

Verify html Directory Contains WordPress Files



To verify that the HTML directory contains WordPress Files, type **sudo ls /var/www/html,** then press enter.

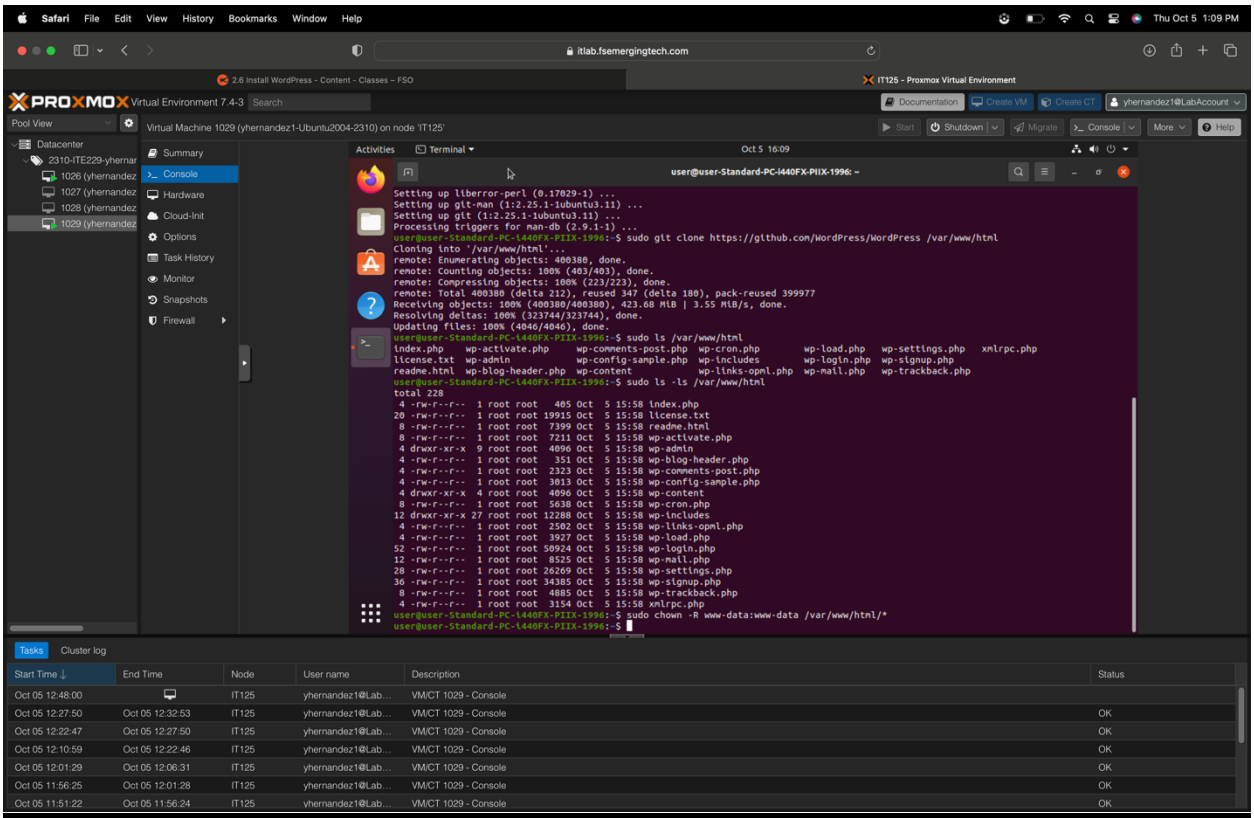
Verify Permissions on html Directory

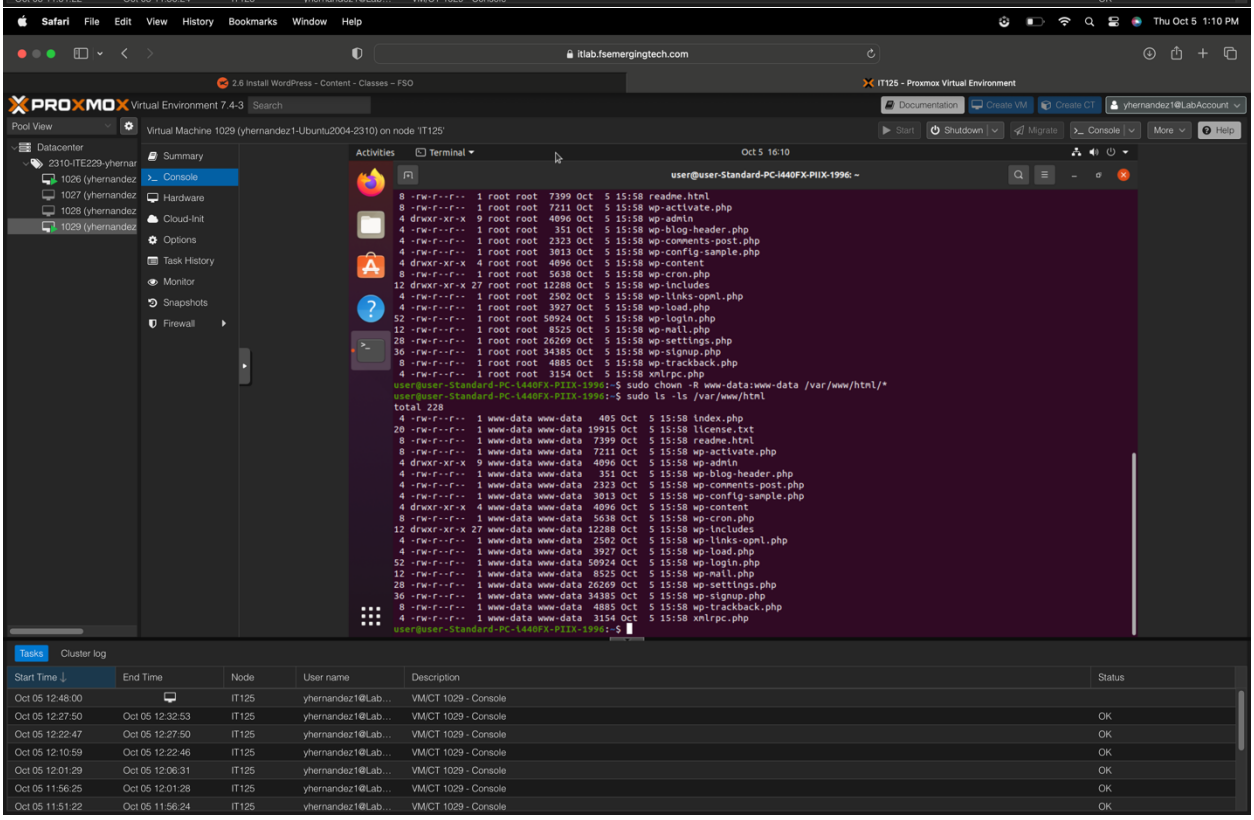


To verify permissions on the HTML file, type **sudo ls -ls /var/www/html,** then press enter.

Edit Ownership

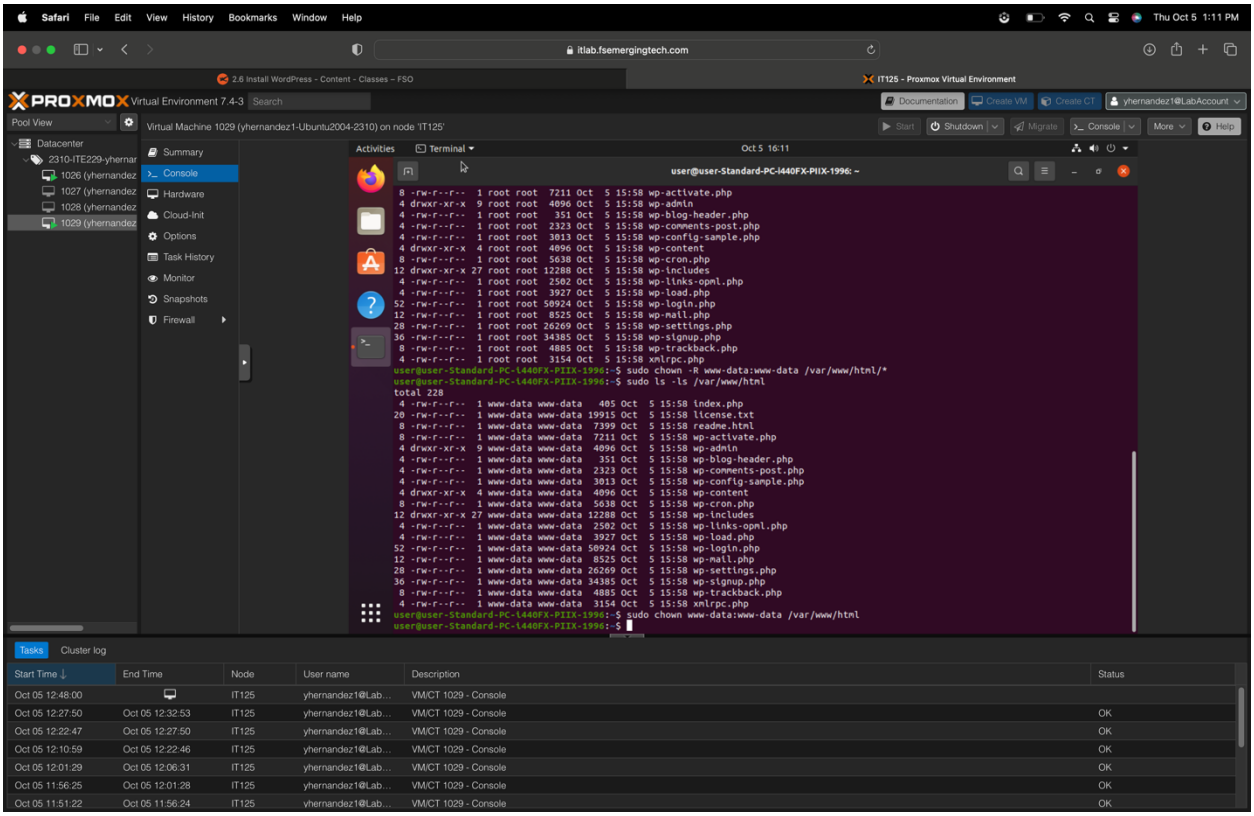
Edit Ownership of Contents of html Directory





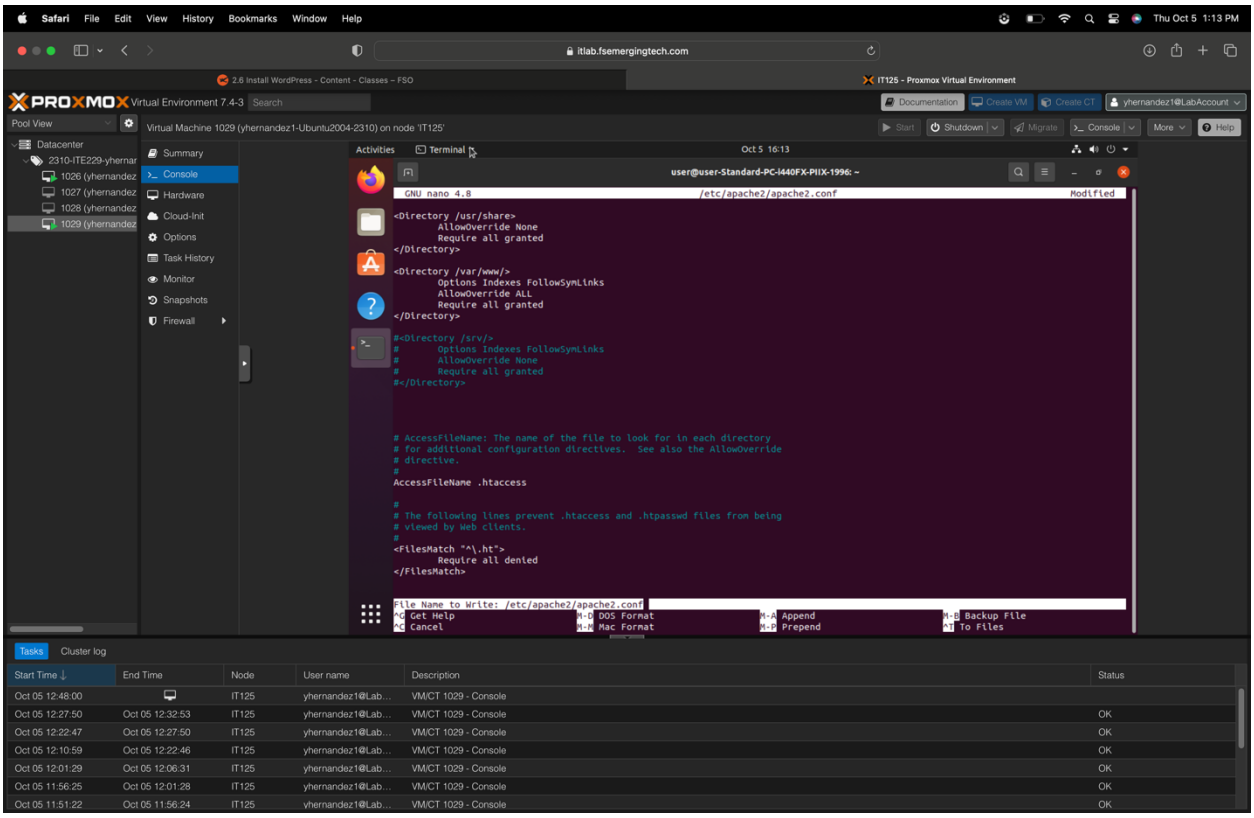
To Edit Ownership of Contents of HTML Directory, you type **sudo chown -R www-data:www-data /var/www/html/*** then press enter and to check that they have changed ownership, type **sudo ls -ls /var/www/html** then press enter.

Edit Ownership of the html Directory Itself



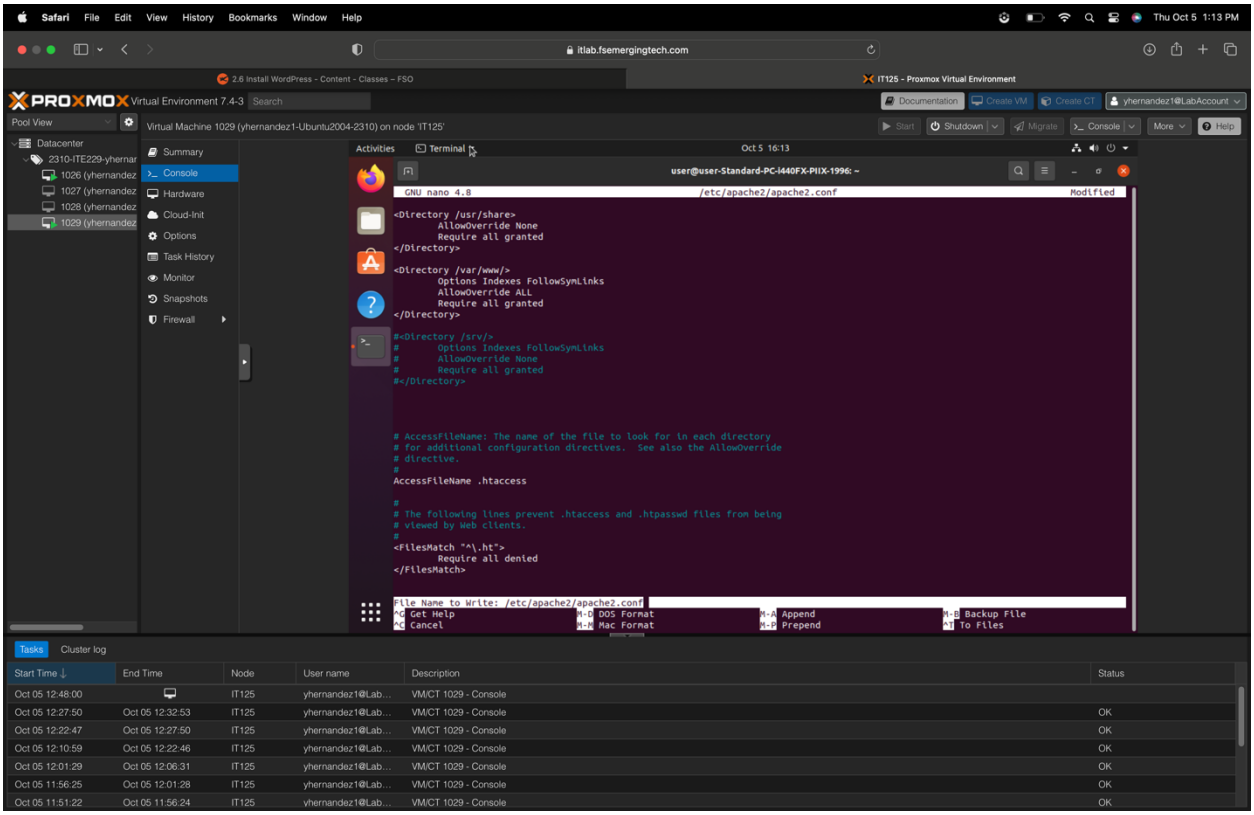
To edit ownership of the HTML directory, type **sudo chown www-data:www-data /var/www/html,** then press enter.

Edit the apache2.conf File



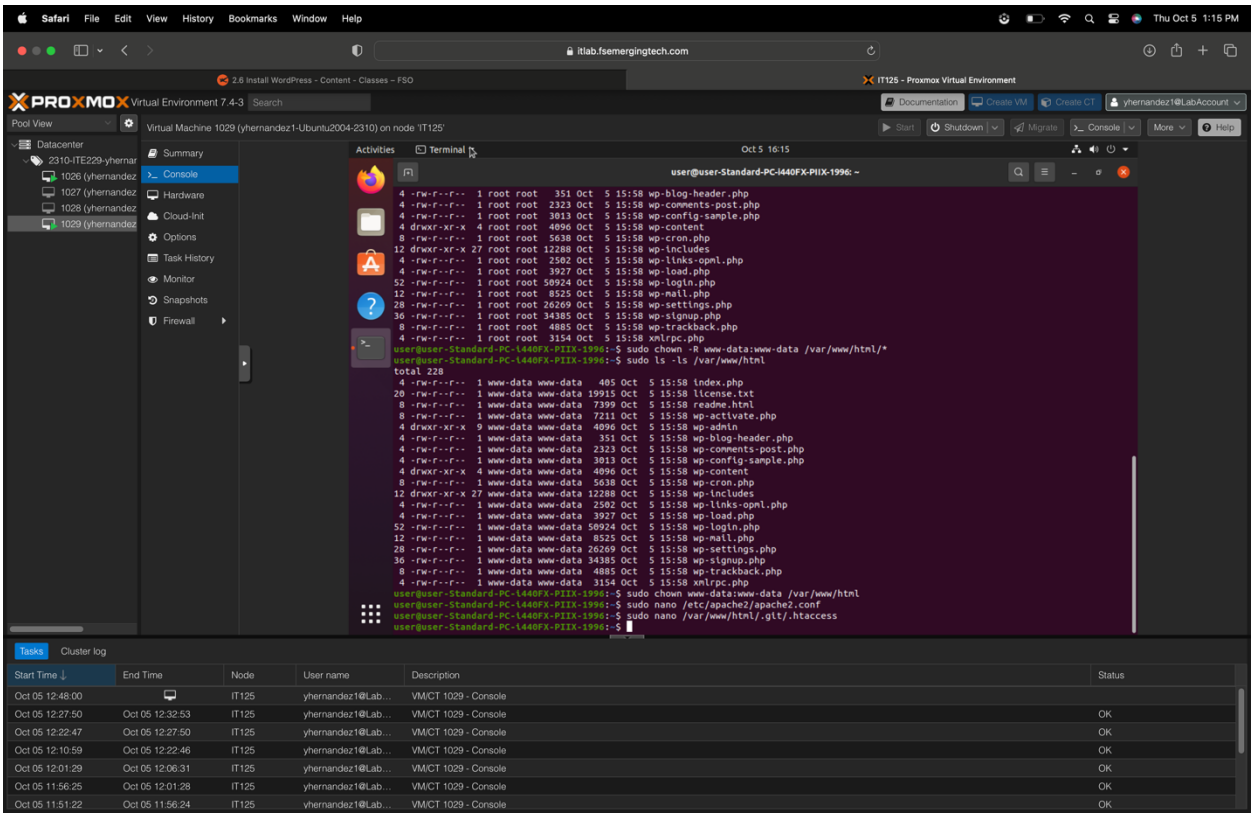
To edit the apache2.conf file type on the terminal **sudo nano /etc/apache2/apache2.conf,** then press enter.

Override All Default Apache Directives



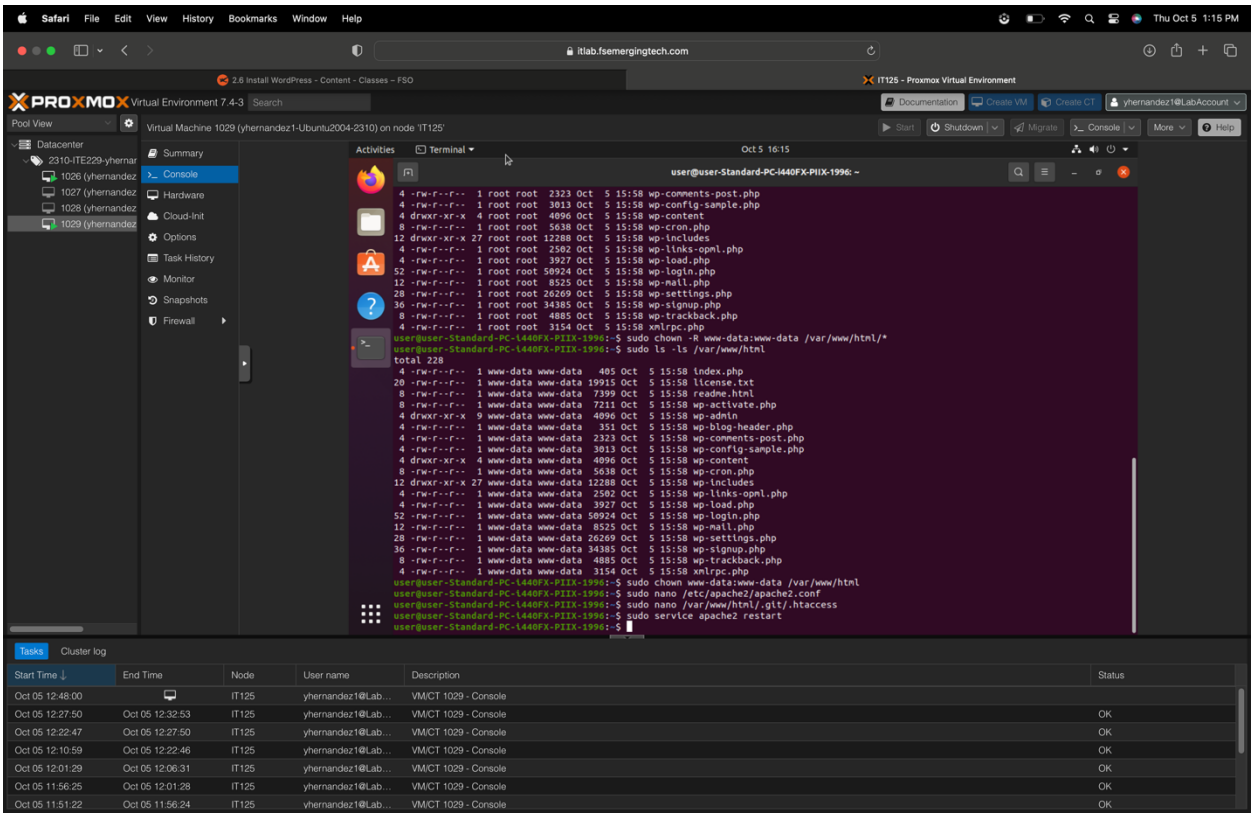
To override all default Apache directives, scroll down until you see **AllowOverride none,** then delete **none** and change it to **ALL.**

Create a .htaccess File in the /var/www/html/.git/ Directory



To create a .htaccess file, type on the terminal **sudo nano /var/www/html/.git/.htaccess,** then press enter. It will take you to the nano page, and you will add on the first line **order deny, allow** then press enter, and on the second line, you will add **deny from all,** then press control (^X) and X, then Y to save.

Restart the Apache Service



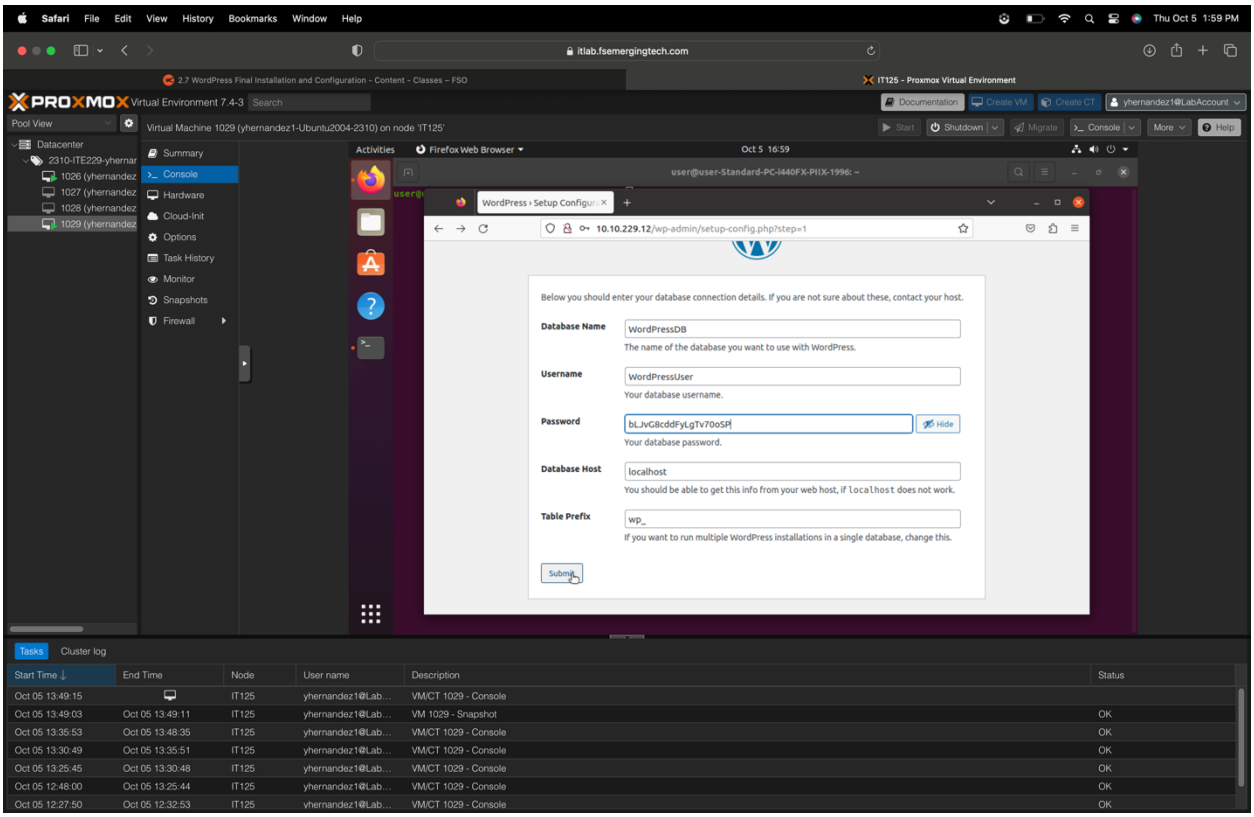
To restart the Apache service, you type on the terminal **sudo service apache2 restart,** then press enter.

IMPORTANT: To earn full credit, ALL screenshots must include a "full view", including your ProxMox title bar with your username showing.

WordPress Configuration

Configure WordPress

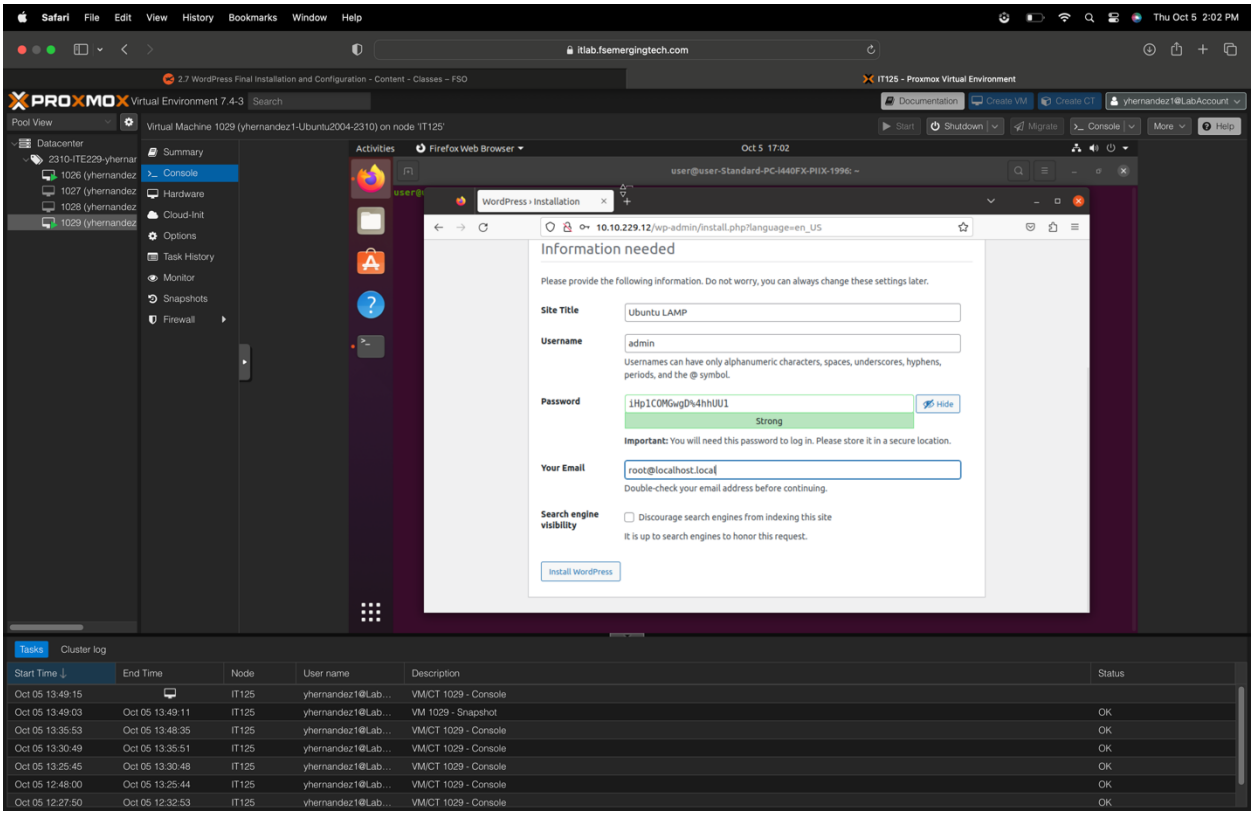
WordPress Configuration Selections



To configure WordPress, go to Firefox web browser, type in the address bar **10.10.229.12,** then press enter. Once there, click through the settings until you reach the page where you enter your database connection details. You fill in the information as directed, then press submit.

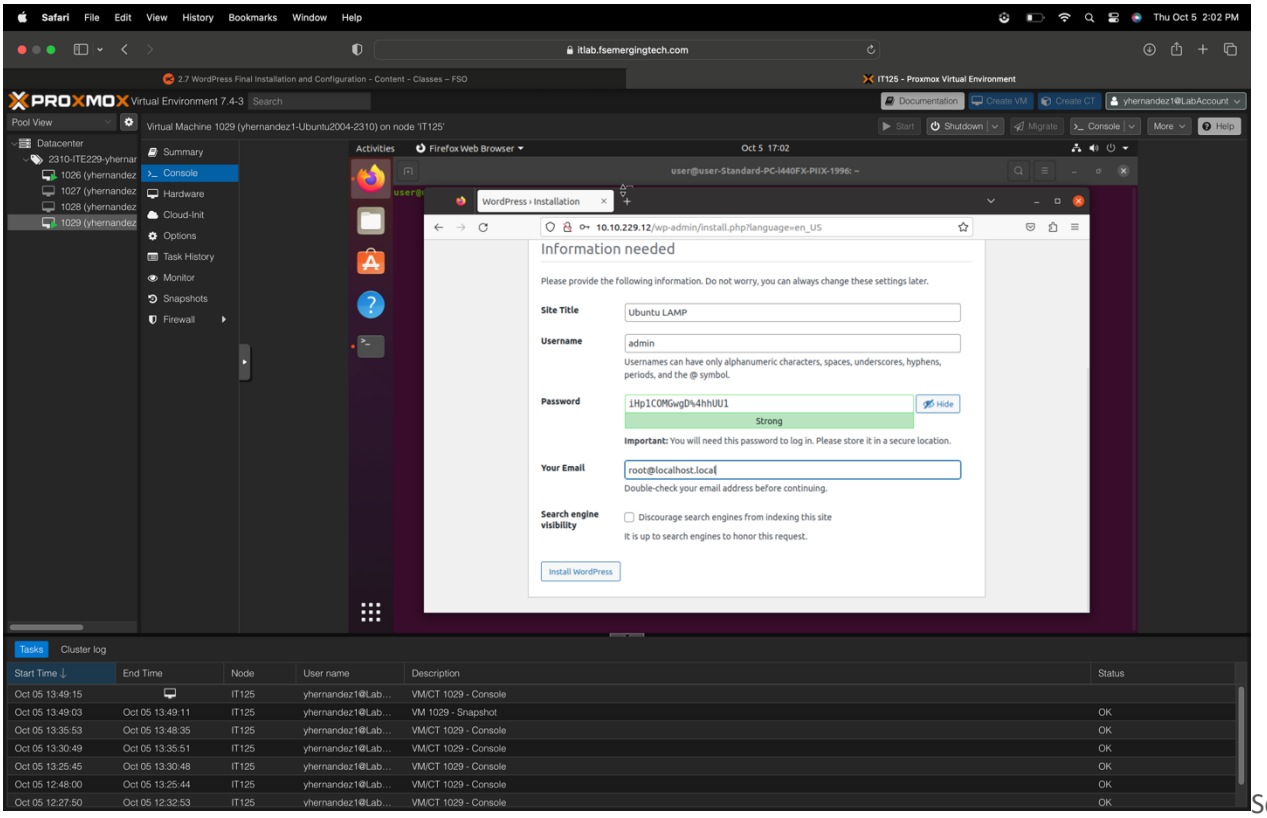
- **Database Name:** WordPressDB
- **Username:** WordPressUser
- **Password:** *this is your WordPressUser password*
- **Database Host:** localhost
- **Table Prefix:** wp_

Run Installation



Once you have all the correct information, you click submit. Then, you will click on the **run installation.**

Create an Admin WordPress User

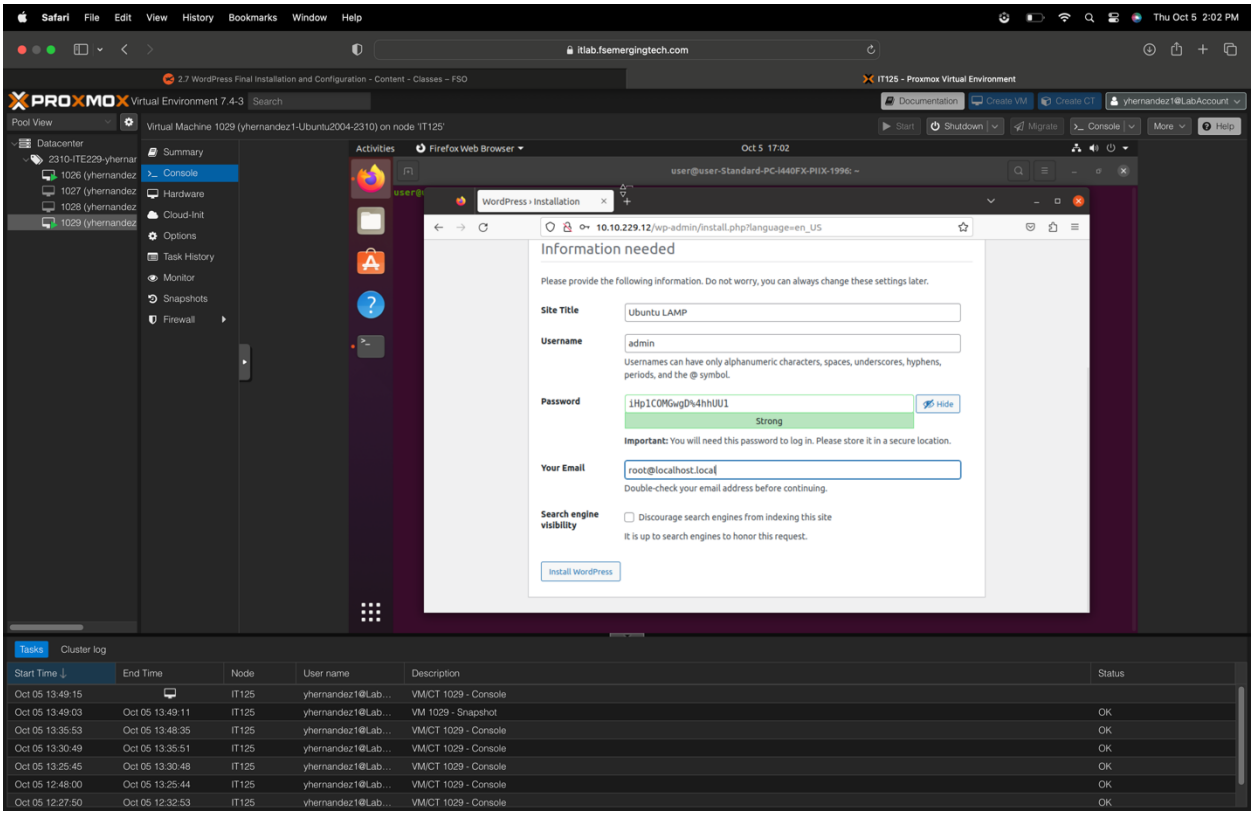


Sc

You will create an admin WordPress user, adding the necessary information that should be added to the similar page above.

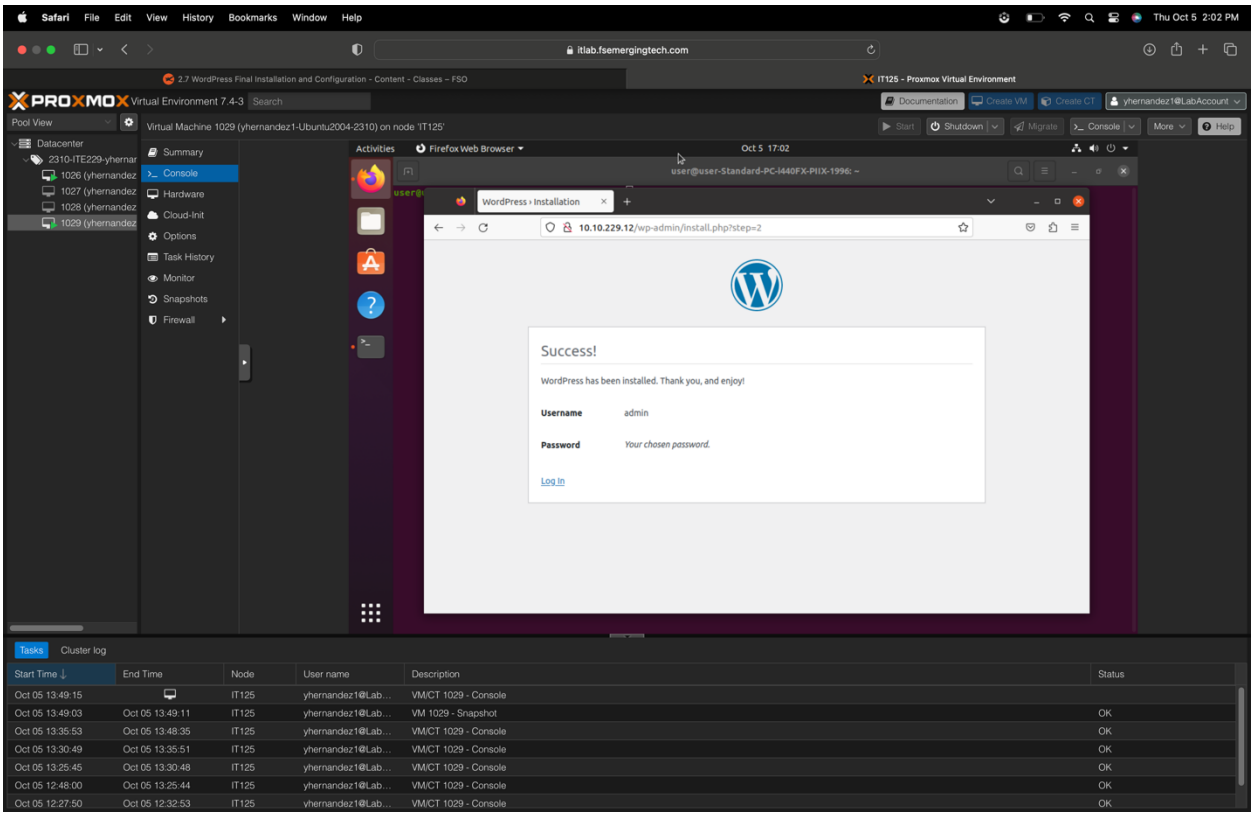
NOTE: Document WordPress admin user password in table at top of document.

WordPress Site Selections

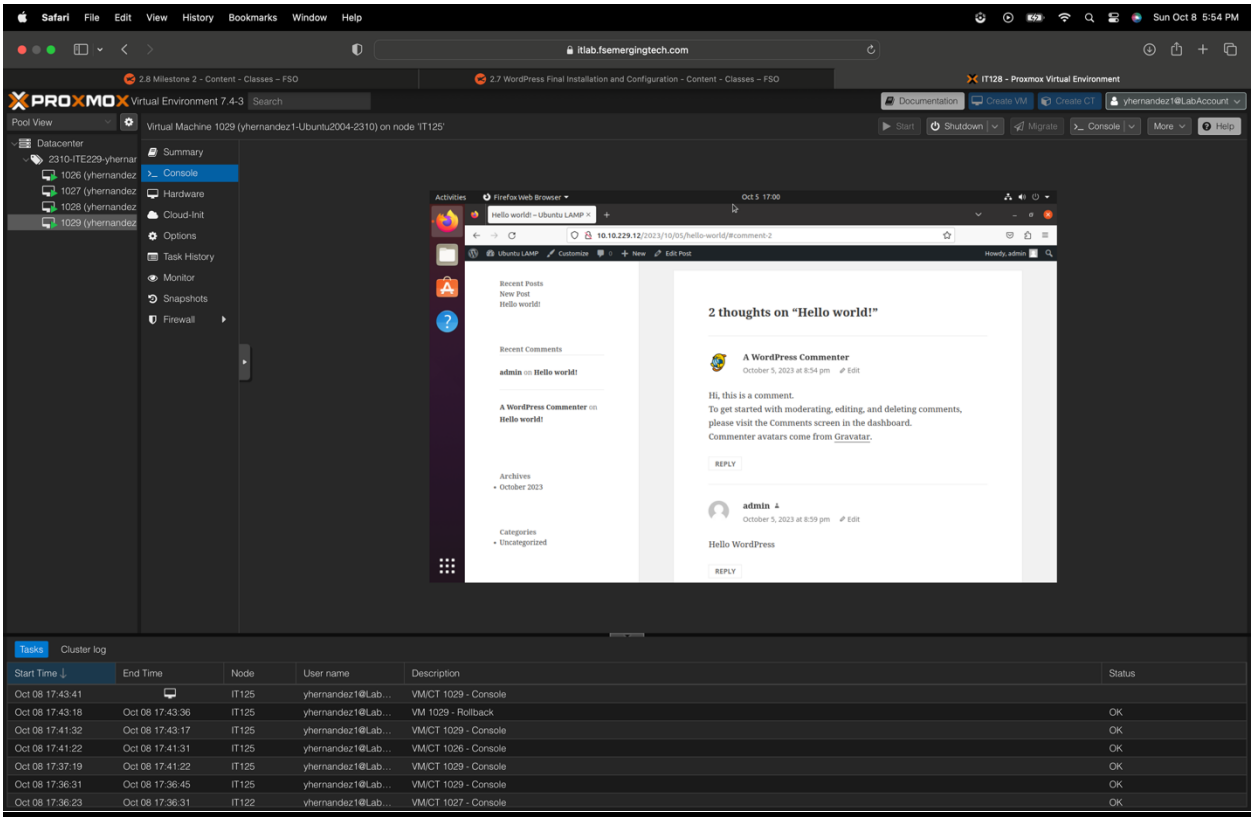


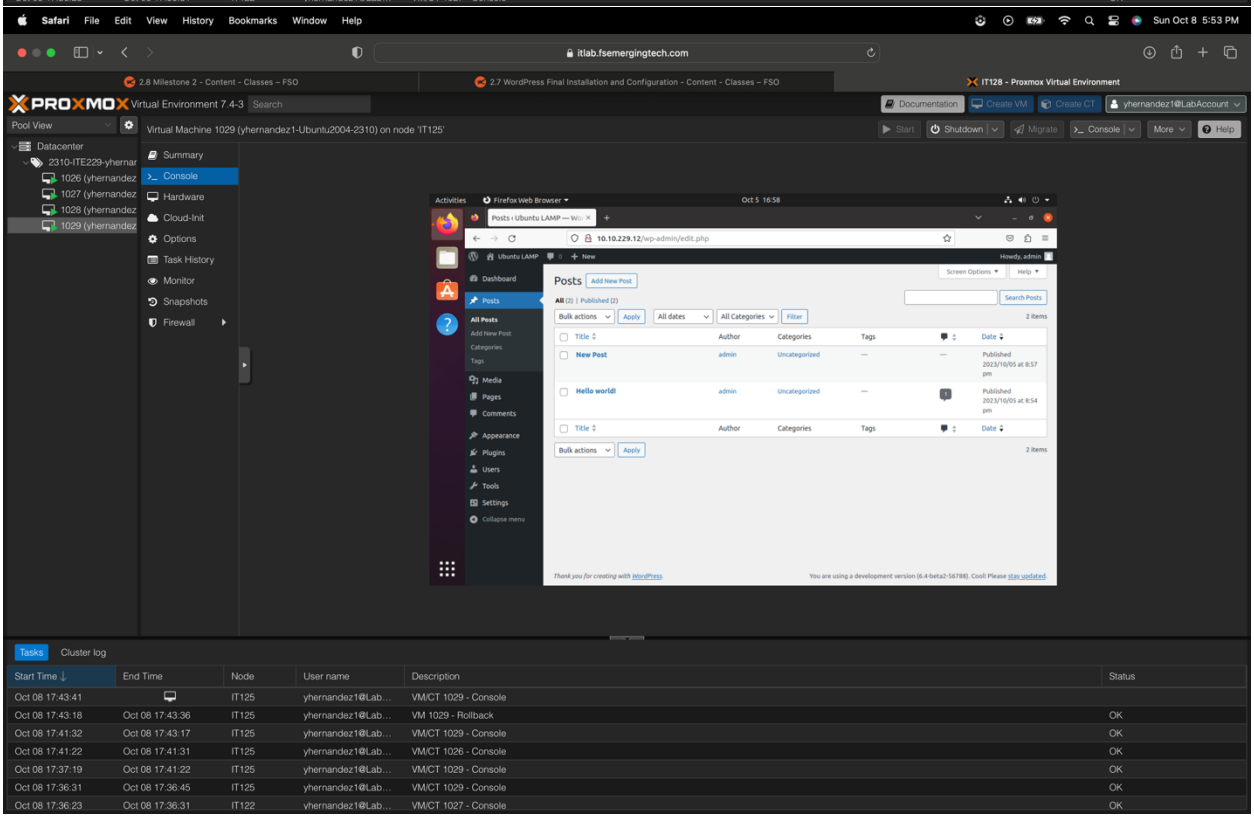
After adding the information, you will click **Install WordPress.**

Site Title: Ubuntu LAMP
Username: admin
Password: *You will create this*
Your email: root@localhost.local
Search Engine Visibility: leave unchecked


Safari File Edit View History Bookmarks Window Help
Thu Oct 5 2:02 PM
itlab.fsemergingtech.com
2.7 WordPress Final Installation and Configuration - Content - Classes – FSO
IT125 - Proxmox Virtual Environment
PROXMOX Virtual Environment 7.4-3
Search
Documentation
Create VM
Create CT
yhernandez1@LabAccount
Pool View
Virtual Machine 1029 (yhernandez1-Ubuntu2004-2310) on node 'IT125'
Start
Shutdown
Migrate
Console
More
Help
Datacenter
2310-ITE229-yhernar
1026 (yhernandez
1027 (yhernandez
1028 (yhernandez
1029 (yhernandez
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Snapshots
Firewall
Activities
Firefox Web Browser
Oct 5 17:02
user@user-Standard-PC-i440FX-PIIX-1996: ~
WordPress › Installation
10.10.229.12/wp-admin/install.php?step=2
Success!
WordPress has been installed. Thank you, and enjoy!
Username
admin
Password
Your chosen password.
Log In
Tasks
Cluster log
Start Time
End Time
Node
User name
Description
Status
Oct 05 13:49:15 IT125 yhernandez1@Lab... VM/CT 1029 - Console
Oct 05 13:49:03 Oct 05 13:49:11 IT125 yhernandez1@Lab... VM 1029 - Snapshot OK
Oct 05 13:35:53 Oct 05 13:48:35 IT125 yhernandez1@Lab... VM/CT 1029 - Console OK
Oct 05 13:30:49 Oct 05 13:35:51 IT125 yhernandez1@Lab... VM/CT 1029 - Console OK
Oct 05 13:25:45 Oct 05 13:30:48 IT125 yhernandez1@Lab... VM/CT 1029 - Console OK
Oct 05 12:48:00 Oct 05 13:25:44 IT125 yhernandez1@Lab... VM/CT 1029 - Console OK
Oct 05 12:27:50 Oct 05 12:32:53 IT125 yhernandez1@Lab... VM/CT 1029 - Console OK

Test WordPress





To test WordPress, click on login on the page that says **Success!** Then, enter the username and password. On the left side of the page, click **Appearance**, then **Theme**, pick a theme, and click on Activate. Then, once that's active, click on **Posts,** then on **All Posts,** then **New Post.** Add information, then publish. Click the **W** on the top left side, which will take you to the dashboard.

IMPORTANT: To earn full credit, ALL screenshots must include a “full view”, including your ProxMox title bar with your username showing.

WordPress Security Settings and Configurations

WordPress Security Summary

I protected files and directories in my blog site, fortified the “wp-config.php” file, and set up a firewall security system. Before altering permissions, we verified our ability to access the files and directories. After confirming our access, we modified the permissions to ensure no unauthorized access. We checked again once the modifications were completed to ensure the changes were effective.
Then, to enhance the security of the “wp-config.php” file, we relocated it to a different folder. We also incorporated a robust code into the “.htaccess” file to prevent unauthorized configuration changes. Lastly, we installed a firewall plugin for security scanning and surveillance. This will help secure the site from any malware or other vulnerable assets.

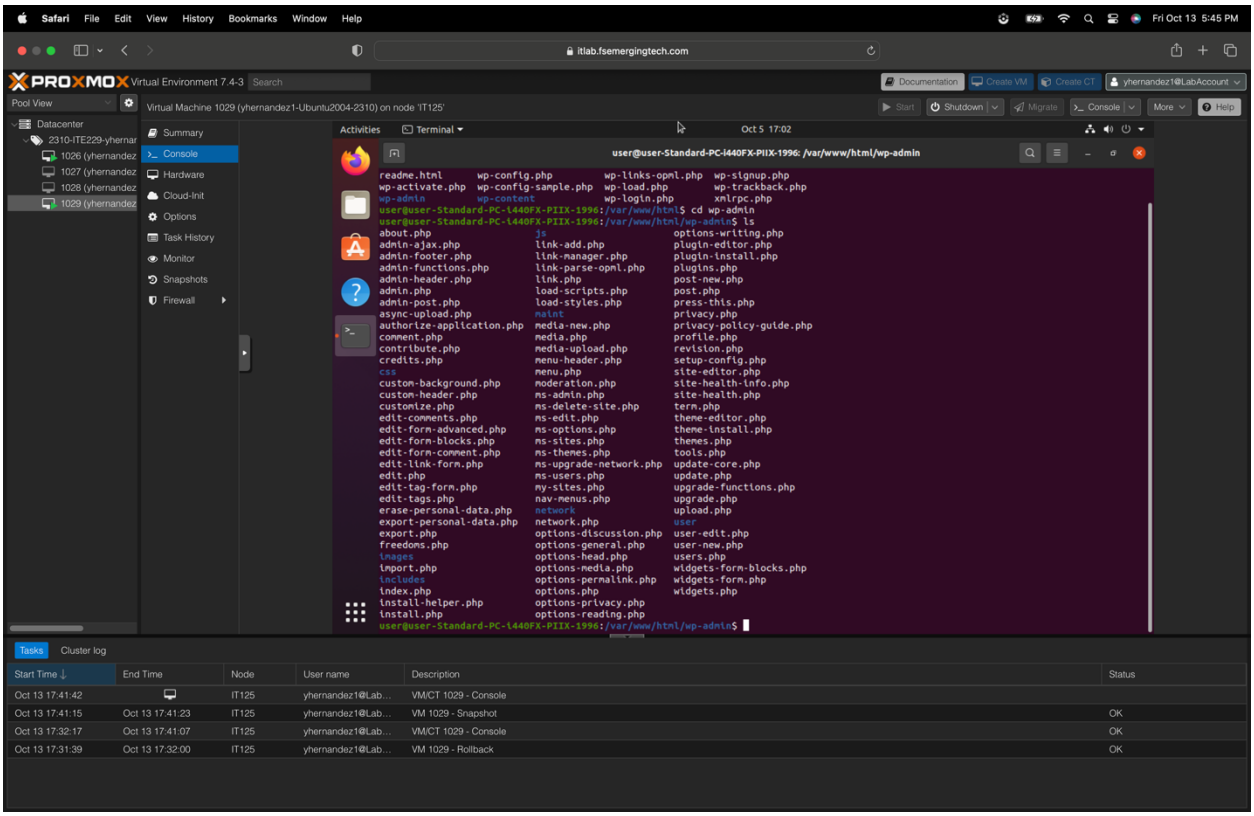
Defense-in-depth

My strategy embodies the defense in depth principle because I've implemented diverse security measures at various levels of the WordPress environment. Each step contributes to the overall security, ensuring that even if one control fails, others are in place to prevent or mitigate a security incident. After setting up our LAMP server with WordPress, we examined the file permissions. We adjusted these permissions to ensure that only the essential level of access was given, providing WordPress and its plugins operated correctly. This minimized any undue access to specific files and directories. Also, we enhanced the security of the wp-config.php file by relocating it to a folder above the one it was before.

Additionally, we updated its permissions and tweaked the .htaccess file to block unwarranted access. This action not only moved the config file from its conventional location but also safeguarded it from unauthorized edits. Finally, we integrated the Shield Security plugin, which offers security scanning, activity monitoring, and IP filtering features. This tool helps in the early detection of vulnerabilities, tracks site activities, and controls site access based on IP addresses, providing a comprehensive security layer.

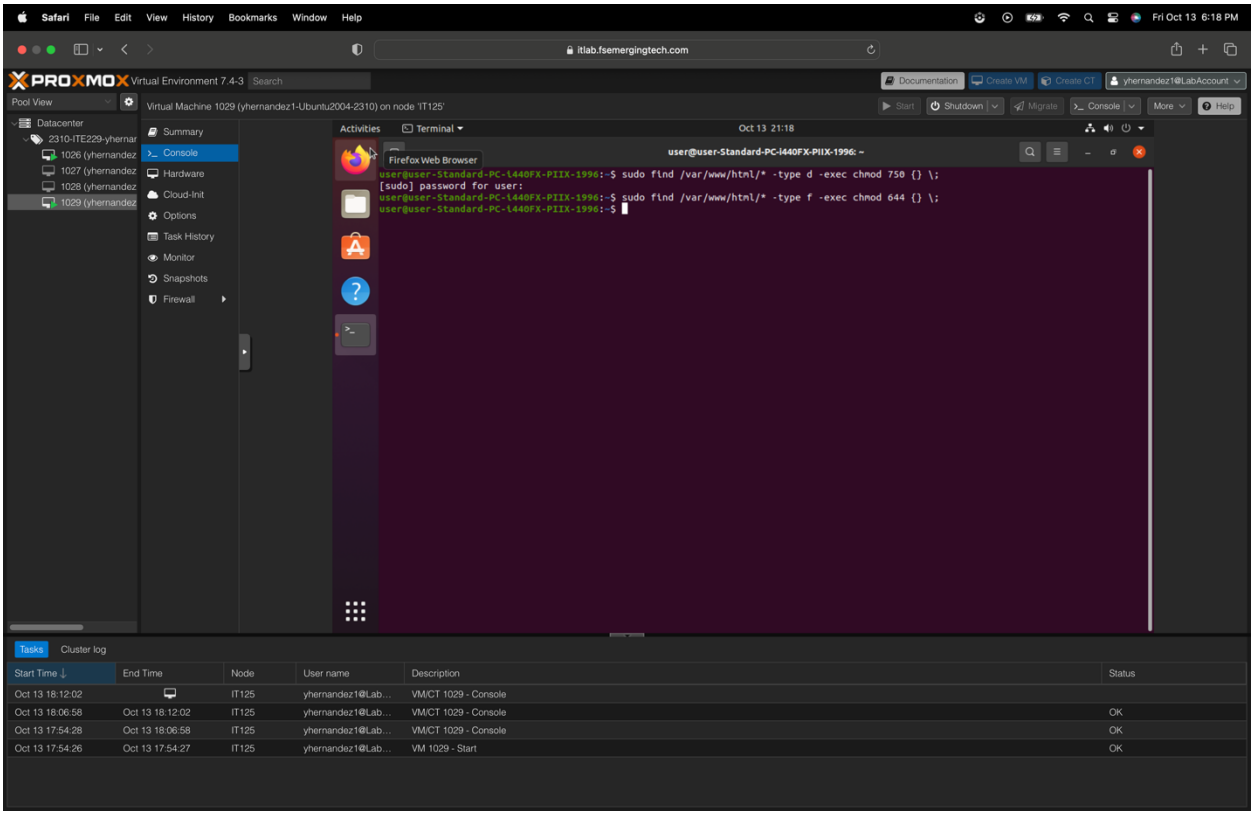
File Permissions

Vulnerability



To check for permissions for files and directories, go to the terminal and, on the command line, type **cd /var/www/html/wp-admin.** Permissions must be changed if it allows you to go into the file.

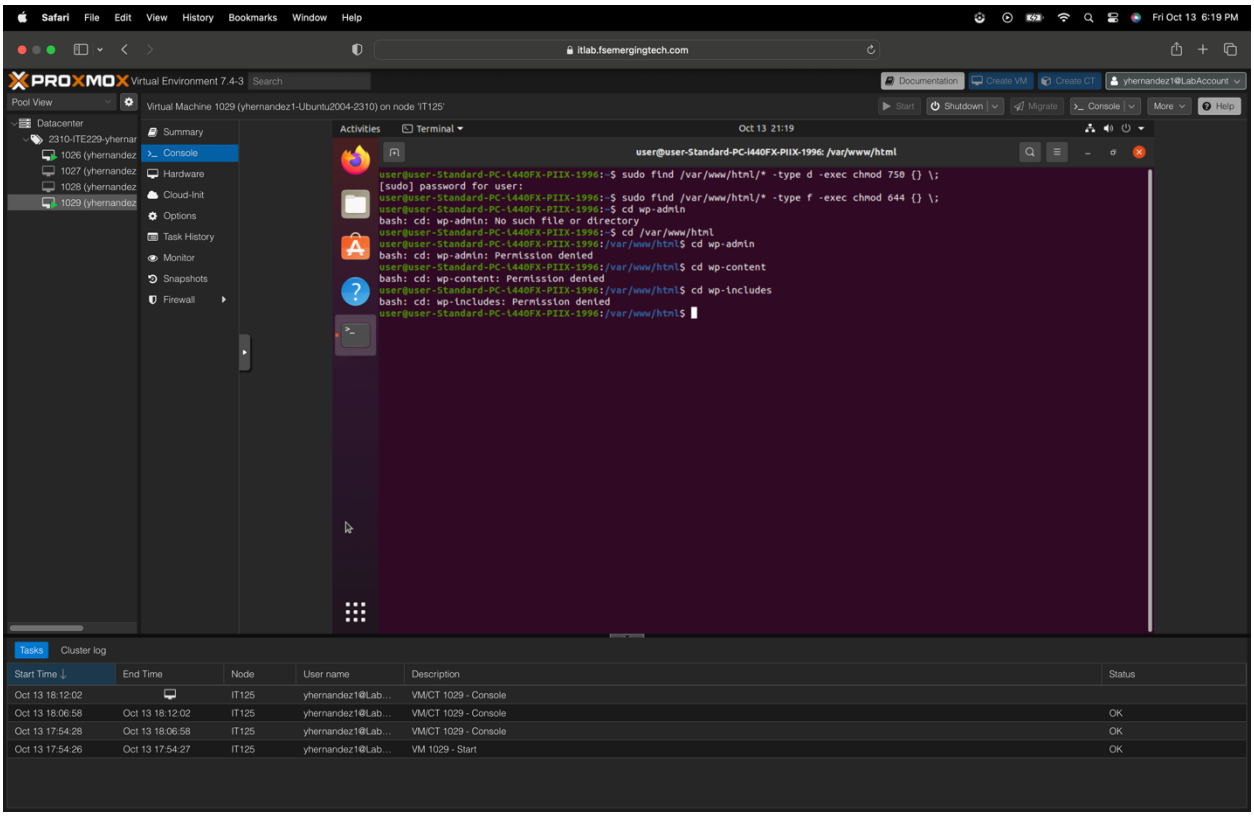
Configuration



To configure files and directories, go to the terminal and on the command line, type **sudo find /var/www/html/* -type d -exec chmod 750 {} \;** this will change the permissions for the directories. Then type **sudo find /var/www/html/* -type f -exec chmod 644 {} \;** this will change permissions for the files.

Validation

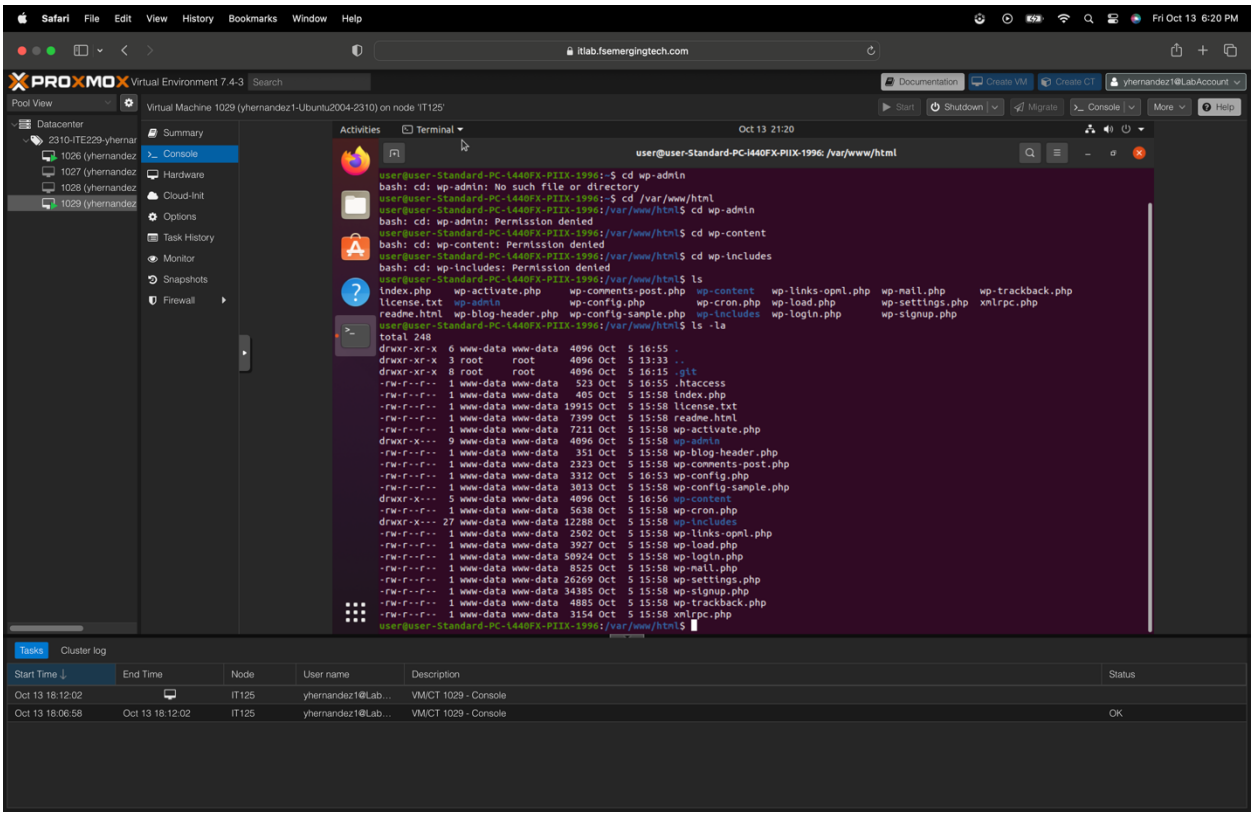
Before making any modifications, I ensured I had complete access to the files and directories by entering the command "cd wp-admin." Successfully accessing it confirmed my full access rights. After making the necessary changes, I tested directory access once more by trying to create a new directory. A "permission denied" message indicated that the modifications were effective, restricting access and enforcing a principle of least privilege.



To verify that permissions were changed, go to the terminal and type cd wp-admin, cd wp-content, and cd wp-includes on the command line. If they all say permission denied, then the configuration worked.

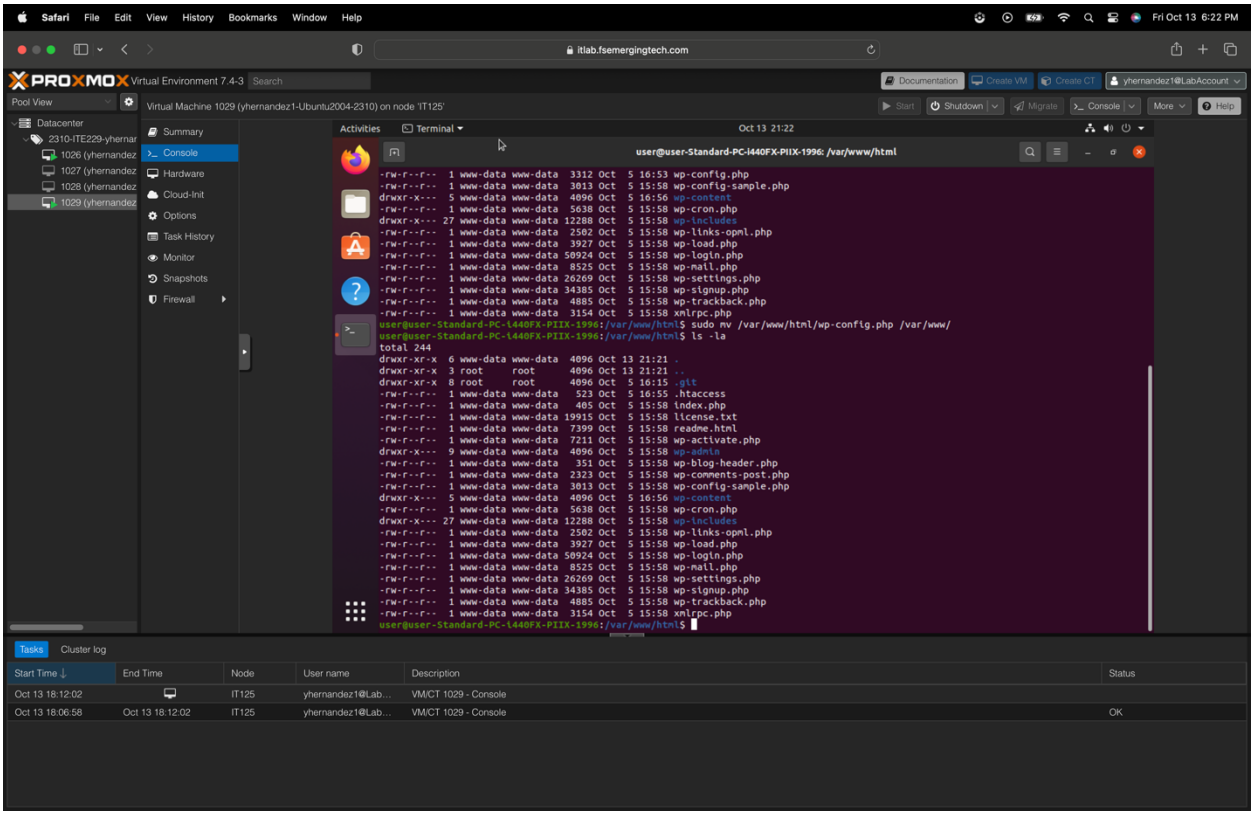
Securing wp-config.php

Vulnerability



To check if the wp-config.php file is vulnerable, go to the terminal and type **cd /var/www/html/wp-config.php.** If able to access it, then configurations need to be changed.

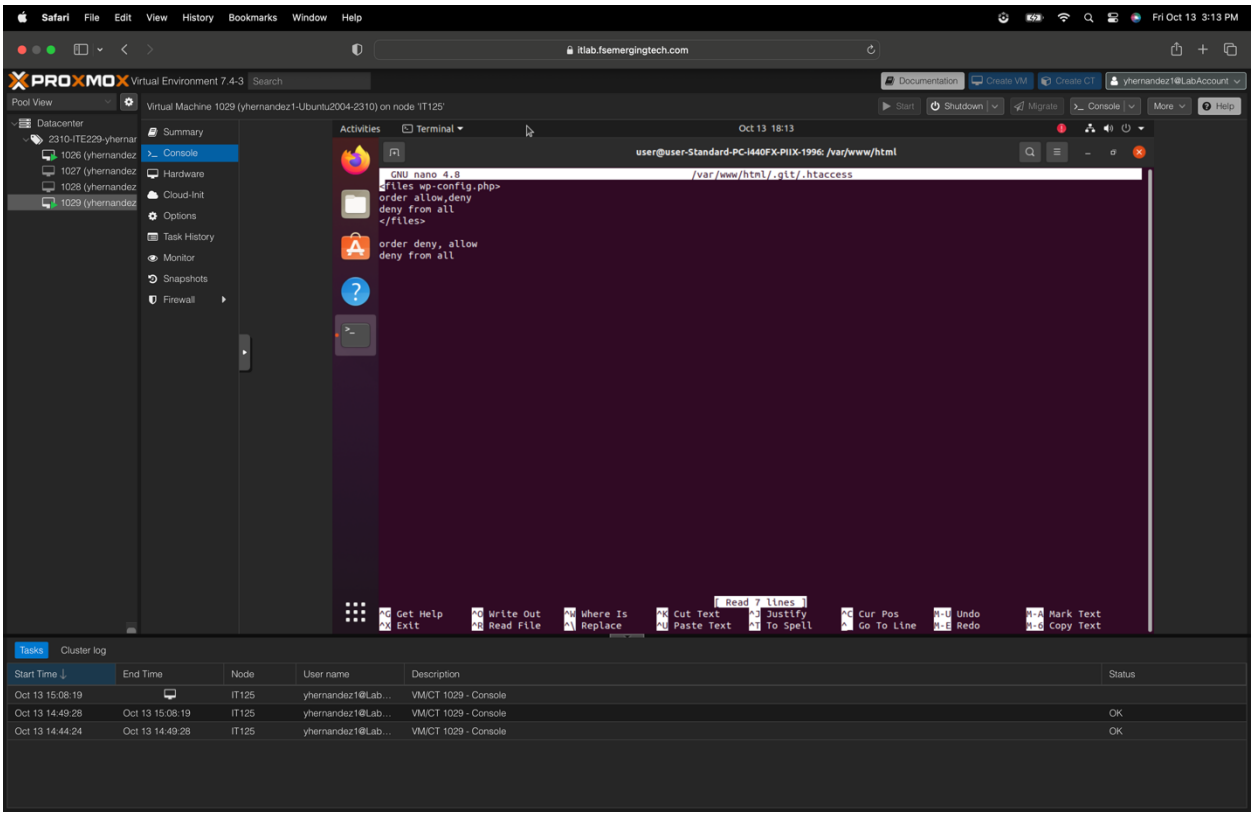
Configuration

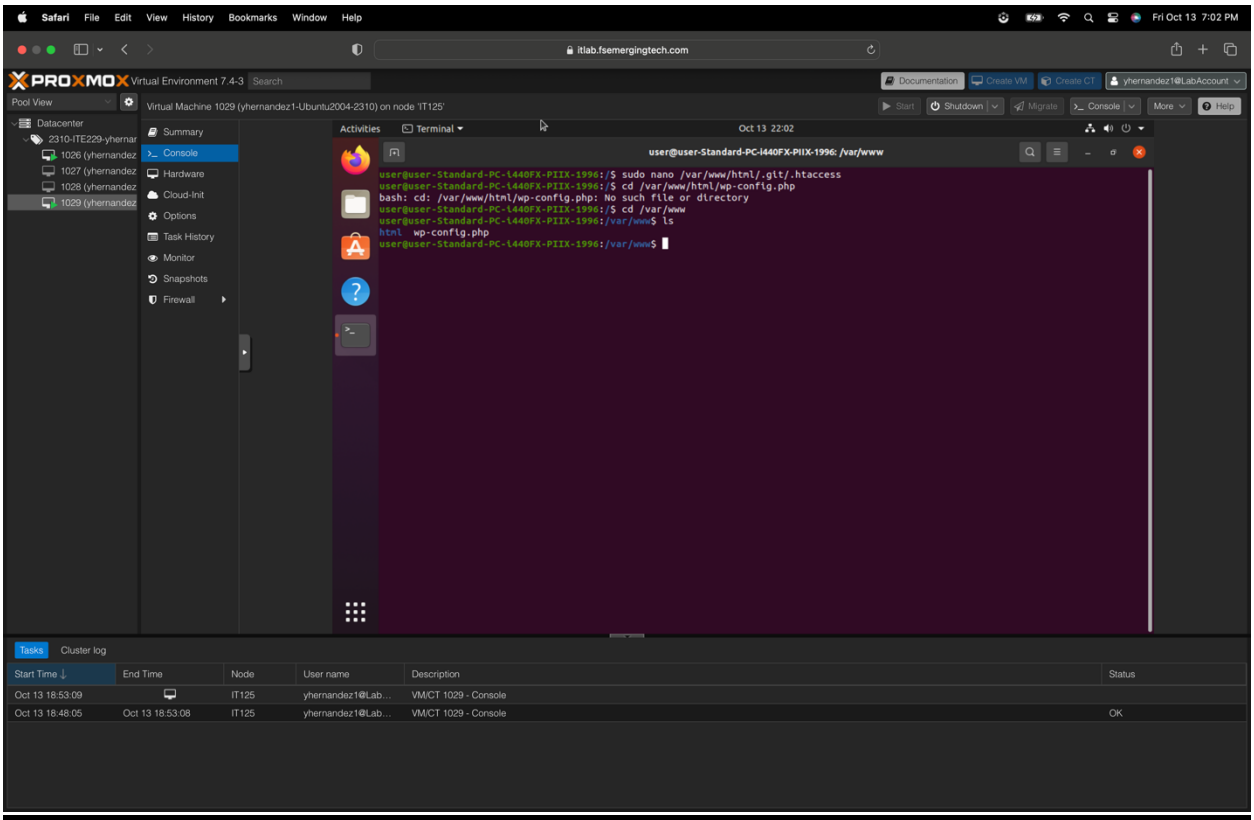


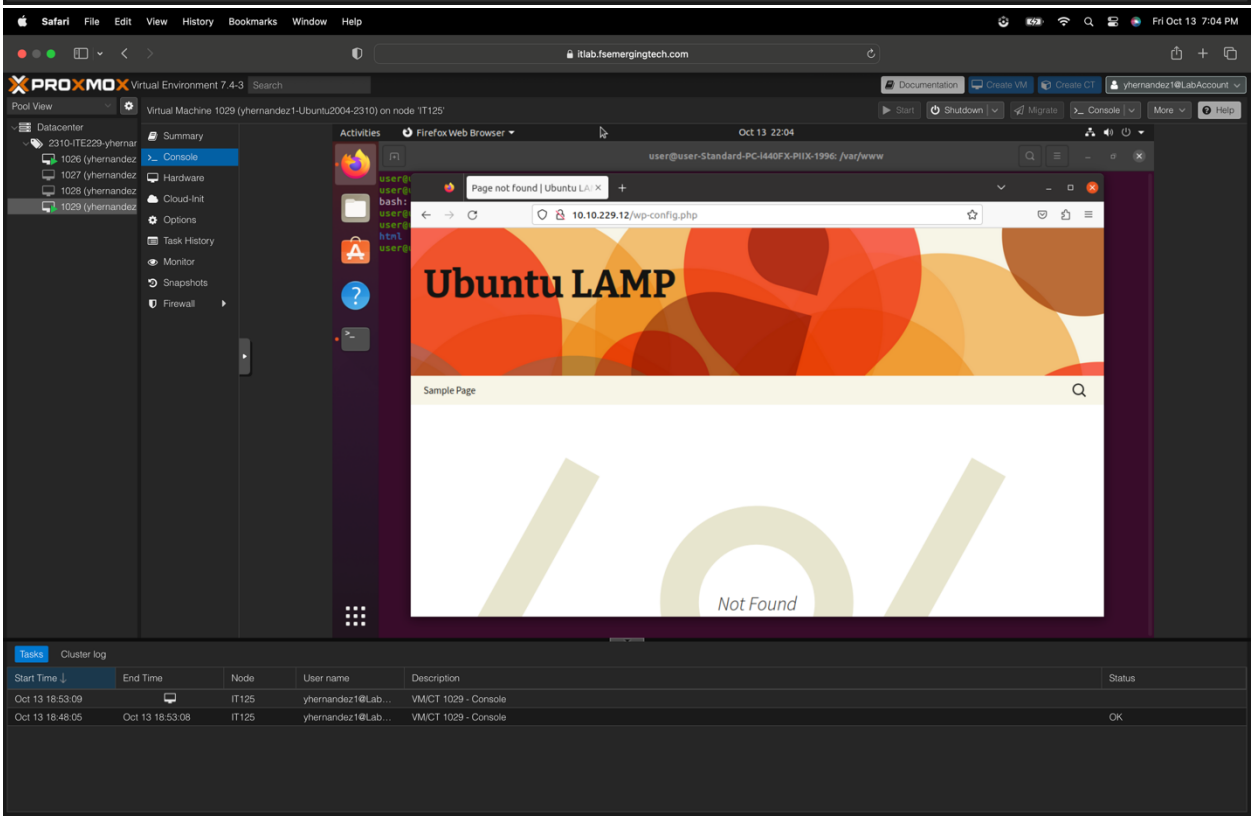
To configure the wp-config.php file, go to the terminal, and on the command line, type **sudo mv /var/www/html/wp-config.php var/www/** this will move the file to another directory. Then type **sudo nano /var/www/html/.git/.htaccess** This will take you to .htaccess, and you will add the following code
<files wp-config.php>
order allow,deny
deny from all
</files>

Validation

Before initiating any adjustments to the file, it was essential to ensure that I had the necessary permissions to access and modify it. To confirm this, I attempted to open the file. Once my access was ascertained, I proceeded with the following steps to enhance its security. Using the 'nano' editor, a popular text editor for many UNIX-based systems, I appended specific instructions to deny unauthorized file access. This is crucial in safeguarding sensitive files, especially if they contain configurations or data that shouldn't be publicly accessible. A practical approach was to try and access the file from a web browser to test the effectiveness of my modifications. So, I navigated to http://10.10.229.12/wp-config.php to see if my held changes. The result was a blank page. In web security, this often signifies that access to a particular resource has been restricted or blocked, making it unavailable for viewing. Seeing this confirmed that my protective measures were effectively implemented, preventing unauthorized access and enhancing the file's security.


Safari File Edit View History Bookmarks Window Help
Fri Oct 13 3:13 PM
itlab.fsemergingtech.com
PROXMOX Virtual Environment 7.4-3
Search
Documentation
Create VM
Create CT
yhernandez1@LabAccount
Pool View
Virtual Machine 1029 (yhernandez1-Ubuntu2004-2310) on node 'IT125'
Start
Shutdown
Migrate
Console
More
Help
Datacenter
2310-ITE229-yhernar
1026 (yhernandez
1027 (yhernandez
1028 (yhernandez
1029 (yhernandez
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Snapshots
Firewall
Activities
Terminal
Oct 13 18:13
user@user-Standard-PC-I440FX-PIIX-1996: /var/www/html
GNU nano 4.8
/var/www/html/.git/.htaccess
<files wp-config.php>
order allow,deny
deny from all
</files>
order deny, allow
deny from all
[Read 7 lines]
^G Get Help
^O Write Out
^W Where Is
^K Cut Text
^J Justify
^C Cur Pos
M-U Undo
M-A Mark Text
^X Exit
^R Read File
^\ Replace
^U Paste Text
^T To Spell
^_ Go To Line
M-E Redo
M-6 Copy Text
Tasks
Cluster log
Start Time
End Time
Node
User name
Description
Status
Oct 13 15:08:19
IT125
yhernandez1@Lab...
VM/CT 1029 - Console
Oct 13 14:49:28
Oct 13 15:08:19
IT125
yhernandez1@Lab...
VM/CT 1029 - Console
OK
Oct 13 14:44:24
Oct 13 14:49:28
IT125
yhernandez1@Lab...
VM/CT 1029 - Console
OK

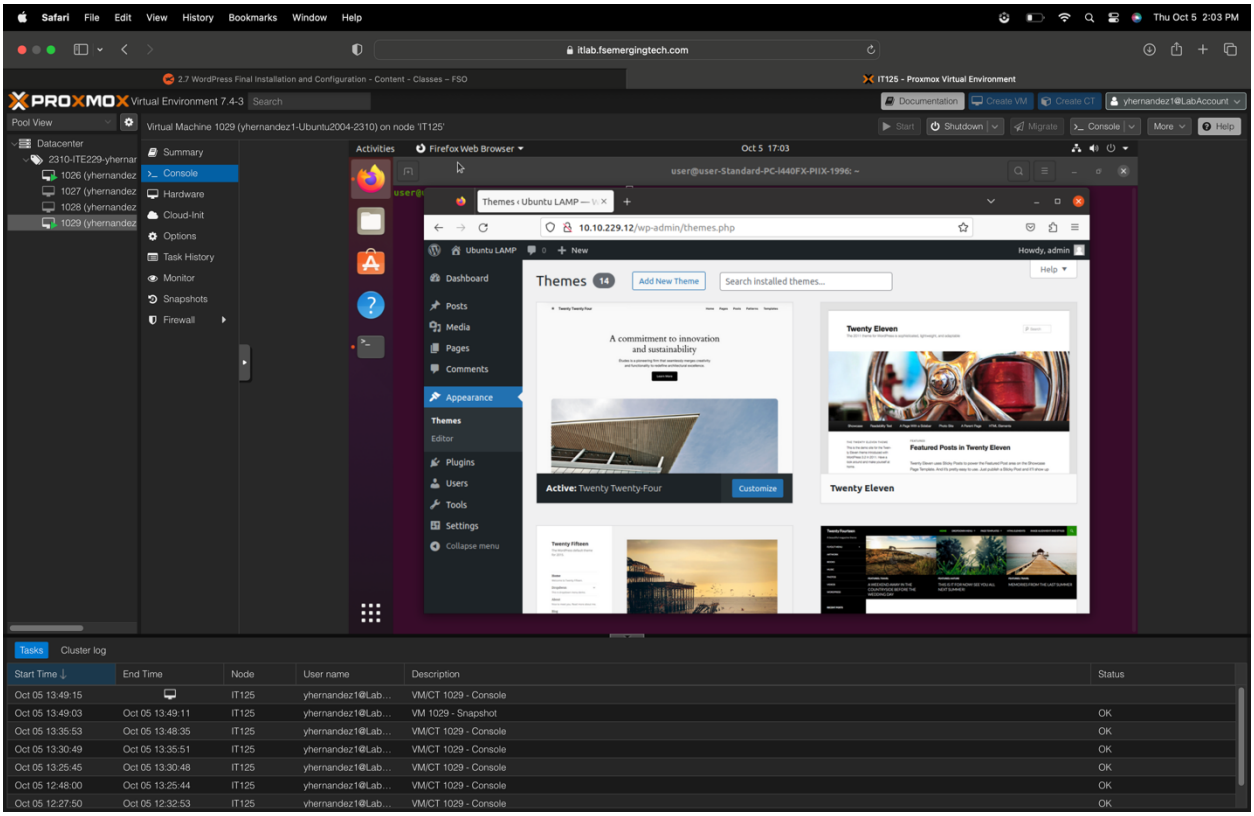

Safari File Edit View History Bookmarks Window Help
Fri Oct 13 7:02 PM
itlab.fsemergingtech.com
PROXMOX Virtual Environment 7.4-3
Search
Documentation
Create VM
Create CT
yhernandez1@LabAccount
Pool View
Virtual Machine 1029 (yhernandez1-Ubuntu2004-2310) on node 'IT125'
Start
Shutdown
Migrate
Console
More
Help
Datacenter
2310-ITE229-yhernar
1026 (yhernandez
1027 (yhernandez
1028 (yhernandez
1029 (yhernandez
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Snapshots
Firewall
Activities
Terminal
Oct 13 22:02
user@user-Standard-PC-i440FX-PIIX-1996: /var/www
user@user-Standard-PC-i440FX-PIIX-1996:/$ sudo nano /var/www/html/.git/.htaccess
user@user-Standard-PC-i440FX-PIIX-1996:/$ cd /var/www/html/wp-config.php
bash: cd: /var/www/html/wp-config.php: No such file or directory
user@user-Standard-PC-i440FX-PIIX-1996:/$ cd /var/www
user@user-Standard-PC-i440FX-PIIX-1996:/var/www$ ls
html wp-config.php
user@user-Standard-PC-i440FX-PIIX-1996:/var/www$
Tasks
Cluster log
Start Time
End Time
Node
User name
Description
Status
Oct 13 18:53:09
IT125
yhernandez1@Lab...
VM/CT 1029 - Console
Oct 13 18:48:05
Oct 13 18:53:08
IT125
yhernandez1@Lab...
VM/CT 1029 - Console
OK


Safari File Edit View History Bookmarks Window Help
Fri Oct 13 7:04 PM
itlab.fsemergingtech.com
PROXMOX Virtual Environment 7.4-3
Search
Documentation
Create VM
Create CT
yhernandez1@LabAccount
Pool View
Virtual Machine 1029 (yhernandez1-Ubuntu2004-2310) on node 'IT125'
Start
Shutdown
Migrate
Console
More
Help
Datacenter
2310-ITE229-yhernar
1026 (yhernandez
1027 (yhernandez
1028 (yhernandez
1029 (yhernandez
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Snapshots
Firewall
Activities
Firefox Web Browser
Oct 13 22:04
user@user-Standard-PC-i440FX-PIIX-1996: /var/www
Page not found | Ubuntu LA
10.10.229.12/wp-config.php
Ubuntu LAMP
Sample Page
Not Found
Tasks
Cluster log
Start Time
End Time
Node
User name
Description
Status
Oct 13 18:53:09
IT125
yhernandez1@Lab...
VM/CT 1029 - Console
Oct 13 18:48:05
Oct 13 18:53:08
IT125
yhernandez1@Lab...
VM/CT 1029 - Console
OK

To validate, you will go to Firefox web browser, then on the address bar, type **10.10229.12/wp-config.php.** This will redirect you to the config page, and if everything was moved and configured correctly, a page not found should load up.

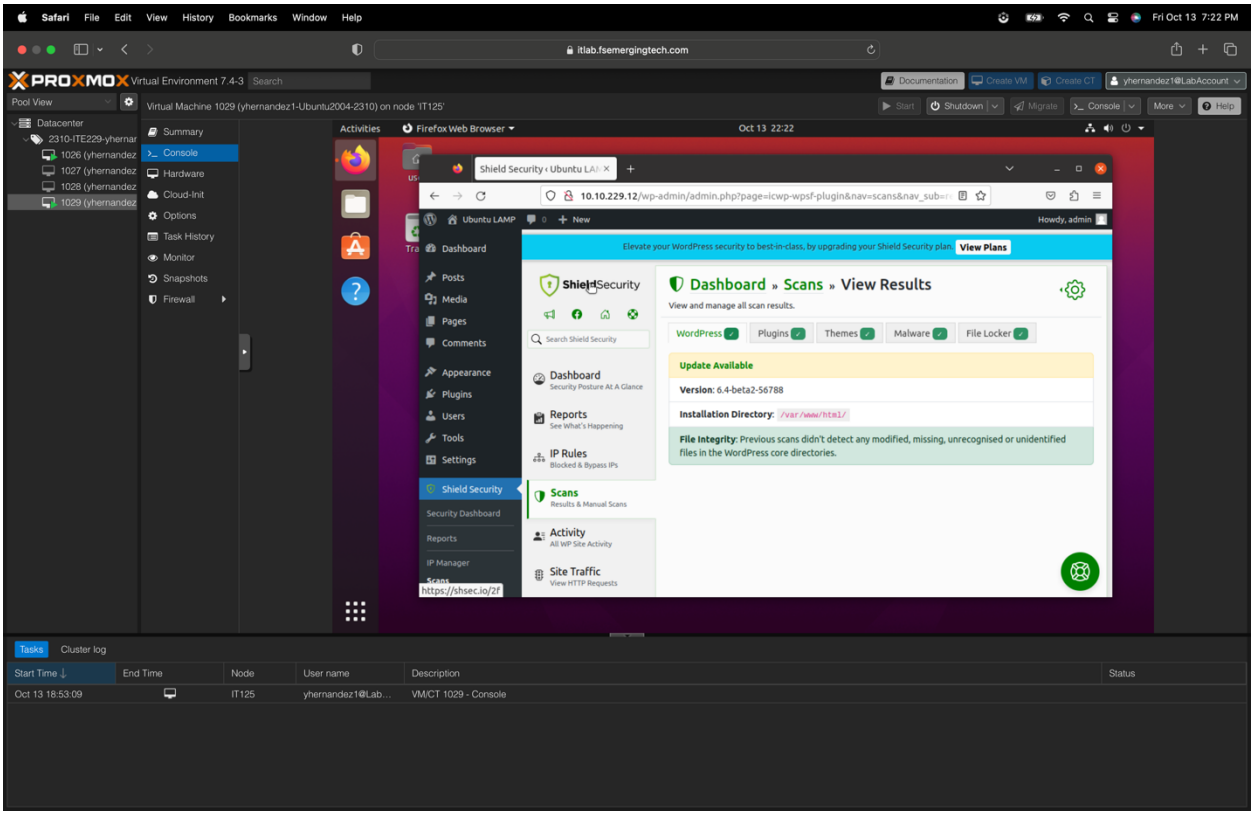
Firewall (Shield)

Vulnerability



On the Firefox web browser, click on the address bar, type **10.10.229.12**, then click enter. If no firewall is running as a plugin, there is a vulnerability.

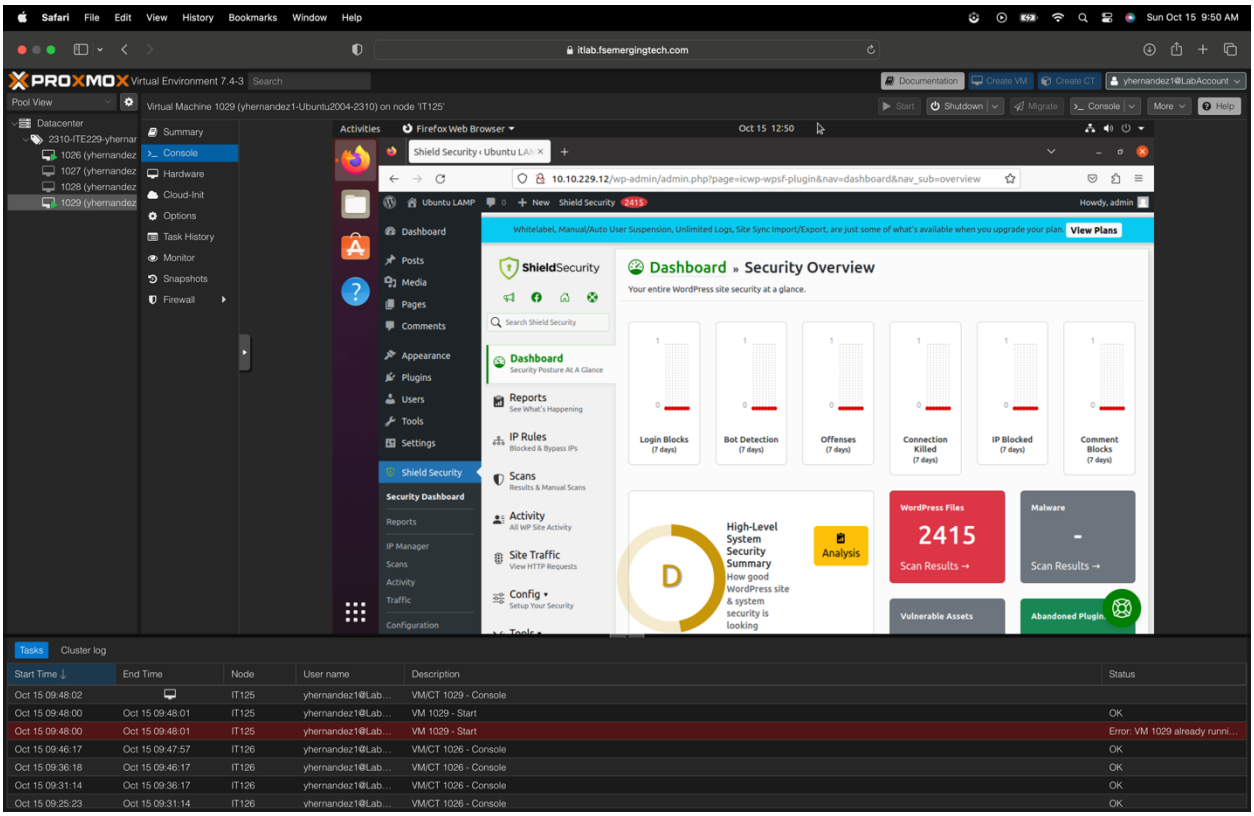
Configuration

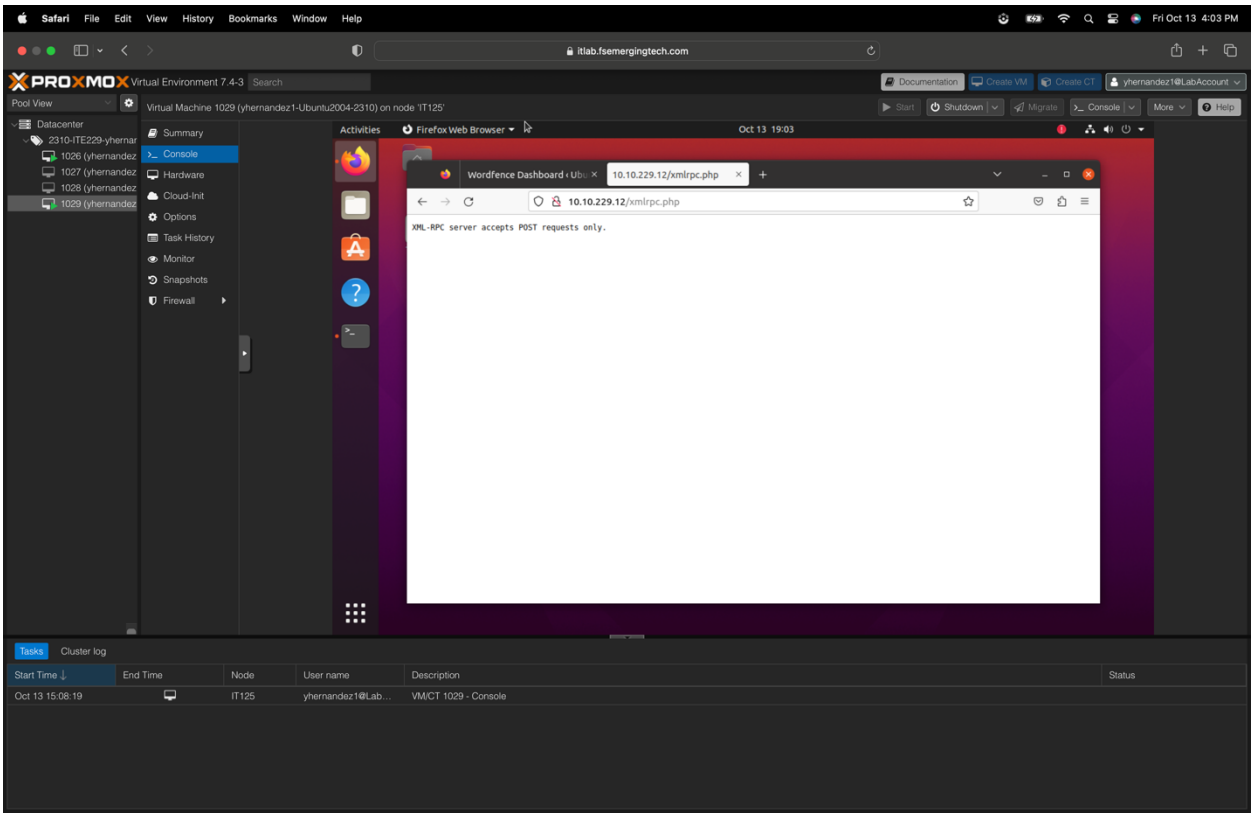


To configure the firewall in WordPress, login to Ubuntu, then on Firefox, go to **10.10.229.12,** then click on plugins. Search for **Shield Security,** install the plugin, and follow the instructions. Once fully established, make sure that it's active and running.

Validation

Before implementing any modifications, I first assessed the status of the firewall. It was found to be inactive, which needed a change. To address this, I integrated a plugin named 'Security Shield.' I opted for the free version, which allows scanning and overseeing the firewall in WordPress. After installing the plugin, I reloaded the page and showed that the firewall was working correctly. This will scan, monitor activity, and filter IP.





To validate the proper functionality of the security shield, go to **10.10.229.12/xmlrpc.php.** A POST requests-only page should load up if it is properly working.

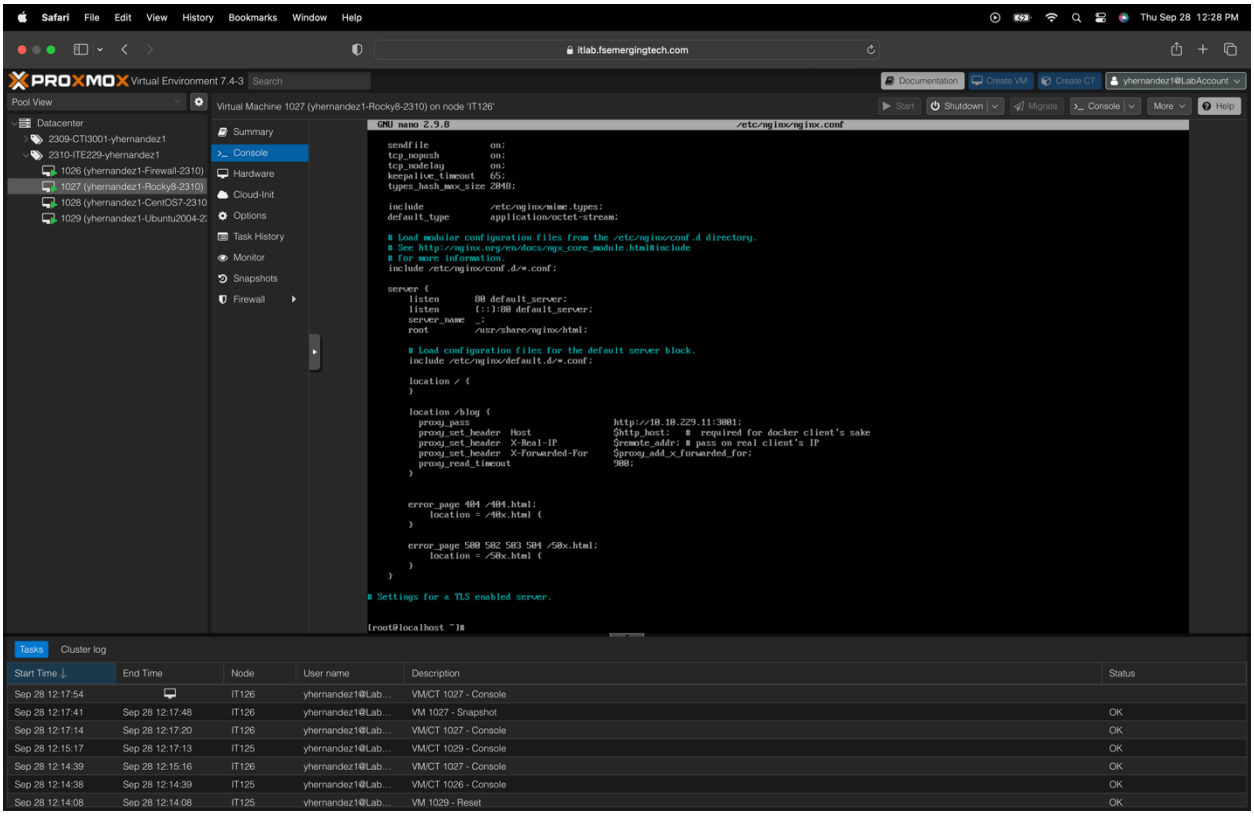
Conclusion

To implement a security methodology, my initial step involved conducting extensive research. Once I had completed my research, I assessed the necessary changes required in files and directories. I verified my access to these files and directories before adjusting their permissions. After completing the permission changes, I revisited the files to ensure I could no longer access them. Once I received "permission denied" for all three files, I moved on to the next task.

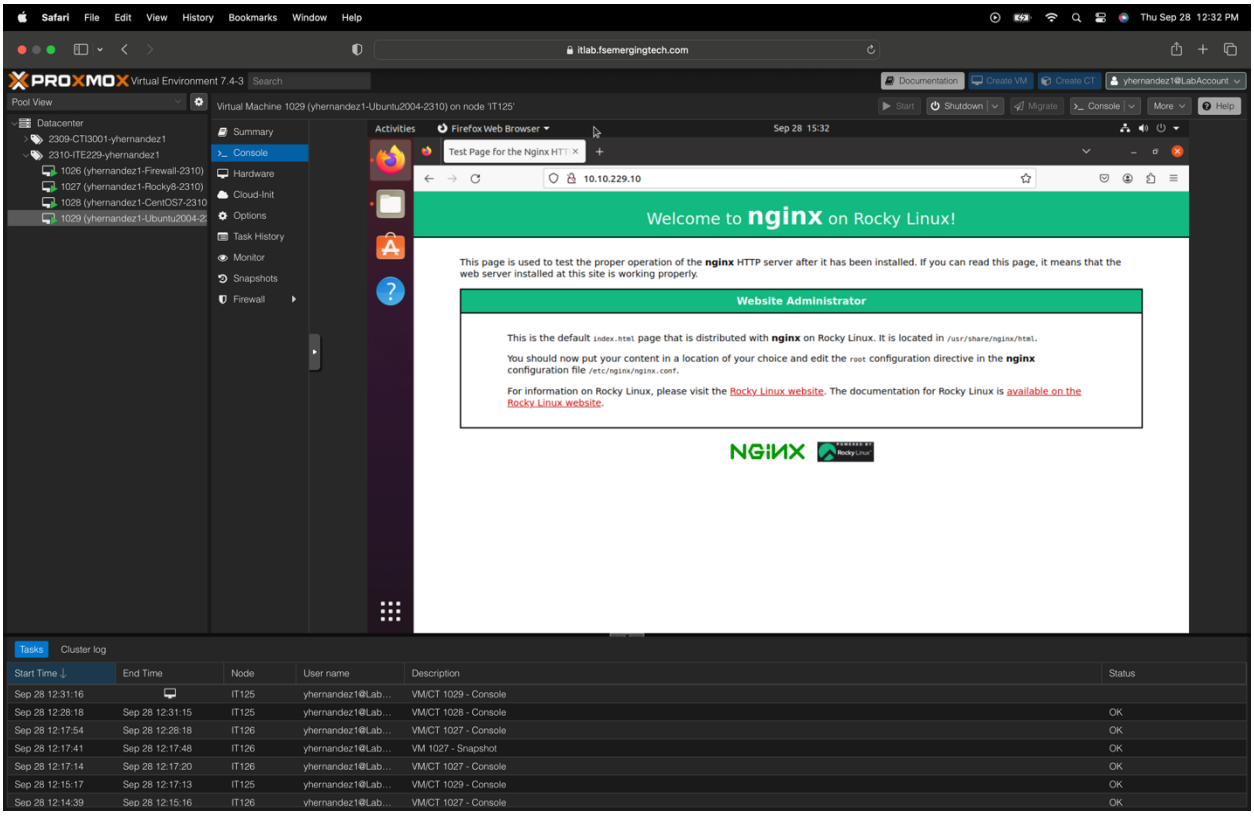
The second vulnerability I addressed involved the wp-config.php file. This was resolved by relocating the directory and modifying the code within the .htaccess file. After completing these tasks, I confirmed that the file was no longer accessible.

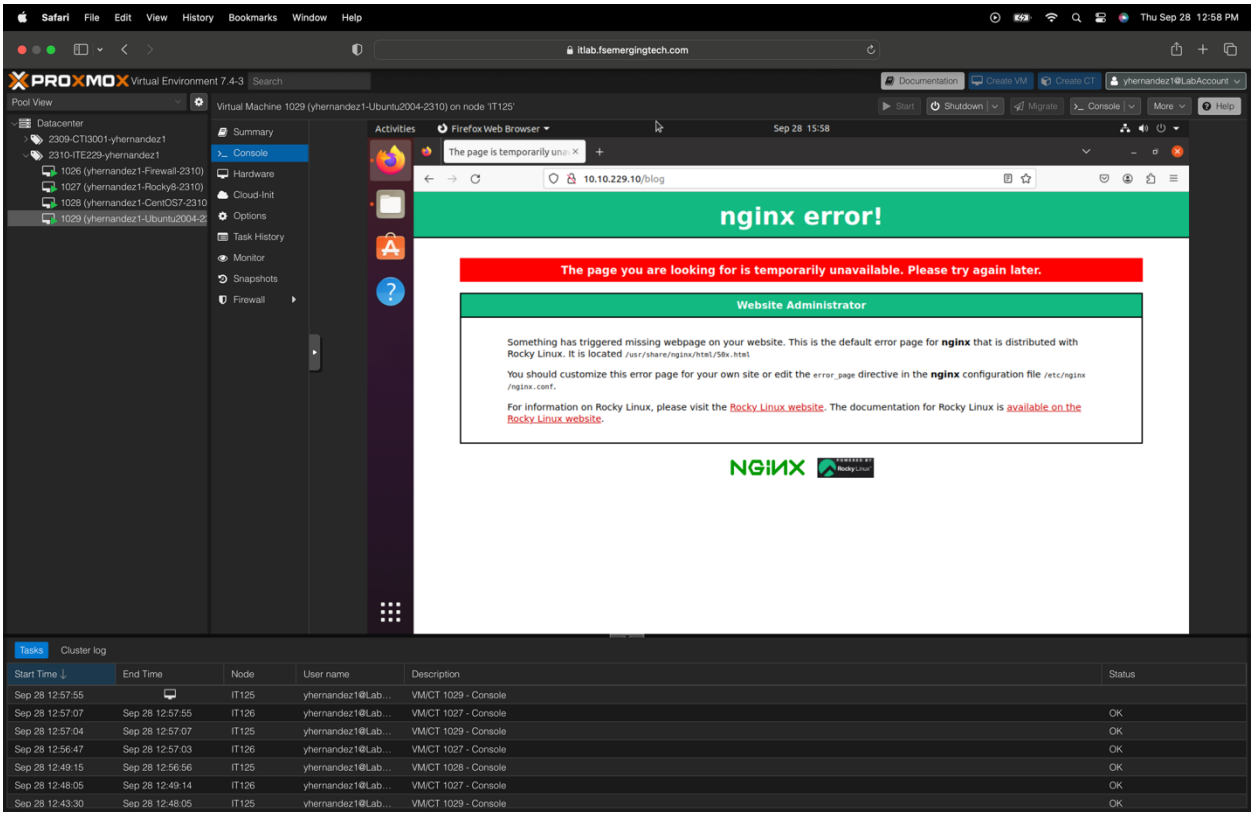
To address the last vulnerability, I implemented a firewall plugin, specifically Shield Security, which operates in the background to conduct security scans for malware, monitor activity, and filter IP addresses.

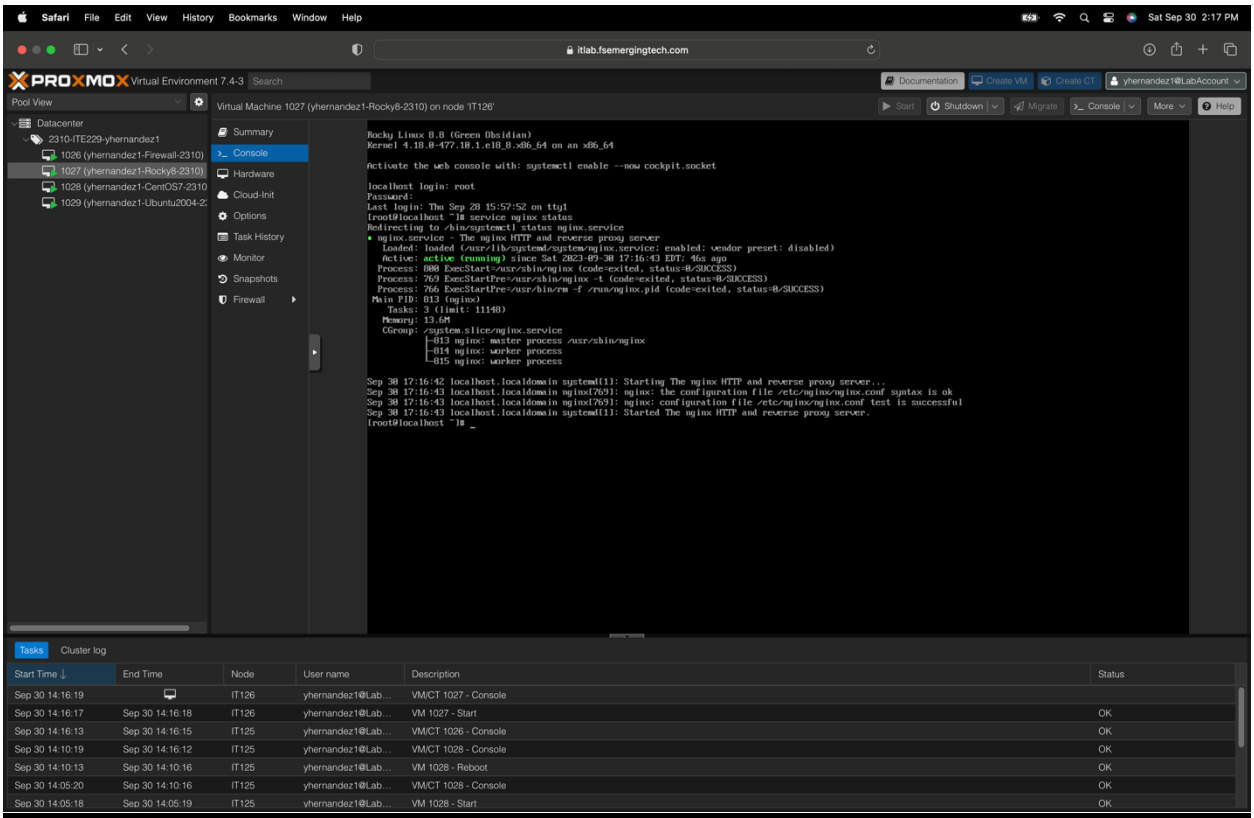
Appendix A

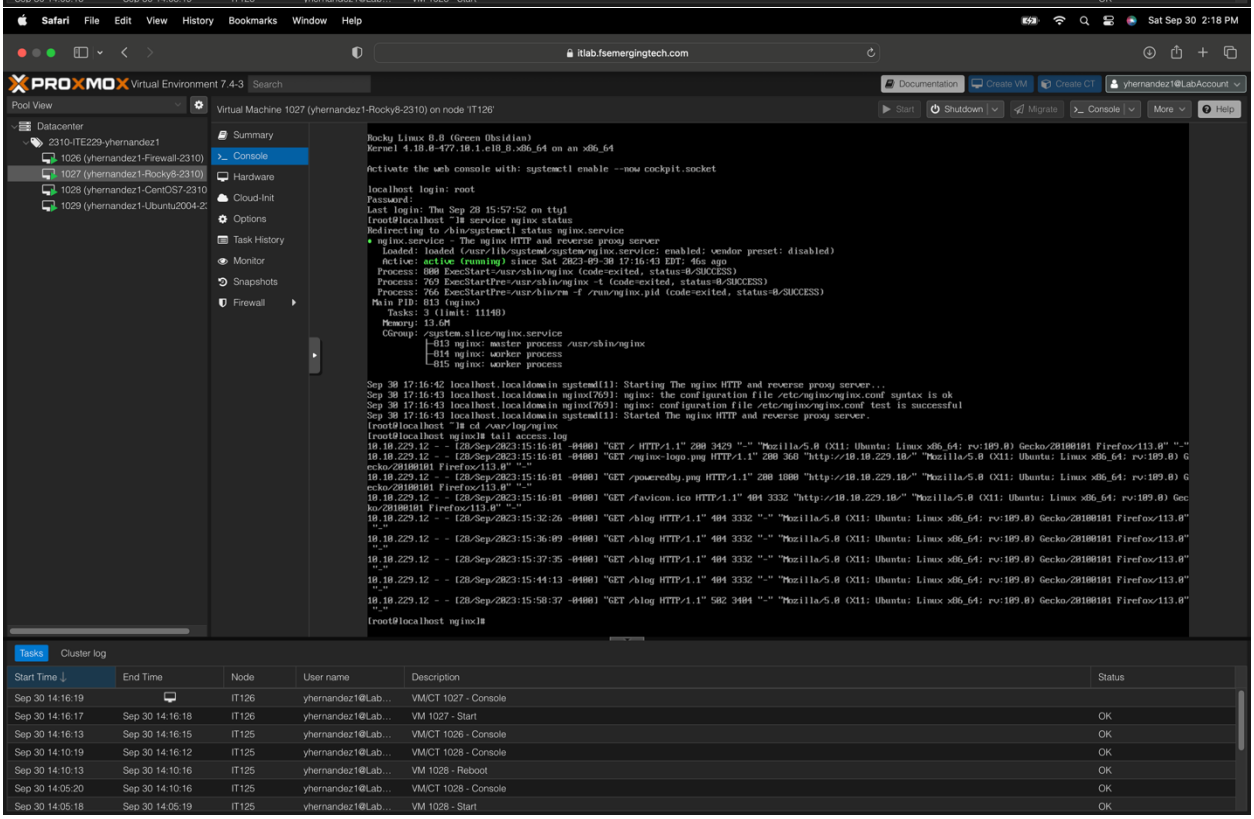


Appendix B


Safari File Edit View History Bookmarks Window Help
Thu Sep 28 12:32 PM
itlab.fsemergingtech.com
PROXMOX Virtual Environment 7.4-3
Virtual Machine 1029 (yhernandez1-Ubuntu2004-2310) on node 'IT125'
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Snapshots
Firewall
Activities
Firefox Web Browser
Sep 28 15:32
10.10.229.10
Welcome to nginx on Rocky Linux!
This page is used to test the proper operation of the nginx HTTP server after it has been installed. If you can read this page, it means that the web server installed at this site is working properly.
Website Administrator
This is the default index.html page that is distributed with nginx on Rocky Linux. It is located in /usr/share/nginx/html.
You should now put your content in a location of your choice and edit the root configuration directive in the nginx configuration file /etc/nginx/nginx.conf.
For information on Rocky Linux, please visit the Rocky Linux website. The documentation for Rocky Linux is available on the Rocky Linux website.
NGINX
Tasks
Cluster log
Start Time
End Time
Node
User name
Description
Status
Sep 28 12:31:16 IT125 yhernandez1@Lab... VM/CT 1029 - Console
Sep 28 12:28:18 Sep 28 12:31:15 IT125 yhernandez1@Lab... VM/CT 1028 - Console OK
Sep 28 12:17:54 Sep 28 12:28:18 IT126 yhernandez1@Lab... VM/CT 1027 - Console OK
Sep 28 12:17:41 Sep 28 12:17:48 IT126 yhernandez1@Lab... VM 1027 - Snapshot OK
Sep 28 12:17:14 Sep 28 12:17:20 IT126 yhernandez1@Lab... VM/CT 1027 - Console OK
Sep 28 12:15:17 Sep 28 12:17:13 IT125 yhernandez1@Lab... VM/CT 1029 - Console OK
Sep 28 12:14:39 Sep 28 12:15:16 IT126 yhernandez1@Lab... VM/CT 1027 - Console OK


Safari File Edit View History Bookmarks Window Help
Thu Sep 28 12:58 PM
itlab.fsemergingtech.com
PROXMOX Virtual Environment 7.4-3
Virtual Machine 1029 (yhernandez1-Ubuntu2004-2310) on node 'IT125'
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Snapshots
Firewall
Activities
Firefox Web Browser
Sep 28 15:58
10.10.229.10/blog
nginx error!
The page you are looking for is temporarily unavailable. Please try again later.
Website Administrator
Something has triggered missing webpage on your website. This is the default error page for nginx that is distributed with Rocky Linux. It is located /usr/share/nginx/html/50x.html
You should customize this error page for your own site or edit the error_page directive in the nginx configuration file /etc/nginx/nginx.conf.
For information on Rocky Linux, please visit the Rocky Linux website. The documentation for Rocky Linux is available on the Rocky Linux website.
NGINX
Tasks
Cluster log
Start Time
End Time
Node
User name
Description
Status
Sep 28 12:57:55 IT125 yhernandez1@Lab... VM/CT 1029 - Console
Sep 28 12:57:07 Sep 28 12:57:55 IT126 yhernandez1@Lab... VM/CT 1027 - Console OK
Sep 28 12:57:04 Sep 28 12:57:07 IT125 yhernandez1@Lab... VM/CT 1029 - Console OK
Sep 28 12:56:47 Sep 28 12:57:03 IT126 yhernandez1@Lab... VM/CT 1027 - Console OK
Sep 28 12:49:15 Sep 28 12:56:56 IT125 yhernandez1@Lab... VM/CT 1028 - Console OK
Sep 28 12:48:05 Sep 28 12:49:14 IT126 yhernandez1@Lab... VM/CT 1027 - Console OK
Sep 28 12:43:30 Sep 28 12:48:05 IT125 yhernandez1@Lab... VM/CT 1029 - Console OK


Safari File Edit View History Bookmarks Window Help
Sat Sep 30 2:17 PM
itlab.fsemergingtech.com
PROXMOX Virtual Environment 7.4-3
Search
Documentation
Create VM
Create CT
yhernandez1@LabAccount
Pool View
Virtual Machine 1027 (yhernandez1-Rocky8-2310) on node 'IT126'
Start
Shutdown
Migrate
Console
More
Help
Datacenter
2310-ITE229-yhernandez1
1026 (yhernandez1-Firewall-2310)
1027 (yhernandez1-Rocky8-2310)
1028 (yhernandez1-CentOS7-2310
1029 (yhernandez1-Ubuntu2004-2
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Snapshots
Firewall
Rocky Linux 8.8 (Green Obsidian)
Kernel 4.18.0-477.10.1.el8_8.x86_64 on an x86_64
Activate the web console with: systemctl enable --now cockpit.socket
localhost login: root
Password:
Last login: Thu Sep 28 15:57:52 on tty1
[root@localhost ~]# service nginx status
Redirecting to /bin/systemctl status nginx.service
● nginx.service - The nginx HTTP and reverse proxy server
Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled)
Active: active (running) since Sat 2023-09-30 17:16:43 EDT; 46s ago
Process: 808 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
Process: 769 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
Process: 766 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
Main PID: 813 (nginx)
Tasks: 3 (limit: 11148)
Memory: 13.6M
CGroup: /system.slice/nginx.service
├─813 nginx: master process /usr/sbin/nginx
├─814 nginx: worker process
└─815 nginx: worker process
Sep 30 17:16:42 localhost.localdomain systemd[1]: Starting The nginx HTTP and reverse proxy server...
Sep 30 17:16:43 localhost.localdomain nginx[769]: nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
Sep 30 17:16:43 localhost.localdomain nginx[769]: nginx: configuration file /etc/nginx/nginx.conf test is successful
Sep 30 17:16:43 localhost.localdomain systemd[1]: Started The nginx HTTP and reverse proxy server.
[root@localhost ~]#
Tasks
Cluster log
Start Time
End Time
Node
User name
Description
Status
Sep 30 14:16:19 IT126 yhernandez1@Lab... VM/CT 1027 - Console
Sep 30 14:16:17 Sep 30 14:16:18 IT126 yhernandez1@Lab... VM 1027 - Start OK
Sep 30 14:16:13 Sep 30 14:16:15 IT125 yhernandez1@Lab... VM/CT 1026 - Console OK
Sep 30 14:10:19 Sep 30 14:16:12 IT125 yhernandez1@Lab... VM/CT 1028 - Console OK
Sep 30 14:10:13 Sep 30 14:10:16 IT125 yhernandez1@Lab... VM 1028 - Reboot OK
Sep 30 14:05:20 Sep 30 14:10:16 IT125 yhernandez1@Lab... VM/CT 1028 - Console OK
Sep 30 14:05:18 Sep 30 14:05:19 IT125 yhernandez1@Lab... VM 1028 - Start OK


Safari File Edit View History Bookmarks Window Help
Sat Sep 30 2:18 PM
itlab.fsemergingtech.com
PROXMOX Virtual Environment 7.4-3
Search
Documentation
Create VM
Create CT
yhernandez1@LabAccount
Pool View
Virtual Machine 1027 (yhernandez1-Rocky8-2310) on node 'IT126'
Start
Shutdown
Migrate
Console
More
Help
Datacenter
2310-ITE229-yhernandez1
1026 (yhernandez1-Firewall-2310)
1027 (yhernandez1-Rocky8-2310)
1028 (yhernandez1-CentOS7-2310
1029 (yhernandez1-Ubuntu2004-2
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Snapshots
Firewall
Rocky Linux 8.8 (Green Obsidian)
Kernel 4.18.0-477.10.1.el8_8.x86_64 on an x86_64
Activate the web console with: systemctl enable --now cockpit.socket
localhost login: root
Password:
Last login: Thu Sep 28 15:57:52 on tty1
[root@localhost ~]# service nginx status
Redirecting to /bin/systemctl status nginx.service
● nginx.service - The nginx HTTP and reverse proxy server
Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled)
Active: active (running) since Sat 2023-09-30 17:16:43 EDT; 46s ago
Process: 808 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
Process: 769 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
Process: 766 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
Main PID: 813 (nginx)
Tasks: 3 (limit: 11148)
Memory: 13.6M
CGroup: /system.slice/nginx.service
├─813 nginx: master process /usr/sbin/nginx
├─814 nginx: worker process
└─815 nginx: worker process
Sep 30 17:16:42 localhost.localdomain systemd[1]: Starting The nginx HTTP and reverse proxy server...
Sep 30 17:16:43 localhost.localdomain nginx[769]: nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
Sep 30 17:16:43 localhost.localdomain nginx[769]: nginx: configuration file /etc/nginx/nginx.conf test is successful
Sep 30 17:16:43 localhost.localdomain systemd[1]: Started The nginx HTTP and reverse proxy server.
[root@localhost ~]# cd /var/log/nginx
[root@localhost nginx]# tail access.log
10.10.229.12 - - [28/Sep/2023:15:16:01 -0400] "GET / HTTP/1.1" 200 3429 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0" "-"
10.10.229.12 - - [28/Sep/2023:15:16:01 -0400] "GET /nginx-logo.png HTTP/1.1" 200 368 "http://10.10.229.10/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0" "-"
10.10.229.12 - - [28/Sep/2023:15:16:01 -0400] "GET /poweredby.png HTTP/1.1" 200 1080 "http://10.10.229.10/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0" "-"
10.10.229.12 - - [28/Sep/2023:15:16:01 -0400] "GET /favicon.ico HTTP/1.1" 404 3332 "http://10.10.229.10/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0" "-"
10.10.229.12 - - [28/Sep/2023:15:32:26 -0400] "GET /blog HTTP/1.1" 404 3332 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0" "-"
10.10.229.12 - - [28/Sep/2023:15:36:09 -0400] "GET /blog HTTP/1.1" 404 3332 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0" "-"
10.10.229.12 - - [28/Sep/2023:15:37:35 -0400] "GET /blog HTTP/1.1" 404 3332 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0" "-"
10.10.229.12 - - [28/Sep/2023:15:44:13 -0400] "GET /blog HTTP/1.1" 404 3332 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0" "-"
10.10.229.12 - - [28/Sep/2023:15:58:37 -0400] "GET /blog HTTP/1.1" 502 3404 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0" "-"
[root@localhost nginx]#
Tasks
Cluster log
Start Time
End Time
Node
User name
Description
Status
Sep 30 14:16:19 IT126 yhernandez1@Lab... VM/CT 1027 - Console
Sep 30 14:16:17 Sep 30 14:16:18 IT126 yhernandez1@Lab... VM 1027 - Start OK
Sep 30 14:16:13 Sep 30 14:16:15 IT125 yhernandez1@Lab... VM/CT 1026 - Console OK
Sep 30 14:10:19 Sep 30 14:16:12 IT125 yhernandez1@Lab... VM/CT 1028 - Console OK
Sep 30 14:10:13 Sep 30 14:10:16 IT125 yhernandez1@Lab... VM 1028 - Reboot OK
Sep 30 14:05:20 Sep 30 14:10:16 IT125 yhernandez1@Lab... VM/CT 1028 - Console OK
Sep 30 14:05:18 Sep 30 14:05:19 IT125 yhernandez1@Lab... VM 1028 - Start OK