Raspberry Pi Project

Michael Winder

CNIT 501-960C

UW-Stout

Introduction:

This project aims to create a SIEM solution for a home network. We will be utilizing a raspberry Pi along with Elastic and Graylog to create a unique GUI application to review logs on a web browser.

Hardware:

- Raspberry Pi

- M.2 Hat

- Raspberry Pi Active Cooler

- SIM Card with RaspOS installed

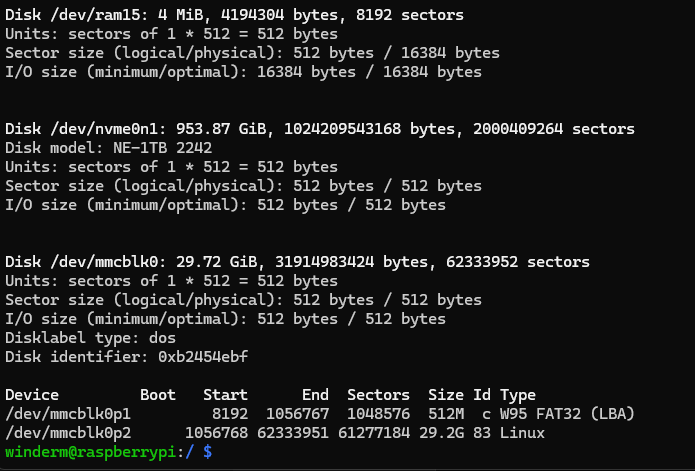
Assumptions:

This project assumes that you can put together and login to your Raspberry Pi.

Steps:

1. After logging into your Raspberry Pi, first steps are you make sure the NVMe drive is mounted. This disk will be used to store incoming logs from other devices.

- Run ‘sudo fdisk -l’ to make sure the NVMe drive is showing up the output should look like below:



2. Create the partition on the NVMe Drive

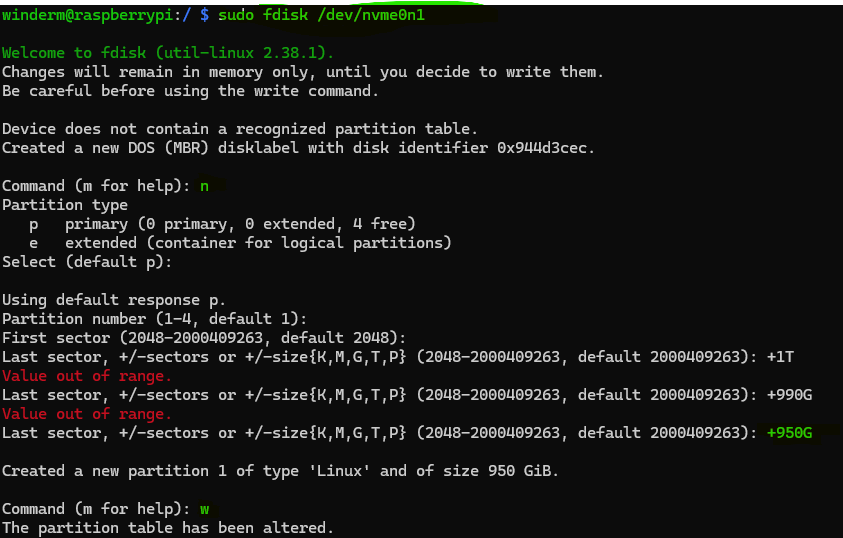
- sudo fdisk /dev/nvme0n1

- n for new

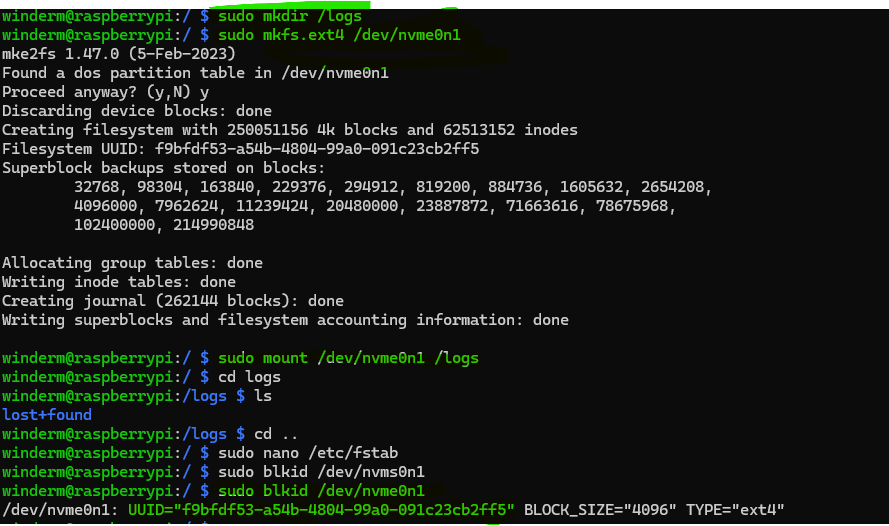
- p for Primary

- +950G to create a proper sized partition

- w to write to the disk

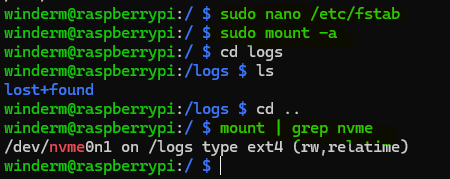


3. Next you need to create a directory and mount the disk to that directory.



4. Take the UUID and add it the the fstab folder so that the drive will mount even after a reboot.



5. Verify the update to the fstab file

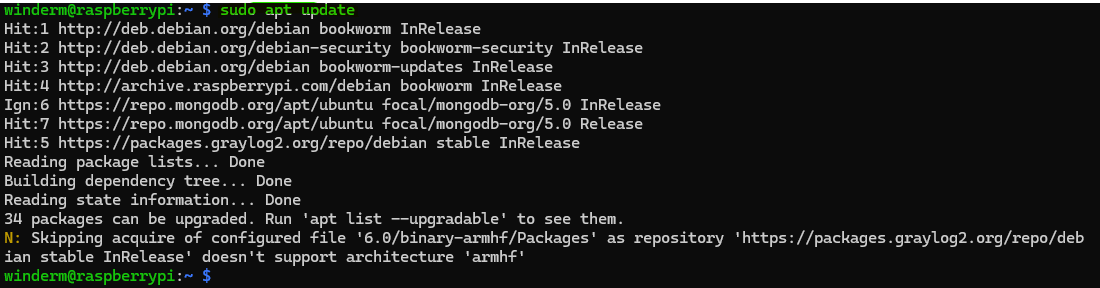
Once this is completed, we can start working on adding the modules that we need to build the web interface.

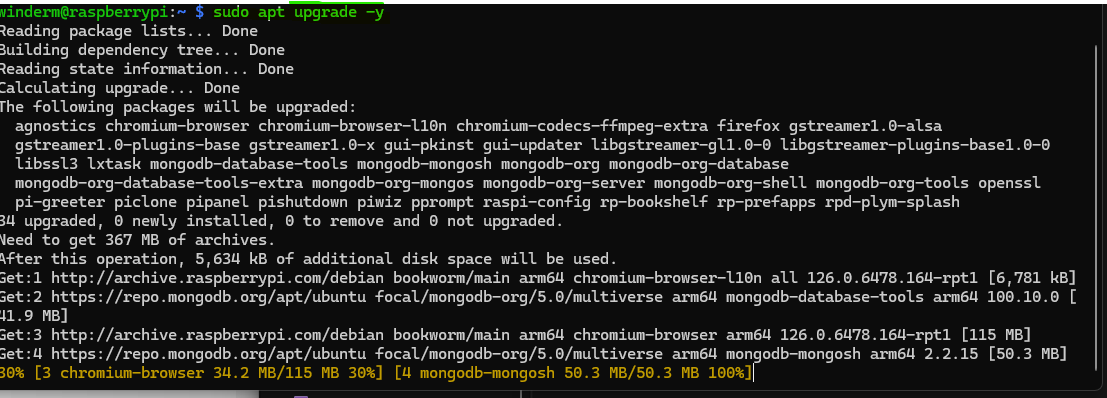
6. The first thing we want to do is make sure that all modules are up to date.

- run sudo ‘apt update’

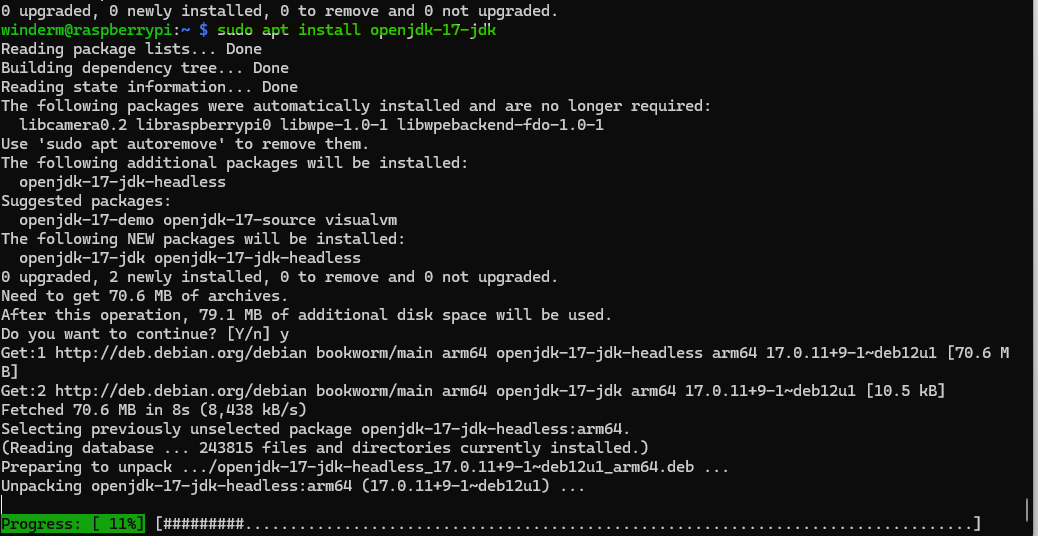
- follow this with ‘sudo apt upgrade -y’

This will get all current modules updated to current versions.



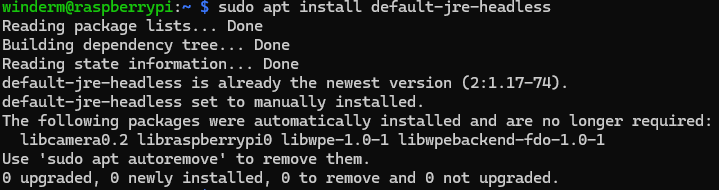


Now that we have everything up to date, we can start by installing a JRE environment, find and install the Java JDK with ‘sudo apt install openjdk-17-jdk’



After this verify that the JRE format for headless is up to date

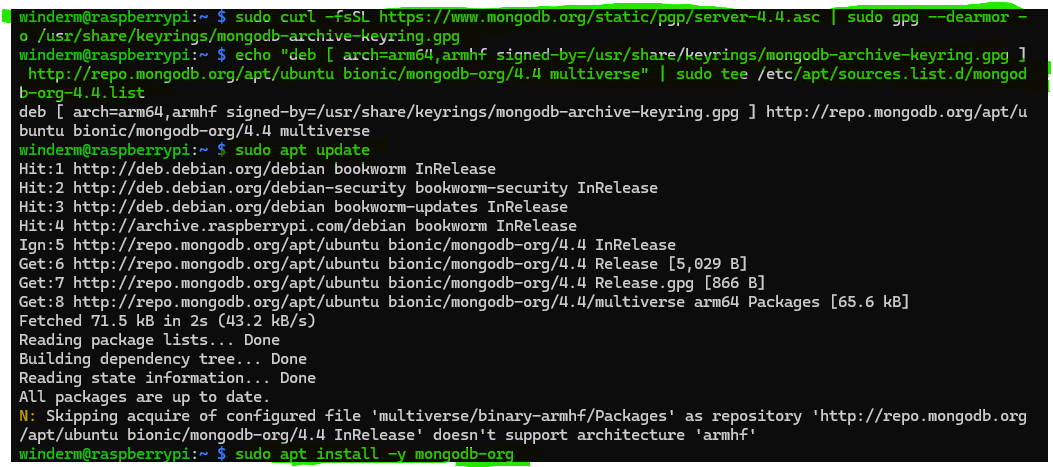
- sudo apt install default-jre-headless



Graylog and Elastic require MongoDB in order to work properly, this will be the next thing we install, run the following commands

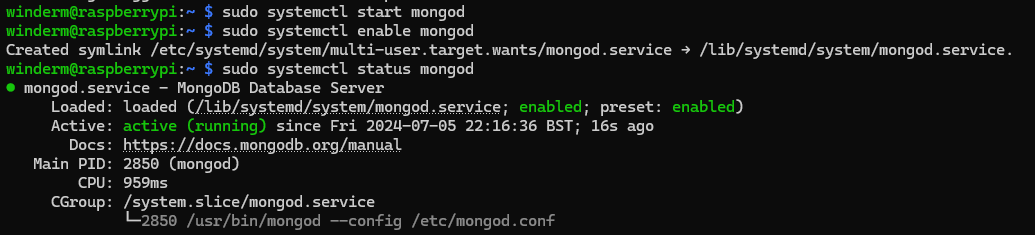
- sudo curl -fsSL <https://www.mongodb.org/statis/pgp/server-4.4.asc> | sudo gpg –dearmor -o /usr/share/keyrings/mongodb-archive-keyring.gpg

- echo “deb [ arch=arm64,armhf signed-by=/usr/share/keyrings/mongodb-archive-keyring.gpg ] [http://repo.mongodb.org/apt/ubuntu bionic/mongodb-org/4.4](http://repo.mongodb.org/apt/ubuntu%20bionic/mongodb-org/4.4) multiverse” | sudo tee /etc/apt/sources.list.d/mongodb-org-4.4.list



Follow this with the ‘sudo apt install -y mongodb-org’ command to install the MongoDB modules.

You then need to start and enable the MongoDB service



Run ‘sudo systemctl start mongod’ followed by ‘sudo systemctl enable mongod’

You could also use the command ‘sudo systemctl enable –now mongod’ to enable and start the service in one command

Now we can install Graylog and Elastic Search on the device.

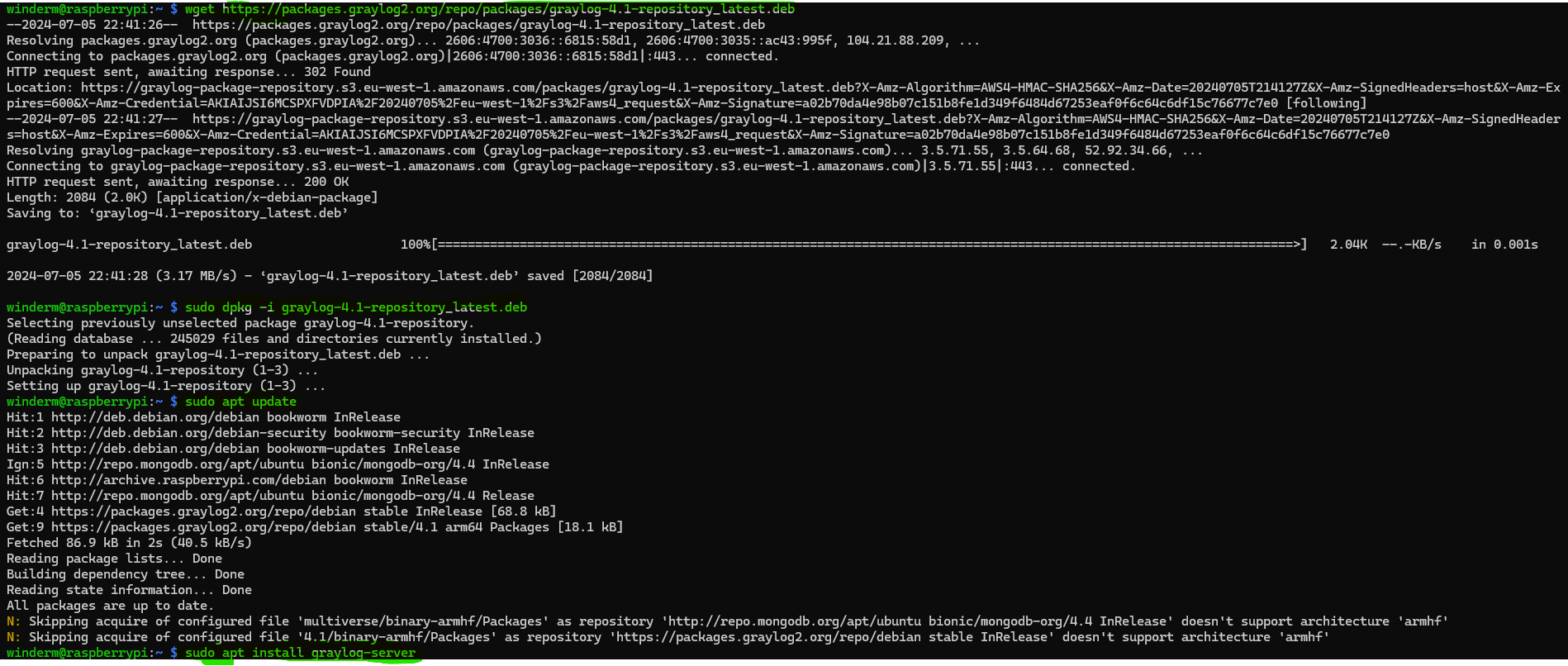
These commands will install everything needed for the Graylog Server

- wget <https://packages.graylog2.org/repo/packages/graylog-4.1-repository_latest.deb>

- sudo dpkg -i graylog-4.1-repository\_latest.deb

- sudo apt update

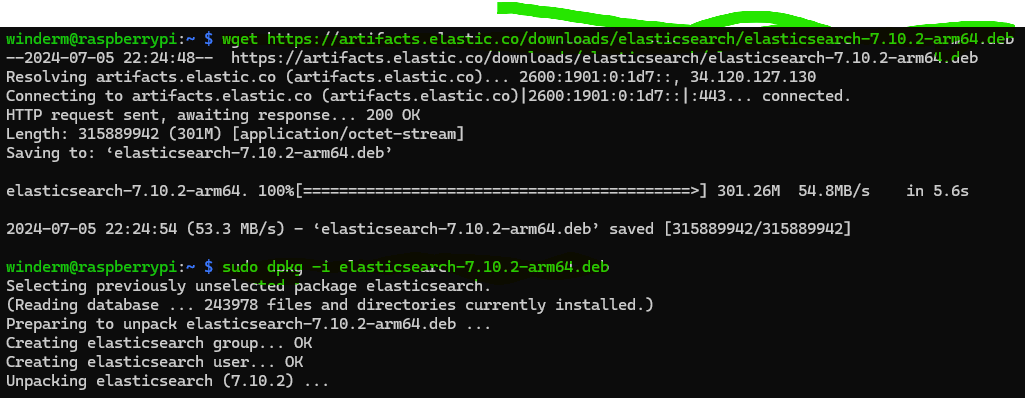
- sudo apt install graylog-server



And finally, you can install Elastic search

- wget <https://srtifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.10.2-arm64.deb>

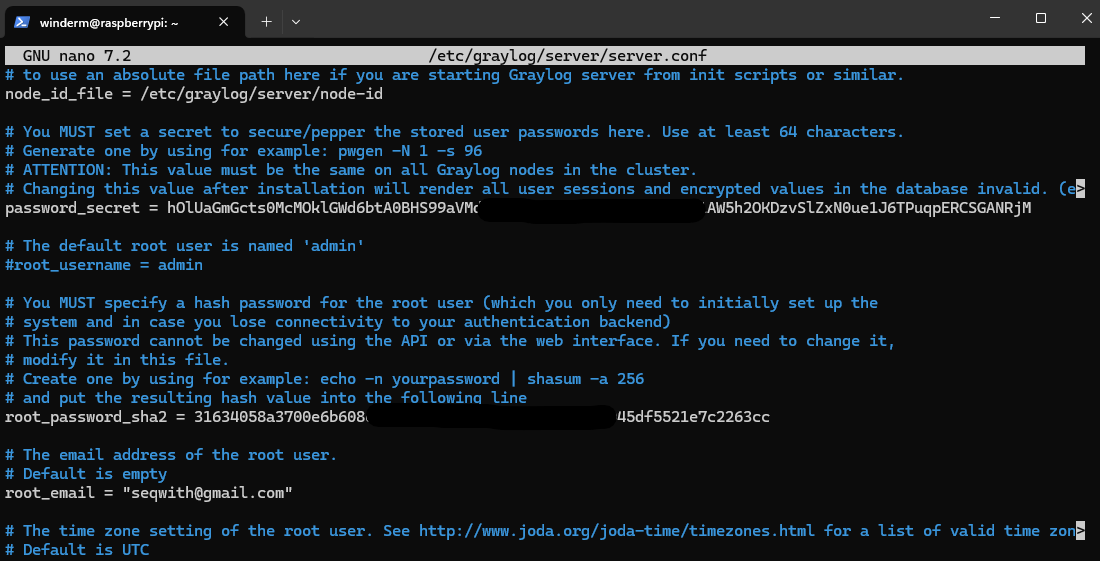
- sudo dpkg -i elasticsearch-7.10.2-arm64.deb



Now that everything is installed, we need to do some configuration to get it all working.

Open the file /etc/graylog/server/server.conf

Look for the line labeled “password\_secret” read the comments above it and create a secret, below that is the default user account that is created, if you want to change it, do that here, also, you need to set the root email and password using a sha2 hash value.



Last but not least we need to configure the .yml file for elasticsearch.

Open the file /etc/elasticsearch/elasticsearch.yml

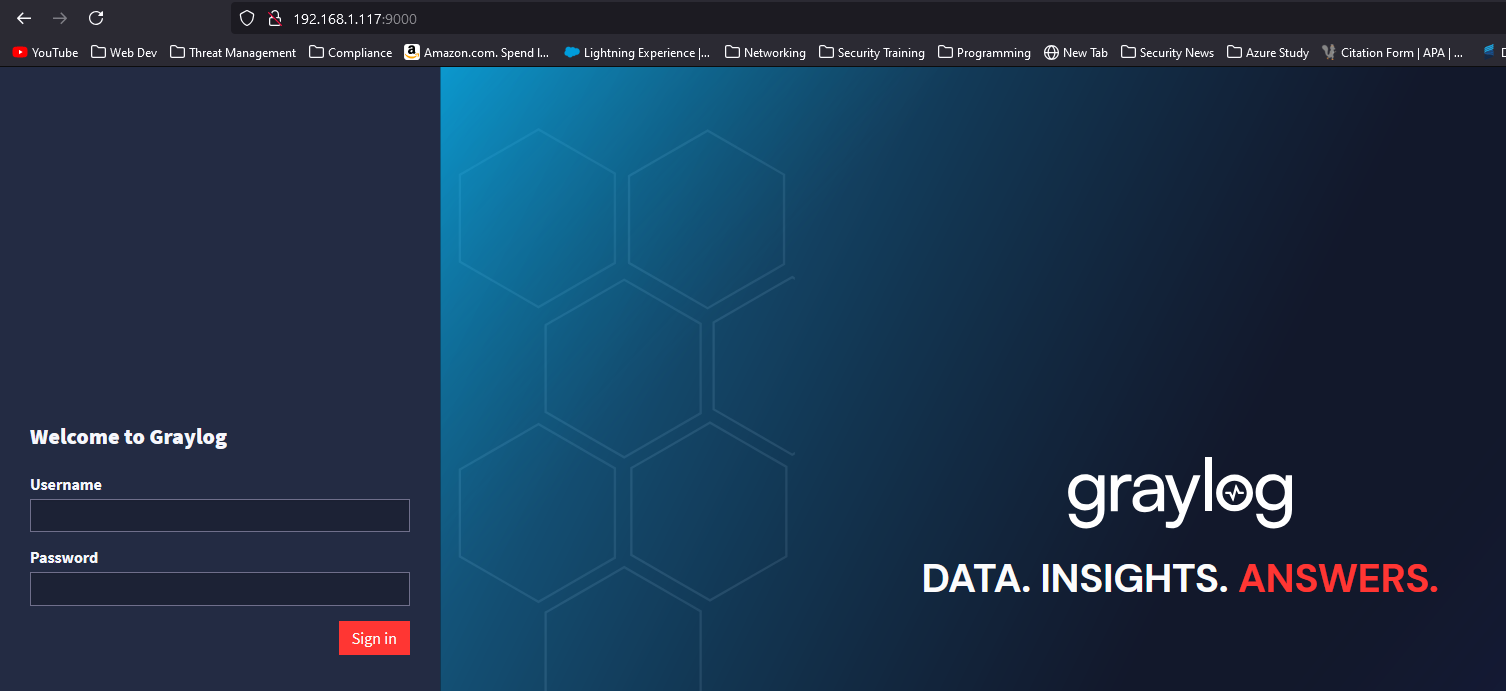
Set the cluster.name (this will need to match the graylog server cluster

Set the node.name

Set the network.host address (This is the IP address of the Raspberry Pi on your network)

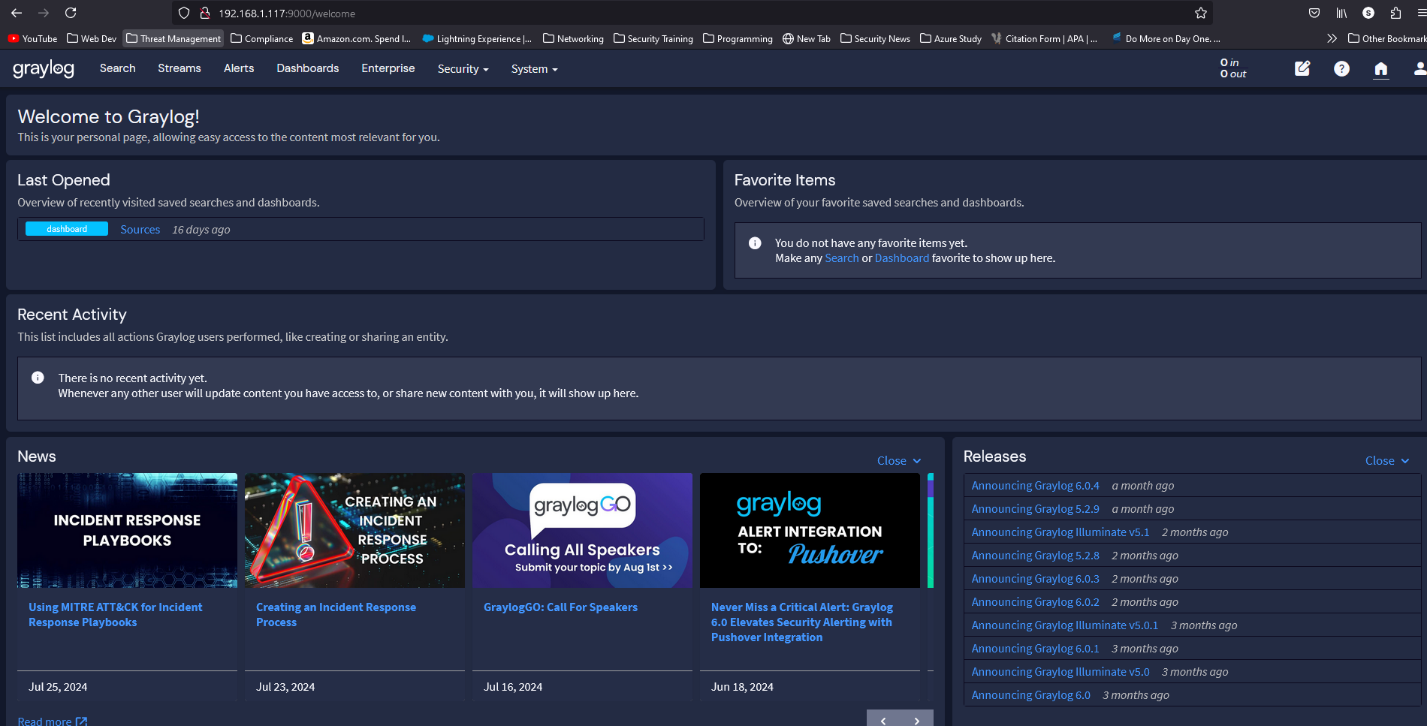


Now you are able to go to a web browser and open the GUI for Graylog



Log in using the default user name, or if you created a different user name in the server.conf file use that name and the password you used to create the sha2 hash.

This will bring you into the home page for Graylog



From here you are able to review logs once you have setup agents on other devices to send logs to your server.