Configuration Manual

MSc Research Project
Programme Name

Muhammad Aashiq Moosa
Student ID:x21186995

School of Computing
National College of Ireland

Supervisor: Apurva Kiran Vangujar

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Muhammad Aashiq Moosa
Student ID:	x21886995
Programme:	Cybersecurity
Year:	2018
Module:	MSc Research Project
Supervisor:	Apurva Kiran Vangujar
Submission Due Date:	14/11/2023
Project Title:	Detecting and Analysis of DDoS Attack using a Collaborative Network Monitoring Stack
Word Count:	1730
Page Count:	9

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Muhammad Aashiq Moosa
Date:	16th September 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Muhammad Aashiq Moosa
x21186995

1 Introduction

This document contains the setup of the network simulated and the installation and configuration of the tools used to build the collaborative monitoring stack.

2 Desktop Specification:

The simulated network and the stack is built and designed in one physical machine. The physical machine configuration are as follows.

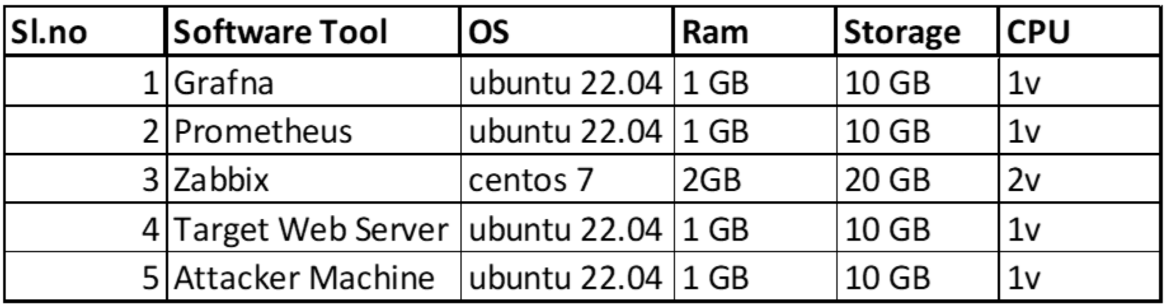
- Performance Oriented CPU: Intel(R) Core(TM) i7-1065G7 CPU
- RAM: 16 GB DDR4
- Storage: 500 GB SSD Storage

3 Software Tools used

To simulate the network, Graphical Network Simulator-3 (GNS3) was used to build the network and Vmware Workstation 15 was used to run Virtual machines needed for the solution stack.

4 Stack Tools Used

Below is the list of Software Tools Used to build the stack

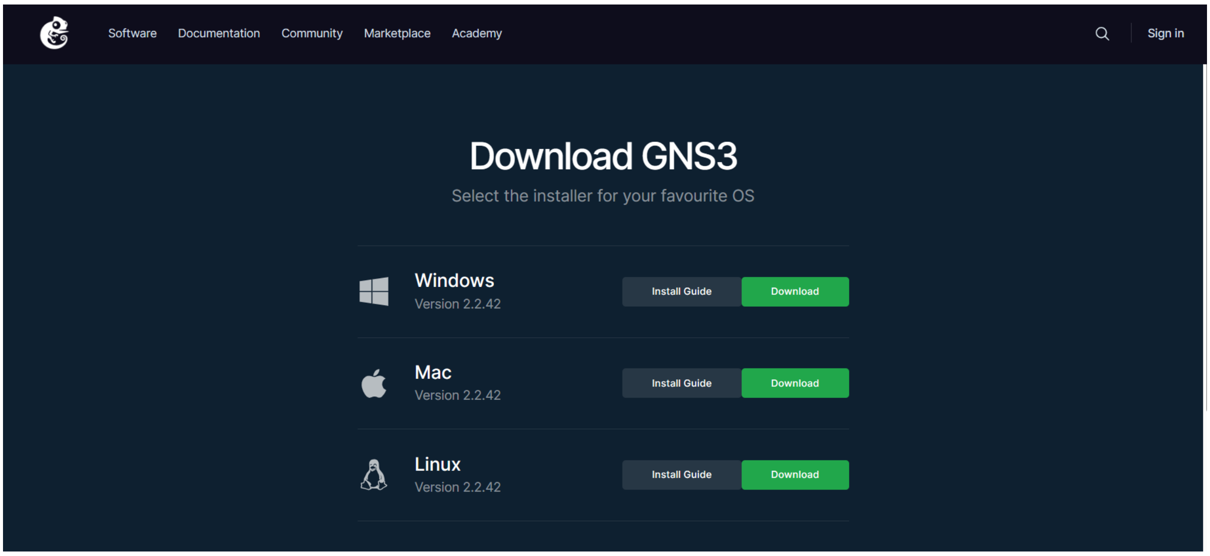


Sl.no	Software Tool	OS	Ram	Storage	CPU
1	Grafna	ubuntu 22.04	1 GB	10 GB	1v
2	Prometheus	ubuntu 22.04	1 GB	10 GB	1v
3	Zabbix	centos 7	2GB	20 GB	2v
4	Target Web Server	ubuntu 22.04	1 GB	10 GB	1v
5	Attacker Machine	ubuntu 22.04	1 GB	10 GB	1v

5 Installation and Configuration

5.1 GNS3 Installation and Configuration

- Step 1 - Download GNS3 from the GNS3 website. https://www.gns3.com/software/download



Download GNS3

Select the installer for your favourite OS

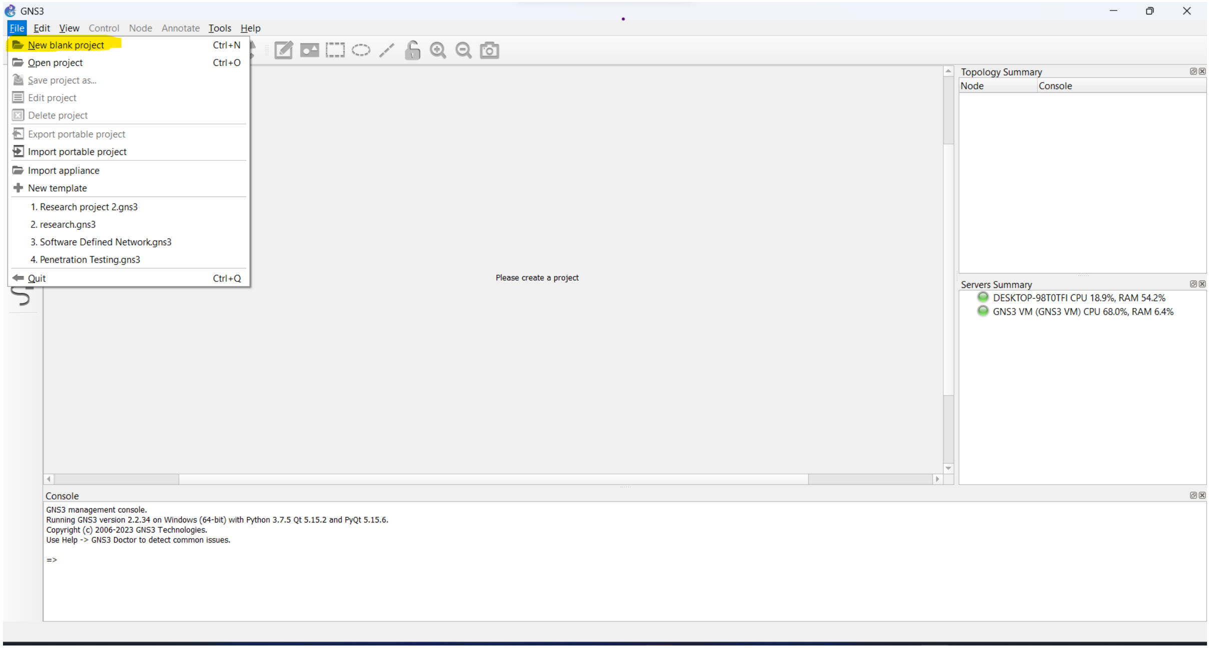
Windows
Version 2.2.42

Mac
Version 2.2.42

Linux
Version 2.2.42

Figure 1: GNS3 website to download GNS3 software.

- Step 2 - Install the software and the default dependencies. Check among the dependecies if GNS3 VM is included. If check that so during installation, even the GNS3 Virtual Machine can be installed as well. This is needed to install and run custom routers and switches that are not pre-loaded in GNS3.



Please create a project

DESKTOP-98T0TFI CPU 18.9%, RAM 54.2%
GNS3 VM (GNS3 VM) CPU 68.0%, RAM 6.4%

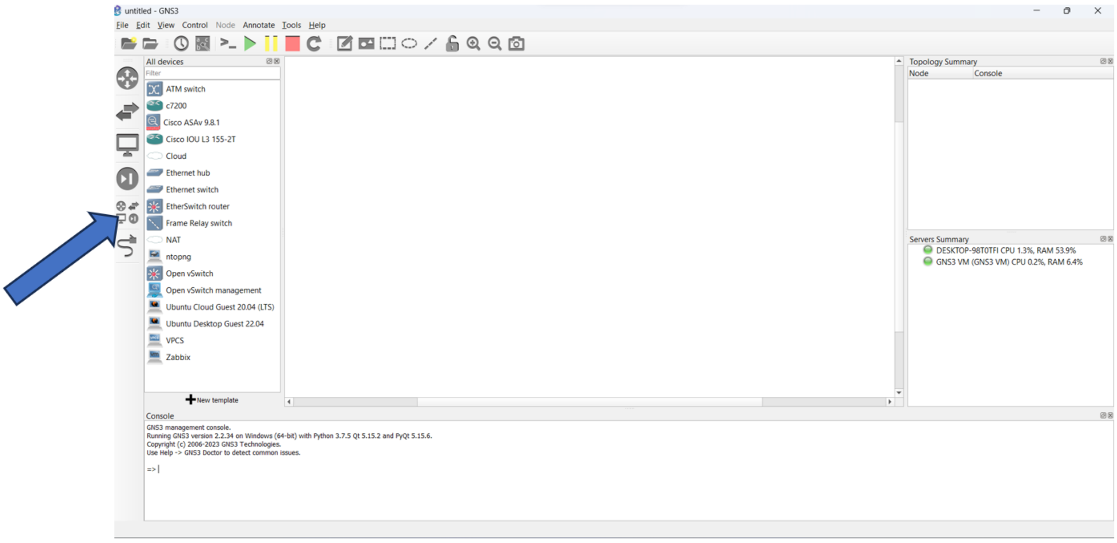
Console

```
GNS3 management console.
Running GNS3 version 2.2.34 on Windows (64-bit) with Python 3.7.5 Qt 5.15.2 and PyQt 5.15.6.
Copyright (c) 2006-2023 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

Figure 2: GNS3 software - Create a new blank project.

- Step 3 - Once installed create a new Blank project to build the designed network



```
DESKTOP-98T0TFI CPU 1.3%, RAM 53.9%
GNS3 VM (GNS3 VM) CPU 0.2%, RAM 6.4%
```

```
GNS3 management console.
Running GNS3 version 2.2.34 on Windows (64-bit) with Python 3.7.5 Qt 5.15.2 and PyQt 5.15.6.
Copyright (c) 2006-2023 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>|
```

Figure 3: Designing the network.

- Step 4 - Access the devices tab to import the required devices to design the network.

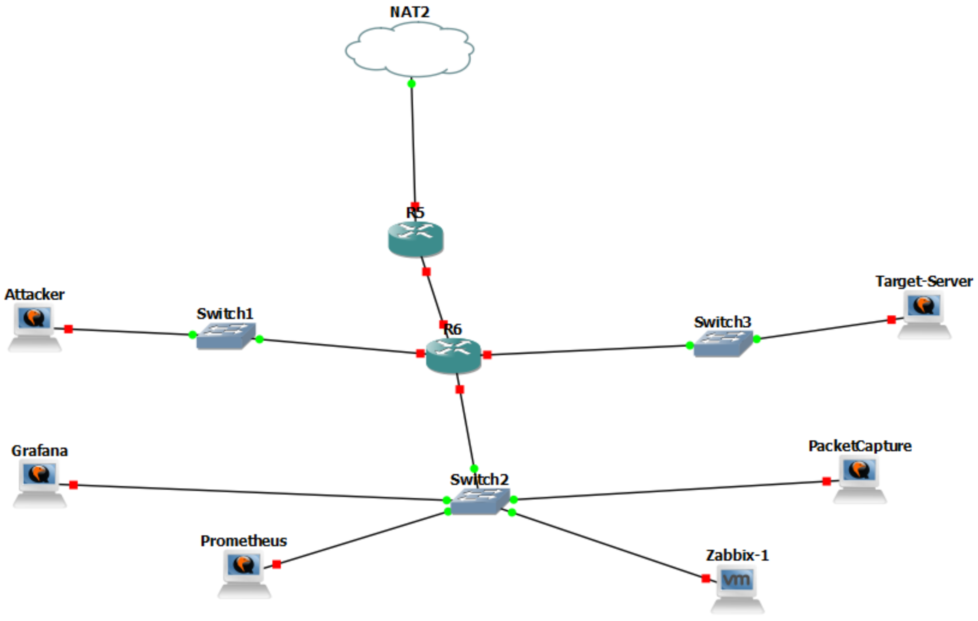


Figure 4: Network topology built

- Step 5 - Design and configure the network based on the designed network planned.

5.2 Zabbix Installation and Configuration

Zabbix is installed in a Centos virtual machine having 2 GB Ram and storage of 20 GB.

- Step 1 - Download Zabbix version 5.0 from by using the following command. This command will install the zabbix repo on the centos machine.

  ```
  rpm -Uvh https://repo.zabbix.com/zabbix/5.0/rhel/7/x86_64
     ↪ /zabbix-release-5.0-1.el7.noarch.rpm
  ```

- Step 2 - Install zabbix server, zabbix front end and zabbix agent.

  ```
  yum install zabbix-server-mysql zabbix-agent
  ```

- Step 3 - Install zabbix front end packages

  ```
  yum install zabbix-web-mysql-scl zabbix-apache-conf-scl
  ```

- Step 4 - Install maria db to run mysql database for zabbix.

  ```
   sudo yum install mariadb-server
  ```

- Step 5 - Login into mysql console and install a database for zabbix.

  ```
  # mysql -uroot -p
  <mysql_password>
  mysql> create database zabbix character set utf8 collate
     ↪ utf8_bin;
  mysql> create user zabbix@localhost identified by '<
     ↪ password>';
  mysql> grant all privileges on zabbix.* to
     ↪ zabbix@localhost;
  mysql> set global log_bin_trust_function_creators = 1;
  mysql> quit;
  ```

- Step 6 - Login into mysql console and install a database for zabbix.

  ```
   zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz |
     ↪  mysql -uzabbix -p <zabbix_password>
  ```

- Step 7 - Start the zabbix services (Zabbix server, zabbix agent, apache webserver and zabbix front end)

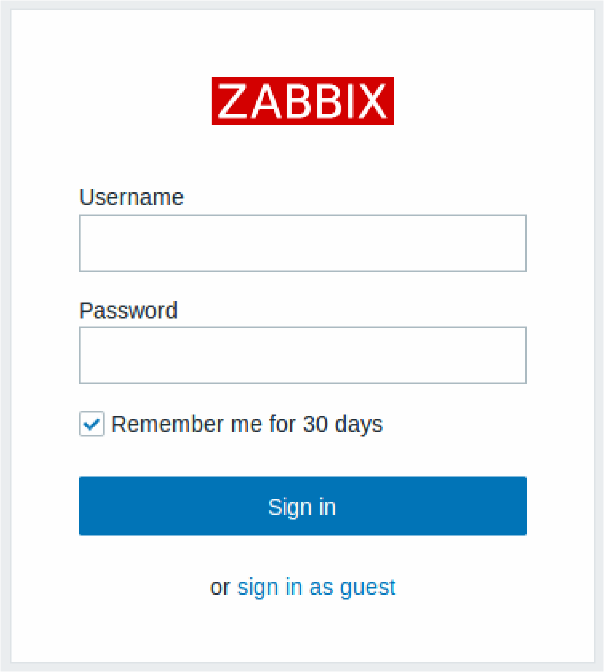
  ```
  systemctl start zabbix-server zabbix-agent httpd rh-php72
     ↪ -php-fpm
  ```

- Step 7 - Enable the zabbix services so they always start when the machine startup.

  ```
  systemctl enable zabbix-server zabbix-agent httpd rh-
     ↪ php72-php-fpm
  ```

- Step 8 - Open the browser and type in the following url to access zabbix front end.

  ```
  http://<zabbix_IP_Address>/zabbix
  ```



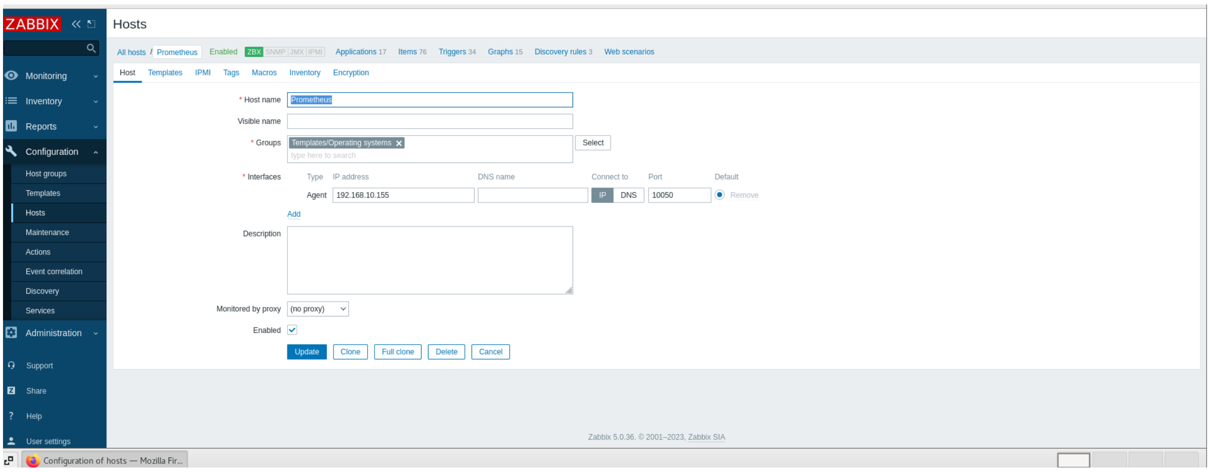
Username

Password

☑ Remember me for 30 days

Figure 5: Zabbix Login Page

- Step 9 - Login with the username Admin and password zabbix.
- Step 10 - Right now zabbix server is only monitoring itself through a zabbix agent. To add more devices head to the configuration tab on left panel and click on hosts.
- Step 11 - Click on "Create Host" button.
- Step 12 - To add an Ubunutu node add the details of the node such as hostname, ip address and template which will be Linux OS.



Hosts

All hosts / Prometheus Enabled ZBX SNMP JMX IPMI Applications 17 Items 76 Triggers 34 Graphs 15 Discovery rules 3 Web scenarios

* Host name: Prometheus

Visible name:

* Groups: Templates/Operating systems

* Interfaces

Type	IP address	DNS name	Connect to	Port	Default
Agent	192.168.10.155		IP	10050	●

Description:

Monitored by proxy: (no proxy)

Enabled: ☑

Zabbix 5.0.36. © 2001–2023, Zabbix SIA

Figure 6: Adding a device in Ubuntu

- Step 13 - Click on add button below. Now the ubuntu node will be avaible for monitoring. However on the node side zabbix agent needs to be installed and configured. Refer section 5.3 to check on how to install zabbix agent.

5.3 Zabbix Agent Installation and Configuration

- Step 1 - Run the following command on the ubuntu terminal to add zabbix agent repository.

```
#wget http://repo.zabbix.com/zabbix/3.4/ubuntu/pool/main/
    ↪ z/zabbix-release/zabbix-release_3.4-1+xenial_all.
    ↪ deb
```

- Step 2 - Run the following command on the ubuntu terminal to install zabbix agent.

```
#sudo apt-get install zabbix-agent
```

- Step 3 - Run the following command on the ubuntu terminal to install zabbix agent.

```
#sudo apt-get install zabbix-agent
```

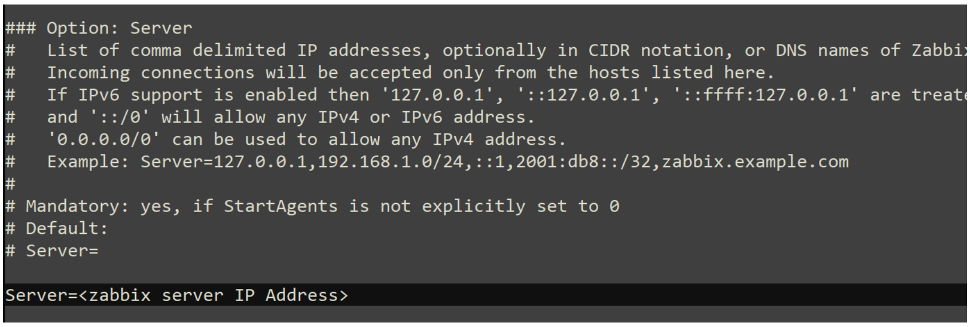
- Step 4 - Open the zabbix agent config file.

```
#sudo vi /etc/zabbix/zabbix_agentd.conf
```

- Step 5 - Open the zabbix agent config file.

```
#sudo vi /etc/zabbix/zabbix_agentd.conf
```

- Step 6 - Under the Server section of the config file enter the IP Address of the zabbix server.



```
### Option: Server
#   List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of Zabbi
#   Incoming connections will be accepted only from the hosts listed here.
#   If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' are treat
#   and '::/0' will allow any IPv4 or IPv6 address.
#   '0.0.0.0/0' can be used to allow any IPv4 address.
#   Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
#
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=

Server=<zabbix server IP Address>
```

Figure 7: Zabbix Agent config file

- Step 7 - Restart the zabbix agent service. Now zabbix server will be able to receive metrics and monitor the node.

```
sudo systemctl restart zabbix-agent
```

5.4 Prometheus Installation and Configuration

- Step 1 - Download Prometheus by using the following command.

```
wget https://github.com/prometheus/prometheus/releases/
    ↪ download/v2.37.6/prometheus-2.37.6.linux-amd64.tar.
    ↪ gz
```

- Step 2 - Extract the downloaded files

  ```
  tar xvfz prometheus-*.tar.gz
  ```

- Step 3 - Create the 2 directories for Prometheus to use and store it's configuration files using the following command.

  ```
  sudo mkdir /etc/prometheus /var/lib/prometheus
  ```

- Step 4 - Move the directories Prometheus and promtool to the usr/local/bin directory.

  ```
  sudo mv prometheus promtool /usr/local/bin/
  ```

- Step 5 - Move the prometheus.yml file to the etc/prometheus directory.

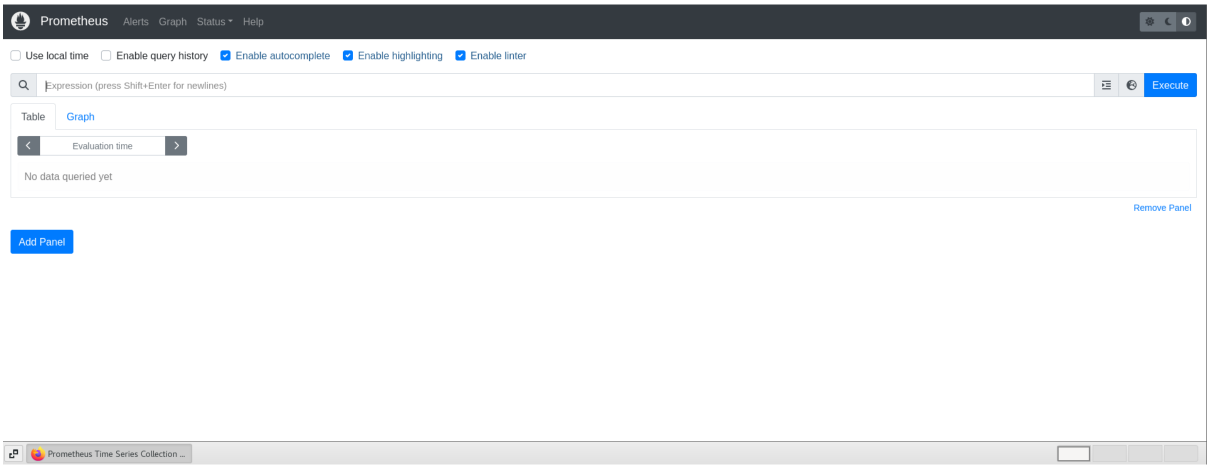
  ```
  sudo mv prometheus.yml /etc/prometheus/prometheus.yml
  ```

- Step 6 - Run the following command to start prometheus.

  ```
  sudo systemctl start prometheus
  ```

- Step 7 - Open a browser and enter the following url to log into the prometheus console.

  ```
  http://<prometheus_IP_Address:9090
  ```



☐ Use local time ☐ Enable query history ☑ Enable autocomplete ☑ Enable highlighting ☑ Enable linter

No data queried yet

Figure 8: Prometheus Front End

5.5 Grafana Installation and Configuration

- Step 1 - Run the following command on the ubuntu terminal to install grafana.

  ```
  sudo apt-get install grafana
  ```

- Step 2 - Start the grafana server and enable it

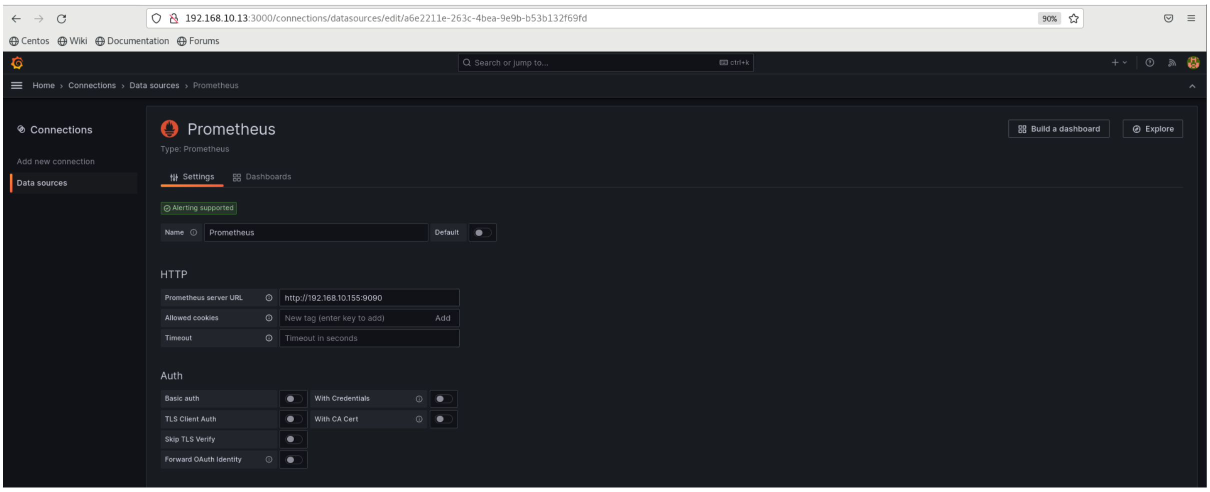
  ```
  systemctl start grafana-server
  systemctl enable grafana-server
  ```

- Step 3 - Open a browser and log into following url to log into the grafana front end. The username is Admin and default password is password.

  ```
  http://<Grafana-Server-IP-Address>:3000
  ```

- Step 4 - Once Logged in on the left panel click on Configuration. and select Data source to add data sources.

- Step 5 - Click on the data source connector you wish to add and add details like URL of the data source and login credentials. Figure 9 shows the screenshot of adding Prometheus as a data source to Grafana.



192.168.10.13:3000/connections/datasources/edit/a6e2211e-263c-4bea-9e9b-b53b132f69fd

Prometheus

Type: Prometheus

Name: Prometheus | Default ○

HTTP

Prometheus server URL: http://192.168.10.155:9090

Allowed cookies: New tag (enter key to add) Add

Timeout: Timeout in seconds

Auth

Basic auth ○ | With Credentials ○

TLS Client Auth ○ | With CA Cert ○

Skip TLS Verify ○

Forward OAuth Identity ○

Figure 9: Adding Prometheus Data source to Grafana

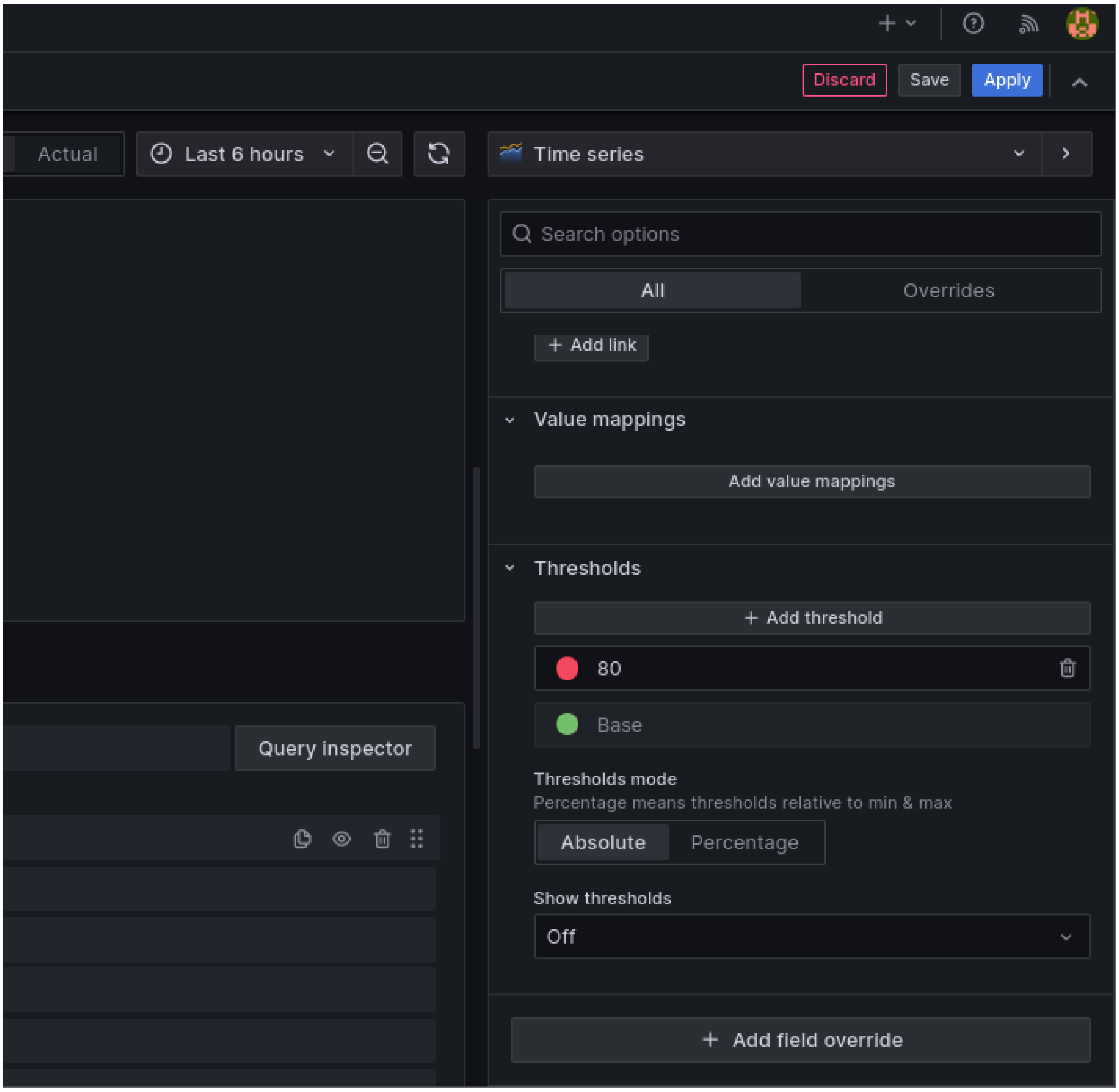
- Step 6 - Once the data sources are successfully added, go to the left panel and click on dashboard and create a new dashboard.

- Step 7 - On the top right click on the option to add a new panel. This will lead to the Grafana Panel editor. Here based on what stat that needs to be displayed or visualised can be configured. and queried in the query editor For the purpose of the Research only Time-series and Stat visualization were used.

- Step 8 - On the right panel scroll to the threshold bar. Here manual threshold can be set based on the type of data being visualised in the panel.

- Step 9 - Once the desired metric is visualised in the format required, click on apply.

- Step 10 - On the Dashboard panel click on save to save the new dashboard.



Thresholds

+ Add threshold

🔴 80

🟢 Base

Thresholds mode
Percentage means thresholds relative to min & max

[✓ Absolute] Percentage

Show thresholds
Off

Figure 10: Setting Thesholds in Grafana