

University of Pretoria  
Software Engineering - COS 301

---

**Defendr User Manual**

---

Dark nITes

12 October 2019



Team members:

MI (Muhammed)

R (Ruslynn)

SNL (Sisa)

CP (Christiaan)

J (Jeandre)

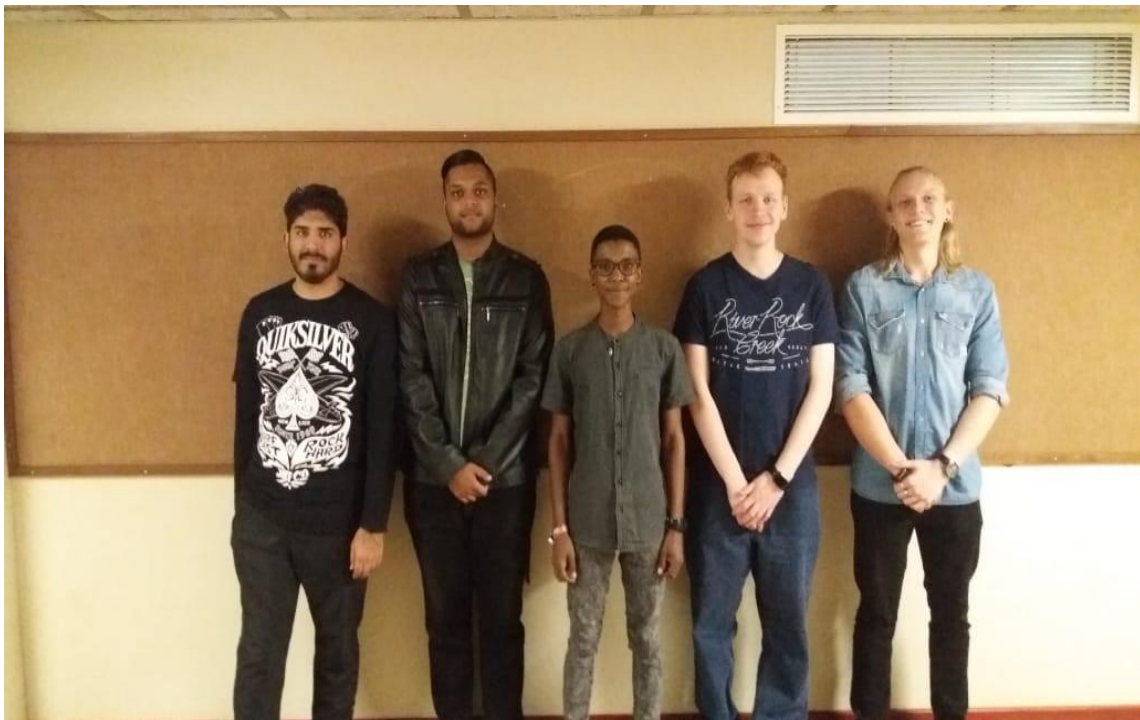
Carrim

Apanna

Khoza

Opperman

Botha



## Contents

1. Introduction .....	3
1.1. System Overview .....	3
1.3. Installation .....	4
2. Getting Started .....	4
2.1. Signing in .....	4
2.2. Registering .....	5
3. Using the System .....	6
3.1. Exploring the home window .....	6
3.3. User Management .....	8
3.4. Changing user details .....	9
3.5. IP blacklisting .....	10
3.6. IP Whitelisting .....	11
3.7. Viewing traffic logs .....	12
3.8. Viewing System metrics .....	12
3.9. Backends and Load balancing .....	18
4. Troubleshooting .....	21
4.1. Missing bpf maps .....	21
4.2. Grafana is not showing any data .....	21
4.3. Interface failures .....	25

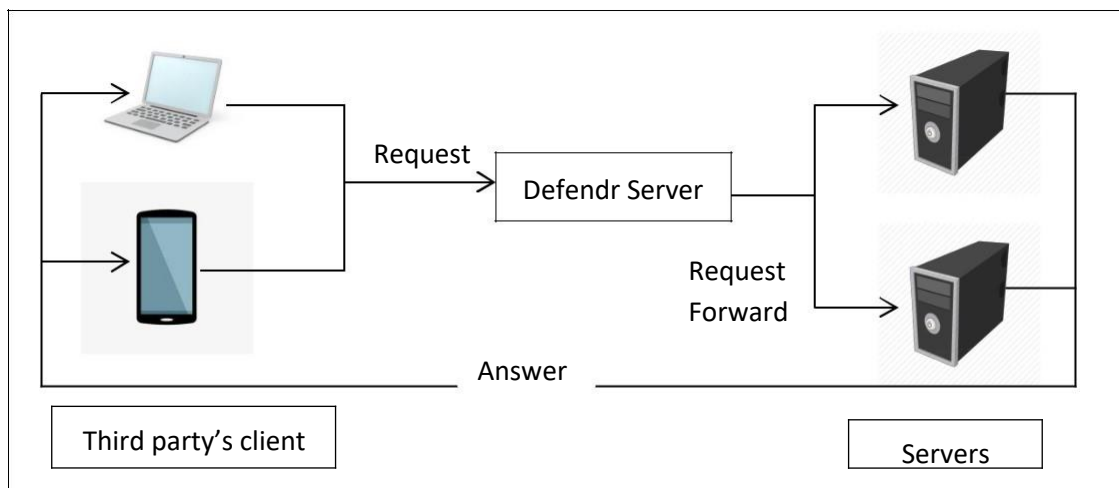
## 1. Introduction

### 1.1. System Overview

The purpose of this system is to protect third party applications from malicious users. The system implements this by detecting DDOS attacks and dropping the packets that are associated with an attack. It also provides load balancing features to control the load for each pool of resources that it is connected to.

The user interacts with the system via an intuitive graphical user interface where the user can to add and remove IP addresses to a white- and blacklist, see packets that traversed the system, view metrics (such as drop rates, packet sizes etc.) and remove and add back-end applications.

#### System Configuration



### 1.2.

There are three main components in this system, namely: servers on which back-end applications run, normal devices that the client uses to connect to the third party application and a server on which Defendr executes. The servers on which back-end

applications run and the normal devices that the client uses to connect to the third party application is beyond the scope of this user manual. Defendr runs on a server that intercepts the packages after they have left the third party's client , but before they reach the application.

### 1.3. Installation

1. The entire Defendr package can be found on <https://github.com/cos301-2019se/Defendr.git>
2. Navigate into the root Defendr Folder
3. Open the terminal
4. Run the command: "chmod +x installcommands.sh"
5. Run the command: "./installcommands.sh"
6. In the ld.so.conf file type this in: "include /usr/local/lib"
7. Open the terminal
8. Follow instructions on the screen
9. For further usage of system after installation.
10. Navigate into the root Defendr Folder
11. Run the command: "chmod +x run.sh"
12. Run the command: "./run.sh"

## 2. Getting Started

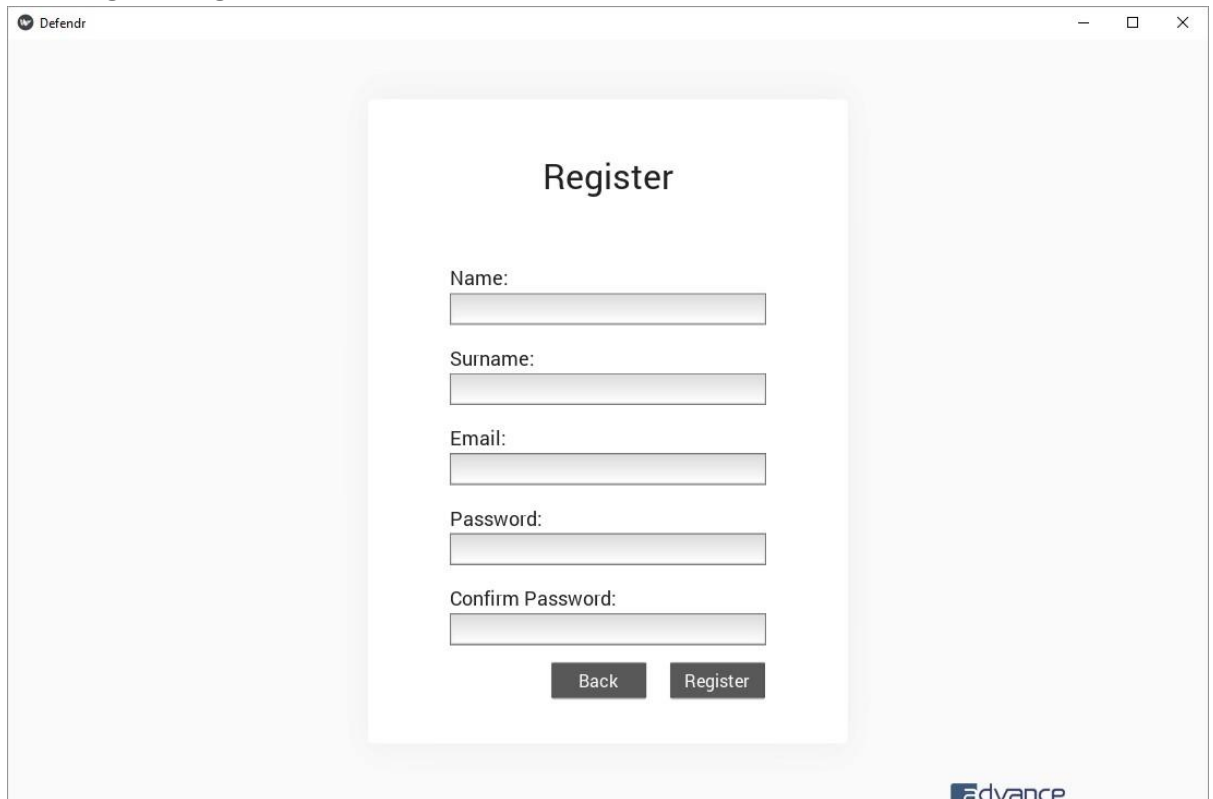
### 2.1. Signing in



The image shows a web browser window titled "Defendr". Inside the window is a login form titled "Defendr Login". The form has two input fields: "Email:" and "Password:". Below the input fields are two buttons: "Register" and "Login". The "Register" button is on the left and the "Login" button is on the right. In the bottom right corner of the browser window, there is a logo for "advance".

After the program installs, this window will appear on the screen. First time users of the system must please click on the **register** button, to register as a user of the system, as explained in section 2.2. Otherwise, log in with your credentials.

## 2.2. Registering

A screenshot of a web application window titled "Defendr". The window contains a "Register" form. The form has five input fields: "Name:", "Surname:", "Email:", "Password:", and "Confirm Password:". Below the input fields are two buttons: "Back" and "Register". The "advance" logo is visible in the bottom right corner of the window.

This window is for registering new users on the system. A user will be requested to fill in:

- His/her name
- Surname
- A valid E-mail address
- A Password • Confirm password.

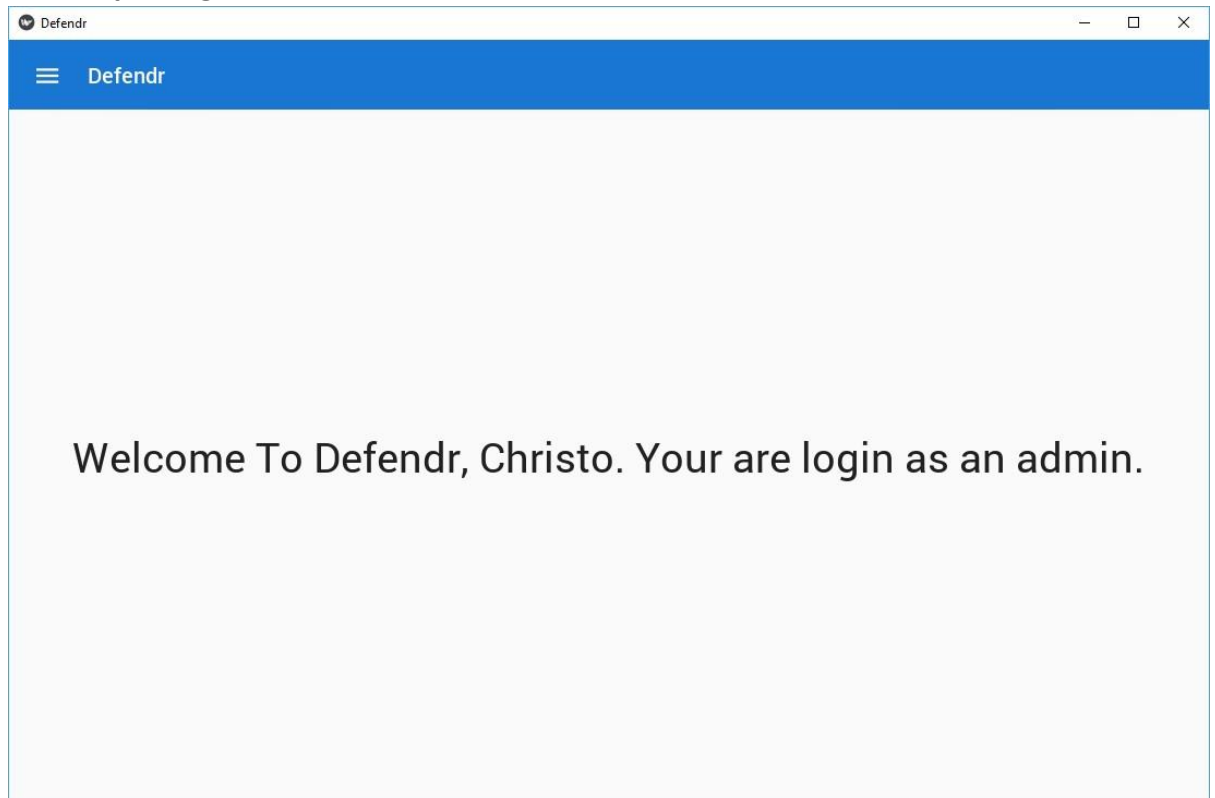
Please note that the password must contain:

- An uppercase character
- A lowercase character
- A symbol
- A number
- Must be at least six characters long.

After the user has completed their details, they will have to click on the **register** button. This will register the user by default as a new user, unless they are the first user on the system. If they are the first user on the system they will be registered as an admin user. Note that a new user can only sign in, after an admin user has verified their account. Once registration is successful, the user will be directed to the sign in screen. The **back** button will return the user to the sign in window.

### 3. Using the System









#### 3.1. Exploring the home window



After successfully signing in as described in section 2, the home window will open. This is the window where the user can see under which account they are logged in, the permission that this account has and can navigate to the nav bar, by clicking on the **menu** button in the top left corner of the screen. (See section 3.2 for more on the nav bar.)

#### 3.2. Nav bar



	Home
	Backends
	Metrics
	System logs
	Blacklisting
	Whitelisting
	User management
	Logout

The Nav bar consists of eight buttons, which are described below. The Nav bar can be accessed from any window, by clicking on the menu button in the top left corner, except on the register- or sign in windows. How to navigate this using the Nav bar:

- Home window: Click on the button that reads home with a home icon,
- Backends window: Click on the button that reads backends with a monitor icon,
- Metrics window: Click on the button that reads metrics with a bar graph icon,
- System logs window: Click on the button that reads system logs with a bullet list icon,
- Blacklisting window: Click on the button that reads blacklisting with a checkered shield icon,
- Whitelisting window: Click on the button that reads whitelisting with a shield with a tick icon,
- User management window: Click on the button that reads user management with a face icon,
- To Log out of the system,

click on the logout button. This will return you to the sign in window.

### 3.3. User Management

NAME	LASTNAME	ROLL	EMAIL	SENDEMAIL
Ruslynn	Appana	admin	u14016304@tuks.co.za	no
Jeandre	Botha	admin	u17094446@tuks.co.za	yes
Muhammed	Carrim	admin	u15019854@tuks.co.za	yes
Sisa	Khoza	admin	u15034993@tuks.co.za	no
Christo	Opperman	admin	u17023239@tuks.co.za	yes
Chris	Osbrone	user	chris@gmail.com	no
Charles	Summers	user	cs@gmail.com	no

The user management plane has five main functions:

1. Adding new users.
  2. Removing users.
  3. Changing a user's details.
  4. Displaying all users.
  5. Verifying new users.
- **To display all registered users**, click the **refresh** button. Note that the users will automatically be displayed, when the window is opened.
  - **To add a new user**, fill in the details as mentioned in in Section 2.2 and then click on the **Add** button to complete the adding process. Note that you can select the role that the new user will have, by clicking on the admin or user button. If the new account is an admin user, the user will have the choice to be notified via email of DOS attacks, new users being registered and blacklisting op IP's.
  - **To remove a user**, provide the e-mail address of the user that needs to be removed in the Email field under the Modify User heading and click the **Remove** button.
  - **To change a user's details**, insert the e-mail address of the user that needs to be changed in the Email field under the Modify User heading and click on the **edit** button which will open the change user window.
  - **To verify a user**, provide the e-mail address of the user that needs to be verified in the Email field under the Modify User heading and click the **Verify** button.



### 3.4. Changing user details

The screenshot shows the Defendr User Management interface. A modal window titled 'Edit user account' is open, allowing a user to change details for a specific user. The modal contains the following fields and options:

- Name: Christo
- Surname: Opperman
- Email: u17023239@tuks.co.za
- Password: (empty field)
- Confirm Password: (empty field)
- Account type: Admin (selected) or User
- Enable email notifications: ☒

Buttons at the bottom of the modal are 'Cancel' and 'Confirm'. In the background, the 'User Management' page is visible, showing a table of users and a 'Refresh' button.

EMAIL	SENDEMAIL
u14016304@tuks.co.za	no
u17094445@tuks.co.za	yes
u15019854@tuks.co.za	yes
u15034993@tuks.co.za	no
u17023239@tuks.co.za	yes
chris@gmail.com	no
ca@gmail.com	no

This window allows the user to change specific details for user accounts, such as name, surname, e-mail address, password and the role of the user.

- **To change user detail**, change the appropriate field and click the **confirm** button. Note that for security reasons, the password will not be completed and thus the user needs to supply the new password and will then have to confirm the new password.(See section 2.2 for password specifications.)
- **To return to the user management plane**, click the **Cancel** button

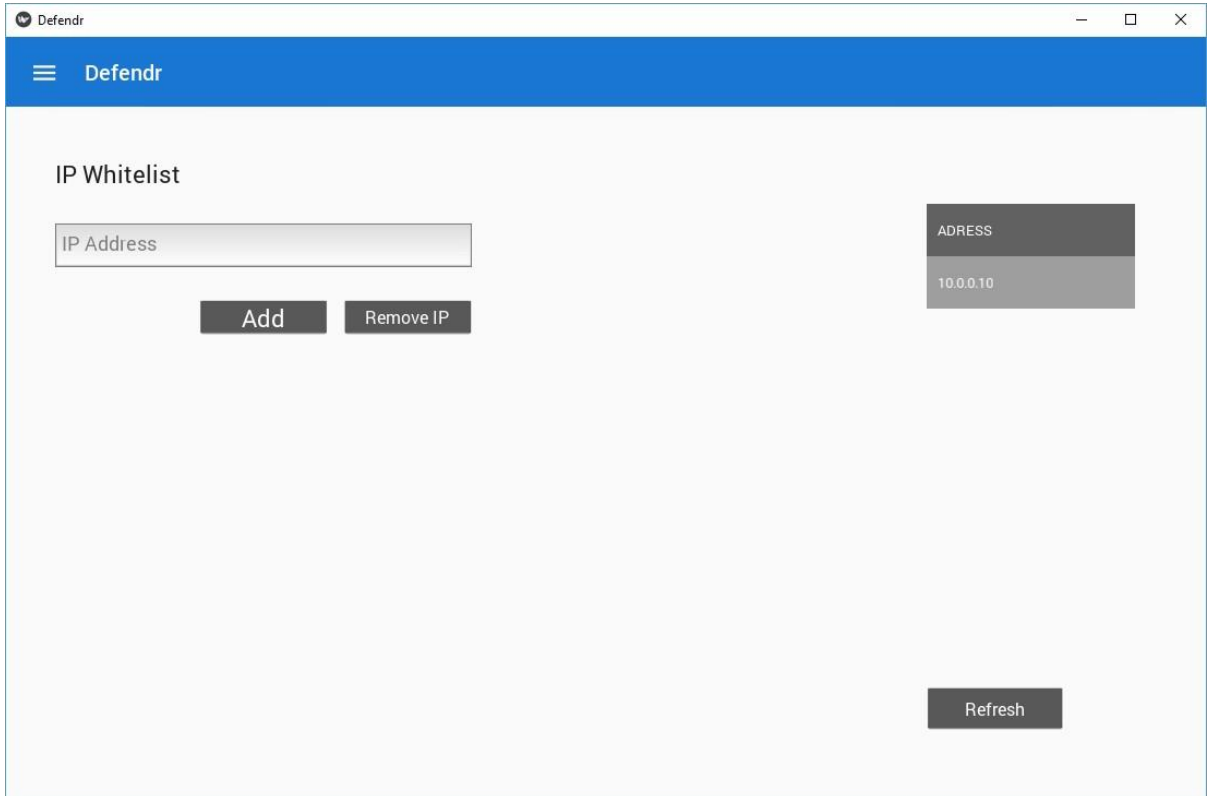
### 3.5. IP blacklisting

The screenshot shows a web application window titled "Defendr". Inside, there is a section labeled "IP Blacklist". Below this heading is a text input field labeled "IP Address". To the right of the input field are two buttons: "Add" and "Remove IP". On the right side of the interface, there is a table with the heading "ADDRESS". The table contains three rows of IP addresses: "127.0.0.1", "96.02.14.65", and "98.02.15.46". At the bottom right of the interface is a "Refresh" button.

ADDRESS
127.0.0.1
96.02.14.65
98.02.15.46

- **To manually blacklist an IP address,** enter the valid IP version 4 address to be blacklisted in the field, which is under the heading, IP Blacklist, then click on **Add IP**.
- **To remove a blacklisted IP address,** enter the valid IP version 4 address to be removed from the blacklisted IP addresses in the field, which is under the heading IP Blacklist, then click on **Remove IP**.
- **To view currently blacklisted IP addresses,** click the **refresh** button. Note that the blacklisted IP's addresses will automatically be displayed, when the window is opened.

### 3.6. IP Whitelisting

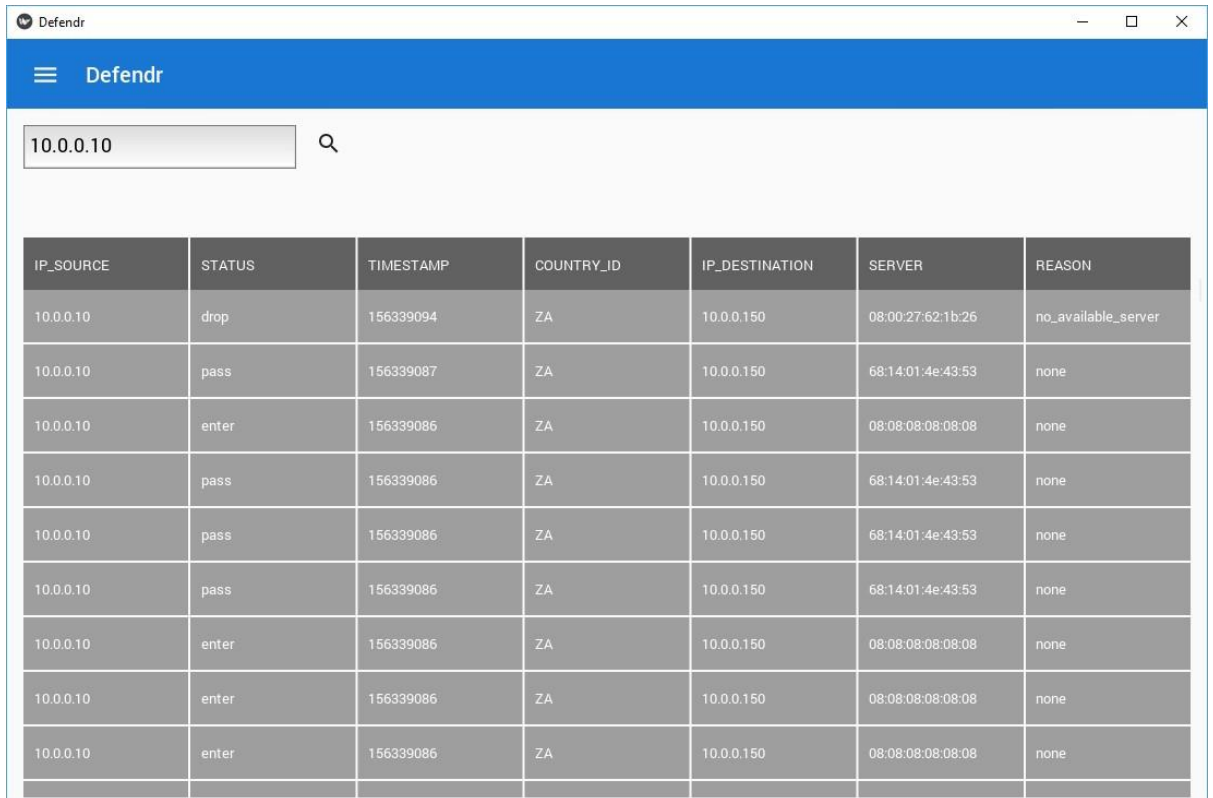


The screenshot shows a web application window titled "Defendr". Inside, there is a section titled "IP Whitelist". Below this title, there is a text input field labeled "IP Address". To the right of the input field, there are two buttons: "Add" and "Remove IP". Below these buttons, there is a "Refresh" button. On the right side of the interface, there is a table with one column labeled "ADDRESS" and one row containing the value "10.0.0.10".

ADDRESS
10.0.0.10

- **To manually whitelist an IP address,** enter the valid IP version 4 address to be whitelisted in the field, which is under the heading, IP Whitelist, then click on **Add IP**.
- **To remove a whitelist IP address,** enter the valid IP version 4 address to be removed from the whitelisted IP addresses in the field, which is under the heading IP whitelist, then click on **Remove IP**.
- **To view currently whitelist IP addresses,** click the **refresh** button. Note that the whitelisted IP's addresses will automatically be displayed, when the window is opened.

### 3.7. Viewing traffic logs



IP_SOURCE	STATUS	TIMESTAMP	COUNTRY_ID	IP_DESTINATION	SERVER	REASON
10.0.0.10	drop	156339094	ZA	10.0.0.150	08:00:27:62:1b:26	no_available_server
10.0.0.10	pass	156339087	ZA	10.0.0.150	68:14:01:4e:43:53	none
10.0.0.10	enter	156339086	ZA	10.0.0.150	08:08:08:08:08:08	none
10.0.0.10	pass	156339086	ZA	10.0.0.150	68:14:01:4e:43:53	none
10.0.0.10	pass	156339086	ZA	10.0.0.150	68:14:01:4e:43:53	none
10.0.0.10	pass	156339086	ZA	10.0.0.150	68:14:01:4e:43:53	none
10.0.0.10	enter	156339086	ZA	10.0.0.150	08:08:08:08:08:08	none
10.0.0.10	enter	156339086	ZA	10.0.0.150	08:08:08:08:08:08	none
10.0.0.10	enter	156339086	ZA	10.0.0.150	08:08:08:08:08:08	none
10.0.0.10	enter	156339086	ZA	10.0.0.150	08:08:08:08:08:08	none

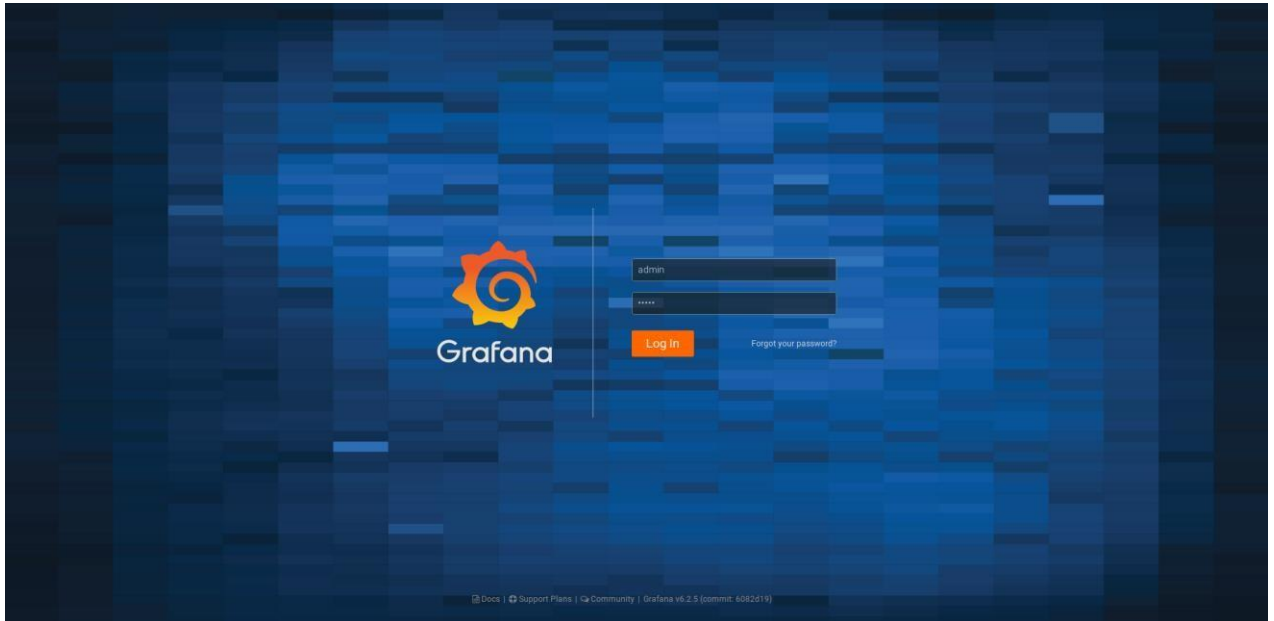
This window enables the user to see either all the packets that went through the system or packets for specific IP addresses.

- **To view all incoming packets**, leave the search field empty and click the **magnifying glass** icon.
- **To view packets with a specific source IP address**, enter the desired IP address in the search field and click on the **magnifying glass** icon.

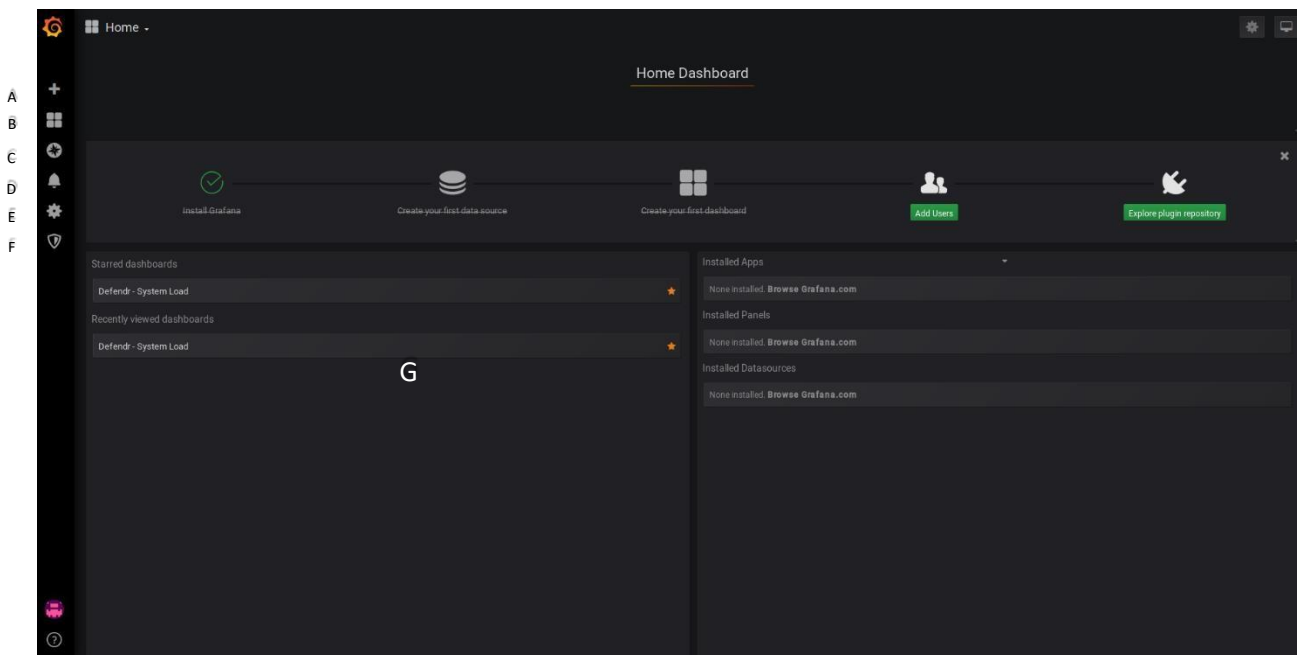
### 3.8. Viewing System metrics

The metrics window has jurisdiction over system load and individual resource monitoring.

### 3.8.1. Sign-in



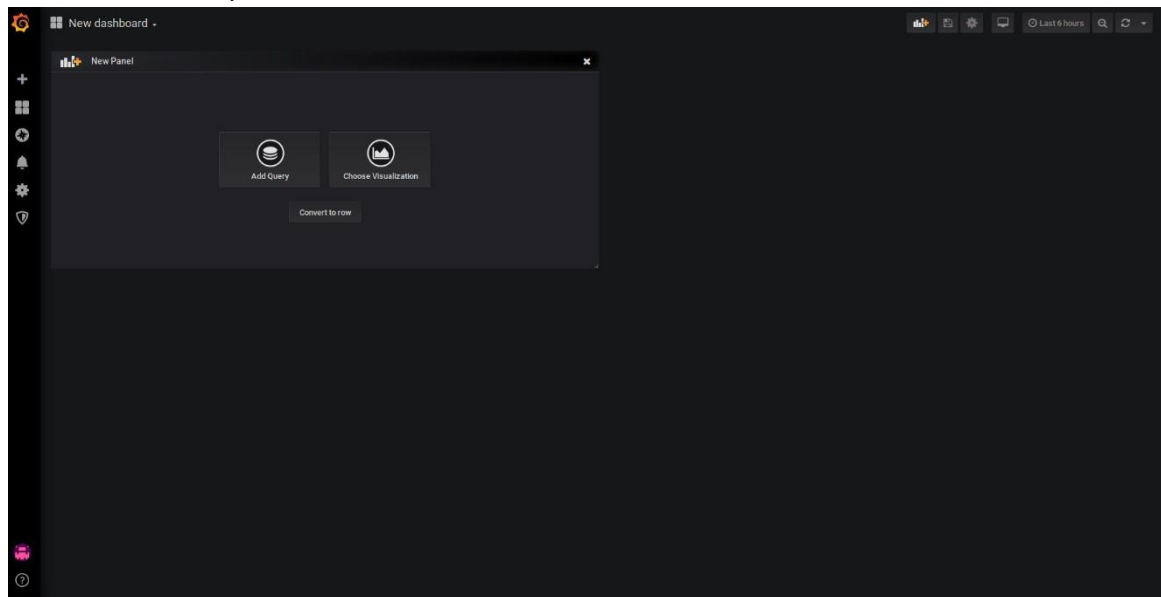
On click of the Metrics button (as shown in Section 3.1) a Grafana sign-in page will open in a browser. The default username is **admin**, and the default password is **admin**. You will be prompted to provide a more secure password at the first successful sign-in. **3.8.2. Home Dashboard**



The dashboard is a centralised portal to access metrics and configuration:

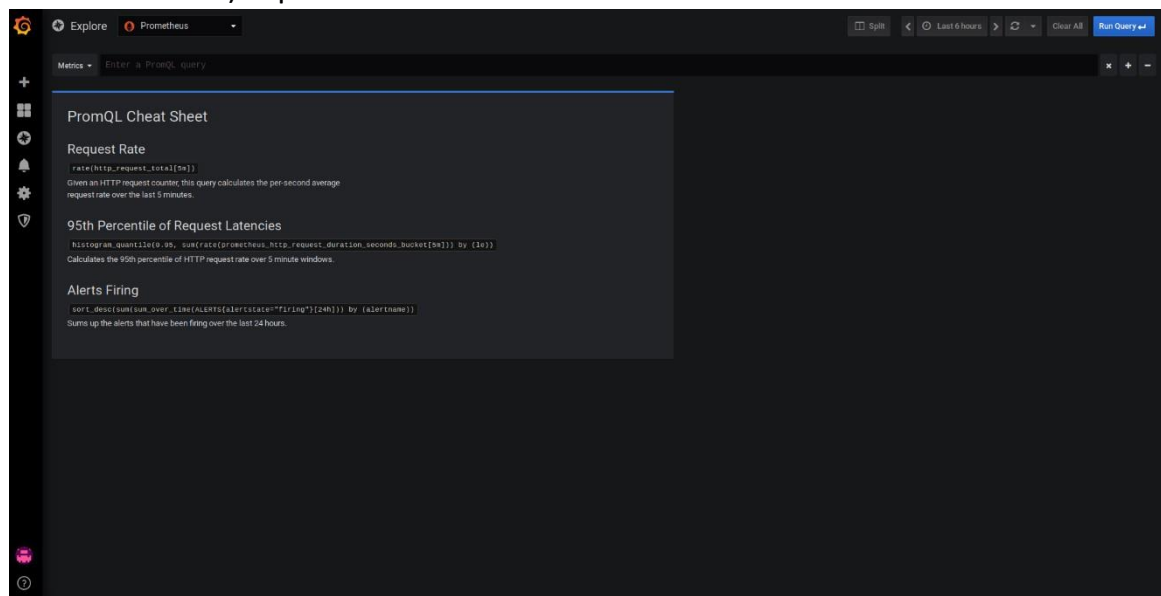
- A. Create > Dashboard, Folder, Import
- B. Dashboards > Home, Manage, Playlists, Snapshots
- C. Explore
- D. Alerting > Alert Rules, Notifications Channels
- E. Configuration > Data Sources, Users, Teams, Plugins, Preferences, API Keys
- F. Server Admin > Users, Orgs, Settings, Stats
- G. Dashboards

### 3.8.3. - A) New dashboard



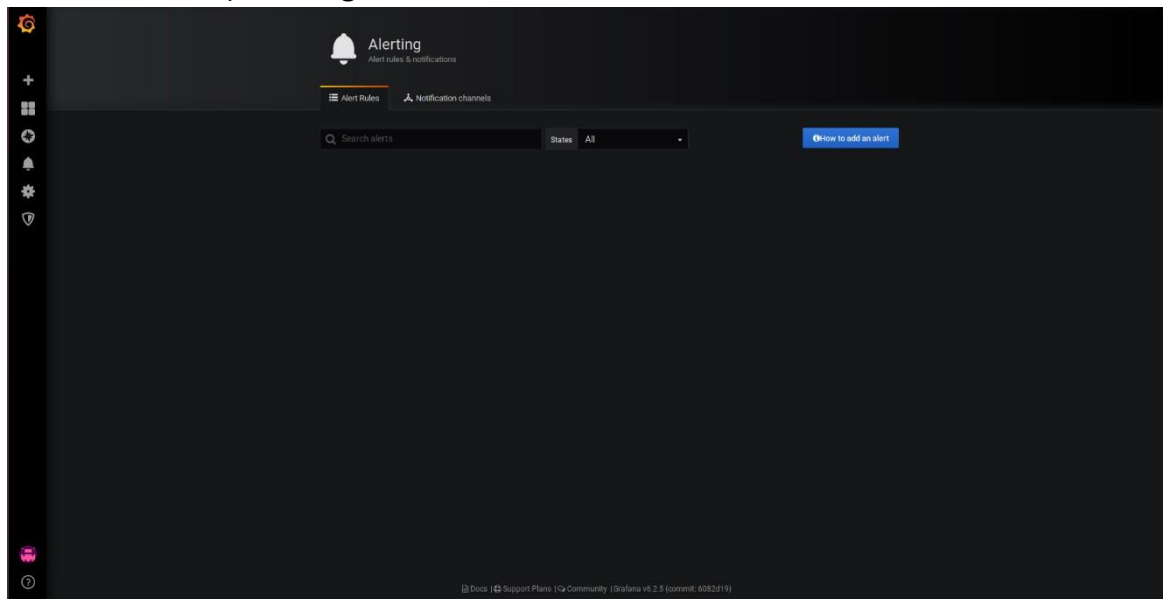
The **New Dashboard** page allows a user to create and customise a new dashboard. It also allows the querying of data from a data source.

### 3.8.4. - C) Explore



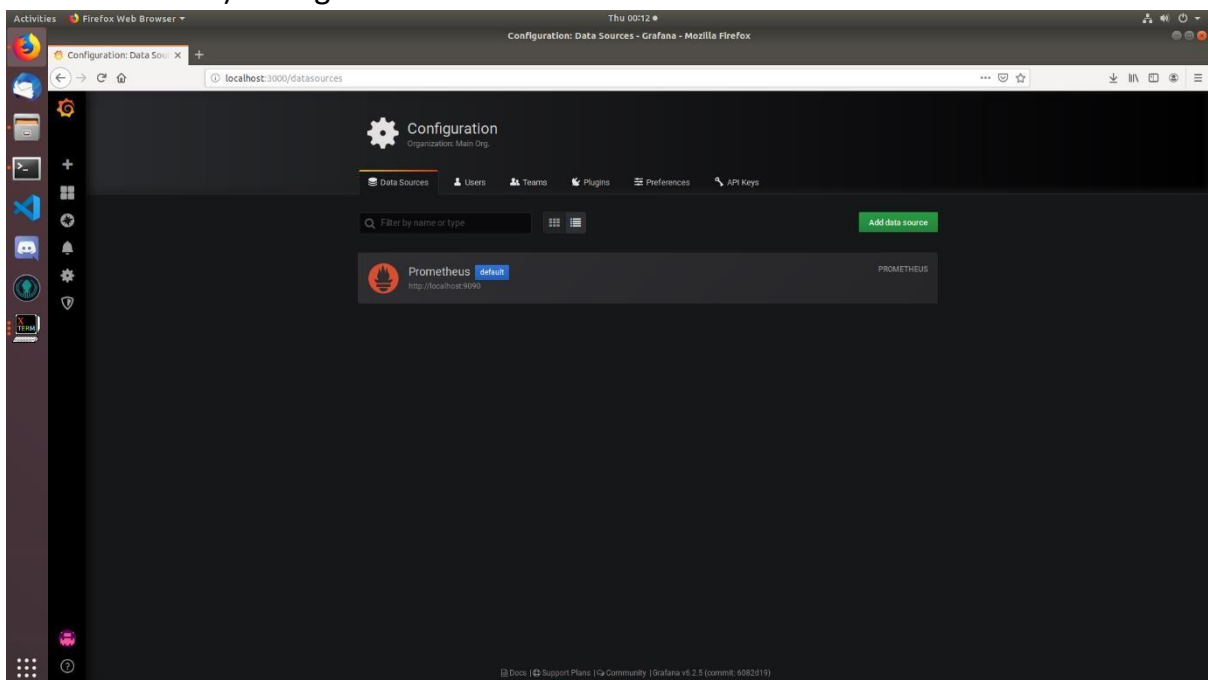
**Explore** is an information hub that give a user tips to better benefit from Grafana.

### 3.8.5. D) Alerting



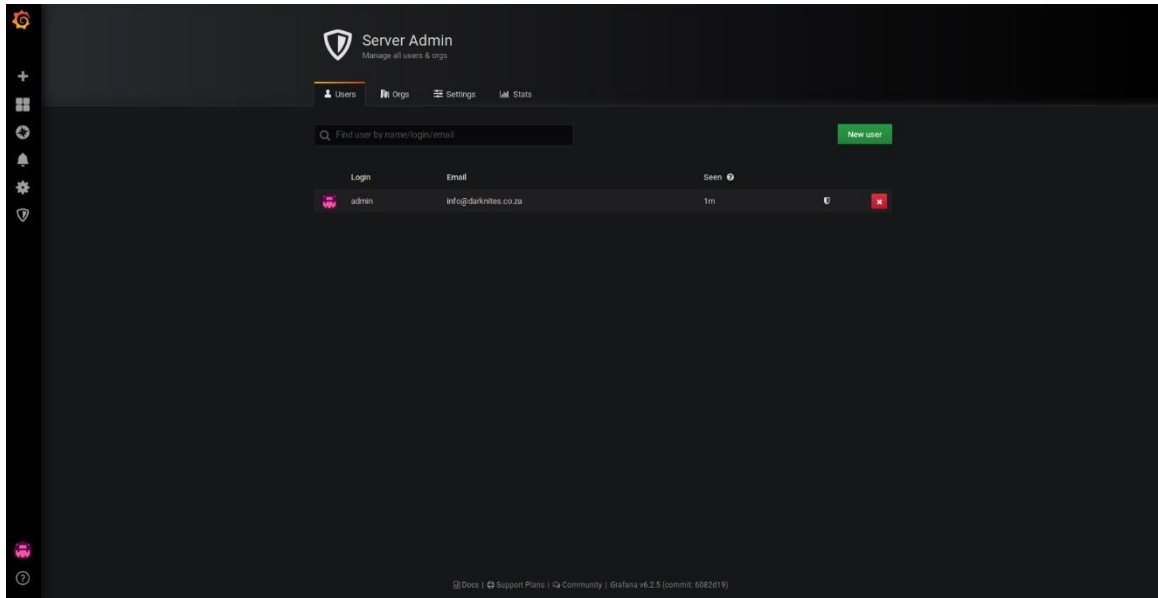
**Alerting** is a featured provided by Grafana to allow real-time updates to another communication channel, e.g. e-mail, Slack, Webhook etc., based on rules attached to a dashboard. One such example could be when the system is under a greater-than-normal network load.

### 3.8.6. - E) Configuration



The **Configuration** page allows a user to add and remove other metrics reporting systems that Grafana can gather data from to graph. At current Prometheus will be visible by default.

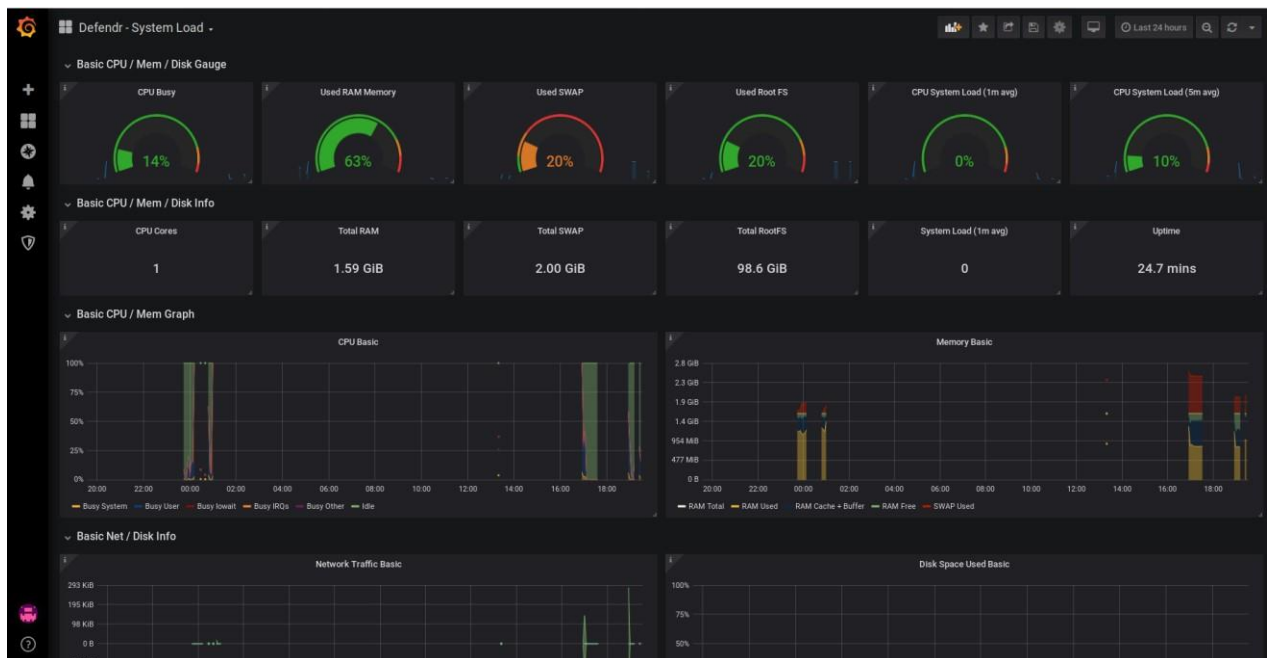
### 3.8.7. F) Server Admin



**Server Admin** is a page to carry out administrative tasks on Grafana. The system administrator will be able to

- create or remove users
- establish organisations (user privileges)
- change settings view Grafana logs.

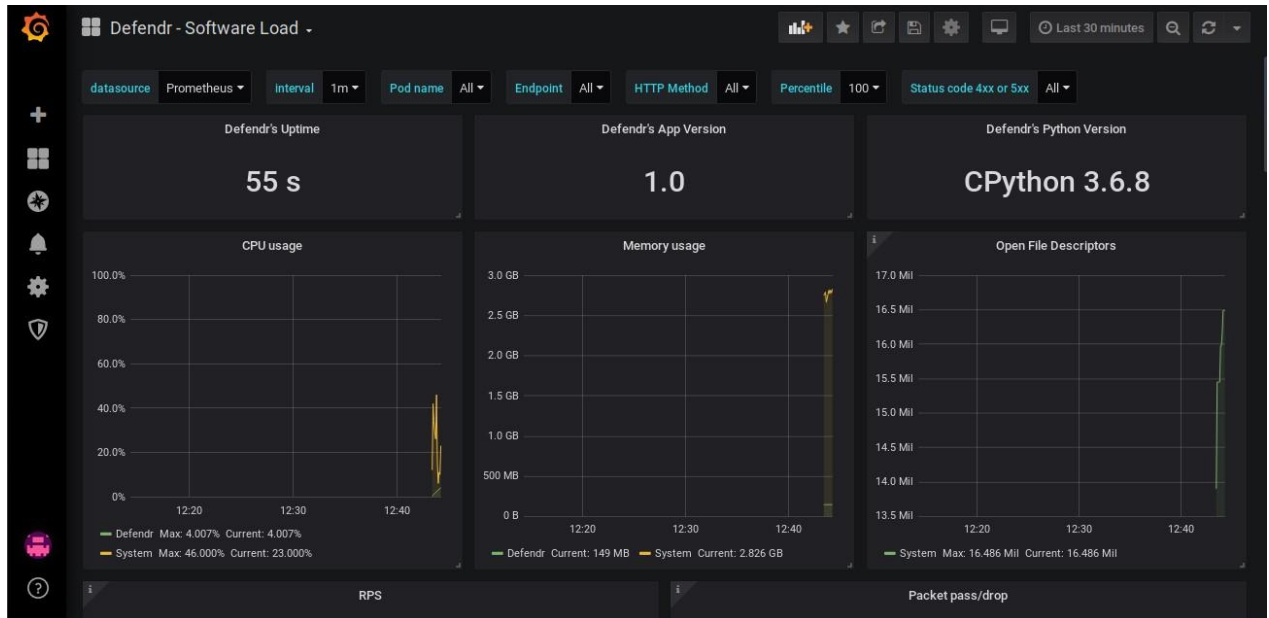
### 3.8.8. - G) Defendr – System Load



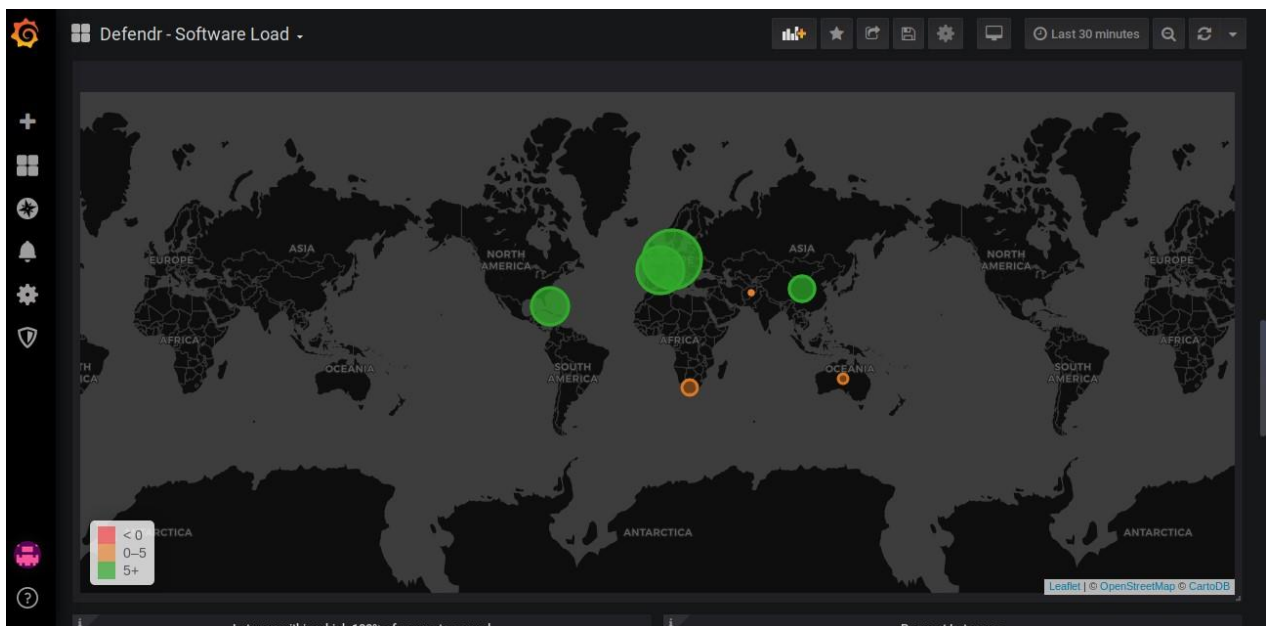


This window is the **Defendr -System Load**. This page will display the hardware-related usage statistics as provided by Prometheus and its exporters. This enables a unified monitoring tool for system load statistics.

### 3.8.9. G) Defendr – Software Load




This window is the **Defendr -Software Load**. This page will display software-related metrics such as software version, uptime and software-related usage statistics. The rate of packets and connections is also displayed, alongside a heatmap.



## 3.9. Backends and Load balancing

### 3.9.1. Backends Interface



HOME    LAST 1000 SINCE STARTUP

#### System Status

Environment	test	Current time	2019-08-21T14:50:49 +0200
Data center	default	Uptime	00:01
		Lease expiration enabled	false
		Renews threshold	1
		Renews (last min)	0

#### DS Replicas

localhost

#### Instances currently registered with Eureka

Application	AMIs	Availability Zones	Status
No instances available			

#### General Info

Name	Value
total-avail-memory	45mb
environment	test
num-of-cpus	1
current-memory-usage	31mb (68%)
server-uptime	00:01
registered-replicas	http://localhost:8761/eureka/
unavailable-replicas	http://localhost:8761/eureka/
available-replicas	

#### Instance Info

Name	Value
ipAddr	192.168.0.193
status	UP

Load balancing will automatically start, when the Defendr application is running. The backend window is divided into five parts, namely:

- System status: This section supplies information about the system as a whole, such as the up time and the renews threshold rate.
- DS Replicas: Contains list of all duplicated Discovery server instances. On default the discovery server will only run locally on the Defendr server.

- Instances currently registered with Eureka: This represents all the backends that are registered on the system, as well as their status.
- General Info: This supplies more information about the system as a whole, such as the total available memory and registered replicas.
- Instance Info: This supplies IP addresses of the backends that are registered on the system.

### 3.9.2. Preparig service backends

1. Open the system command line terminal on the desired machine. (This can be achieved by pressing Ctrl+Alt+T)
2. (Optional: skip this step and go to step 3 if arptables in already installed) Run The following commonad in the open command line terminal:

```
sudo apt-get install arptables
```

3. Enter the following commands in sequesnce.
  - `sudo arptables -A INPUT <virtual-service-ip> -j DROP`
  - `sudo arptables -A OUTPUT <virtual-service-ip> -j mangle - mangle-ip-s <backend-real-ip>`
  - `sudo ip addr add <virtual-service-ip> dev <network-device>`

### 3.9.3. Adding service backends

To add a new backend:

1. Start up the desired machine that contains the service instance.
2. Copy the “serviceInstance” folder from the downloaded Defendr package to any location on the machine.
3. Open navigate to serviceInstance/src/main/recources/
4. Open the file application.properties.
5. Change the property “app.name” to the applications ip address.
6. Change the property “client.instance\_id” to the machine’s own ip address.
7. Return to the “serviceInstance” root folder : serviceInstance/
8. Open the command line terminal in this location. (right click in the folder and click on “Open Terminal Here”)
9. In the command line terminal type “gradle clean build deploy” without the quotations and press enter.

10. After the build finishes, in the terminal, type “java -jar build/libs/serviceInstance.jar” without quotations and press enter.
11. The backend will now automatically register itself with the Defendr application.

## 4. Troubleshooting

### 4.1. Missing bpf maps

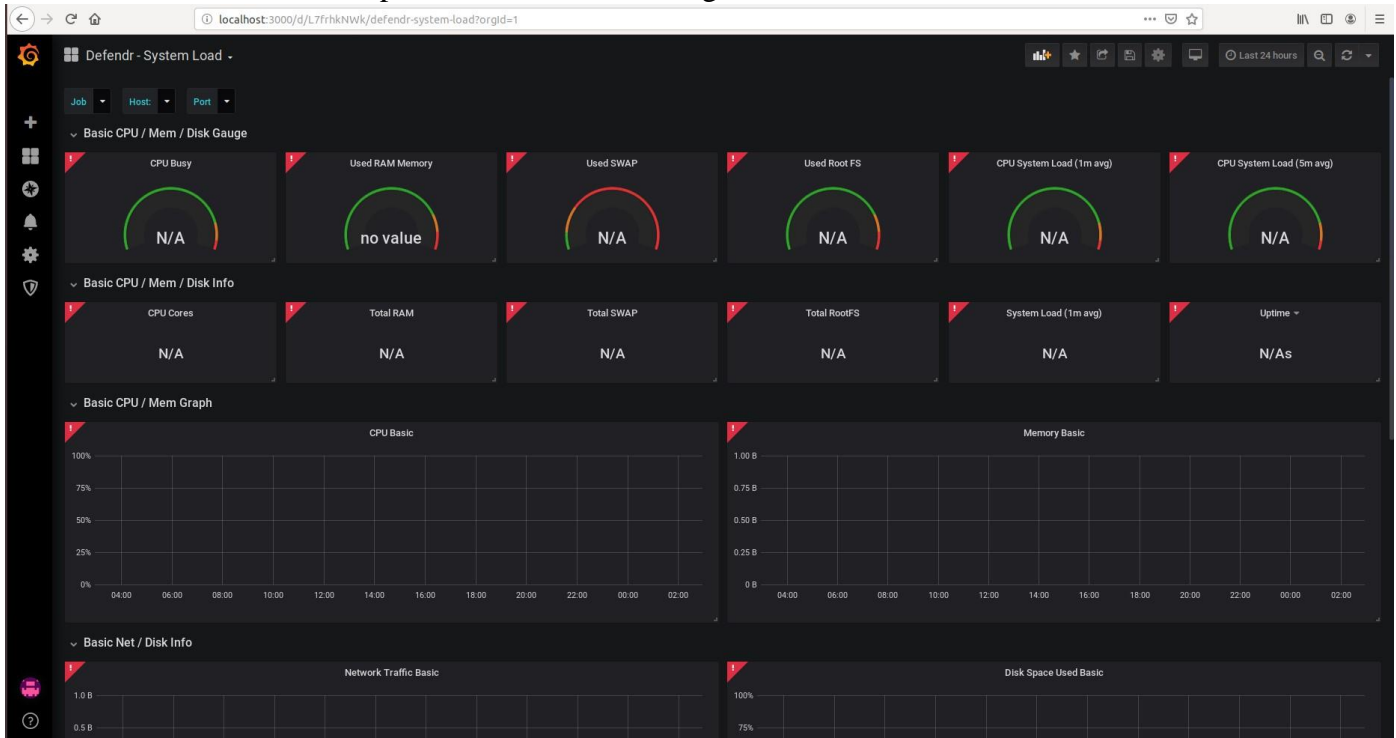
In the unlikely event that the following error appears in a pop up terminal while opening the Defendr application

```
ERR: specified path /sys/fs/bpf/ddos_blacklist is not on BPF FS
```

Mount the bpf file system by entering the command “`sudo mount -t bpf bpf /sys/fs/bpf/`” without the quotations within the terminal and press enter. If confronted with a request for the user password, enter the server password obtained from the server admin and press enter. The application can now be safely restarted. In the event that the system interface becomes unresponsive the interface can simply be closed without doing any harm and restarted. This will not affect the system in any way.

### 4.2. Grafana is not showing any data

At time an improper start-up of a server may cause a disruption in the proper display of metrics. This may be due to delays or disruptions in service start-ups. A Defendr restart may cause the system to return to normal functionality, however for persistent cases more steps can be taken to investigate and remediate.



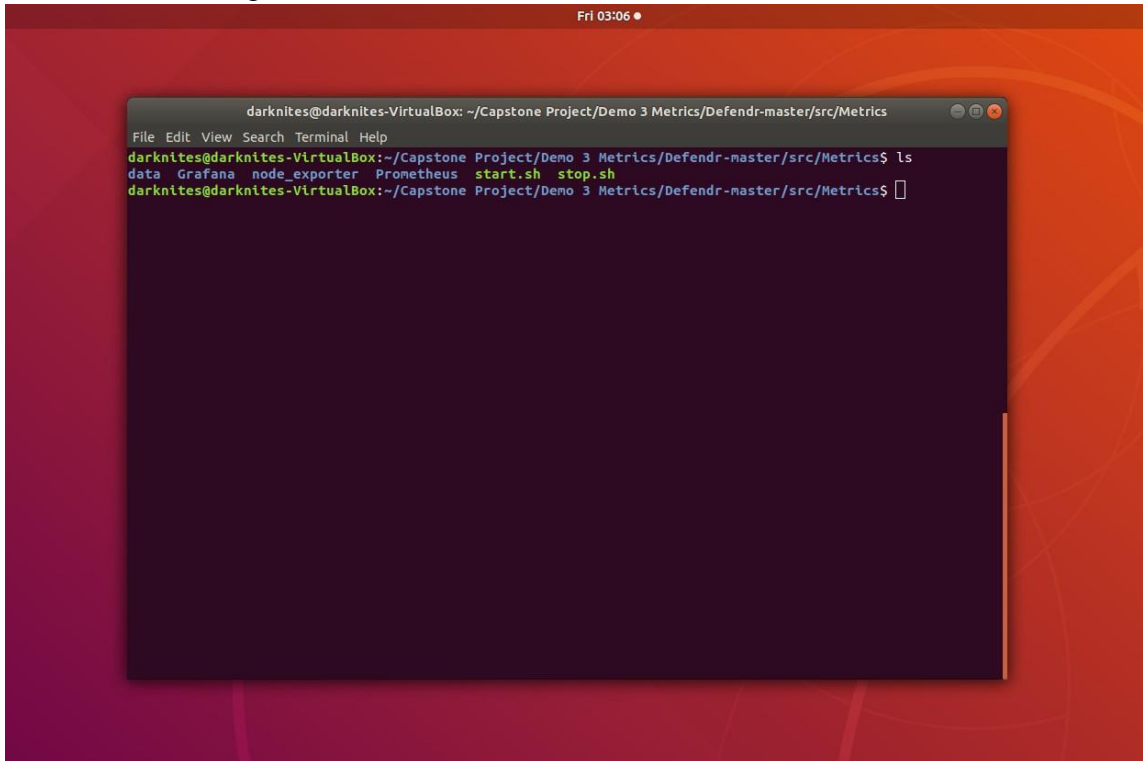
To determine the cause, open a browser and navigate to:

- <http://localhost:9190>\*

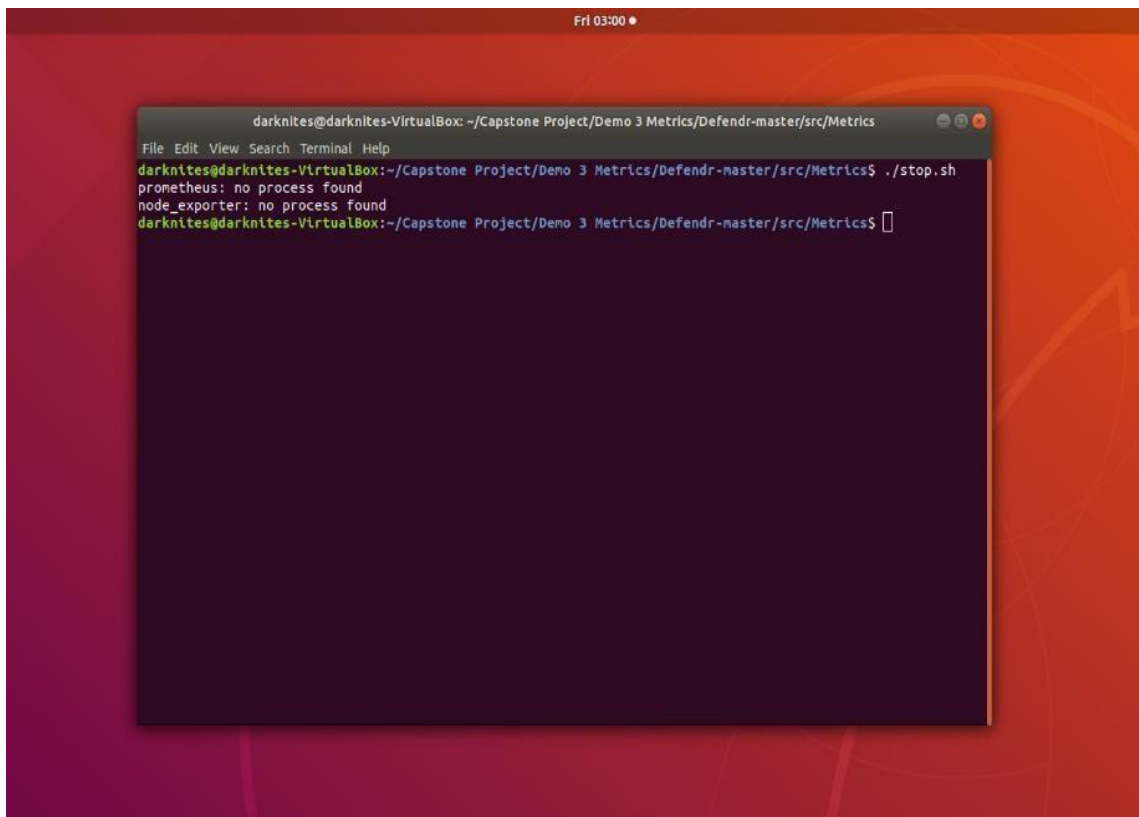
- <http://localhost:9090>\*
  - <http://localhost:3000>\*
- \*curl <address> can be used in terminal as well

If no response is received, please try the following:

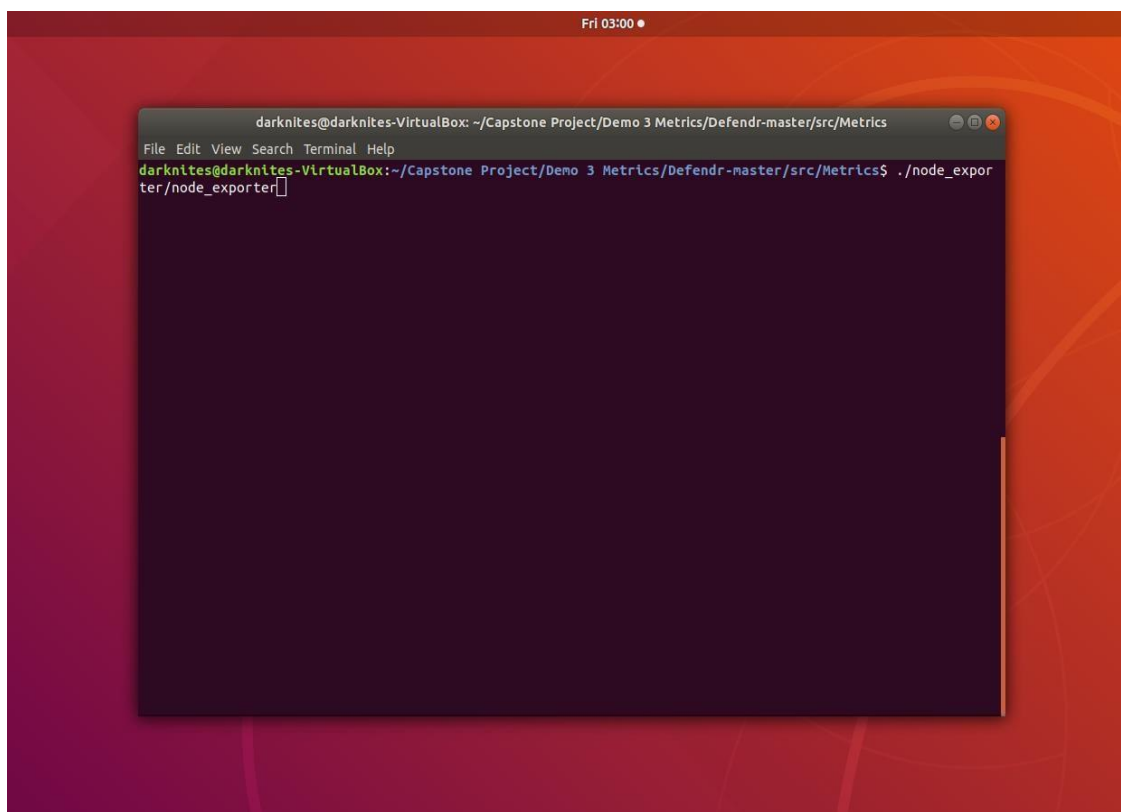
- Open a terminal in “/Defendr/src/Interfaces/Metrics”. This is the working directory and all the following commands, unless otherwise stated, will start here.



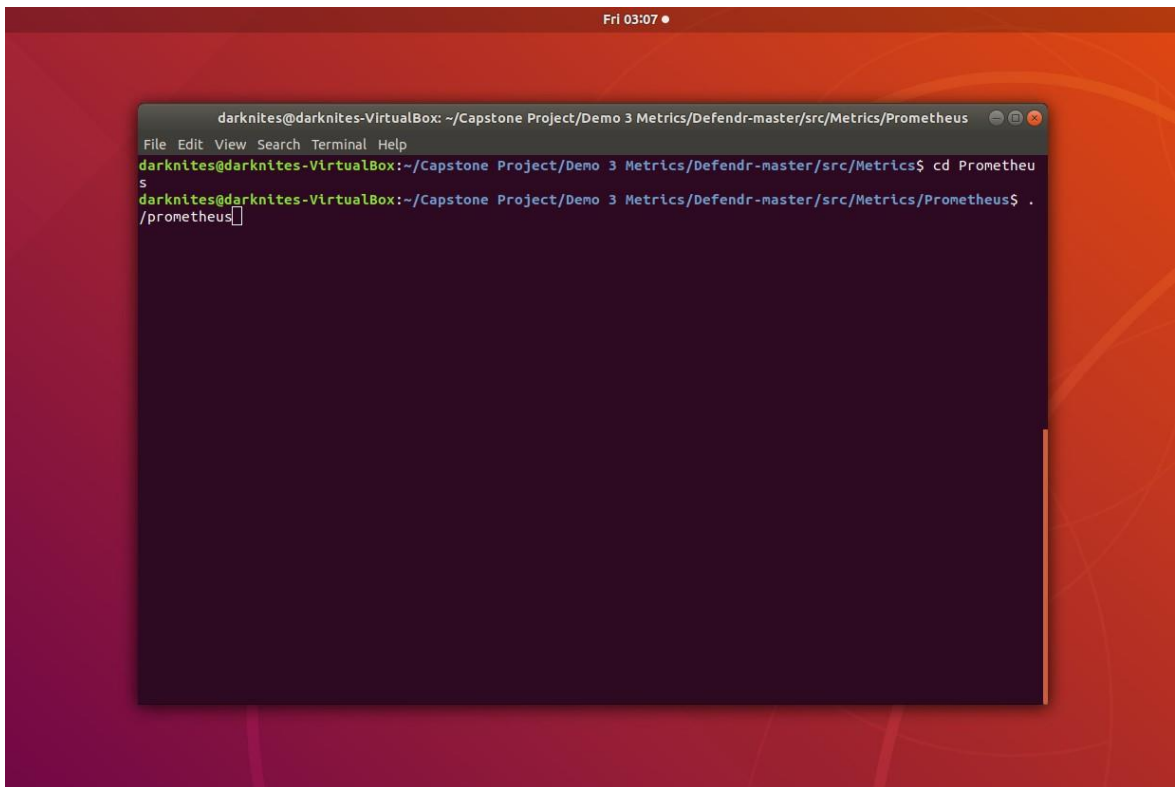
- Enter “./stop.sh”. Any rouge servers will stop. If a no process message appears, that just means the particular service was not running.



- Open a terminal and enter “./node\_exporter/node\_exporter”. Allow 5 seconds.



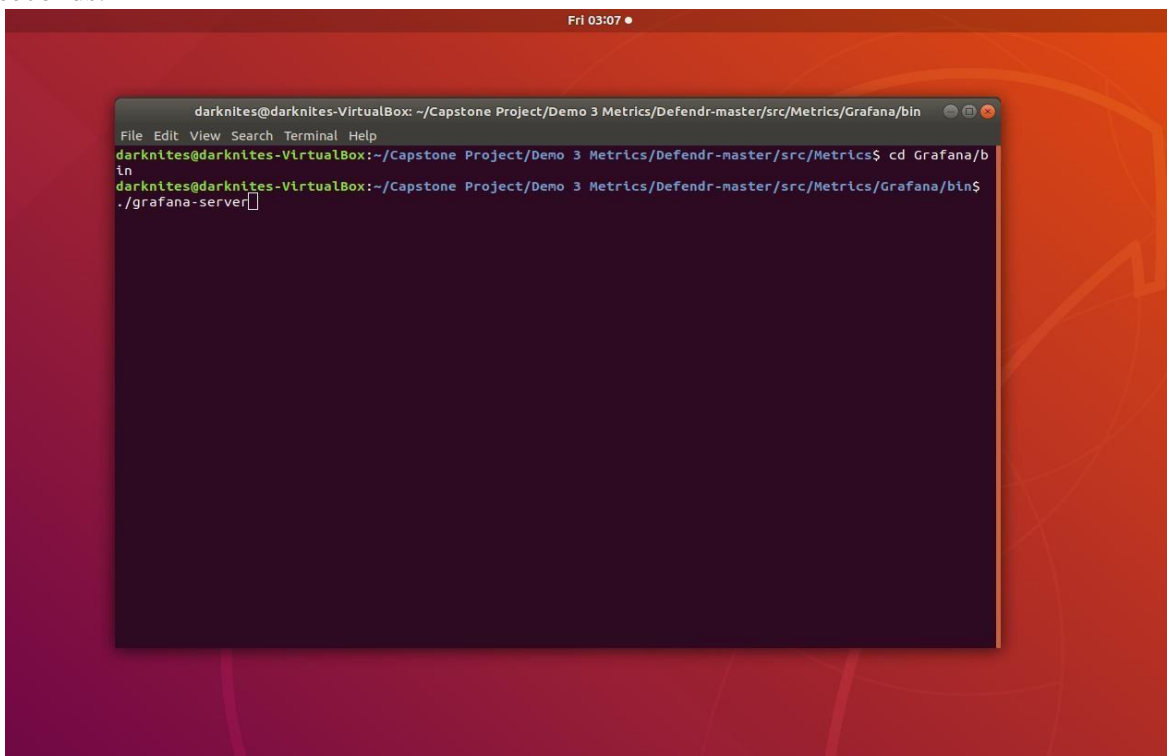
- Open a terminal and enter “cd Prometheus”. Then enter “./prometheus”. Allow 5 seconds.



A terminal window titled "darknites@darknites-VirtualBox: ~/Capstone Project/Demo 3 Metrics/Defendr-master/src/Metrics/Prometheus" is shown. The terminal has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The command history shows the user navigating to the Prometheus directory and starting the service.

```
darknites@darknites-VirtualBox: ~/Capstone Project/Demo 3 Metrics/Defendr-master/src/Metrics/Prometheus
darknites@darknites-VirtualBox:~/Capstone Project/Demo 3 Metrics/Defendr-master/src/Metrics$ cd Prometheus
darknites@darknites-VirtualBox:~/Capstone Project/Demo 3 Metrics/Defendr-master/src/Metrics/Prometheus$ ./prometheus
```

- Open a terminal and enter “cd Grafana/bin”. Then enter “./grafana-server”. Allow 5 seconds.

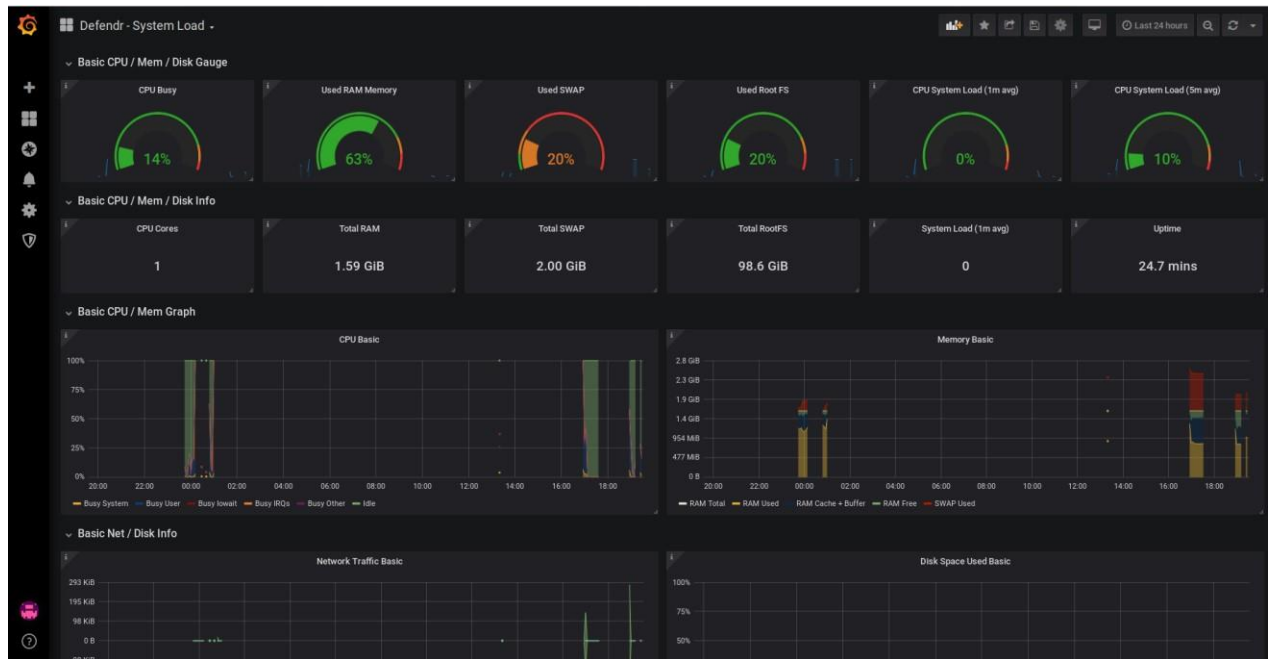


A terminal window titled "darknites@darknites-VirtualBox: ~/Capstone Project/Demo 3 Metrics/Defendr-master/src/Metrics/Grafana/bin" is shown. The terminal has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The command history shows the user navigating to the Grafana bin directory and starting the server.

```
darknites@darknites-VirtualBox: ~/Capstone Project/Demo 3 Metrics/Defendr-master/src/Metrics/Grafana/bin
darknites@darknites-VirtualBox:~/Capstone Project/Demo 3 Metrics/Defendr-master/src/Metrics$ cd Grafana/bin
darknites@darknites-VirtualBox:~/Capstone Project/Demo 3 Metrics/Defendr-master/src/Metrics/Grafana/bin$ ./grafana-server
```

- Open a browser, and navigate to “<http://localhost:3000>”





Provided the above services started with no errors, Grafana log-in should be displayed and metrics accessible again.

### 4.3. Interface failures

#### 4.3.1. Failure to Sign in

If the system fails to sign in, make sure that the computer is connected to the Internet.

If the user has newly registered, the user should request admin to verify the account. Note that a user only receives three attempts to enter the correct password and e-mail address. After this an e-mail will be sent to the admin users and the user that tried to sign in will be forced to wait a minute.

#### 4.3.2. Failure to open certain windows

This can only be caused by the user not having sufficient permission. See table below for permissions.

	Windows					
	Backends	Metrics	System logs	Blacklisting	Whitelisting	User management
Min permission needed	User	User	User	Admin	Admin	Admin

#### 4.3.3. Failure to add IP address to black list:

This can be due to three reasons, namely:

- An invalid IP version 4 address.(See <https://www.noip.com/support/knowledgebase/what-is-a-valid-ip-address/> for format of valid IP Addresses)
- The IP address has already been added.
- The IP address is in the White list and can thus not be blacklisted, before being removed from the White list.

#### **4.3.4. Failure to add new User:**

This can be due to four reasons, namely:

- An invalid password. Sees section 2.2 for valid passwords specifications.
- An invalid email.
- Empty fields. Note that all fields needs to been filed in.
- A user with this email has already being registered.

**For further assisting please contact the developers at the following address:**

*[info@darknites.co.za](mailto:info@darknites.co.za)*