

# LAB 10 – Containerization+SIEM

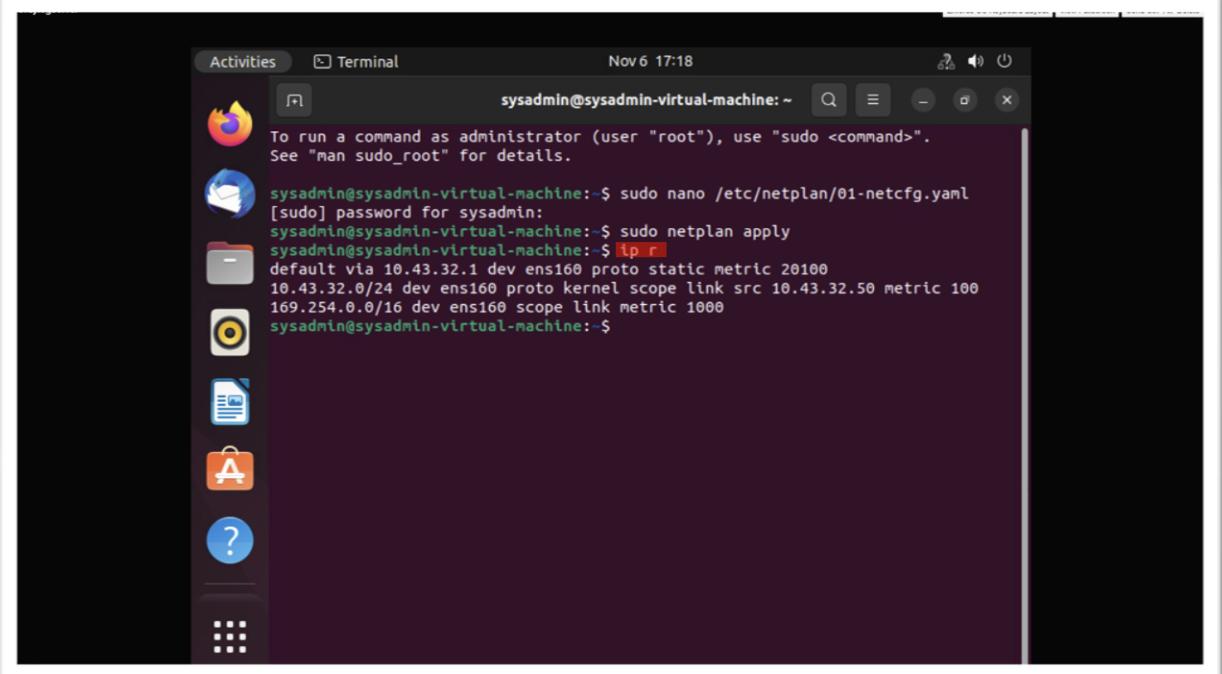
By :- Faraz Ahmed

## Table of Contents

<b>1. GraylogServer Setup .....</b>	3
<b>2. GraylogServer: Configure Graylog .....</b>	4
<b>3. Configure Graylog Forwarders .....</b>	5
a. On Linux :-.....	5
b. On pfSenseRouter.....	6
<b>4. Update Firewall Rules.....</b>	7
<b>5. Applied Graylog Capabilities .....</b>	8
<b>6. Creating new alerts and a dashboard .....</b>	11
<b>7. Update Topology .....</b>	12

## 1. GraylogServer Setup

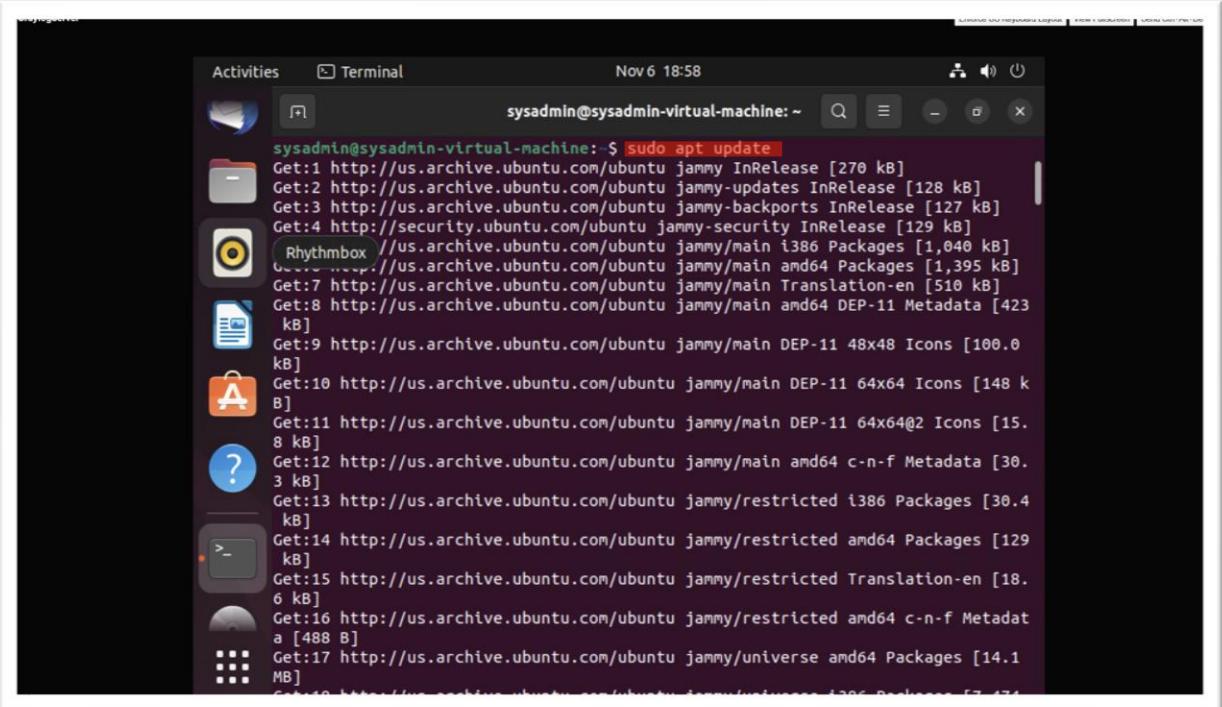
- After installing basic GraylogServer and changing network configuration of that device, we enter “ip r” to check if the configurations are entered properly or not as highlighted in Figure 1.



```
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
sysadmin@sysadmin-virtual-machine:~$ sudo nano /etc/netplan/01-netcfg.yaml  
[sudo] password for sysadmin:  
sysadmin@sysadmin-virtual-machine:~$ sudo netplan apply  
sysadmin@sysadmin-virtual-machine:~$ ip r  
default via 10.43.32.1 dev ens160 proto static metric 20100  
10.43.32.0/24 dev ens160 proto kernel scope link src 10.43.32.50 metric 100  
169.254.0.0/16 dev ens160 scope link metric 1000  
sysadmin@sysadmin-virtual-machine:~$
```

**Figure 1: Screenshot of command “ip r” to check network configuration of GraylogServer.**

- Now we enter command “sudo apt update” as highlighted below to update and upgrade the overall operating system in GraylogServer.



```
sysadmin@sysadmin-virtual-machine:~$ sudo apt update  
Get:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease [270 kB]  
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]  
Get:3 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]  
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]  
Get:5 http://us.archive.ubuntu.com/ubuntu jammy/main i386 Packages [1,040 kB]  
Get:6 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 Packages [1,395 kB]  
Get:7 http://us.archive.ubuntu.com/ubuntu jammy/main Translation-en [510 kB]  
Get:8 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 DEP-11 Metadata [423 kB]  
Get:9 http://us.archive.ubuntu.com/ubuntu jammy/main DEP-11 48x48 Icons [100.0 kB]  
Get:10 http://us.archive.ubuntu.com/ubuntu jammy/main DEP-11 64x64 Icons [148 kB]  
Get:11 http://us.archive.ubuntu.com/ubuntu jammy/main DEP-11 64x64@2 Icons [15.8 kB]  
Get:12 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 c-n-f Metadata [30.3 kB]  
Get:13 http://us.archive.ubuntu.com/ubuntu jammy/restricted i386 Packages [30.4 kB]  
Get:14 http://us.archive.ubuntu.com/ubuntu jammy/restricted amd64 Packages [129 kB]  
Get:15 http://us.archive.ubuntu.com/ubuntu jammy/restricted Translation-en [18.6 kB]  
Get:16 http://us.archive.ubuntu.com/ubuntu jammy/restricted amd64 c-n-f Metadata [488 B]  
Get:17 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
```

**Figure 2: Screenshot of command “sudo apt update” to update O.S. of GraylogServer.**

## 2. GraylogServer: Configure Graylog

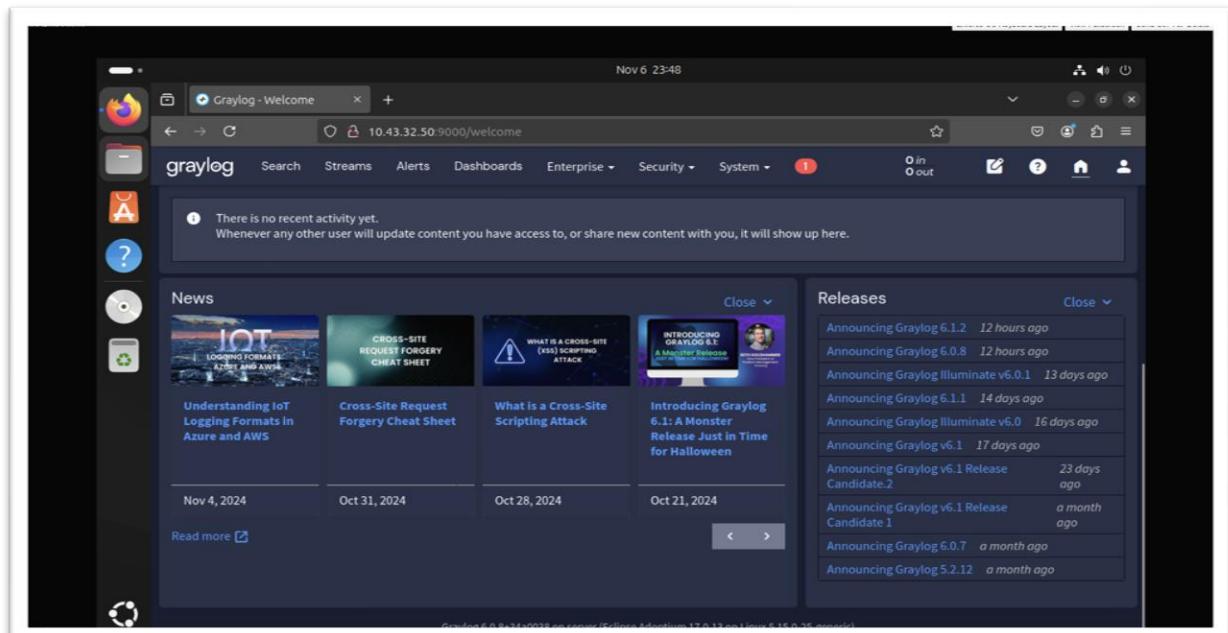
- Then we install VMWare in GraylogServer and then enable it by inputting “sudo systemctl enable –now open-vm-tools”, then check the status by entering “systemctl status open-vm-tools” (as highlighted in figure 3) and from Figure 3 we can see that the VMWare is active and running.

The screenshot shows a terminal window titled "Activities Terminal" with the command history and output:

```
*** vgauth.conf (Y/N/D/Z) [default=N] ? y
Installing new version of config file /etc/vmware-tools/vgauth.conf ...
Created symlink /etc/systemd/system/vmtoolsd.service → /lib/systemd/system/open-vm-tools.service.
Created symlink /etc/systemd/system/multi-user.target.wants/open-vm-tools.service → /lib/systemd/system/open-vm-tools.service.
Created symlink /etc/systemd/system/open-vm-tools.service.requires/vgauth.service → /lib/systemd/system/vgauth.service.
Setting up ethtool (1:5.16-1ubuntu0.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3) ...
sysadmin@sysadmin-virtual-machine: $ sudo systemctl enable --now open-vm-tools
Synchronizing state of open-vm-tools.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable open-vm-tools
sysadmin@sysadmin-virtual-machine: $ systemctl status open-vm-tools
● open-vm-tools.service - Service for virtual machines hosted on VMware
   Loaded: loaded (/lib/systemd/system/open-vm-tools.service; enabled; vendor
   Active: active (running) since Wed Nov  6 18:58:14 EST 2024; 2min 9s ago
     Docs: http://open-vm-tools.sourceforge.net/about.php
          Main PID: 3592 (vmtoolsd)
             Tasks: 3 (limit: 9459)
            Memory: 1.7M
              CPU: 416ms
            CGroup: /system.slice/open-vm-tools.service
                    └─3592 /usr/bin/vmtoolsd
Nov 06 18:58:14 sysadmin-virtual-machine systemd[1]: Started Service for virtu
12:--> 4 enter/exit
```

**Figure 3: Screenshot of sudo systemctl enable –now open-vm-tools” to enable VMWare and “systemctl status open-vm-tools” to check the status of VMWare.**

- By installing Docker, Docker compose and then Graylog using a docker compose .yaml file, we can access Graylog webpage using URL- <http://10.43.32.50:9000> to enter admin as default username and password to open welcome page as shown in Figure 4.

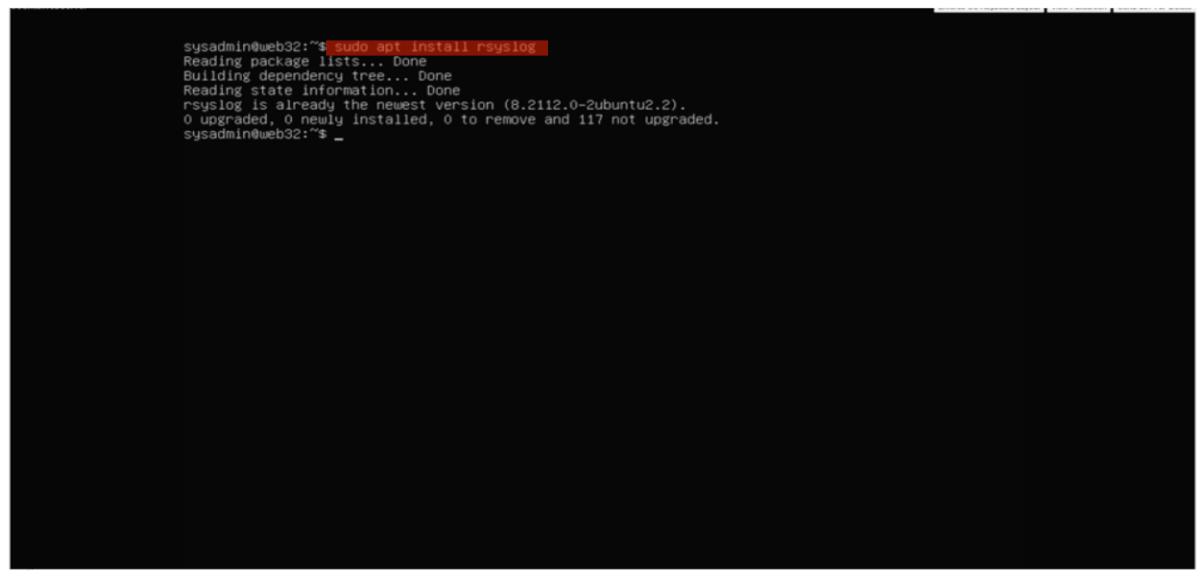


**Figure 4: Screenshot of Welcome page of Graylog by entering “http://10.43.32.50:9000”.**

### 3. Configure Graylog Forwarders

#### a. On Linux :-

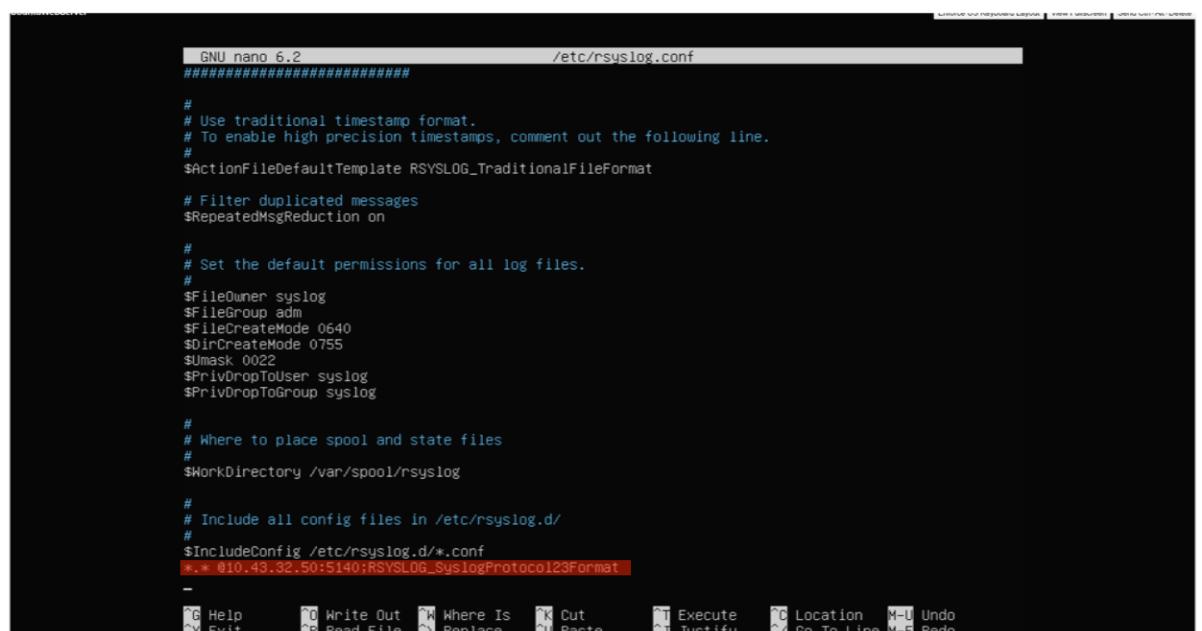
- First we install rsyslog in Linux using command “sudo apt install rsyslog” as highlighted in Figure 5.



```
sysadmin@web32:~$ sudo apt install rsyslog
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
rsyslog is already the newest version (8.21.2.0-2ubuntu2.2).
0 upgraded, 0 newly installed, 0 to remove and 117 not upgraded.
sysadmin@web32:~$ _
```

**Figure 5: Screenshot of “sudo apt install rsyslog” to install rsyslog in Linux.**

- After installing necessary files, we edit rsyslog configuration file using “sudo nano /etc/rsyslog.conf” and enter a new line - “\*.\* @10.43.32.50:5140;RSYSLOG\_SyslogProtocol23Format” ( as highlighted) and then Press CTRL+X then select Y to do Yes and then press Enter to exit the edit mode.



```
GNU nano 6.2                               /etc/rsyslog.conf
#####
#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
#
# Filter duplicated messages
$RepeatedMsgReduction on
#
# Set the default permissions for all log files.
#
$fileOwner syslog
$fileGroup adm
$fileCreateMode 0640
$dirCreateMode 0755
$umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog
#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog
#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
*.* @10.43.32.50:5140;RSYSLOG_SyslogProtocol23Format
-
```

**Figure 6: Screenshot of adding new line “\*.\* @10.43.32.50:5140;RSYSLOG\_SyslogProtocol23Format” to edit rsyslog configuration.**

- After that we will enter “`sudo systemctl restart rsyslog`” to start rsyslog services then enter “`sudo systemctl status rsyslog`” to check if rsyslog services are running or not as highlighted below.

```

# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
.* @10.43.32.50:5140;RSYSLOG_SysLogProtocol123Format

sysadmin@web32:~$ sudo systemctl restart rsyslog
sysadmin@web32:~$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
    Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
      Active: active (running) since Thu 2024-11-07 01:44:51 UTC; 4s ago
        TriggeredBy: • syslog.socket
          Docs: man:rsyslogd(8)
                  man:rsyslog.conf(5)
                  https://www.rsyslog.com/doc/
        Main PID: 1990 (rsyslogd)
          Tasks: 4 (limit: 9387)
         Memory: 1.0M
            CPU: 20ms
          CGroup: /system.slice/rsyslog.service
                  └─1990 /usr/sbin/rsyslogd -n -inone

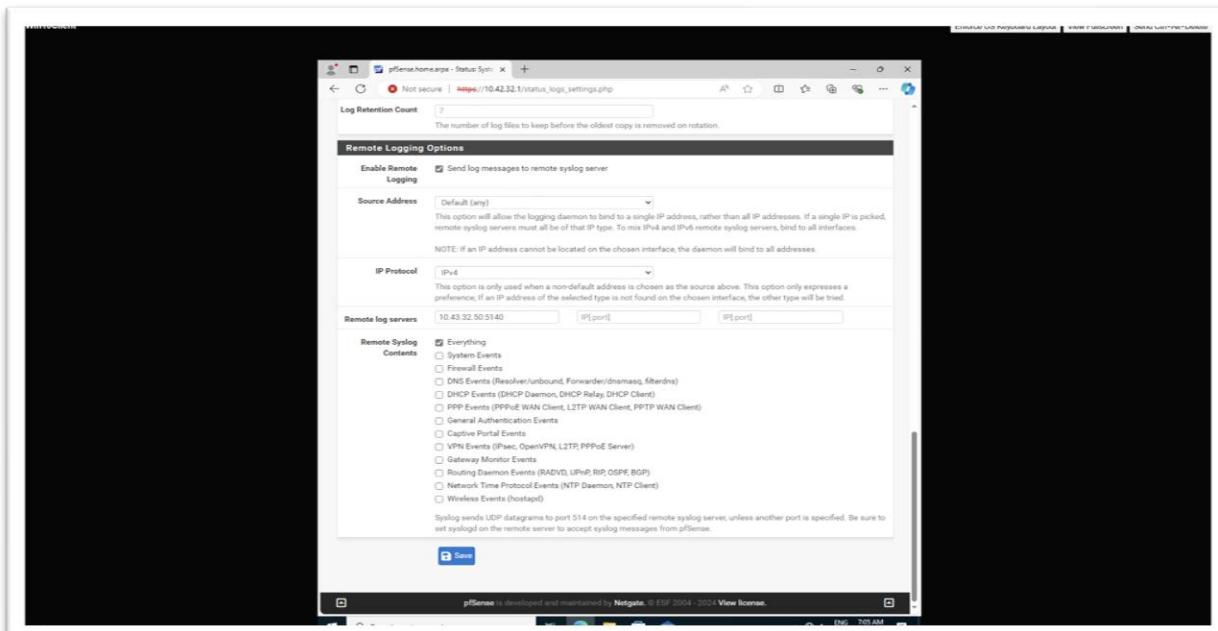
Nov 07 01:44:51 web32 systemd[1]: Starting System Logging Service...
Nov 07 01:44:51 web32 rsyslogd[1990]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' ✘
Nov 07 01:44:51 web32 systemd[1]: Started System Logging Service.
Nov 07 01:44:51 web32 rsyslogd[1990]: rsyslogd's groupid changed to 113
Nov 07 01:44:51 web32 rsyslogd[1990]: rsylogd's userid changed to 107
Nov 07 01:44:51 web32 rsyslogd[1990]: [origin software="rsyslog" x-pid="1990"] ✘
11:44:51.19017911 [root]


```

**Figure 7: Screenshot of “`sudo systemctl restart rsyslog`” to restart rsyslog services and “`sudo systemctl status rsyslog`” to check if services is up and running or not.**

### b. On pfSenseRouter

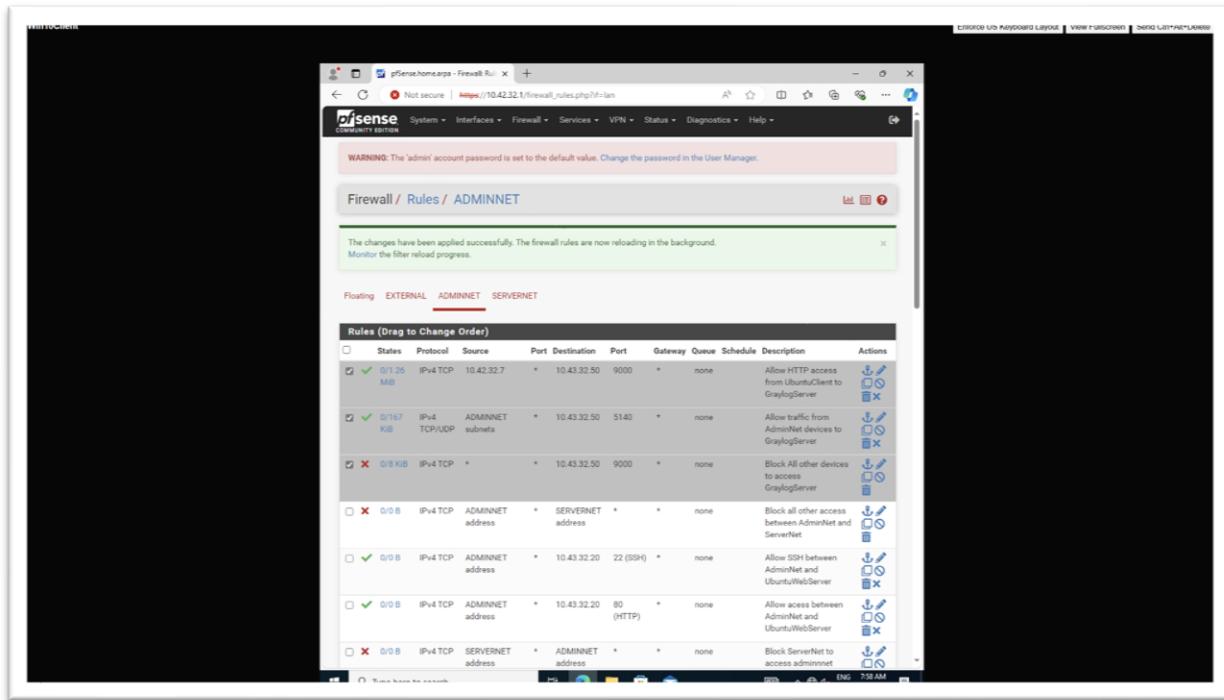
- To configure rsyslog in pfSenseRouter, we navigate to “`http://10.42.32.1`” and go to Status → System Logs → Settings and under “Remote Logging Options” select Enable Remote Logging and enter GraylogServer’s IP- “10.43.32.50:5140” and select Save.



**Figure 8: Screenshot of configure rsyslog in pfSenseRouter by “Enabling Remote Logging”.**

## 4. Update Firewall Rules

- From Figure 9 we can see three highlighted firewall rules from which, first one is to “Allow HTTP access from UbuntuClient to GraylogServer” and second rule is “Allow traffic from AdminNet device to GraylogServer” and last one is “Block all other devices to access GraylogServer” to establish proper firewall rules.



**Figure 9: Screenshot of all three highlighted firewall rules.**

## 5. Applied Graylog Capabilities

- Now we send SSH to UbuntuWebServer by entering SSH to their IP address like “ssh nonexistinguser@10.43.32.7”. Then we can note that the ssh was denied and fails. So, we can see the error message of SSH as shown in the Figure 10 in Graylog Web Server when we navigate to “Search → In search type- sysadmin and we can get the specific error of SSH.

The screenshot shows the Graylog web interface with a search bar containing 'sysadmin'. The results list several log entries related to NetworkManager and the SSH service, all originating from 'sysadmin-virtual-machine'. The log entries include messages about NetworkManager state changes and SSH failed attempts for non-existent users.

Timestamp	Source	Message
2024-11-07 06:13:04.323	sysadmin-virtual-machine	NetworkManager-dispatcher.service: Deactivated successfully.
2024-11-07 06:12:54.300	sysadmin-virtual-machine	<info> [1739959974.2985] manager: NetworkManager state is now CONNECTED_GLOBAL
2024-11-07 06:12:50.815	sysadmin-virtual-machine	Started Network Manager Script Dispatcher Service.
2024-11-07 06:12:50.814	sysadmin-virtual-machine	[system] Successfully activated service 'org.freedesktop.nm_dispatcher'
2024-11-07 06:12:50.780	sysadmin-virtual-machine	Starting Network Manager Script Dispatcher Service...
2024-11-07 06:12:50.747	sysadmin-virtual-machine	[system] Activating via systemd: service name='org.freedesktop.nm_dispatcher' unit='dbus-org.freedesktop.nm-dispatcher.service' requested by 11:18 (uid= pid=97 comm="/usr/sbin/NetworkManager --no-daemon --label='unconfined')
2024-11-07 06:12:50.738	sysadmin-virtual-machine	

**Figure 10: Screenshot of error message in “Search in Graylog Web Server”.**

- Now after that we will navigate to Alerts → Events → Create new events (green button), then enter all the details for that event and press save to create it as a new alert for event. As we can see from Figure 11, alert for SSH failed for non-existent user on UbuntuWebServer (highlighted in Figure 11).

The screenshot shows the 'Alerts Definitions' page in the Graylog web interface. It lists several event definitions, with one specific rule highlighted: 'Attempted SSH into non-existent user on UbuntuWebServer'. This rule is set to priority 2, runs every 20 seconds, and has been enabled.

Title	Description	Priority	Last Matched	Status	Scheduling	Actions
Attempted SSH into non-existent user on UbuntuWebServer		2	Never	enabled	Runs every 20 seconds, searching within the last 20 seconds.	<a href="#">Share</a> <a href="#">More</a>
Failed login attempt to pfSense webConfigurator GUI		2	Never	enabled	Runs every 20 seconds, searching within the last 20 seconds.	<a href="#">Share</a> <a href="#">More</a>
Firewall rules changed on pfSenseRouter		2	Never	enabled	Runs every 20 seconds, searching within the last 20 seconds.	<a href="#">Share</a> <a href="#">More</a>
System notification events	Reserved event definition for system notifications.	1	3 hours ago	enabled	Not Scheduled.	<a href="#">Share</a> <a href="#">More</a>
User added to sudo group on Linux device		2	Never	enabled	Runs every 20 seconds, searching within the last 20 seconds.	<a href="#">Share</a> <a href="#">More</a>

**Figure 11: Screenshot of highlighted alert rule for “SSH for non-existent user on UbuntuWebServer”.**

- So, we will do the same to make an alert rule for “Failed login attempts in pfSense webConfigurator GUI as shown in Figure 12.

The screenshot shows the Graylog web interface with the URL `10.43.32.50:9000/alerts/definitions`. The left sidebar has icons for Alerts & Events, Event Definitions (which is selected), and Notifications. The main content area displays a table of event definitions:

Title	Description	Priority	Last Matched	Status	Scheduling	Actions
<input type="checkbox"/> Attempted SSH into non-existent user on UbuntuWebServer		2	Never	enabled	Runs every 20 seconds, searching within the last 20 seconds.	<a href="#">Share</a> <a href="#">More</a>
<input checked="" type="checkbox"/> Failed login attempt to pfSense webConfigurator GUI		2	Never	enabled	Runs every 20 seconds, searching within the last 20 seconds.	<a href="#">Share</a> <a href="#">More</a>
<input type="checkbox"/> Firewall rules changed on pfSenseRouter		2	Never	enabled	Runs every 20 seconds, searching within the last 20 seconds.	<a href="#">Share</a> <a href="#">More</a>
<input type="checkbox"/> System notification events	Reserved event definition for system notification events	1	3 hours ago	enabled	Not Scheduled.	<a href="#">Share</a> <a href="#">More</a>
<input type="checkbox"/> User added to sudo group on Linux device		2	Never	enabled	Runs every 20 seconds, searching within the last 20 seconds.	<a href="#">Share</a> <a href="#">More</a>

**Figure 12: Screenshot of highlighted alert rule for “failed login attempt to pfSense GUI”.**

- We will do the same to create alert rule for “firewall rules changed on pfSenseRouter” as shown in Figure 13.

The screenshot shows the Graylog web interface with the URL `10.43.32.50:9000/alerts/definitions`. The left sidebar has icons for Alerts & Events, Event Definitions (selected), and Notifications. The main content area displays a table of event definitions, identical to Figure 12:

Title	Description	Priority	Last Matched	Status	Scheduling	Actions
<input type="checkbox"/> Attempted SSH into non-existent user on UbuntuWebServer		2	Never	enabled	Runs every 20 seconds, searching within the last 20 seconds.	<a href="#">Share</a> <a href="#">More</a>
<input checked="" type="checkbox"/> Firewall rules changed on pfSenseRouter		2	Never	enabled	Runs every 20 seconds, searching within the last 20 seconds.	<a href="#">Share</a> <a href="#">More</a>
<input type="checkbox"/> System notification events	Reserved event definition for system notification events	1	3 hours ago	enabled	Not Scheduled.	<a href="#">Share</a> <a href="#">More</a>

**Figure 13: Screenshot of highlighted alert rule for “failed login attempt to pfSense GUI”.**

- Now same we will do to create a new alert rule “user added to sudo group on Linux device” as shown in Figure 14.

The screenshot shows the Graylog web interface with the URL [10.43.32.50:9000/alerts/definitions](http://10.43.32.50:9000/alerts/definitions). The left sidebar has icons for Search, Streams, Alerts, Dashboards, Enterprise, Security, System, and a user profile. The main area displays a table of alert definitions:

Title	Description	Priority	Last Matched	Status	Scheduling	Actions
<input type="checkbox"/> Attempted SSH into non-existent user on UbuntuWebServer		2	Never	<span>Enabled</span>	Runs every 20 seconds, searching within the last 20 seconds.	<span>Share</span> More
<input type="checkbox"/> Failed login attempt to pfSense webConfigurator GUI		2	Never	<span>Enabled</span>	Runs every 20 seconds, searching within the last 20 seconds.	<span>Share</span> More
<input type="checkbox"/> Firewall rules changed on pfSenseRouter		2	Never	<span>Enabled</span>	Runs every 20 seconds, searching within the last 20 seconds.	<span>Share</span> More
<input type="checkbox"/> System notification events	Reserved event definition for system notifications	1	17 hours ago	<span>Enabled</span>	Not Scheduled.	<span>Share</span> More
<input checked="" type="checkbox"/> User added to sudo group on Linux device		2	Never	<span>Enabled</span>	Runs every 20 seconds, searching within the last 20 seconds.	<span>Share</span> More

**Figure 14: Screenshot of highlighted alert rule for “user added to sudo group on Linux device”.**

## 6. Creating new alerts and a dashboard

- Navigate to “Dashboard option” and then select “Create a new dashboard” then add new “Events Overview” and add widgets to it by selecting plus symbol in the left and adding “time range by selecting drop down near clock icon”. Using this we can make a proper organized alert system and dashboard as shown in Figure 15.

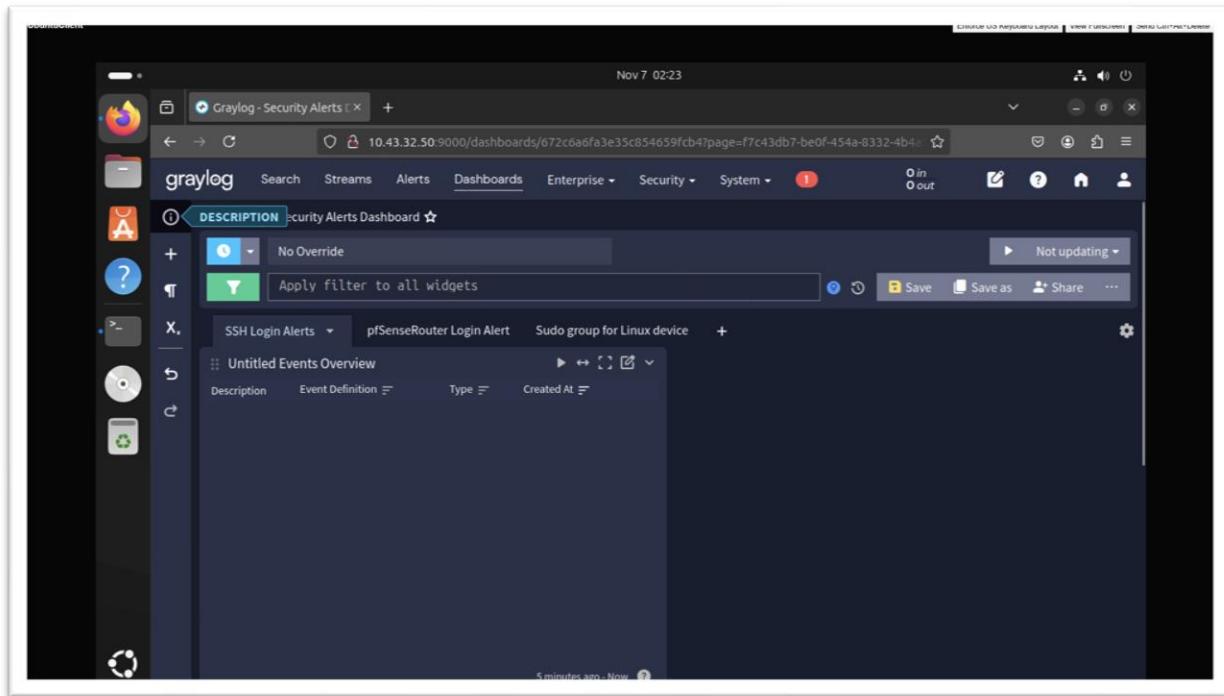
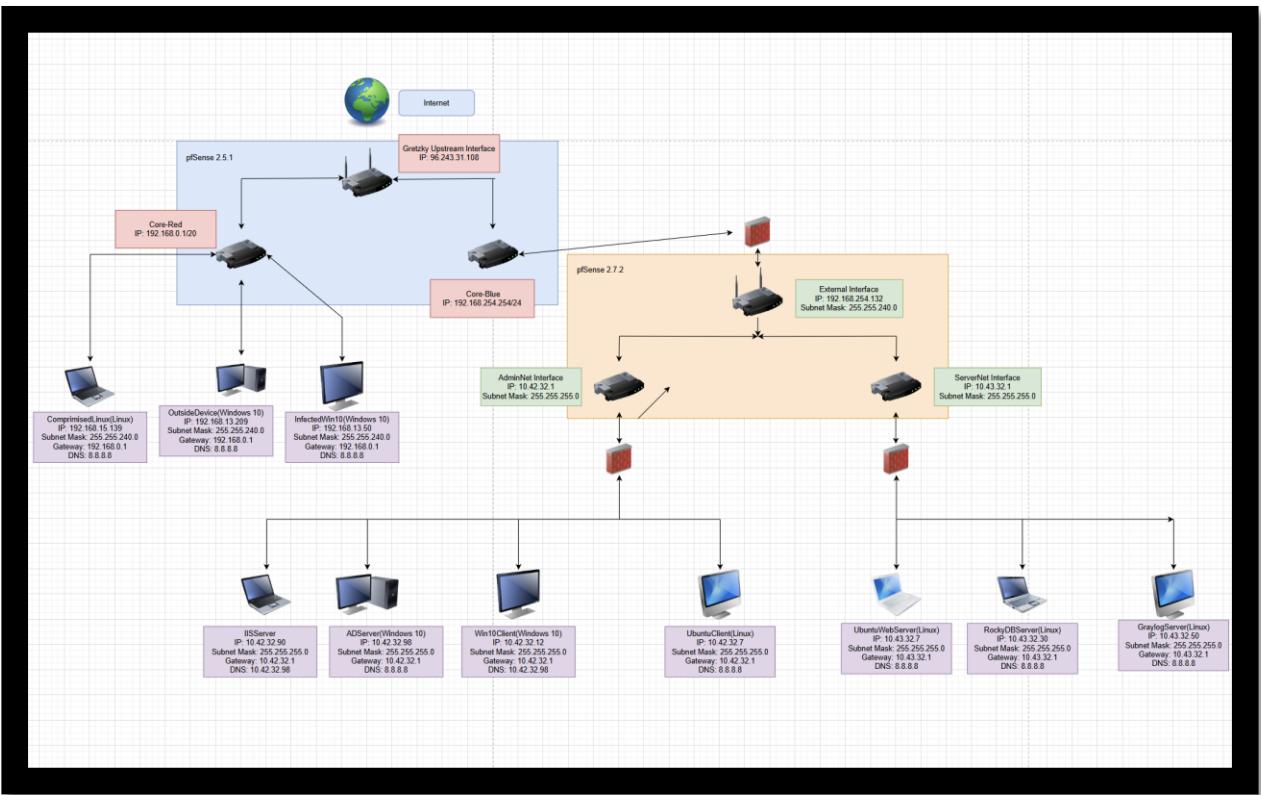


Figure 15: Screenshot of creating new dashboards and alerts in Graylog Web Server.

## 7. Update Topology



**Figure 16: Screenshot of Updated Topology.**