System Logging Protocol

In this exercise, you will learn to setup a syslog client in Ubuntu environment. Also, you will be inspecting syslog packets to explore their content and relate these to the protocol specifications defined in the syslog RFC.

I. Setting-up the syslog client in Ubuntu

1. Before starting up the Ubuntu virtual machine using VMWare, configure the network settings of the Ubuntu VM.
   a) Go to settings (right click the Ubuntu VM tab) → Network Adapter
   b) Network Connection → select '**Bridged: Connected directly to the physical network'**. Click OK.
2. Run the Ubuntu VM.
3. Normally, rsyslog is installed by default on a freshly installed Ubuntu 20.04.
   a) Check the status of the rsyslog by entering the following command:

```
# sudo service rsyslog status
```

If the status isn't active, you can always start it by running:

```
# sudo service rsyslog start
```

   b) If the status isn't active, you can always start it by running: After the installation, do the steps in #3a and #3b.

```
# sudo apt-get update

# sudo apt-get install rsyslog
```

4. Now, we need to edit the syslog configuration file. Enter the following command.

```
# sudo nano /etc/rsyslog.conf
```

5. We need to configure the syslog server IP address. In this case, you need to enter your assigned IP address in your Host's OS (not vm). Add a line before the Module section. Enter the following command. (See Fig. 1)

```
*.* @OS IP ADDRESS:514
```

6. Please remove the comment symbol (#) for the following lines: (See figure 1)

```
module(load="imudp")
input(type="imudp" port="514")
module(load="imtcp")
input(type="imtcp" port="514")
```

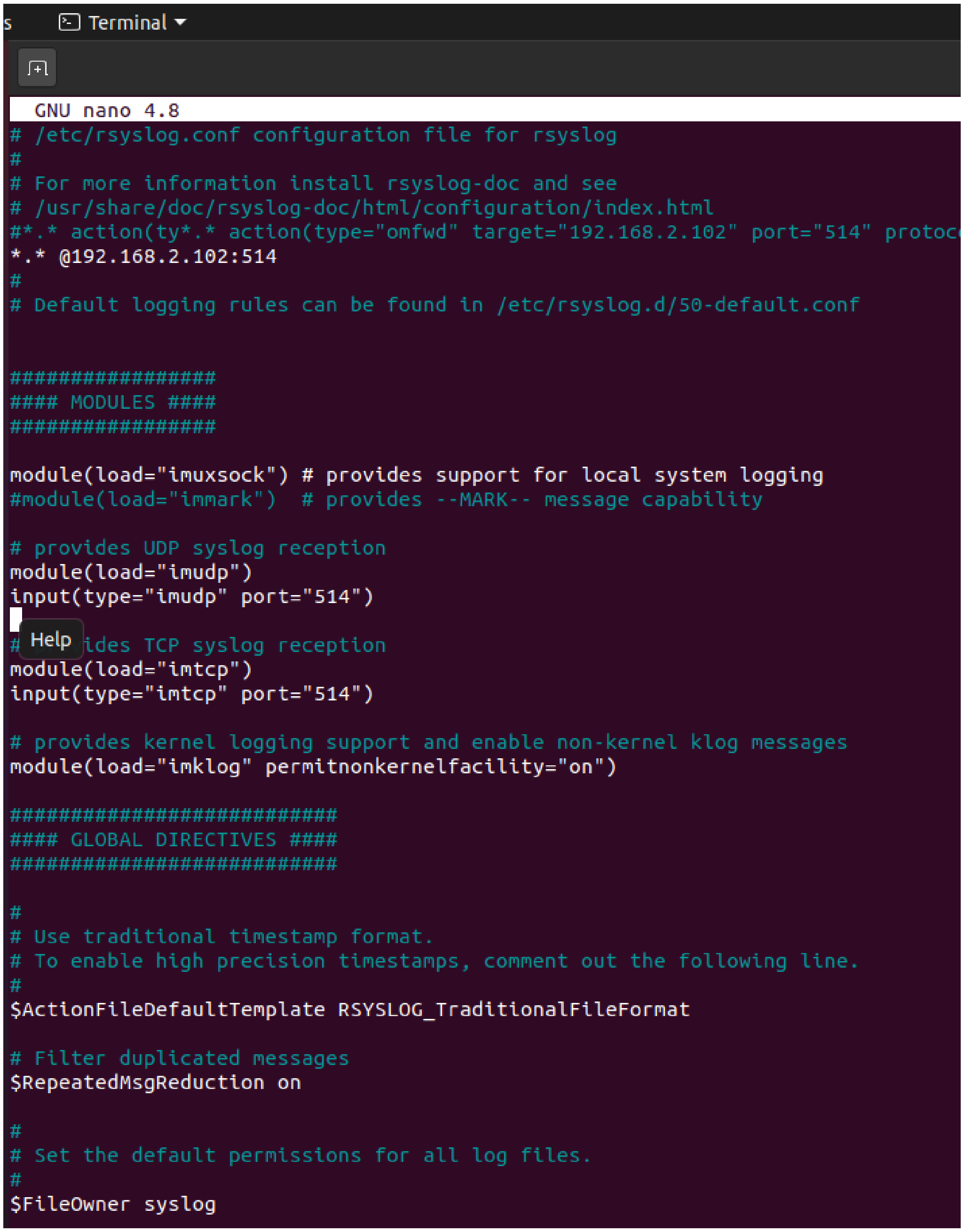
7. To save the configuration file, press "CTRL+X", then type 'Y'.
8. We need to edit the firewall rules. Enter the following commands:

```
# sudo ufw allow 514/tcp

# sudo ufw allow 514/udp
```

9. Lastly, restart the syslog service.

```
# sudo service rsyslog restart
```



```
  GNU nano 4.8
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html
#*.* action(ty*.* action(type="omfwd" target="192.168.2.102" port="514" protoc
*.* @192.168.2.102:514
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf


#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system logging
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

#       ides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

###########################
#### GLOBAL DIRECTIVES ####
###########################

#
# 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
```

Figure 1: rsyslog.conf

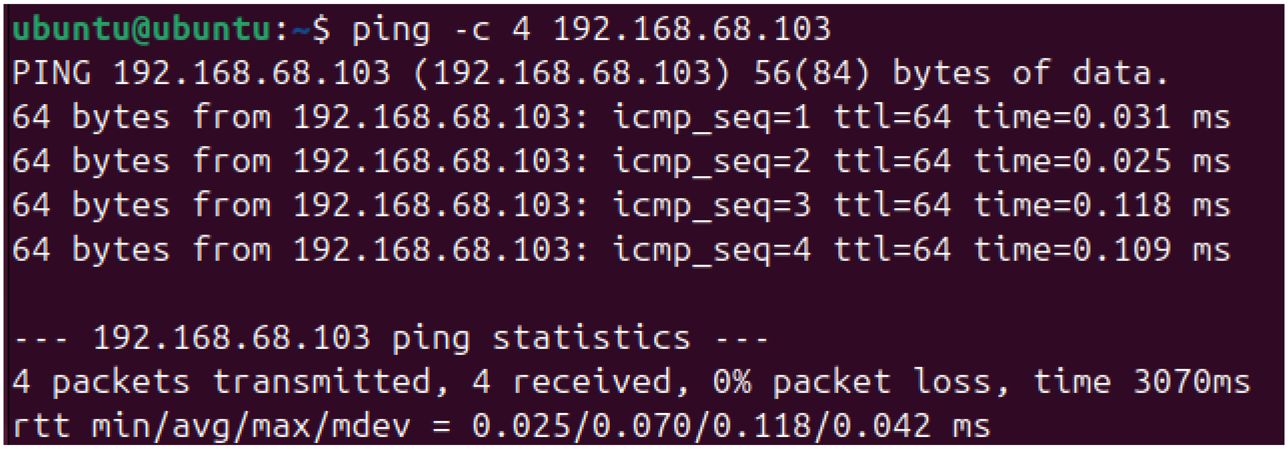
II. Installing the tftpd64

1. Install the tftpd64, by downloading here
2. After installing, run the application as administrator.
3. Go to settings → GLOBAL, uncheck everything except Syslog Server
4. Go to settings → SYSLOG, check Save syslog messages to file syslog.txt
5. Then, restart the application.

III. Capturing the syslog packets

1. First, confirm connection from the Ubuntu VM to Host's OS IP address, by sending four (4) ICMP messages. Attach a screenshot. **[1pt]**

```
# ping -c 4 xxx.xxx.xxx.xxx
```



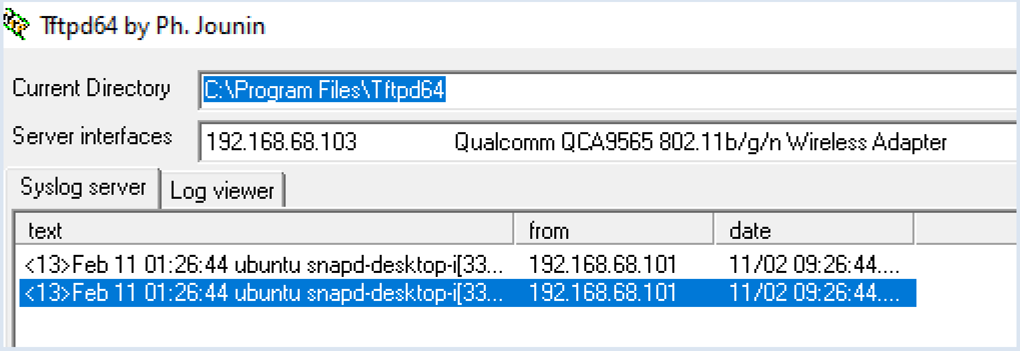
```
ubuntu@ubuntu:~$ ping -c 4 192.168.68.103
PING 192.168.68.103 (192.168.68.103) 56(84) bytes of data.
64 bytes from 192.168.68.103: icmp_seq=1 ttl=64 time=0.031 ms
64 bytes from 192.168.68.103: icmp_seq=2 ttl=64 time=0.025 ms
64 bytes from 192.168.68.103: icmp_seq=3 ttl=64 time=0.118 ms
64 bytes from 192.168.68.103: icmp_seq=4 ttl=64 time=0.109 ms

--- 192.168.68.103 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3070ms
rtt min/avg/max/mdev = 0.025/0.070/0.118/0.042 ms
```

2. Go back to tftpd application. Click "Clear" buttong. Set the server interface to your host's OS IP address by selecting from the drop-down menu then click on the syslog tab.
3. Also, run the Wireshark application on the OS, setting the capture interface to your Ethernet Connection. Apply a filter by using the string 'syslog'
4. On the Ubuntu VM, do the following actions by checking messages logged in TFTPd:
   i. Logout from the Ubuntu VM. Click the power button on the upper right side of the desktop. See the results in the tftpd64 application. Answer the following questions:
   ii. What is the most common priority # in the results? **[1 pt]**

13

   iii. Attach a screenshot of the tftpd syslog results below. **[3pts]**



Tftpd64 by Ph. Jounin

Current Directory: C:\Program Files\Tftpd64

Server interfaces: 192.168.68.103 Qualcomm QCA9565 802.11b/g/n Wireless Adapter

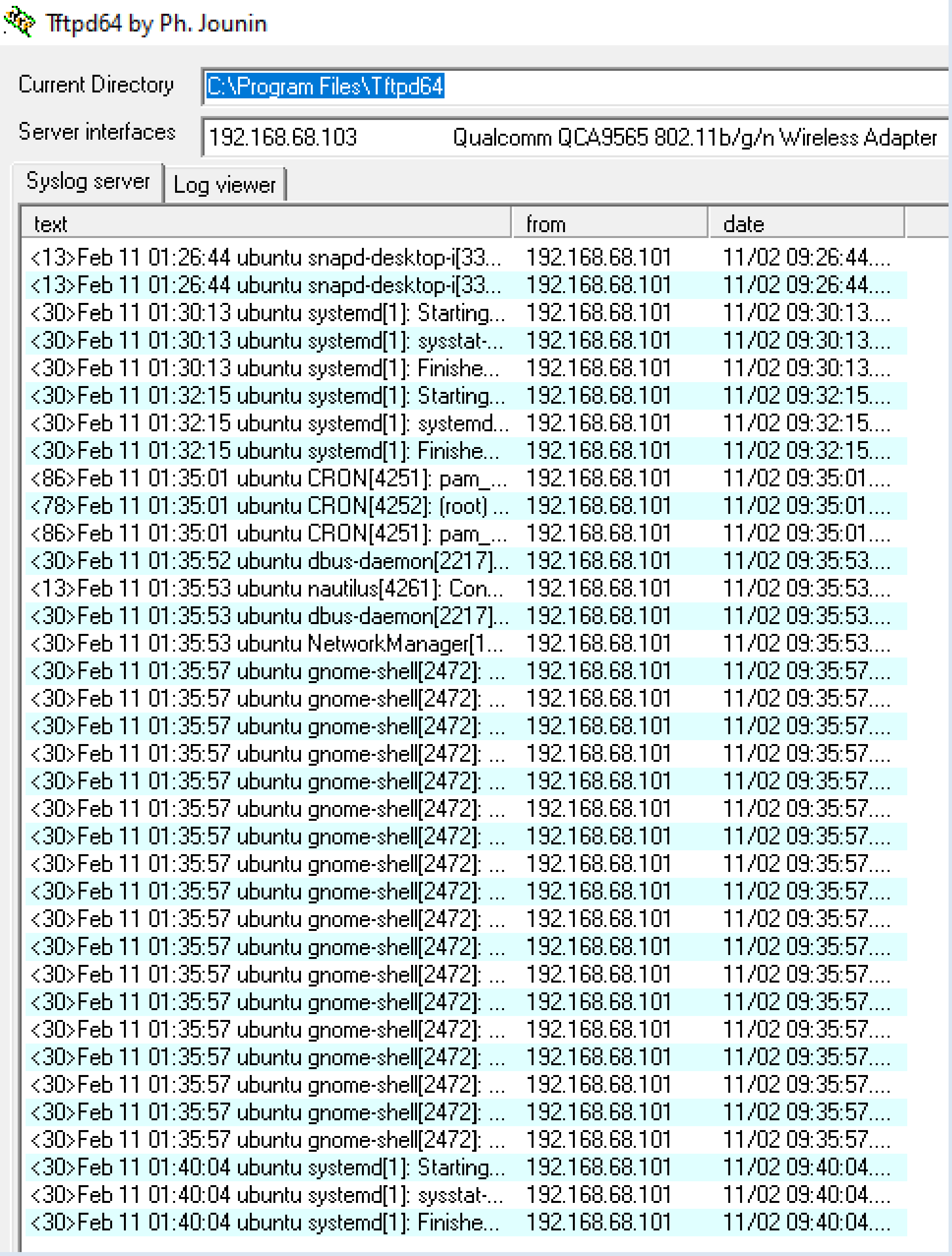
text	from	date
<13>Feb 11 01:26:44 ubuntu snapd-desktop-i[33...	192.168.68.101	11/02 09:26:44....
<13>Feb 11 01:26:44 ubuntu snapd-desktop-i[33...	192.168.68.101	11/02 09:26:44....

iv. Select a syslog entry and fill the information below.[**3pts**]

Facility (Value and Interpretation)	1
Severity (Value and Interpretation)	3
Date and Time	11/02 09:26:44
Host	192.168.68.101
Source Process	ubuntu snapd-desktop

v. Your Ubuntu VM is currently logged out. Click your profile (do not enter password yet). Get the details of the second message generated. Attach a screenshot of the tftpd syslog results . **[3pts]**

Facility (Value and Interpretation)	3
Severity (Value and Interpretation)	0
Date and Time	11/02 09:37:44
Host	192.168.68.101
Source Process	ubuntu system[1] starting



Current Directory: C:\Program Files\Tftpd64

Server interfaces: 192.168.68.103 Qualcomm QCA9565 802.11b/g/n Wireless Adapter

```
text                                              from            date
<13>Feb 11 01:26:44 ubuntu snapd-desktop-i[33...  192.168.68.101  11/02 09:26:44....
<13>Feb 11 01:26:44 ubuntu snapd-desktop-i[33...  192.168.68.101  11/02 09:26:44....
<30>Feb 11 01:30:13 ubuntu systemd[1]: Starting...  192.168.68.101  11/02 09:30:13....
<30>Feb 11 01:30:13 ubuntu systemd[1]: sysstat-...  192.168.68.101  11/02 09:30:13....
<30>Feb 11 01:30:13 ubuntu systemd[1]: Finishe...  192.168.68.101  11/02 09:30:13....
<30>Feb 11 01:32:15 ubuntu systemd[1]: Starting...  192.168.68.101  11/02 09:32:15....
<30>Feb 11 01:32:15 ubuntu systemd[1]: systemd...  192.168.68.101  11/02 09:32:15....
<30>Feb 11 01:32:15 ubuntu systemd[1]: Finishe...  192.168.68.101  11/02 09:32:15....
<86>Feb 11 01:35:01 ubuntu CRON[4251]: pam_...  192.168.68.101  11/02 09:35:01....
<78>Feb 11 01:35:01 ubuntu CRON[4252]: (root) ...  192.168.68.101  11/02 09:35:01....
<86>Feb 11 01:35:01 ubuntu CRON[4251]: pam_...  192.168.68.101  11/02 09:35:01....
<30>Feb 11 01:35:52 ubuntu dbus-daemon[2217]...  192.168.68.101  11/02 09:35:53....
<13>Feb 11 01:35:53 ubuntu nautilus[4261]: Con...  192.168.68.101  11/02 09:35:53....
<30>Feb 11 01:35:53 ubuntu dbus-daemon[2217]...  192.168.68.101  11/02 09:35:53....
<30>Feb 11 01:35:53 ubuntu NetworkManager[1...  192.168.68.101  11/02 09:35:53....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:35:57 ubuntu gnome-shell[2472]: ...  192.168.68.101  11/02 09:35:57....
<30>Feb 11 01:40:04 ubuntu systemd[1]: Starting...  192.168.68.101  11/02 09:40:04....
<30>Feb 11 01:40:04 ubuntu systemd[1]: sysstat-...  192.168.68.101  11/02 09:40:04....
<30>Feb 11 01:40:04 ubuntu systemd[1]: Finishe...  192.168.68.101  11/02 09:40:04....
```

vi. Log-in to your Ubuntu VM by entering password. Open a terminal and go back to tftpd, click ‘Clear’. Restart the syslog service (`sudo service rsyslog restart`). Get the details of the 3rd and 4th messages generated. [**6pts**]

Facility (Value and Interpretation)	3
Severity (Value and Interpretation)	0
Date and Time	11/02 09:43:44
Host	192.168.68.101
Source Process	Stopping rsyslog service

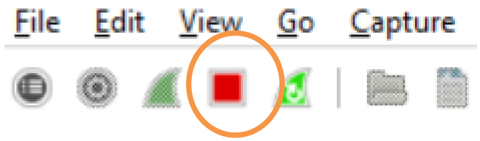
Facility (Value and Interpretation)	4
Severity (Value and Interpretation)	6

Date and Time	11/02 09:43:44
Host	192.168.68.101
Source Process	ubuntu rsyslog … exiting signal 15

Why do you think is it essential to include a priority field containing the facility and severity codes? [**1pt**]

I think it is essential to include a priority field containing the facility and severity codes because it ensures structured, efficient, and actionable log management.

5. Stop the packet capture on Wireshark



6. Expand the network layer details of syslog packets captured and inspect contents

   Based on the source and destination addresses of the packets, which host serves as syslog originator and which host serves as syslog collector? [**1pt**]

The host that serves as the syslog originator is the VMWare's IP address and the host that serves as the syslog collector is the client's own IP address.

7. Expand transport layer details of syslog packets captured.

   What transport protocol and port number used to transfer syslog packets? [**1pt**]

The transport protocol and port number used to transfer syslog packets are UDP on port number 514.

Are any of these packets acknowledged by the collector? [**1pt**]

Yes, the packets are acknowledged by the collector.

8. Inspect the raw data of the packets by looking at the Hex dump on the bottom most window pane of Wireshark.

   Can you easily read the message content of syslog messages? [**1pt**]

Yes

What does this imply in terms of security for the syslog protocol? [**1pt**]

What this implies in terms of security for the syslog protocol is that it helps analyst with sourcing out the problem or action a user has done on the network.

9. **Upload the generated syslog.txt with this document.** [**2pts**]

```
Tue Feb  4 12:21:12 2025;192.168.68.103; <46>Feb  4 04:21:12 ubuntu rsyslogd: [origin software="rsyslogd" swVersion="8.2312.0" x-pid="1904" x-info="https://www.rsyslog.com"] exiting on signal 15.

Tue Feb  4 12:21:12 2025;192.168.68.103; <30>Feb  4 04:21:12 ubuntu systemd[1]: rsyslog.service: Deactivated successfully.

Tue Feb  4 12:21:12 2025;192.168.68.103; <30>Feb  4 04:21:12 ubuntu systemd[1]: Stopped rsyslog.service - System Logging Service.
Tue Feb  4 12:21:12 2025;192.168.68.103; <30>Feb  4 04:21:12 ubuntu systemd[1]: Starting rsyslog.service -
System Logging Service...

Tue Feb  4 12:21:12 2025;192.168.68.103; <5>Feb  4 04:21:12 ubuntu kernel: audit: type=1400
audit(1738642872.421:73): apparmor="STATUS" operation="profile_replace" info="same as current profile,
skipping" profile="unconfined" name="rsyslogd" pid=5098 comm="apparmor_parser"

Tue Feb  4 12:21:12 2025;192.168.68.103; <46>Feb  4 04:21:12 ubuntu rsyslogd: imuxsock: Acquired UNIX
socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.2312.0]

Tue Feb  4 12:21:12 2025;192.168.68.103; <46>Feb  4 04:21:12 ubuntu rsyslogd: rsyslogd's groupid changed to
102

Tue Feb  4 12:21:12 2025;192.168.68.103; <30>Feb  4 04:21:12 ubuntu systemd[1]: Started rsyslog.service -
System Logging Service.

Tue Feb  4 12:21:12 2025;192.168.68.103; <46>Feb  4 04:21:12 ubuntu rsyslogd: rsyslogd's userid changed to
102

Tue Feb  4 12:21:12 2025;192.168.68.103; <46>Feb  4 04:21:12 ubuntu rsyslogd: [origin software="rsyslogd"
swVersion="8.2312.0" x-pid="5099" x-info="https://www.rsyslog.com"] start

Tue Feb  4 12:21:12 2025;192.168.68.103; <86>Feb  4 04:21:12 ubuntu sudo: pam_unix(sudo:session): session
closed for user root

Tue Feb  4 12:25:01 2025;192.168.68.103; <86>Feb  4 04:25:01 ubuntu CRON[5115]: pam_unix(cron:session):
session opened for user root(uid=0) by root(uid=0)

Tue Feb  4 12:25:01 2025;192.168.68.103; <78>Feb  4 04:25:01 ubuntu CRON[5116]: (root) CMD (command -v
debian-sa1 > /dev/null && debian-sa1 1 1)

Tue Feb  4 12:25:01 2025;192.168.68.103; <86>Feb  4 04:25:01 ubuntu CRON[5115]: pam_unix(cron:session):
session closed for user root

Tue Feb  4 12:27:01 2025;192.168.68.103; <30>Feb  4 04:27:02 ubuntu systemd[1]: Starting systemd-tmpfiles-
clean.service - Cleanup of Temporary Directories...

Tue Feb  4 12:27:02 2025;192.168.68.103; <30>Feb  4 04:27:02 ubuntu systemd[1]: systemd-tmpfiles-
clean.service: Deactivated successfully.

Tue Feb  4 12:27:02 2025;192.168.68.103; <30>Feb  4 04:27:02 ubuntu systemd[1]: Finished systemd-tmpfiles-
clean.service - Cleanup of Temporary Directories.

Tue Feb  4 12:30:01 2025;192.168.68.103; <30>Feb  4 04:30:02 ubuntu systemd[1]: Starting sysstat-
collect.service - system activity accounting tool...

Tue Feb  4 12:30:02 2025;192.168.68.103; <30>Feb  4 04:30:02 ubuntu systemd[1]: sysstat-collect.service:
Deactivated successfully.

Tue Feb  4 12:30:02 2025;192.168.68.103; <30>Feb  4 04:30:02 ubuntu systemd[1]: Finished sysstat-
collect.service - system activity accounting tool.
```