Best Current Practise

OCSBC – syslog configuration

Category: Informational

February 2024, Version 1.00

Revision History

Version	Author	Description of Changes	Date Revision Completed
1.00	Devon Thomas	Initial version	

Abstract

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

The configurations provided in this document SHOULD NOT be treated as RECOMMENDED. The information is intended to provide guidance as to the OCSBC behaviour when configurations present in this document is applied.

This document is intended to provide, the reader, with information regarding configuration of an OCSBC. The OCSBC will send system event information (as per RFC 3164) to remote syslog servers. Sending syslog events in SNMP traps, generating Intrusion Detection System Reporting system messages are outside the scope of this document.

Applicability

The details provided are relevant to physical & virtual Oracle Communications Session Border Controller (OCSBC) instances.

Contents

Figures

Tables

1. Network Functions

An AP3900 SBC (product setup: Oracle Enterprise SBC) was used to provide the CLI/GUI information, in this document.

2. Software

OCSBC s/w release nnSCZ920p3.bz

Oracle Linux 8.5, rsyslogd 8.2102.0-5.el8

3. Introduction

By default, OCSBCs stores system events in instances of file '/opt/logs/acmelog'. OCSBCs can also be configured to send these events to one or more remote syslog servers.

3.1. Test environment Overview

Figure 1 & Table 1 show:

1. The IP addresses used in the test environment.
2. The Linux servers represent 2 syslog server instances.
3. Syslog servers are in the same subnet as the OCSBC management interface. OCSBC's normally have their default-gateway configured to be the management interface's gateway. If this is not the case then 'host-route' instance(s) may be required to reach the remote server(s).

Figure 1 - Test setup

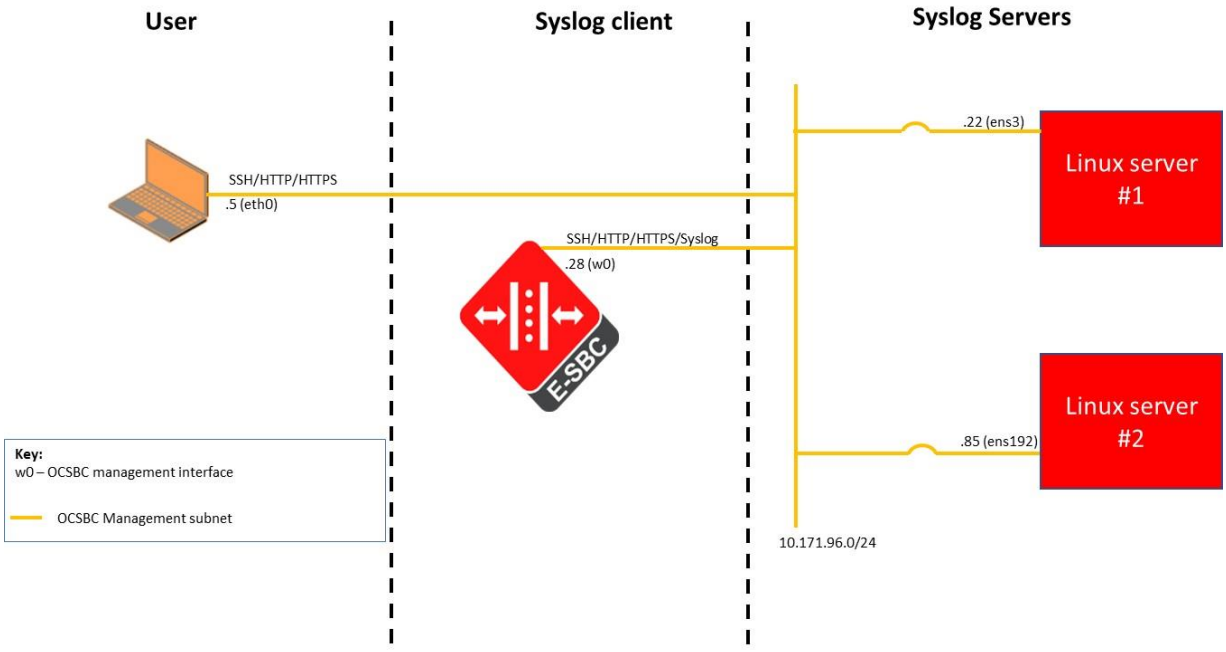


Table 1 - Syslog server instances

Linux Server number	Linux server IP address	OCSBC ingress/egress phy-interface for syslog
1	10.171.96.22	wancom0
2	10.171.96.85	wancom0

4. OCSBC configuration summary

This section provides details of the configuration elements necessary to send syslog messages to remote syslog servers. The OCSBC sends each system event to all configured syslog servers simultaneously. As per page 514 of Ref 1, it is RECOMMENDED that no more than 8 syslog servers should be configure. Appendix A contains the OCSBC configuration used in this document.

4.1. media-manager

This section shows media-manager parameters that are using their default values. The reason being features where syslog can be used, such as Intrusion Detection System (IDS) & Admin Security are outside the scope of this document. For brevity not all the media-manager parameters are shown below.

4.1.1. Configuration element – CLI View

```
media-manager
        state                                 enabled
        : (for brevity parameters have been removed)
        syslog-on-demote-to-deny              disabled
        syslog-on-demote-to-untrusted         disabled
        : (for brevity parameters have been removed)
        syslog-on-call-reject                 disabled
        : (for brevity parameters have been removed)
```

Note: 'syslog-on-call-reject' is not a parameter, linked to the IDS feature, but it remains disabled, since the reader is likely to use other products (such as OCOM/EOM, OCSDM …etc to be notified of call rejections.

Table 2, provides information concerning the configured parameters.

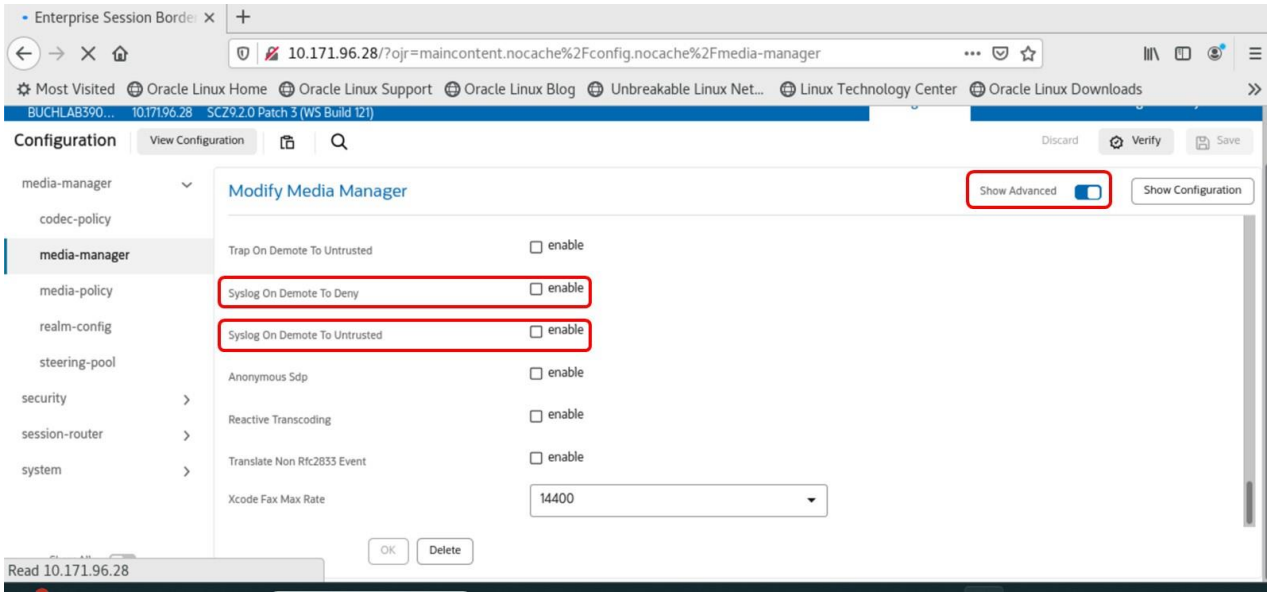
Table 2 – media-manager parameters

Parameter Name	Parameter Setting	Notes
media-manager>syslog-on-demote-to-deny	disabled	disable/enable send syslog message when a SIP client is demoted to deny.
media-manager>syslog-on-demote-to-untrusted	disabled	disable/enable send syslog message when a SIP client is demoted to untrusted.
media-manager>syslog-on-call-reject	disabled	disable/enable send syslog message when a SIP call is rejected.

4.1.2. Configuration element – GUI view

To see 'syslog-on-demote-to-deny' & 'syslog-on-demote-to-untrusted' parameters ensure that "Show Advanced" is enabled (as shown in Figure 2).

Figure 2 – media-manager element not immediately visible from GUI



4.2. system-config

The system-config element contains parameters necessary for the OCSBC to send system events to syslog servers.

4.2.1. Configuration element – CLI view

For brevity, some of the system-config parameters are not shown below.

```
system-config
        : (for brevity parameters have been removed)
        enable-snmp-syslog-notify               disabled
        : (for brevity parameters have been removed)
        snmp-syslog-his-table-length            1
        snmp-syslog-level                       WARNING
        syslog-server
                address                                 10.171.96.22
                port                                    514
                facility                                4
        syslog-server
                address                                 10.171.96.85
                port                                    514
                facility                                4
        system-log-level                        WARNING
        : (for brevity parameters have been removed)
        default-gateway                         0.0.0.0
        : (for brevity parameters have been removed)
        ids-syslog-facility                     -1
              :
```

Table 3 - system-config and system-config>syslog-server parameters

Parameter Name	Parameter Setting	Notes
system-config> enable-snmp-syslog-notify	disabled	Use default value, since OCSBC will not send system events in SNMP traps.
system-config> snmp-syslog-his-table-length	1	Parameter is not used by OCSBC, since 'enable-snmp-syslog-notify' is disabled.
system-config> snmp-syslog-level	WARNING	Parameter is not used by OCSBC, since 'enable-snmp-syslog-notify' is disabled.
system-config> syslog-server>address	10.171.96.22	IP address of syslog server.
system-config> syslog-server>port	514	UDP Port on which the syslog server listens for syslog messages.
system-config> syslog-server>facility	4	Use default facility code (i.e. value typically used for OCSBCs).
system-config> system-log-level	WARNING	System events of this severity level or higher (for a system event) are sent to the syslog server(s). See page 502 of Ref 1 for more details.
system-config>default-gateway	0.0.0.0	This is normally set to the IP address of the management interface's gateway.
system-config> ids-syslog-facility	-1	Left 'disabled' (i.e. Value left as '-1') since IDS feature is not used.

4.2.2. Configuration element – GUI view

Figure 3 to Figure 6 show the 'system-config' parameters linked to syslog. For brevity not all system-config parameters are shown.

Figure 3 - system-config pt1

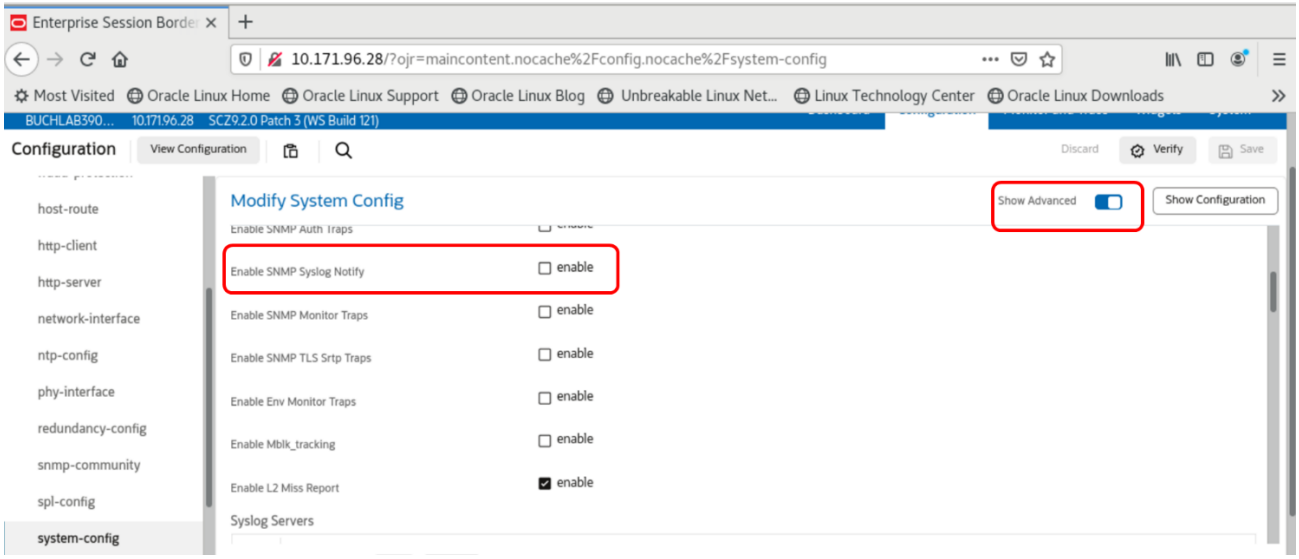


Figure 4 - system-config pt2

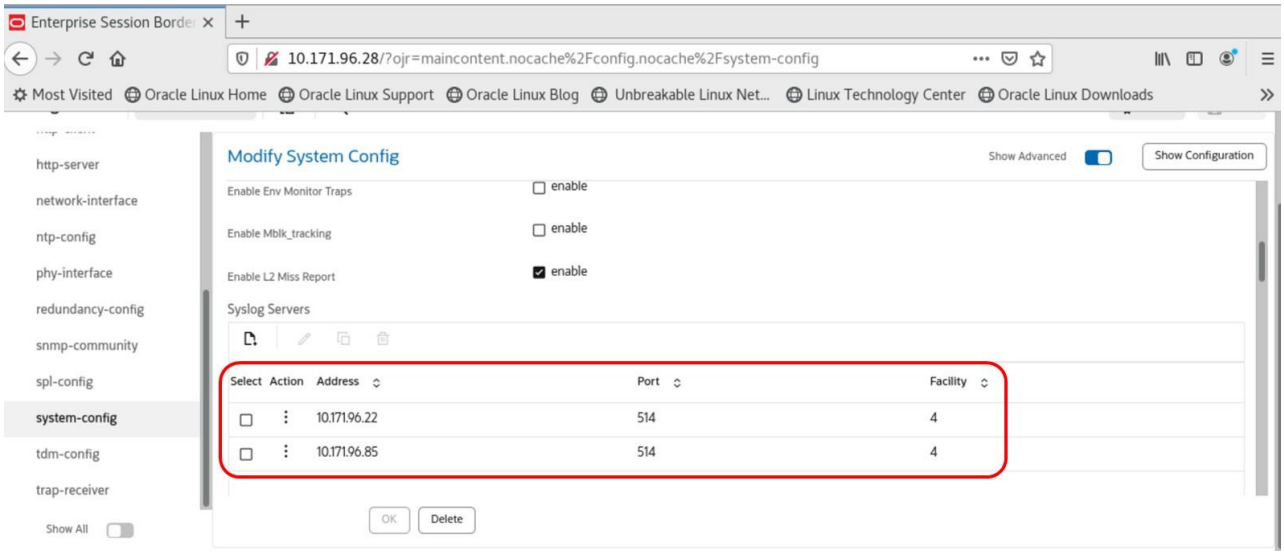


Figure 5 – system-config pt3

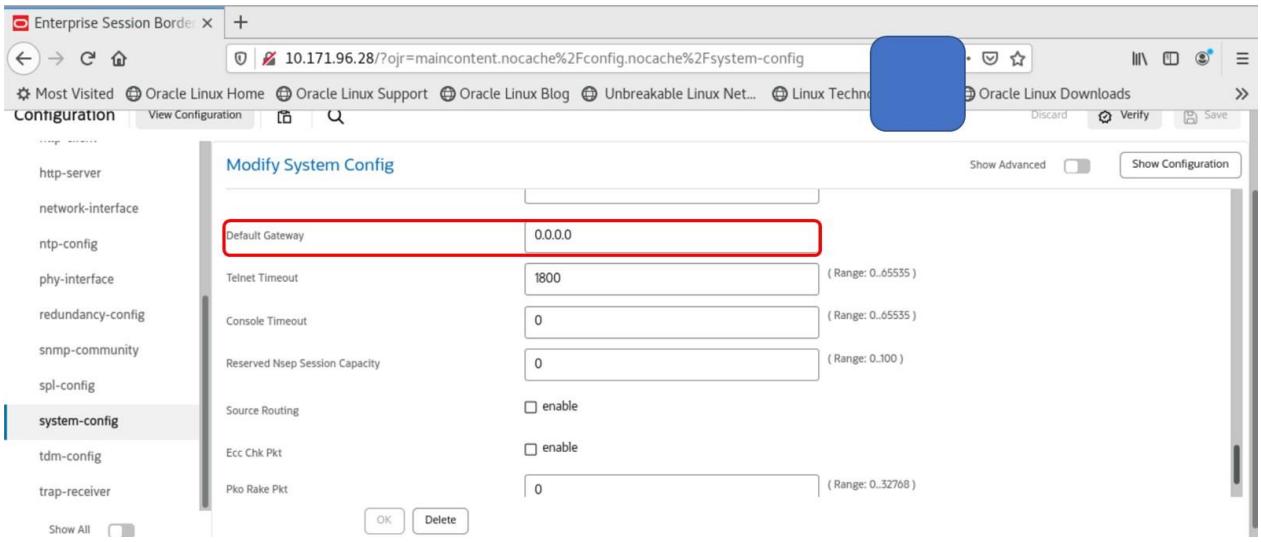
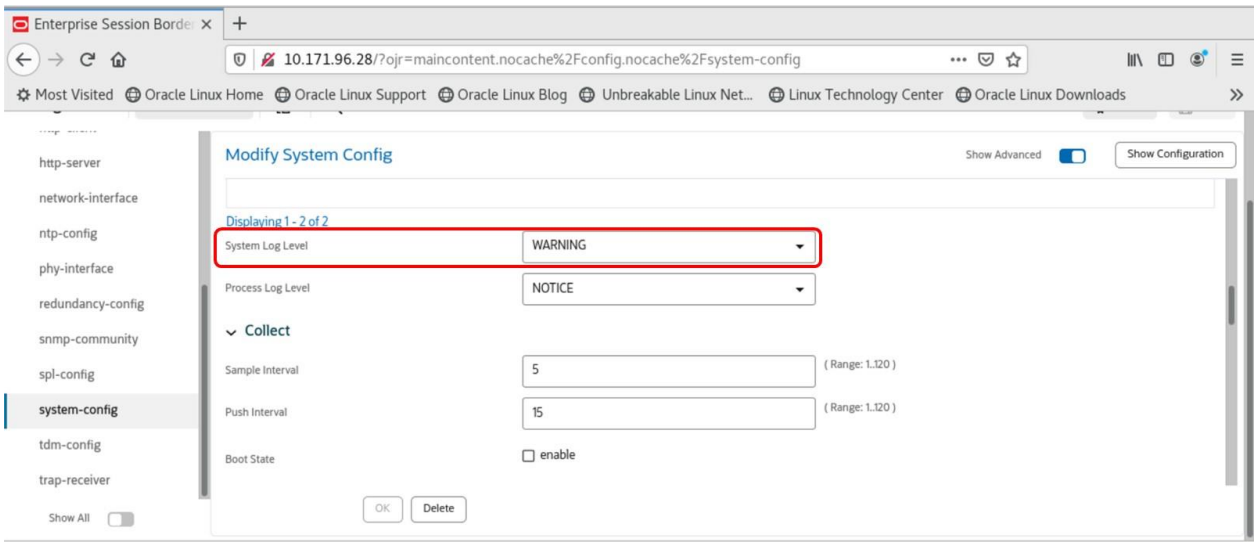


Figure 6 - system-config pt4



4.3. host-route (optional)

The OCSBC's default gateway is normally the management interface's gateway. If this is not the case then a host-route object MAY be required, to reach remote syslog server(s). The syslog servers, referred to in this document are in the same subnet as the OCSBC management interface. As a result, host-route instances are not part of the configuration in Appendix A.

4.3.1. Configuration element – CLI view

For reasons explained above, the instance below is not part of the configuration in Appendix A.

```
        dest-network                          192.168.0.100
        netmask                               255.255.255.0
        gateway                               10.171.96.1
        description                           Example host route to fictional
Syslog server
```

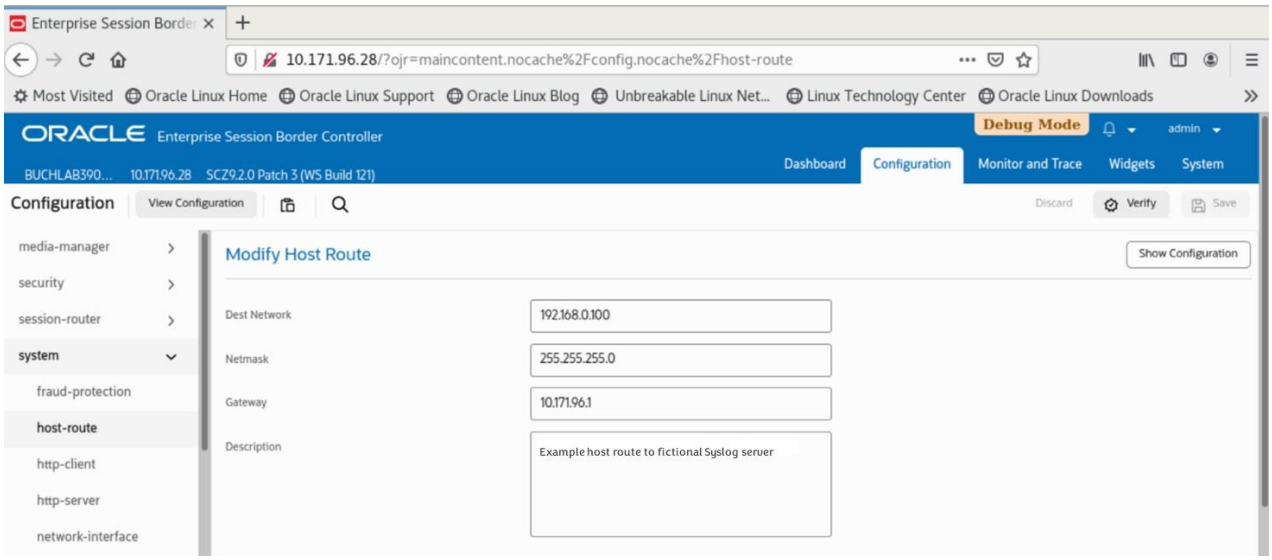
Table 4 - host-route parameters

Parameter Name	Parameter Setting	Notes
host-route>dest-network	192.168.0.100	IP/Subnet address of remote server
realm-config>network-interface	255.255.255.0	Netmask of destination IP/Subnet address
gateway	10.171.96.1	IP address of management interface's gateway. Necessary to the remote server

4.3.2. Configuration element – GUI view

Figure 7 shows the GUI view of the host-route configuration shown in section 4.3.1.

Figure 7 - Example - host-route element



5. OCSBC-Syslog Server Messages

This section's sub-sections provide information regarding the rsyslog config file and example syslog messages, sent by the OCSBC to the configured syslog servers.

5.1. Syslog Server – rsyslog.conf

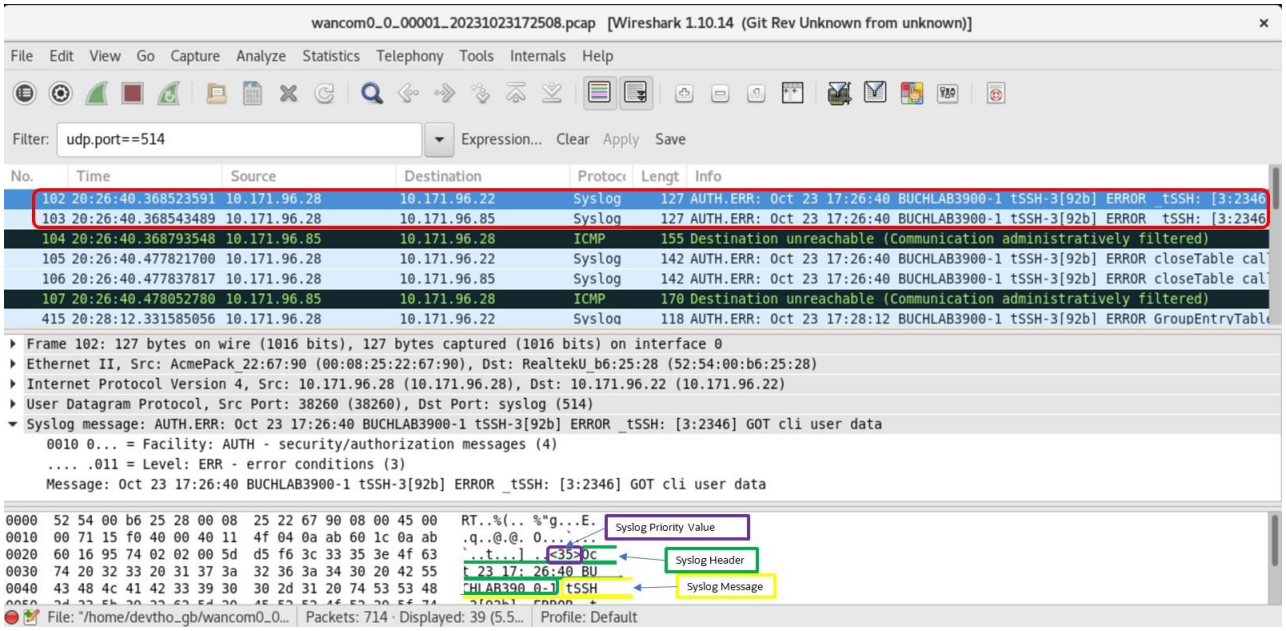
Below are details of a rsyslog configuration file on the Linux servers. With reference to this document, the rsyslog config file used was '/etc/rsyslog_buchlab.conf'. The differences between this file and the original 'rsyslog.conf' are highlighted in yellow.

```
# more /etc/rsyslog_buchlab.conf | awk '/^[^#]/ {print}'
module(load="imuxsock"       # provides support for local system logging (e.g. via
logger command)
       SysSock.Use="off") # Turn off message reception via local log socket;
                          # local messages are retrieved through imjournal now.
module(load="imjournal"        # provides access to the systemd journal
       StateFile="imjournal.state") # File to store the position in the journal
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")
global(workDirectory="/var/lib/rsyslog")
module(load="builtin:omfile" Template="RSYSLOG_TraditionalFileFormat")
include(file="/etc/rsyslog.d/*.conf" mode="optional")
*.info;mail.none;authpriv.none;cron.none                /var/log/messages
authpriv.*                                              /var/log/secure
mail.*                                                  -/var/log/maillog
cron.*                                                  /var/log/cron
*.emerg                                                 :omusrmsg:*
uucp,news.crit                                          /var/log/spooler
local7.*                                                /var/log/boot.log
#
```

5.2. Example syslog messages

Figure 8 shows OCSBC sending syslog messages to two syslog servers. Note, in Figure 8. there is less than 1msec between the messages highlighted by the red box. Also highlighted in Figure 8 are the 3 parts of the syslog layer (i.e. Priority value, Header & Message as described in RFC 3164).

Figure 8 - Example syslog messages



6. Appendix A - OCSBC 'show run short'

The CLI output (show below) is from ‘show running-config short’ command.

```
BUCHLAB3900-1# show run short
http-server
        name                                    wancom0-gui
media-manager
network-interface
        name                                    M00
        sub-port-id                             98
        ip-address                              10.171.98.28
        netmask                                 255.255.255.0
        gateway                                 10.171.98.2
        hip-ip-list                             10.171.98.28
        icmp-address                            10.171.98.28
network-interface
        name                                    M01
        ip-address                              10.171.99.28
        netmask                                 255.255.255.0
        gateway                                 10.171.99.2
        gw-heartbeat
                state                                   enabled
                heartbeat                               10
                retry-count                             3
                retry-timeout                           3
        hip-ip-list                             10.171.99.28
        icmp-address                            10.171.99.28
phy-interface
        name                                    M00
        operation-type                          Media
        duplex-mode
        speed
phy-interface
        name                                    M01
        operation-type                          Media
        port                                    1
        duplex-mode
        speed
system-config
        syslog-server
                address                                 10.171.96.22
        syslog-server
                address                                 10.171.96.85
        telnet-timeout                          1800
BUCHLAB3900-1#
```

7. References

Ref 1 - https://docs.oracle.com/en/industries/communications/session-border-controller/9.2.0/aclireference/acli-reference-guide.pdf