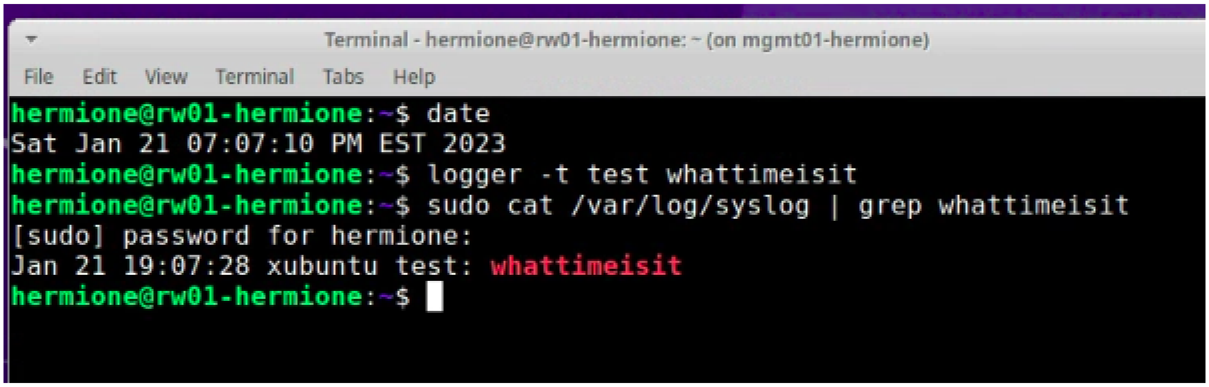
Updated Jan 21, 2023

Lab 2.1 Standardizing on Time

> 💡Time is not recorded consistently across all of our systems. You will note very quickly that none of your systems record the timezone within the syslog entry. Without this data it is very hard to develop a cohesive timeline for events that span multiple log sources and multiple time zones. We are going to fix this.

RW01

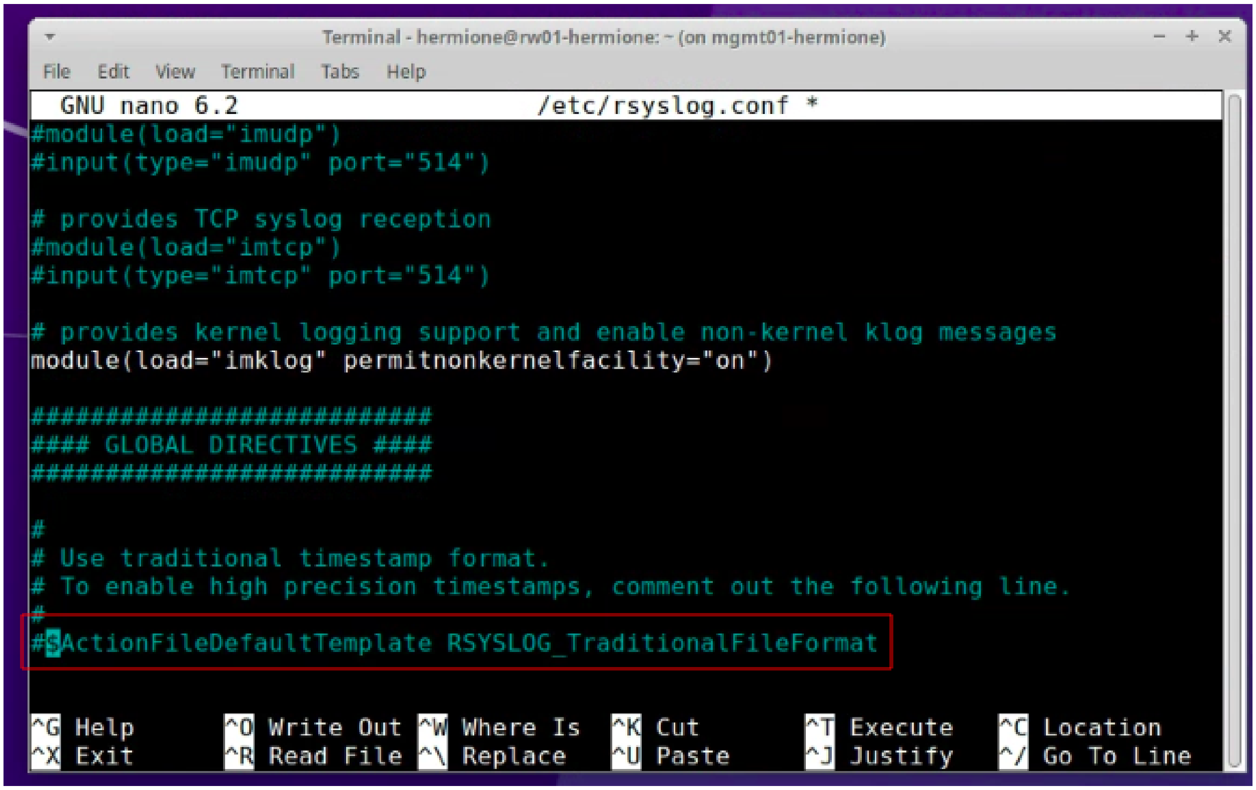
The following screenshot demonstrates what we are talking about. Though the date is set for EST, the specific log entry that may or may not be forwarded to a log server has no indication of the timezone or the year.


Terminal - hermione@rw01-hermione: ~ (on mgmt01-hermione)
File Edit View Terminal Tabs Help

```
hermione@rw01-hermione:~$ date
Sat Jan 21 07:07:10 PM EST 2023
hermione@rw01-hermione:~$ logger -t test whattimeisit
hermione@rw01-hermione:~$ sudo cat /var/log/syslog | grep whattimeisit
[sudo] password for hermione:
Jan 21 19:07:28 xubuntu test: whattimeisit
hermione@rw01-hermione:~$
```

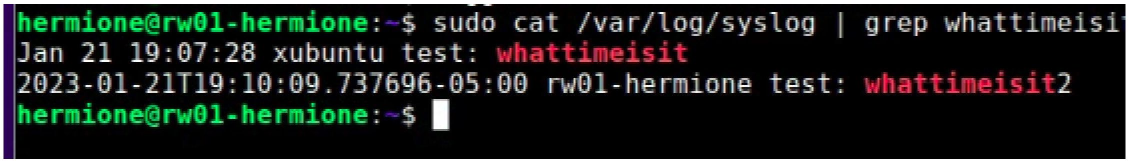
We fix this by hunting down and commenting out the line shown below in RW01's main rsyslog.conf file. We then restart the service.

Updated Jan 21, 2023


Terminal - hermione@rw01-hermione: ~ (on mgmt01-hermione)
File Edit View Terminal Tabs Help

```
  GNU nano 6.2                        /etc/rsyslog.conf *
#module(load="imudp")
#input(type="imudp" port="514")

# provides 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


^G Help         ^O Write Out  ^W Where Is  ^K Cut         ^T Execute    ^C Location
^X Exit         ^R Read File  ^\ Replace   ^U Paste       ^J Justify    ^/ Go To Line
```

`Deliverable 1.  Provide a screenshot similar to the one below that shows increased fidelity as well as timezone/offset information on rw01.`



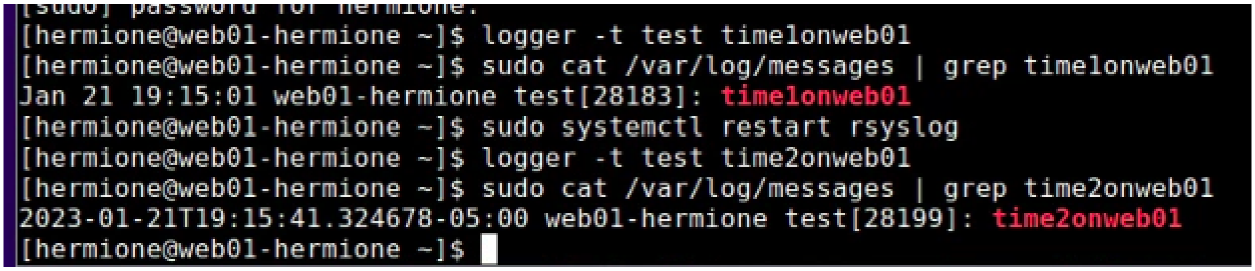
```
hermione@rw01-hermione:~$ sudo cat /var/log/syslog | grep whattimeisi
Jan 21 19:07:28 xubuntu test: whattimeisit
2023-01-21T19:10:09.737696-05:00 rw01-hermione test: whattimeisit2
hermione@rw01-hermione:~$ 
```

💡VyOS's syslog options are rather crude but it does indeed log the local timezone which by default is UTC, let's consider vyos taken care of. Later in the semester we may consider some hackery on vyos to get it to log just the way we want to. We are still missing the year, but that can be handled on the remote syslog or siem server.

Updated Jan 21, 2023

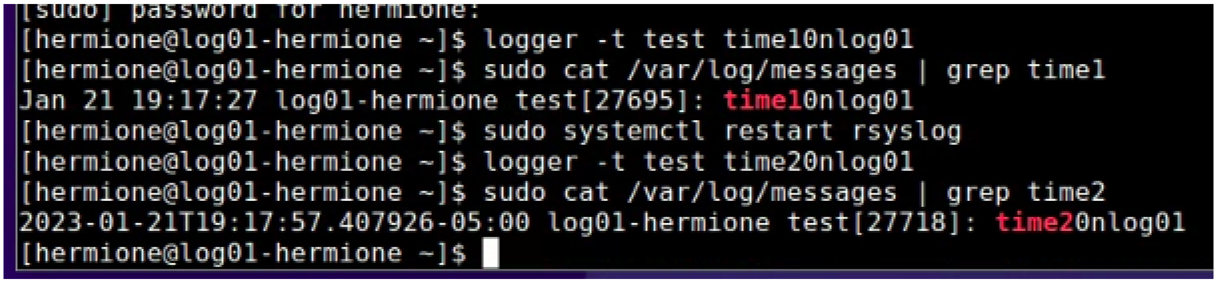
Apply change to web01 and log01

Deliverable 2. Provide a screenshot similar to the one below that shows increased fidelity as well as timezone/offset information for web01. The rsyslog.conf line to comment might look slightly different than rw01.



```
[sudo] password for hermione:
[hermione@web01-hermione ~]$ logger -t test time1onweb01
[hermione@web01-hermione ~]$ sudo cat /var/log/messages | grep time1onweb01
Jan 21 19:15:01 web01-hermione test[28183]: time1onweb01
[hermione@web01-hermione ~]$ sudo systemctl restart rsyslog
[hermione@web01-hermione ~]$ logger -t test time2onweb01
[hermione@web01-hermione ~]$ sudo cat /var/log/messages | grep time2onweb01
2023-01-21T19:15:41.324678-05:00 web01-hermione test[28199]: time2onweb01
[hermione@web01-hermione ~]$
```

Deliverable 3. Provide a screenshot similar to the one below that shows increased fidelity as well as timezone/offset information for log01.



```
[sudo] password for hermione:
[hermione@log01-hermione ~]$ logger -t test time10nlog01
[hermione@log01-hermione ~]$ sudo cat /var/log/messages | grep time1
Jan 21 19:17:27 log01-hermione test[27695]: time10nlog01
[hermione@log01-hermione ~]$ sudo systemctl restart rsyslog
[hermione@log01-hermione ~]$ logger -t test time20nlog01
[hermione@log01-hermione ~]$ sudo cat /var/log/messages | grep time2
2023-01-21T19:17:57.407926-05:00 log01-hermione test[27718]: time20nlog01
[hermione@log01-hermione ~]$
```

Deliverable 4. Create a Tech Journal page on time settings for various operating system logs, you can start with ubuntu and rocky linux. How do you enhance the logs so that time stamp information is captured? Provide a link.