Syslog

Local syslog
Procedure:
This command displays all the currently stored log messages. All the latest processes and corresponding transactions are stored in the "syslog" file. This file is saved in the path /var/log and can be viewed by giving the command sudo cat syslog as this requires root login.

```
admin@sonic:~$ show logging
```

Optionally, you can follow the log live as entries are written to it by specifying the -f or --follow flag

```
admin@sonic:~$ show logging --follow
```

Send out syslog to remote syslog server
Topology:
mceclip0.png

Pre-configuration:
Make sure switch IP address and connectivity works well. (refer to [Edgecore SONiC] Management and front port IPv4/IPv6 Address)
Procedure :
Step 1. Add the remote syslog

```
admin@sonic:~$ sudo config syslog add 192.168.1.1
Syslog server 188.188.99.10 added to configuration
Restarting rsyslog-config service...
```

To specify the use of the management VRF, please include the '-r' or '--vrf' option

```
admin@sonic:~$ sudo config syslog add 192.168.1.1 -r mgmt
```

Adjust severity level for remote syslog server
Topology:
mceclip0.png

Pre-configuration:
Make sure switch IP address and connectivity works well. (refer to [Edgecore SONiC] Management and front port IPv4/IPv6 Address)
Remote syslog server can get switch's syslog(refer to Send out syslog to remote syslog server)
Procedure:
Step 1. Edit the file /usr/share/sonic/templates/rsyslog.conf.j2

Warning and below. (Level 0 ~ 4)

```
admin@sonic:~$ sudo vi /usr/share/sonic/templates/rsyslog.conf.j2
{% for server in SYSLOG_SERVER %}
*.warning @{{ server }}:514;SONiCFileFormat
{% endfor %}
```

The 202111 branch contains some modifications. You should apply the changes before 'action'(as in version 202111.0).

Send with using management VRF

```
*.warning action(type="omfwd" target="{{server}}" port="514" protocol="udp"
Template="SONiCFileFormat_RFC3164" Device="eth0")
```

Send without using management VRF

```
*.warning @[{{ server }}]:514;SONiCFileFormat_RFC3164
```

Only warning level. (Only Level 4)

```
admin@sonic:~$ sudo vi /usr/share/sonic/templates/rsyslog.conf.j2
```

```
{% for server in SYSLOG_SERVER %}
*.=warning @{{ server }}:514;SONiCFileFormat
{% endfor %}
```

All severity levels except warning. (Level 0 ~ 7 except Level 4)

```
admin@sonic:~$ sudo vi /usr/share/sonic/templates/rsyslog.conf.j2
{% for server in SYSLOG_SERVER %}
*.debug;*.!=warning @{{ server }}:514;SONiCFileFormat
{% endfor %}
```

Note:

Here's the Severity level by the standard.

Value	Severity	Keyword
0	Emergency	emerg
1	Alert	alert
2	Critical	crit
3	Error	err
4	Warning	warning
5	Notice	notice
6	Informational	info
7	Debug	debug

Step 2: Restart syslog service

```
admin@sonic:~$ sudo systemctl restart rsyslog-config
```

Frequently Asked Question

How to prevent a lot of LLDP logs in syslog.

Tested model & firmware version:

Switch model name:
DCS204 (AS7726-32X)

Edgecore SONiC version:
202012.4

Problem description:

There are a lot of log LLDP logs in syslog.

mceclip0.png

Solution:

Users could separate the LLDP log from "/var/log/syslog" to "/var/log/lldp.log".

Step 1: Please add the configuration in "/etc/rsyslog.d/00-sonic.conf".

```
## LLDP rules
if $programname contains "lldp#" then {
   /var/log/lldp.log
   stop
}
```

Step 2: Reboot the switch to activate the setting.

Result:

mceclip1.png