How To Manage Logging Across Many Systems

Ken Eshelby
ken@opennms.com

Logging for Systems Management

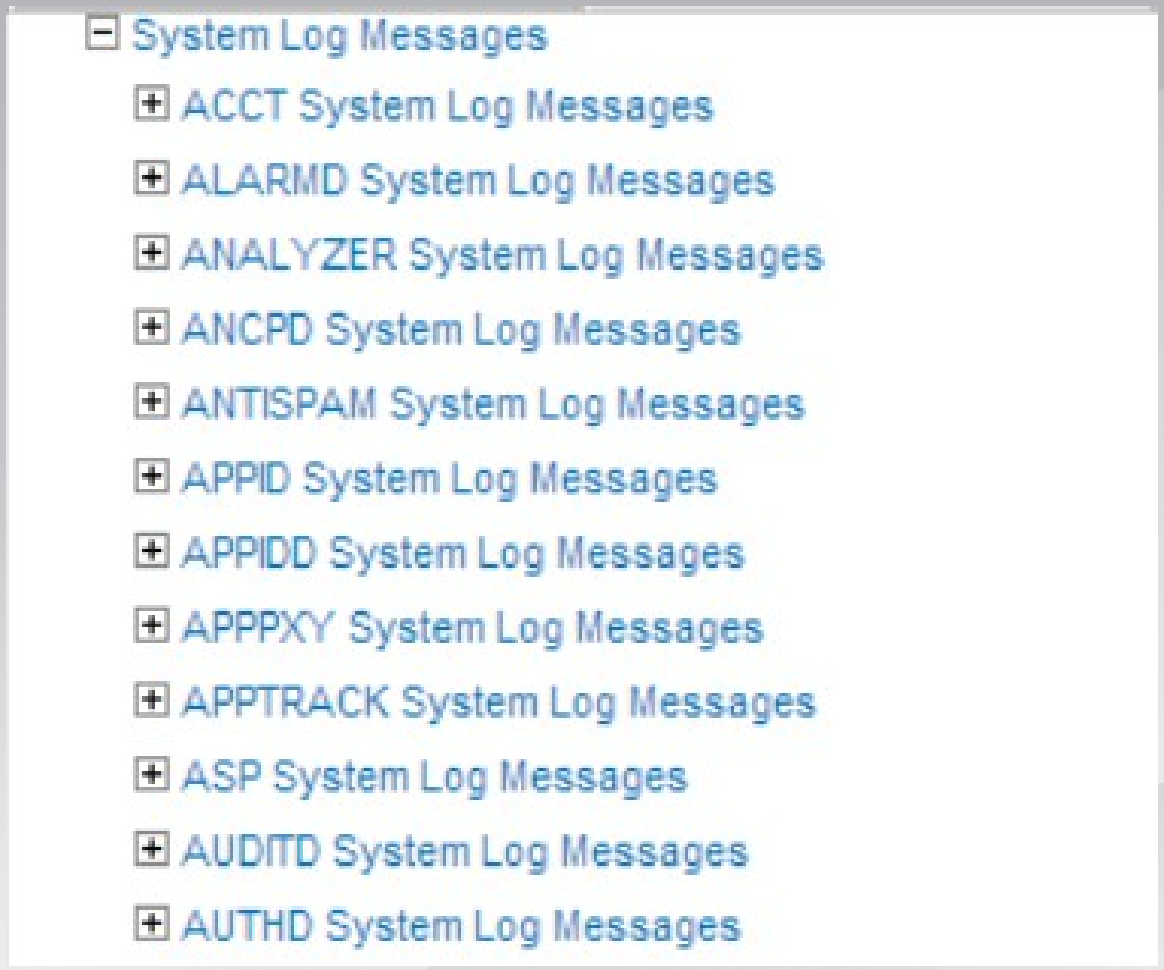
- Huge variety of detailed messages
- Detection of minor component failure
- Sometimes the only indication of an issue

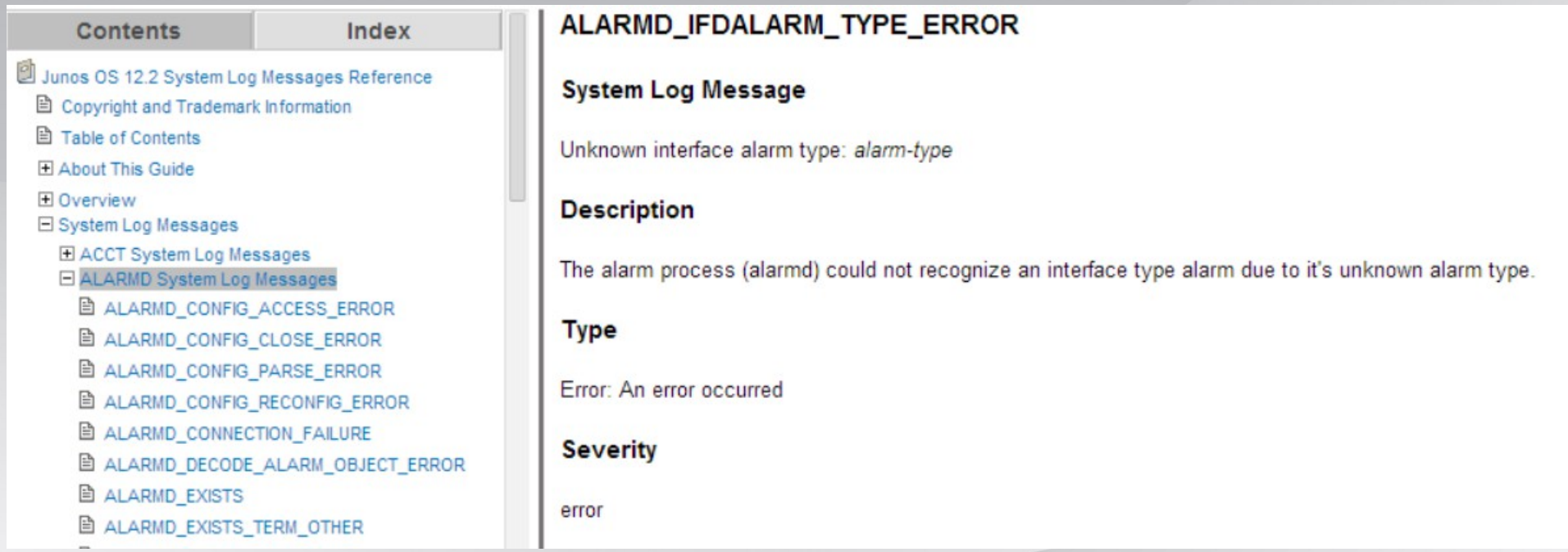
Logging gets development priority

“Cat6500 IOS 12.2(18)SXF contains about 90 SNMP traps, but has over 6000 syslog event messages.” -Clayton Dukes

JunOS 12.2

- Defined trap events in OpenNMS = 199
- Syslog messages starting with “A” = 197

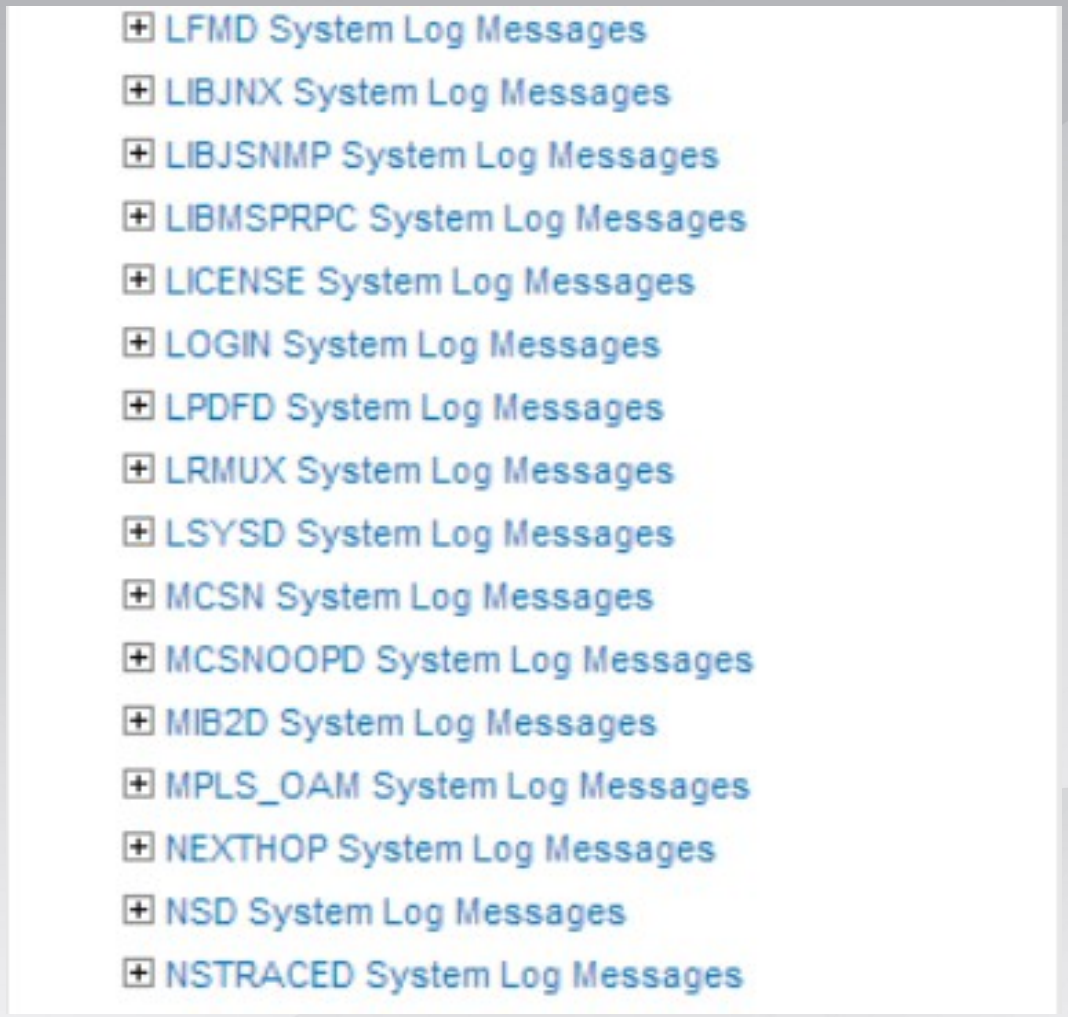

System Log Messages
ACCT System Log Messages
ALARMD System Log Messages
ANALYZER System Log Messages
ANCPD System Log Messages
ANTISPAM System Log Messages
APPID System Log Messages
APPIDD System Log Messages
APPPXY System Log Messages
APPTRACK System Log Messages
ASP System Log Messages
AUDITD System Log Messages
AUTHD System Log Messages


Contents
Index
Junos OS 12.2 System Log Messages Reference
Copyright and Trademark Information
Table of Contents
About This Guide
Overview
System Log Messages
ACCT System Log Messages
ALARMD System Log Messages
ALARMD_CONFIG_ACCESS_ERROR
ALARMD_CONFIG_CLOSE_ERROR
ALARMD_CONFIG_PARSE_ERROR
ALARMD_CONFIG_RECONFIG_ERROR
ALARMD_CONNECTION_FAILURE
ALARMD_DECODE_ALARM_OBJECT_ERROR
ALARMD_EXISTS
ALARMD_EXISTS_TERM_OTHER
ALARMD_IFDALARM_TYPE_ERROR
System Log Message
Unknown interface alarm type: alarm-type
Description
The alarm process (alarmd) could not recognize an interface type alarm due to it's unknown alarm type.
Type
Error: An error occurred
Severity
error

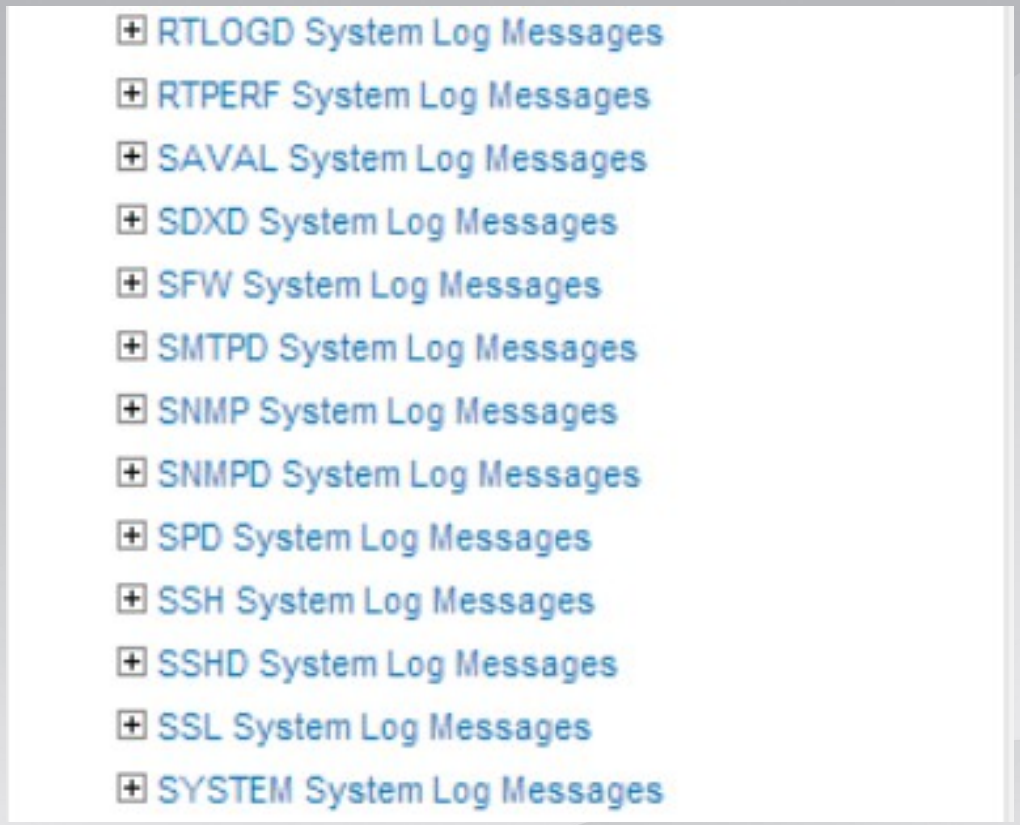
- AUTOCONFD System Log Messages
- AUTOD System Log Messages
- AV System Log Messages
- BFDD System Log Messages
- BOOTPD System Log Messages
- CFMD System Log Messages
- CHASSISD System Log Messages
- CHASSISM System Log Messages
- COSD System Log Messages
- DCBX System Log Messages
- DCD System Log Messages
- DDOS System Log Messages
- DFCD System Log Messages
- DFWD System Log Messages
- DHCPD System Log Messages

- DOT1XD System Log Messages
- DYNAMIC System Log Messages
- ESWD System Log Messages
- EVENTD System Log Messages
- FABOAMD System Log Messages
- FC System Log Messages
- FCOE System Log Messages
- FIP System Log Messages
- FIPS System Log Messages
- FLOW System Log Messages
- FPCLOGIN System Log Messages
- FSAD System Log Messages
- FUD System Log Messages
- FWAUTH System Log Messages
- GPRSD System Log Messages
- HNCACHED System Log Messages

- ICCPD System Log Messages
- IDP System Log Messages
- JADE System Log Messages
- JCS System Log Messages
- JDIAMETERD System Log Messages
- JIVED System Log Messages
- JPTSPD System Log Messages
- JSRPD System Log Messages
- JTASK System Log Messages
- JTRACE System Log Messages
- KMD System Log Messages
- L2ALD System Log Messages
- L2CPD System Log Messages
- L2TPD System Log Messages
- LACP System Log Messages
- LACPD System Log Messages


LFMD System Log Messages
LIBJNX System Log Messages
LIBJSNMP System Log Messages
LIBMSPRPC System Log Messages
LICENSE System Log Messages
LOGIN System Log Messages
LPDFD System Log Messages
LRMUX System Log Messages
LSYSD System Log Messages
MCSN System Log Messages
MCSNOOPD System Log Messages
MIB2D System Log Messages
MPLS_OAM System Log Messages
NEXTHOP System Log Messages
NSD System Log Messages
NSTRACED System Log Messages

- NTPDATE System Log Messages
- NTPD System Log Messages
- PARSE System Log Messages
- PFE System Log Messages
- PFED System Log Messages
- PGCPD System Log Messages
- PING System Log Messages
- PKID System Log Messages
- PPMD System Log Messages
- PPPD System Log Messages
- PROFILER System Log Messages
- RDD System Log Messages
- RMOPD System Log Messages
- RPD System Log Messages
- RT System Log Messages


RTLOGD System Log Messages
RTPERF System Log Messages
SAVAL System Log Messages
SDXD System Log Messages
SFW System Log Messages
SMTPD System Log Messages
SNMP System Log Messages
SNMPD System Log Messages
SPD System Log Messages
SSH System Log Messages
SSHD System Log Messages
SSL System Log Messages
SYSTEM System Log Messages

- TFTPD System Log Messages
- UFDD System Log Messages
- UI System Log Messages
- UTMD System Log Messages
- VCCPD System Log Messages
- VM System Log Messages
- VRRPD System Log Messages
- WEB System Log Messages
- WEBFILTER System Log Messages

This matters because you may not know that pieces of your system are degraded or failing!

What is Syslog?

- Client/Server messaging protocol
- Standardized message format
- Broadly adopted
- Simple configuration

Message elements

- Timestamp
- Facility
- Host
- Severity
- Message

Timestamp

Configure and use reliable NTP service throughout your network.

Troubleshooting issues across many nodes without reliable timestamps becomes very confusing!

pool.ntp.org

Note on facility

Facilities are required but not strictly organized.

This makes facilities useful as categories to route or parse messages.

Severity

- 0 – Emergency
- 1 – Alert
- 2 – Critical
- 3 – Error
- 4 – Warning
- 5 – Notice
- 6 – Informational
- 7 – Debug

Severity is interpreted by vendors differently. Use classification by severity levels with caution.

We are usually interested in severity levels 0-6. Debug level messages should to go log repositories.

Centralized loghost

- rsyslog or syslog-ng for Linux
- Organize by hardware type or vendor
- Use format controls or templates to make messages uniform. Parsing is coming...
- Copy messages to a single log file for troubleshooting

Configure your systems

(Cisco)

- service timestamps log datetime localtime show-timezone
- logging source-interface Loopback0
- logging host 10.255.0.10
- logging trap informational
- logging facility local5
- ntp server 10.0.10.10

Process and correlate messages

- newlogcheck.sh
- http://www.campin.net/newlogcheck.html
  - (https://web.archive.org/web/20111229162722/http://www.campin.net/newlogcheck.html)
- logtail from logcheck package
- pkgs.org for dependencies

Become friends with Regular Expressions

- Or become friends with an online regex evaluator
- http://regexpal.com/
- http://www.regexr.com/ (very nice)

The realities of parsing

```
# let's sanity check the message, as some
# syslog-ng messages don't have the proper format
## comment out this if block if everything gets clumped as
## "badly_formatted_logs" output
if ( $_ !~ /^[A-Z][a-z]{2}\s+\d{1,2}\s+\d{2}:\d{2}:\d{2}\s+\w+/ ) {
open(JUNK, ">> $LOGCHECK_DIR/tmp/hosts/badly_formatted_logs");
print JUNK "$_";
next SCAN;
}

@msg = split(/[ ]+/);    # split it for easy parsing
$month = $msg[0];
$day = $msg[1];
$hostname = $msg[3];     # get the hostname
$message = "";           # null out the log message variable

for( $i = 3 ; $i <= $#msg ; $i++ ){
        # put everything from the hostname till
        # the end of the log message into the KEY
       $message .= $msg[$i] . " "; # with a space in there
}
chop $message;           # get rid of the trailing space
$message =~ s/ \d+://; # get rid of the [PID], or no messages will ever match
# trim date/time
# looks like: Mar 3 21:52:29.278 pst: %ILPOWER-5-IEEE_DISCONNECT: Interface Fa1/0/44: PD removed
$message =~ s/ \./ /;
$message =~ s/ \*/ /;
$message =~ s/ \w+//;
$message =~ s/ \d+//;
$message =~ s/ \S+//;
$message =~ s/ \w+://;
```

Strip elements that create unique messages

```
# strip dest port from TCP-6-BADAUTH messages
$message =~ s/\%TCP-6-BADAUTH: No MD5 digest from (\S+) to (\S+)\(\d+\)/\%TCP-6-BADAUTH: No MD5 digest from \1 to \2/;
$message =~ s/Phyport (\S+) count=\d+/Phyport \1/;

# strip ACL violation high ports and packet count
$message =~ s/denied tcp (\d+.\d+.\d+.\d+)\S+ -> (\S+), .*/denied tcp \1 -> \2/;
$message =~ s/denied icmp (\S+) \((.*)\) -> (\S+) (\S+), .*/denied icmp \1 \(\2\) -> \3 \4/;
$message =~ s/denied udp (\d+.\d+.\d+.\d+)\S+ \((.*)\) -> (\S+), .*/denied udp \1 \(\2\) -> \3/;
$message =~ s/denied udp (\S+) -> (\S+), .*/denied udp \1 -> \2/;
$message =~ s/denied tcp (\d+.\d+.\d+.\d+)\S+ \((.*)\) -> (\S+), .*/denied tcp \1 \(\2\) -> \3/;
$message =~ s/permitted tcp (\S+) -> (\S+), .*/permitted tcp \1 -> \2/;
$message =~ s/logging rate-limited .*/logging rate-limited/;

##########################################
# here's the spot to strip unwanted junk #
#   to make more matches                 #
##########################################
$message =~ s/qmail: [\d\w]+\.[\d\w]+/qmail: /;                 # strip the qmail msg id
$message =~ s/sendmail:\s+[\d\w]+:/sendmail: /;                 # strip the sendmail msg id
$message =~ s/sendmail:\s+[\d\w]+:\s+[\d\w]+:/sendmail: /;      # strip the sendmail msg id


# trim down named "denied update" messages like this one:
#   ns1 named: [ID 295310 daemon.notice] denied update from +[206.221.195.214].2649 for "hotwired.com"
$message =~ s/(named:)\s+\[ID \d+ daemon.notice\] (denied update from \[\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}])\.\d+/$1 $2/;
```

One of many resulting reports

```
BEGIN REPORT


Jul 9 - 16 times(s): lgr-reg5eqprm-s1 %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet3
/0/19 (21), with Region5_Portable_2950 FastEthernet0/12 (1).
Jul 9 - 16 times(s): lgr-reg5eqprm-s1 %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet3
/0/19 (21), with Region5_Portable_2950 FastEthernet0/12 (1). (LGR-REG5EQPRM-S1-3)
Jul 9 - 161 times(s): lgr-reg5eqprm-s1 %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet
4/0/31 (21), with Region5_Portable_2950 FastEthernet0/1 (1).
Jul 9 - 162 times(s): lgr-reg5eqprm-s1 %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet
4/0/31 (21), with Region5_Portable_2950 FastEthernet0/1 (1). (LGR-REG5EQPRM-S1-4)

Jul 9 - 863 times(s): pdx-deq6th-s1 %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet1/0
/45 (61), with DEQHQ1.deq.state.or.us GigabitEthernet2/48 (60).

Jul 9 - 20 times(s): slm-reg2bb-s1 %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet3/0/
31 (20), with Switch FastEthernet0/1 (1).
Jul 9 - 20 times(s): slm-reg2bb-s1 %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet3/0/
31 (20), with Switch FastEthernet0/1 (1). (SLM-REG2BB-S1-3)
Jul 9 - 3 times(s): slm-reg2bb-s1 %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet1/0/1
6 (20), with Switch FastEthernet0/1 (1).
Jul 9 - 3 times(s): slm-reg2bb-s1 %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet1/0/1
8 (20), with Switch FastEthernet0/1 (1).
Jul 9 - 3 times(s): slm-reg2bb-s1 %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet3/0/1
9 (20), with Switch FastEthernet0/1 (1).
Jul 9 - 3 times(s): slm-reg2bb-s1 %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet3/0/1
9 (20), with Switch FastEthernet0/1 (1). (SLM-REG2BB-S1-3)
Jul 9 - 6 times(s): slm-reg2bb-s1 %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet1/0/2
5 (20), with Switch FastEthernet0/1 (1).
Jul 9 - 6 times(s): slm-reg2bb-s1 %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet1/0/2
7 (20), with Switch FastEthernet0/1 (1).
Jul 9 - 6 times(s): slm-reg2bb-s1 %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet3/0/3
0 (20), with Switch FastEthernet0/1 (1).
Jul 9 - 6 times(s): slm-reg2bb-s1 %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet3/0/3
0 (20), with Switch FastEthernet0/1 (1). (SLM-REG2BB-S1-3)

END OF REPORT
```

Criteria for useful messages

Is the event actionable?

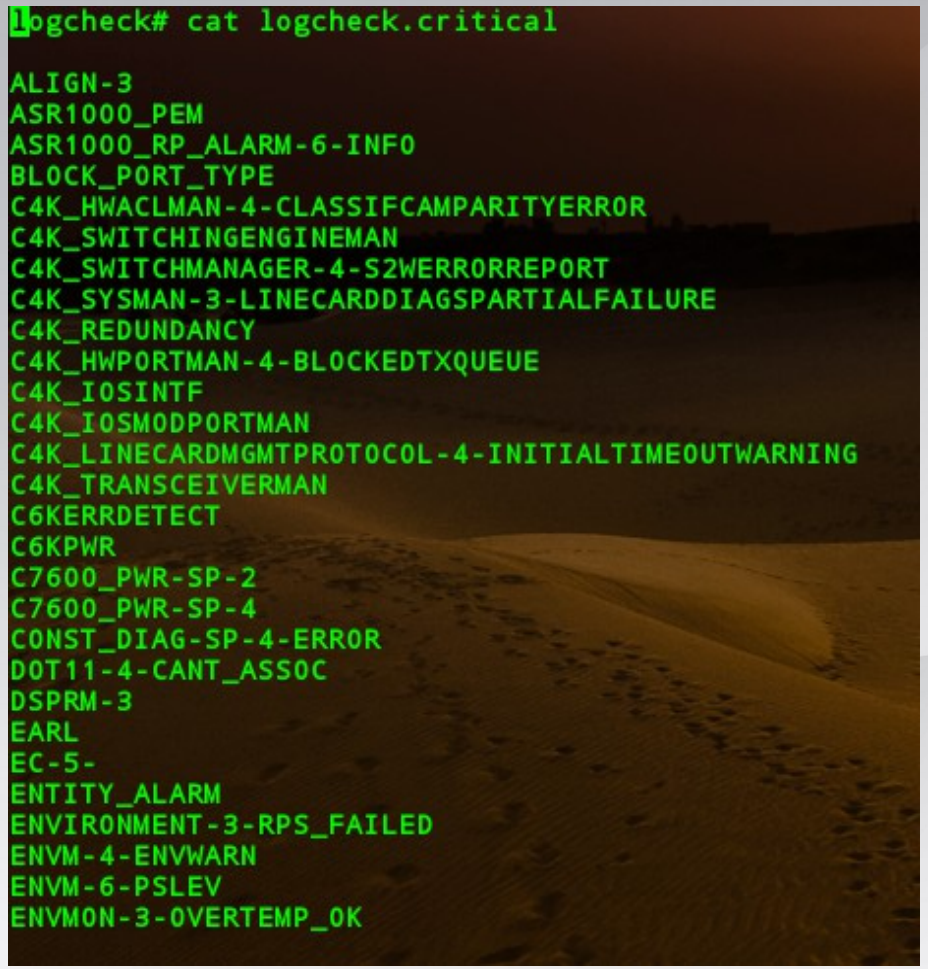
Is this a new type of event?

Many report types are possible

```
# If there are results, concatenate them to the final report

if [ "$CRITICAL" -eq 1 ]; then
        cat $TMPDIR/critreport.$$ >> $TMPDIR/criticalreport.$$
fi
if [ "$BGP" -eq 1 ]; then
        cat $TMPDIR/bgpreport.$$ >> $TMPDIR/bgpsummaryreport.$$
fi
if [ "$SECURITY" -eq 1 ]; then
        cat $TMPDIR/secreport.$$ >> $TMPDIR/securityreport.$$
fi
if [ "$FOUND" -eq 1 ]; then
        cat $TMPDIR/report.$$ >> $TMPDIR/finalreport.$$
fi
if [ "$ACL" -eq 1 ]; then
        cat $TMPDIR/aclreport.$$ >> $TMPDIR/accesslistreport.$$
fi
if [ "$VLAN" -eq 1 ]; then
        cat $TMPDIR/vlreport.$$ >> $TMPDIR/vlanreport.$$
fi
```

Driven by keywords



Resulting in syslogd filters

/etc/syslog-ng/syslog-ng.conf

```
filter f_opennms_critical {
        match("ALIGN-3") OR
        match("ASR1000_PEM") OR
        match("ASR1000_RP_ALARM-6-INFO");
};

log { source(src); filter(f_opennms_critical); destination(opennms); };

destination opennms { udp("10.0.0.1" port(514)); };
```

Review reports weekly

Why?

Interesting messages from failures may not appear for months or years.

Forward useful messages to a management system

OpenNMS...

- FOSS, AGPLv3 license
- Enterprise-level scaling
- Event-driven workflow
- Service monitoring, data collection, fault management
- much more...
- opennms.org/opennms.com

More parsing...

syslogd-configuration.xml

```
<syslogd-configuration>
    <configuration
            syslog-port="10514"
            new-suspect-on-message="false"
            parser="org.opennms.netmgt.syslogd.SyslogNGParser"
            forwarding-regexp="^(\S.+?) (\S.+?) (\S.+?) (\S.+?) (\S.+?)
                (\S.+?) (\S.+?) (\S.+?) (\S.+?) (\S.+?) (\S.+?) (\S.+?) (\S.*)"
            matching-group-host="4"
            matching-group-message="14"
            discard-uei="DISCARD-MATCHING-MESSAGES"
            />

    <import-file>syslog/Cisco.syslog.xml</import-file>

</syslogd-configuration>
```

Apply keywords

Cisco.syslog.xml

```
<ueiMatch>
    <match type="substr" expression="C6KPWR-SP-2-PSFAIL"/>
    <uei>state.or.us/sdc/C6KPWR-SP-2-PSFAIL</uei>
</ueiMatch>
<ueiMatch>
    <match type="substr" expression="C6KPWR-SP-4-PSOK"/>
    <uei>state.or.us/sdc/C6KPWR-SP-4-PSOK</uei>
</ueiMatch>
```

Identify event definition

Define alarm

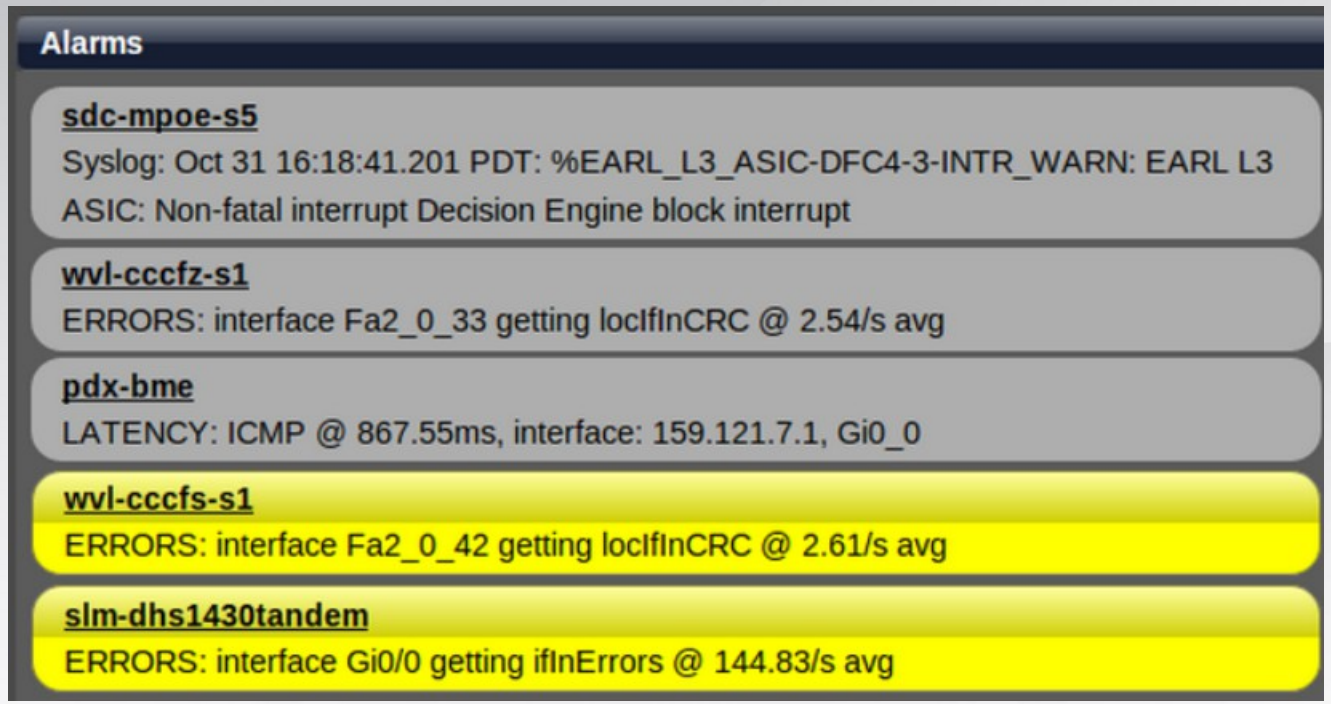
foo.events.xml

```
<event>
    <uei>state.or.us/sdc/C6KPWR-SP-2-PSFAIL</uei>
    <event-label>_State of Oregon: C6K System Power Supply Failure</event-label>
    <descr>A Cisco 6000 series platform power supply has failed. %parm[syslogmessage]% </descr>
    <logmsg dest="logndisplay">Power Supply Failure- %parm[syslogmessage]%</logmsg>
    <severity>Major</severity>
    <alarm-data reduction-key="%uei%:%nodeid%" alarm-type="1"/>
</event>
<event>
    <uei>state.or.us/sdc/C6KPWR-SP-4-PSOK</uei>
    <event-label>_State of Oregon: C6K System Power Supply OK</event-label>
    <descr>A Cisco 6000 series platform power supply is OK. %parm[syslogmessage]% </descr>
    <logmsg dest="logndisplay">Power Supply OK- %parm[syslogmessage]%</logmsg>
    <severity>Normal</severity>
    <alarm-data reduction-key="%uei%:%nodeid%" alarm-type="2" clear-key="state.or.us/sdc/C6KPWR-SP-2-PSFAIL:%nodeid%"/>
</event>
```

- Create human readable message
- Deduplicate messages
- Can be made auto-clearing

Outcomes

- Events for history
- Notifications for alerting
- Alarms for dashboard display



Ken Eshelby
ken@opennms.com