

Cisco Syslog Parser & Reporting Tool

PDX.pm

Nov 12, 2008

Gabrielle Roth

Cisco Syslog Parser & Reporting Tool

Cisco Syslog Parser & Reporting Tool

- SITTER
- Super Cisco Syslog Parser
- Cisco Syslog Sampler
- Cisco Syslog SomethingSomething

Cisco Syslog Parser & Reporting Tool

- SITTER
- Super Cisco Syslog Parser
- Cisco Syslog Sampler
- Cisco Syslog SomethingSomething

- SPARTAN - Syslog PARser, ReporTer and ANalyzer
- SPANKT - syslog parser and network knowledge tool
- SNARK - syslog network analysis reporting
... damn

Cisco Syslog Parser & Reporting Tool

- SITTER
- Super Cisco Syslog Parser
- Cisco Syslog Sampler
- Cisco Syslog SomethingSomething

- SPARTAN - Syslog PARser, ReporTer and ANalyzer
- SPANKT - syslog parser and network knowledge tool
- SNARK - syslog network analysis reporting
... damn

ACRONYM FAIL

Aug 23 03:14:17 zagging.demo.net 2201: Aug 23 04:14:16.128 EDT: %CONTROLLER-5-UPDOWN: Controller T1 3/1, changed state to down

Aug 23 03:14:17 zagreb.demo.net 9397: Aug 23 04:14:17.577 EDT: %LINK-3-UPDOWN: Interface Serial1/2:0, changed state to down

Aug 23 03:14:18 zagging.demo.net 2202: Aug 23 04:14:18.128 EDT: %LINK-3-UPDOWN: Interface Serial3/1:0, changed state to down

Aug 23 03:14:18 zagreb.demo.net 9398: Aug 23 04:14:17.577 EDT: %DUAL-5-NBRCHANGE: IP-EIGRP 666: Neighbor 10.1.5.181 (Serial1/2:0) is down: interface down

Aug 23 03:14:18 zagreb.demo.net 9399: Aug 23 04:14:18.577 EDT: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/2:0, changed state to down

Aug 23 03:14:19 zagging.demo.net 2203: Aug 23 04:14:18.128 EDT: %DUAL-5-NBRCHANGE: IP-EIGRP 666: Neighbor 10.1.5.182 (Serial3/1:0) is down: interface down

Aug 23 03:14:19 zagging.demo.net 2204: Aug 23 04:14:19.128 EDT: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1:0, changed state to down

Aug 23 03:14:34 zagreb.demo.net 9400: Aug 23 04:14:33.577 EDT: %CONTROLLER-5-UPDOWN: Controller T1 1/2, changed state to up

Aug 23 03:14:35 zagging.demo.net 2205: Aug 23 04:14:34.136 EDT: %CONTROLLER-5-UPDOWN: Controller T1 3/1, changed state to up

Aug 23 03:14:36 zagreb.demo.net 9401: Aug 23 04:14:35.577 EDT: %LINK-3-UPDOWN: Interface Serial1/2:0, changed state to up

Aug 23 03:14:36 zagreb.demo.net 9402: Aug 23 04:14:36.577 EDT: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/2:0, changed state to up

Aug 23 03:14:37 zagging.demo.net 2206: Aug 23 04:14:36.136 EDT: %LINK-3-UPDOWN: Interface Serial3/1:0, changed state to up

Aug 23 03:14:37 zagging.demo.net 2207: Aug 23 04:14:37.136 EDT: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1:0, changed state to up

Aug 23 03:38:02 zealot.demo.net 11371: Aug 23 03:38:01.952 CDT: %LINK-4-ERROR: FastEthernet0/21 is experiencing errors

Aug 23 03:38:04 zealous.demo.net 2008 Aug 23 01:37:57 PDT -07:00 %CDP-4-NVLANMISMATCH: Native vlan mismatch detected on port 2/18

Aug 23 03:38:05 zachary.demo.net 72130: SEC 7:5y8w: %MEM_ECC-3-BADADDR_SBE: Invalid SBE dram address: 0x638368C0 latched by ECC Ctrl

Aug 23 03:38:45 zebra.demo.net 2008 Aug 23 03:38:45 CDT -05:00 %MCAST-4-RX_LVRANGE: IGMP: Rcvd Leave in the range 01-00-5e-00-00-xx

Aug 23 03:38:45 zebra.demo.net last message repeated 1 time

Aug 24 19:45:39 zoom.demo.net 104042: Aug 24 17:45:38.882 PDT: %IP-3-LOOPPAK: Looping packet detected and dropped -

Aug 24 19:45:39 zoom.demo.net 104043: src=10.8.1.8, dst=10.7.7.8, hl=20, tl=357, prot=17, sport=67, dport=68

Aug 24 19:45:39 zoom.demo.net 104044: in=FastEthernet5/0, nexthop=10.1.0.1, out=POS1/1

Aug 24 19:45:39 zoom.demo.net 104045: options=none

Aug 24 19:50:42 zeiss.demo.net 2008 Aug 24 19:50:42 CDT -05:00 %SYS-4-P2_WARN: 1/Invalid traffic from multicast source address 65:8d:63:a2:c2:65 on port 2/49

Network Management Basics

...FCAPS

Config = what does this look like.

Config = what does this look like.

Performance = what is it doing.

Config = what does this look like.

Performance = what is it doing.

Fault = oh god what just happened.

Fault Management

Fault Management

- irate phone call

Fault Management

- irate phone call
- SNMP Traps

Fault Management

- irate phone call
- SNMP Traps
 - low-priority
 - trap handler (additional layer)
 - trap coverage
 - not that great for post-event analysis

Fault Management

- irate phone call
- SNMP Traps
 - low-priority
 - trap handler (additional layer)
 - trap coverage
 - not that great for post-event analysis
- syslog

It's a trivial matter to look through the logs
and find what you need.

It's a trivial matter to look through the logs
and find what you need.

...to whom?

- can be HYOOGE

- can be HYOOGE
- information overload/distractions

- can be HYOOGE
- information overload/distractions
- no idea what normal is

%LINK-3-UPDOWN: Interface Serial1/2:0, changed state to down

%LINK-3-UPDOWN: Interface Serial1/2:0, changed state to up

%LINK-3-UPDOWN: Interface Serial1/2:0, changed state to down

%LINK-3-UPDOWN: Interface Serial1/2:0, changed state to up

%RTD-1-ADDR_FLAP: FastEthernet0/11 relearning 80 addrs per min

%LINK-3-UPDOWN: Interface Serial1/2:0, changed state to down

%LINK-3-UPDOWN: Interface Serial1/2:0, changed state to up

%RTD-1-ADDR_FLAP: FastEthernet0/11 relearning 80 addrs per min

%CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port
4/13

%LINK-3-UPDOWN: Interface Serial1/2:0, changed state to down

%LINK-3-UPDOWN: Interface Serial1/2:0, changed state to up

%RTD-1-ADDR_FLAP: FastEthernet0/11 relearning 80 addrs per min

%CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port
4/13

%MEM_ECC-3-BADADDR_SBE: Invalid SBE dram address: 0x638368C0 latched
by ECC Ctrl

"What is the definition of a weed?"

"What is the definition of a weed?"

...anything I don't want growing in my yard.

"What is the definition of a weed?"

...anything I don't want growing in my yard.



The Problem:

Nobody has their finger on the pulse of the
logs.

The Problem:

Nobody has their finger on the pulse of the
logs.

The Solution:

Help them out!

The Problem:

Nobody has their finger on the pulse of the logs.

The Solution:

Help them out!

- perhaps a more meaningful format.

The Problem:

Nobody has their finger on the pulse of the logs.

The Solution:

Help them out!

- perhaps a more meaningful format.
- get a feel for what's "normal" (and define "normal")

The Problem:

Nobody has their finger on the pulse of the logs.

The Solution:

Help them out!

- perhaps a more meaningful format.
- get a feel for what's "normal" (and define "normal")
- reduce the amount of crap in the logs

The Problem:

Nobody has their finger on the pulse of the logs.

The Solution:

Help them out!

- perhaps a more meaningful format.
- get a feel for what's "normal" (and define "normal")
- reduce the amount of crap in the logs
- side effect: improve the users' experience



...I did it myyyyyy waaaaaaaay...

(<http://www.baconandtech.com/2008/11/10/quick-guide-ubuntu-box-as-syslog-server/>)

On the log host:

configure syslog:

/etc/syslog.conf:

local6.debug

/var/logs/cisco.log

(<http://www.baconandtech.com/2008/11/10/quick-guide-ubuntu-box-as-syslog-server/>)

On the log host:

configure syslog:

/etc/syslog.conf:

local6.debug /var/logs/cisco.log

*.err;local6.none /var/adm/messages

(<http://www.baconandtech.com/2008/11/10/quick-guide-ubuntu-box-as-syslog-server/>)

On the log host:

configure syslog:

/etc/syslog.conf:

local6.debug /var/logs/cisco.log

*.err;local6.none /var/adm/messages

touch new files; restart syslogd (kill -HUP [pid], pkill -1 syslogd, whatever)

(<http://www.baconandtech.com/2008/11/10/quick-guide-ubuntu-box-as-syslog-server/>)

On the log host:

configure syslog:

/etc/syslog.conf:

local6.debug /var/logs/cisco.log

*.err;local6.none /var/adm/messages

touch new files; restart syslogd (kill -HUP [pid], pkill -1 syslogd, whatever)

log rotation:

/etc/logadm.conf (Solaris)

/etc/logrotate.conf

(<http://www.baconandtech.com/2008/11/10/quick-guide-ubuntu-box-as-syslog-server/>)

On the log host:

configure syslog:

/etc/syslog.conf:

local6.debug /var/logs/cisco.log

*.err;local6.none /var/adm/messages

touch new files; restart syslogd (kill -HUP [pid], pkill -1 syslogd, whatever)

log rotation:

/etc/logadm.conf (Solaris)

/etc/logrotate.conf

test with logger:

(demo!)

(<http://www.baconandtech.com/2008/11/10/quick-guide-ubuntu-box-as-syslog-server/>)

On the log host:

configure syslog:

```
/etc/syslog.conf:
```

```
local6.debug
```

```
/var/logs/cisco.log
```

```
*.err;local6.none
```

```
/var/adm/messages
```

```
touch new files; restart syslogd
```

log rotation:

```
/etc/logadm.conf (Solaris)
```

```
/etc/logrotate.conf
```

test with logger:

(demo!)

logger is not my personal plaything. logger is not my personal
plaything. logger is not my personal plaything. logger is not
my personal plaything. logger is not my personal plaything.



The Cisco part...

```
config t
logging [ip_of_log_server]
logging facility [default is local7]
logging history [severity]
```

<0-7>	Logging severity level	
emergencies	System is unusable	(severity=0)
alerts	Immediate action needed	(severity=1)
critical	Critical conditions	(severity=2)
errors	Error conditions	(severity=3)
warnings	Warning conditions	(severity=4)
notifications	Normal but significant conditions	(severity=5)
informational	Informational messages	(severity=6) <--
debugging	Debugging messages	(severity=7)

Decisions...

```
Aug 24 19:45:39 zoom.demo.net 104042: Aug 24 17:45:38.882 PDT: %IP-3-LOOPPAK: Looping packet detected and dropped -
Aug 24 19:45:39 zoom.demo.net 104043: src=10.8.1.8, dst=10.7.7.8, hl=20, tl=357, prot=17, sport=67, dport=68
Aug 24 19:45:39 zoom.demo.net 104044: in=FastEthernet5/0, nexthop=10.1.0.1, out=POS1/1
Aug 24 19:45:39 zoom.demo.net 104045: options=none
Aug 24 19:47:51 zealand.demo.net 2008 Aug 24 19:47:48 CDT -05:00 %CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on
port 4/13
Aug 24 19:57:25 zagging.demo.net 2861: Aug 24 20:57:24.105 EDT: %CONTROLLER-5-UPDOWN: Controller T1 3/1, changed state to up
Aug 24 19:57:26 zagreb.demo.net 10057: Aug 24 20:57:25.931 EDT: %LINK-3-UPDOWN: Interface Serial1/2:0, changed state to up
Aug 24 19:57:26 zagreb.demo.net 10058: Aug 24 20:57:26.931 EDT: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/2:0,
changed state to up
Aug 24 19:57:27 zagging.demo.net 2862: Aug 24 20:57:26.105 EDT: %LINK-3-UPDOWN: Interface Serial3/1:0, changed state to up
Aug 24 19:57:28 zagging.demo.net 2863: Aug 24 20:57:27.085 EDT: %DUAL-5-NBRCHANGE: IP-EIGRP 666: Neighbor 10.1.1.82
(Serial3/1:0) is up: new adjacency
Aug 24 19:57:28 zagging.demo.net 2864: Aug 24 20:57:27.105 EDT: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1:0,
changed state to up
```

Decisions...

```
Aug 24 19:45:39 zoom.demo.net 104042: Aug 24 17:45:38.882 PDT: %IP-3-LOOPPAK: Looping packet detected and dropped -
Aug 24 19:45:39 zoom.demo.net 104043: src=10.8.1.8, dst=10.7.7.8, hl=20, tl=357, prot=17, sport=67, dport=68
Aug 24 19:45:39 zoom.demo.net 104044: in=FastEthernet5/0, nexthop=10.1.0.1, out=POS1/1
Aug 24 19:45:39 zoom.demo.net 104045: options=none
Aug 24 19:47:51 zealand.demo.net 2008 Aug 24 19:47:48 CDT -05:00 %CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on
port 4/13
Aug 24 19:57:25 zagging.demo.net 2861: Aug 24 20:57:24.105 EDT: %CONTROLLER-5-UPDOWN: Controller T1 3/1, changed state to up
Aug 24 19:57:26 zagreb.demo.net 10057: Aug 24 20:57:25.931 EDT: %LINK-3-UPDOWN: Interface Serial1/2:0, changed state to up
Aug 24 19:57:26 zagreb.demo.net 10058: Aug 24 20:57:26.931 EDT: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/2:0,
changed state to up
Aug 24 19:57:27 zagging.demo.net 2862: Aug 24 20:57:26.105 EDT: %LINK-3-UPDOWN: Interface Serial3/1:0, changed state to up
Aug 24 19:57:28 zagging.demo.net 2863: Aug 24 20:57:27.085 EDT: %DUAL-5-NBRCHANGE: IP-EIGRP 666: Neighbor 10.1.1.82
(Serial3/1:0) is up: new adjacency
Aug 24 19:57:28 zagging.demo.net 2864: Aug 24 20:57:27.105 EDT: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1:0,
changed state to up
```

- multiline messages

Decisions...

```
Aug 24 19:45:39 zoom.demo.net 104042: Aug 24 17:45:38.882 PDT: %IP-3-LOOPPAK: Looping packet detected and dropped -
Aug 24 19:45:39 zoom.demo.net 104043: src=10.8.1.8, dst=10.7.7.8, hl=20, tl=357, prot=17, sport=67, dport=68
Aug 24 19:45:39 zoom.demo.net 104044: in=FastEthernet5/0, nexthop=10.1.0.1, out=POS1/1
Aug 24 19:45:39 zoom.demo.net 104045: options=none
Aug 24 19:47:51 zealand.demo.net 2008 Aug 24 19:47:48 CDT -05:00 %CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on
port 4/13
Aug 24 19:57:25 zagging.demo.net 2861: Aug 24 20:57:24.105 EDT: %CONTROLLER-5-UPDOWN: Controller T1 3/1, changed state to up
Aug 24 19:57:26 zagreb.demo.net 10057: Aug 24 20:57:25.931 EDT: %LINK-3-UPDOWN: Interface Serial1/2:0, changed state to up
Aug 24 19:57:26 zagreb.demo.net 10058: Aug 24 20:57:26.931 EDT: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/2:0,
changed state to up
Aug 24 19:57:27 zagging.demo.net 2862: Aug 24 20:57:26.105 EDT: %LINK-3-UPDOWN: Interface Serial3/1:0, changed state to up
Aug 24 19:57:28 zagging.demo.net 2863: Aug 24 20:57:27.085 EDT: %DUAL-5-NBRCHANGE: IP-EIGRP 666: Neighbor 10.1.1.82
(Serial3/1:0) is up: new adjacency
Aug 24 19:57:28 zagging.demo.net 2864: Aug 24 20:57:27.105 EDT: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1:0,
changed state to up
```

- multiline messages

- timestamps

Decisions...

```
Aug 24 19:45:39 zoom.demo.net 104042: Aug 24 17:45:38.882 PDT: %IP-3-LOOPPAK: Looping packet detected and dropped -
Aug 24 19:45:39 zoom.demo.net 104043: src=10.8.1.8, dst=10.7.7.8, hl=20, tl=357, prot=17, sport=67, dport=68
Aug 24 19:45:39 zoom.demo.net 104044: in=FastEthernet5/0, nexthop=10.1.0.1, out=POS1/1
Aug 24 19:45:39 zoom.demo.net 104045: options=none
Aug 24 19:47:51 zealand.demo.net 2008 Aug 24 19:47:48 CDT -05:00 %CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on
port 4/13
Aug 24 19:57:25 zagging.demo.net 2861: Aug 24 20:57:24.105 EDT: %CONTROLLER-5-UPDOWN: Controller T1 3/1, changed state to up
Aug 24 19:57:26 zagreb.demo.net 10057: Aug 24 20:57:25.931 EDT: %LINK-3-UPDOWN: Interface Serial1/2:0, changed state to up
Aug 24 19:57:26 zagreb.demo.net 10058: Aug 24 20:57:26.931 EDT: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/2:0,
changed state to up
Aug 24 19:57:27 zagging.demo.net 2862: Aug 24 20:57:26.105 EDT: %LINK-3-UPDOWN: Interface Serial3/1:0, changed state to up
Aug 24 19:57:28 zagging.demo.net 2863: Aug 24 20:57:27.085 EDT: %DUAL-5-NBRCHANGE: IP-EIGRP 666: Neighbor 10.1.1.82
(Serial3/1:0) is up: new adjacency
Aug 24 19:57:28 zagging.demo.net 2864: Aug 24 20:57:27.105 EDT: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1:0,
changed state to up
```

- multiline messages
- timestamps
- what to keep

```
Aug 24 19:47:51 zealand.demo.net 2008 Aug 24 19:47:48 CDT -05:00
%CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port 4/13
```

- find date/timestamp to match

```
use Date::Format;
my @timespan_to_search = (localtime time - 3600);
my $template_date_to_match = ("%b %e %H");
my $date_to_match = strftime($template_date_to_match, @timespan_to_search);
```

```
Aug 24 19:47:51 zealand.demo.net 2008 Aug 24 19:47:48 CDT -05:00
%CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port 4/13
```

- find date/timestamp to match

```
use Date::Format;
my @timespan_to_search = (localtime time - 3600);
my $template_date_to_match = ("%b %e %H");
my $date_to_match = strftime($template_date_to_match, @timespan_to_search);
```

- split into timestamp/src host info + message

```
my @message_array = split(/%/,$msg);
```

```
Aug 24 19:47:51 zealand.demo.net 2008 Aug 24 19:47:48 CDT -05:00
%CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port 4/13
```

- find date/timestamp to match

```
use Date::Format;
my @timespan_to_search = (localtime time - 3600);
my $template_date_to_match = ("%b %e %H");
my $date_to_match = strftime($template_date_to_match, @timespan_to_search);
```

- split into timestamp/src host info + message

```
my @message_array = split(/%/,$msg);
```

- split out timestamp & src host

```
my @source_info_array = split(/\s+/, $message_array[0]);
```

```
Aug 24 19:47:51 zealand.demo.net 2008 Aug 24 19:47:48 CDT -05:00
%CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port 4/13
```

- find date/timestamp to match

```
use Date::Format;
my @timespan_to_search = (localtime time - 3600);
my $template_date_to_match = ("%b %e %H");
my $date_to_match = strftime($template_date_to_match, @timespan_to_search);
```

- split into timestamp/src host info + message

```
my @message_array = split(/%/,$msg);
```

- split out timestamp & src host

```
my @source_info_array = split(/\s+/, $message_array[0]);
```

- split into cisco message + details

```
my @syslog_detail_array = split(/:/, $message_array[$#message_array]);
```

split Cisco system message into facility,
severity, mnemonic

MEM_ECC-3-BADADDR_SBE

CONTROLLER-5-UPDOWN

SPANTREE-2-BPDUGUARD_SHUTDOWN

Easy! Split on the hyphen, pull out
\$array[1]!

split Cisco system message into facility,
severity, mnemonic

```
MEM_ECC-3-BADADDR_SBE  
CONTROLLER-5-UPDOWN  
SPANTREE-2-BPDUGUARD_SHUTDOWN
```

Easy! Split on the hyphen, pull out
\$array[1]!

```
C6K_POWER-SP-1-PD_HW_FAULTY
```

...or not :P

split Cisco system message into facility,
severity, mnemonic

```
MEM_ECC-3-BADADDR_SBE  
CONTROLLER-5-UPDOWN  
SPANTREE-2-BPDUGUARD_SHUTDOWN
```

Easy! Split on the hyphen, pull out
\$array[1]!

```
C6K_POWER-SP-1-PD_HW_FAULTY
```

...or not :P

```
#THIS MAKES HULK ANGRY  
$syslog_level =~ s/.*-([0-7])-.*/$1/;
```

mail it to people

```
my $program = '/usr/lib/sendmail';

open(my $mail_fh, "|$program -t") || die "can't open $program";

print $mail_fh "To: somebody\n";
print $mail_fh "From: snark\n";
print $mail_fh "Reply-to: me\n";
print $mail_fh "Subject: fix this please\n\n";

foreach my $line (@message) {
    print $mail_fh $line;
}

close($mail_fh);
```

Overview of Syslog messages received on 19 October 2008

----- Total Syslog messages, sorted by severity level -----

Message	Count
IP-3-LOOPPAK	89
LINK-3-UPDOWN	4
MEM_ECC-3-BADADDR_SBE	1440
SYS-3-PKTBUFBAD	6
CDP-4-DUPLEXMISMATCH	48
CDP-4-NATIVE_VLAN_MISMATCH	1411
CDP-4-NVLANMISMATCH	144
LINK-4-ERROR	27

----- Syslog messages per host -----

zilch	Total messages:2
• LINK-3-UPDOWN	2
zippy	Total messages:21
• IP-3-LOOPPAK	21
zanzibar	Total messages:1436
• CDP-4-NATIVE_VLAN_MISMATCH	1411
• LINK-4-ERROR	25

...and so on.

Cisco Syslog messages requiring attention

zachary

- 2 messages: SPANTREE-2-RX_PORTFAST: Received BPDU on PortFast enable port. Disabling 7/25

Report run at 24-Oct-2008 08:05 with the following options: type=detail, timespan=hourly, verbose=0

Files searched: /logs/cisco/cisco.log

Date/timestamp matched: Oct 24 07

This message was automatically generated. If you have questions, contact me@demo.net.

What happened...

What happened...

- cleaned up lots of minor network issues

What happened...

- cleaned up lots of minor network issues
- reduced raw # of messages by an order of magnitude

What happened...

- cleaned up lots of minor network issues
- reduced raw # of messages by an order of magnitude
- (side bennie: minor reduction in WAN traffic?)

What happened...

- cleaned up lots of minor network issues
- reduced raw # of messages by an order of magnitude
- (side bennie: minor reduction in WAN traffic?)
- evolved!

Overview of Syslog messages received on 16 September 2008

host	acl	packets	protocol	source IP
zagreb	bad_guys	214	icmp	10.38.4.8 -> 20.20.20.19
zagreb	bad_guys	11	tcp	10.38.4.8 -> 20.20.20.25
zagreb	bad_guys	2	icmp	10.38.4.8 -> 20.20.20.32

zucchini

- Authentication failure for SNMP req from host 80.152.152.190 (82)

Configured from console by billybob on vty0 (10.18.2.24):

- zambia (1)

Configured from console by cletus on vty0 (10.32.1.157):

- zoroaster (3), zigzag (1)

Report run at 26-Sep-2008 00:15 with the following options: type=security,
timespan=daily, verbose=0

Files searched: /logs/cisco/cisco.log

Date/timestamp matched: Sep 16

Issues

Issues

- not immediate

Issues

- not immediate
- not scalable

Issues

- not immediate
- not scalable

Next steps:

Issues

- not immediate
- not scalable

Next steps:

- daemonize it/hack syslogd

Issues

- not immediate
- not scalable

Next steps:

- daemonize it/hack syslogd
- incoming events kick off an SNMP trap (trapgen)

Issues

- not immediate
- not scalable

Next steps:

- daemonize it/hack syslogd
- incoming events kick off an SNMP trap (trapgen)
- keep it interesting

----- EIGRP messages -----

zinnia:

EeP-IIGRP(0) 666: Neeeghbur 10.0.0.1 (FfastEthernet5/1) ees doon:
eenterfffacea delay chunghed ()

EeP-IIGRP(0) 666: Neeeghbur 10.0.0.1 (FfastEthernet5/1) ees oop: nev
adjacency ()

zwieback:

EeP-IIGRP(0) 666: Neeeghbur 10.0.0.2 (GeegabitEthernet5/2) ees doon:
peer restarted ()

EeP-IIGRP(0) 666: Neeeghbur 10.0.0.2 (GeegabitEthernet5/2) ees oop:
nev adjacency ()

Repurt roon at 11-Nuf-2008 00:06 veeth zee ffullooeeng opteeuns:
typea=eeegrp, teemespun=huoorly, ferbusea=0

Ffeeles searched: /lugs/ceesco/cisco.lug

Datea/teemestamp matched: Nuf 10 23. Bork Bork Bork!

This message was automatically generated. If you have questions, contact
me@demo.net.

<0-7>	Logging severity level	
FAIL!	SISTEM IZ UNUSABLE	(severity=0)
OH_NOEZ	IMMEDIATE ACSHUN NEEDD	(severity=1)
OMGWTF	CRITICAL CONDISHUNS	(severity=2)
GTFO	ERROR CONDISHUNS	(severity=3)
YA_RLY	WARNIN CONDISHUNS	(severity=4)
OH_RLY	NORMAL BUT SIGNIFICANT CONDISHUNS	(severity=5)
OH_HAI	INFORMASHUNAL MESSAGEZ	(severity=6)
TLDR	DEBUGGIN MESSAGEZ	(severity=7)

%DUAL-OH_RLY-NBRCHANGE: IP-EIGRP 666: Naybr 10.0.0.1 (Vlan3): Iz lonely, no frendz.

%DUAL-OH_RLY-NBRCHANGE: IP-EIGRP 666: Naybr 10.0.0.1 (Vlan3): Iz wunderin, is dat u? IZ!

...and more ideas

- database for storage/searching

...and more ideas

- database for storage/searching
- with a web front-end :)

...and more ideas

- database for storage/searching
- with a web front-end :)
- link back to Cisco's translator

...and more ideas

- database for storage/searching
- with a web front-end :)
- link back to Cisco's translator
- link to KB

References

Getopt::Long

Date::Format

Lingua::Bork

http://www.cisco.com/en/US/docs/ios/12_0/system/messages/emover.h