Non-DIY* Logging

using

A Smalltalk Syslog library

* DIY: Do It Yourself

What is Syslog?

What is Syslog?

- RFC 3164 - The BSD syslog Protocol
- It's not a standard, but it is widely used

> Status of this Memo
>
> This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

What is Syslog?

From RFC 3164:

1. Introduction

Since the beginning, life has relied upon the transmission of messages. For the self-aware organic unit, these messages can ...

What is Syslog?

- It's way of using sockets to pass messages of 1024 octets in length that look like this:

```
<34>Oct 11 22:14:15 mymachine su: 'su root' failed
for lonvickon /dev/pts/8
```

What is Syslog?

- It's way of using sockets to pass messages of 1024 octets in length that look like this:

```
<34>Oct 11 22:14:15 mymachine su: 'su root' failed
for lonvickon /dev/pts/8
```

```
<165>Aug 24 05:34:00 CST 1987 mymachine myproc[10]:
%% It's time to make the do-nuts.  %% Ingredients:
Mix=OK, Jelly=OK #Devices: Mixer=OK, Jelly_Injector
=OK, Frier=OK #Transport:Conveyer1=OK, Conveyer2=OK #
%%
```

What is Syslog?

- It's way of using sockets to pass messages of 1024 octets in length that look like this:

```
<34>Oct 11 22:14:15 mymachine su: 'su root' failed
for lonvickon /dev/pts/8
```

```
<165>Aug 24 05:34:00 CST 1987 mymachine myproc[10]:
%% It's time to make the do-nuts.  %% Ingredients:
Mix=OK, Jelly=OK #Devices: Mixer=OK, Jelly_Injector
=OK, Frier=OK #Transport:Conveyer1=OK, Conveyer2=OK #
%%
```

```
Use the BFG!
```

Messages

- 1024 octets in length & composed like this:
  - PRI
    - e.g. <12> (User-Level Warning)
  - Header
    - e.g. Oct 11 22:14:15 myhost
  - MSG
    - e.g. hyper: bad request received from 12.63.103.16

The 3 Players

- Device (aka a Sender)
  - Remarkably, sends syslog messages
- Collector (aka Receiver)
  - A syslog server
- Relay
  - Both a Receiver and a Sender
  - Typically will filter and route messages
  - Could also act as a collector

The Smalltalk Syslog Library

- OskSyslog in the public Store
  - Developed in VW using Sport
  - Available under the LGPL
  - Used by OpenSkills in VW and GemStone
- An implementation of RFC 3164, including:
  - Message
  - Sender
  - Receiver
  - Relay

Sender

- The RFC says that messages must be sent to UDP port 514
- Really should make sure the message is well formed.
  - “Use the BFG” is not so good

Simple Sender

- Using the logger command:

  - >logger Hello, World.
  - Sends a user notice to the local syslog server
  - tail -f /var/log/messages

The Syslog Library

- OskSyslog in the public Store
- To repeat the Dead Simple Example:

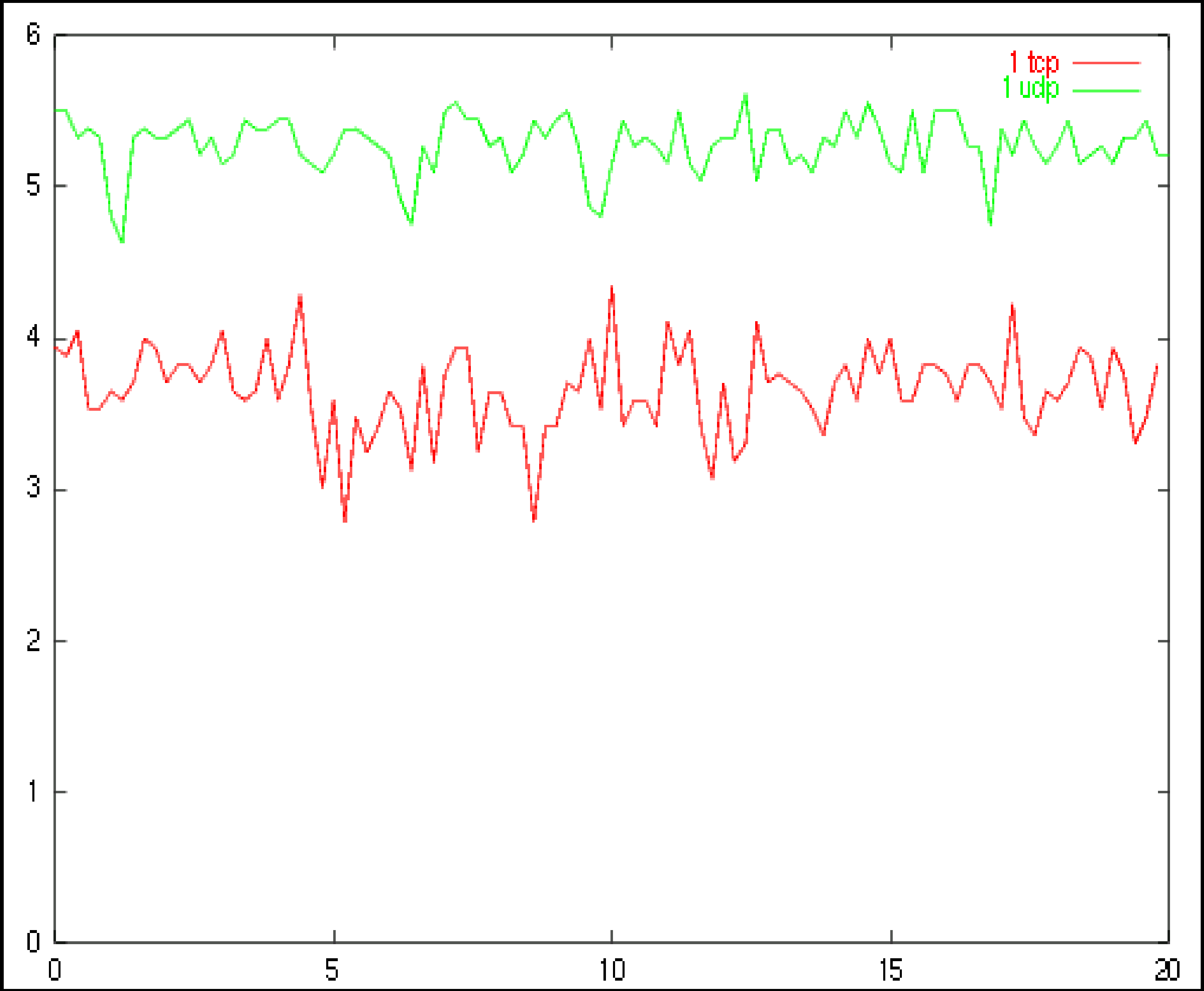
```
| sender |
[| message |
sender := OSkSyslogSender sendingToHostNamed: '192.168.29.129'.
message := OSkSyslogEventMessage userLevelNotice:
'vwnc: A test from Smalltalk'.
sender send: message] ensure: [sender close].
```

Are you listening?

- Many syslog servers don't listen on UDP by default
  - They mostly listen on local *nix sockets
  - Easy to switch on UDP listening, though. In Debian:

```
vi /etc/default/syslogd (ensure SYSLOGD="-r")
/etc/init.d/sysklogd restart
sudo netstat -a | grep syslog (shows if it is indeed listening on UDP)
```

UDP vs. TCP



Jim Snow: http://syn.cs.pdx.edu/~jsnow/

UDP vs. TCP

- Speed vs reliable delivery
  - TCP does not guarantee delivery, but it will let you know if a delivery failed.
- If you can't afford to lose a message or three
  - ask yourself if what you are doing is really logging

Receiver

- Listens on UDP port 514
  - Note that you'll need to run as root or use iptables to redirect traffic from 514 to a port with a number > 1024

```
server := OSkSyslogReceiver onPort: 514
        forEachMessageDo:
            [:aSyslogMessage |
            Transcript
                cr;
                show: aSyslogMessage asOctetArray asString].
```

Collector

- Uses a Receiver to get messages
  - Keep
  - Summarise
  - Discard
- OpenSkills will be using PostgreSQL
  - Looking for patterns over time
  - ... and whatever else comes to mind

Relay

- Combination of
  - a Receiver
  - a Sender
- Can be used to
  - Filter & Route messages
  - Redirect messages over a port > 1024
  - perhaps send alerts to pagers?

Summary

- Lots of existing tools
  - e.g. less
- Best effort delivery with UDP
  - If it absolutely definitely has to be there, use TCP
- Syslog
  - The only way to fly for extra-image logging