

Centralizing Syslog with Syslog-ng and Logmuncher

Russell Adams

Who is this guy?

- Russell Adams
- Over a Decade in Information Technology
- Professional Systems Administrator
- Large systems (1000+ users)
- Linux only for over Seven Years
- Gentoo rocks!

Why did he drag me here?!

- Talk about Log Management
- Recommend Software for Log Management
- Tutorial on Configuring Recommended Software

What's so special about system logs?

- System Events
- User Activity
- Network Connections
- Authentication Failures
- Device Errors
- Kernel Messages
- Firewall Rule Violations
- Database Warnings

Sounds great! What's the catch?

- Verbose
- Repetitive
- Host Specific
- Accumulate Rapidly
- Cumbersome Archival
- Low Signal to Noise Ratio
- Easily Tampered With

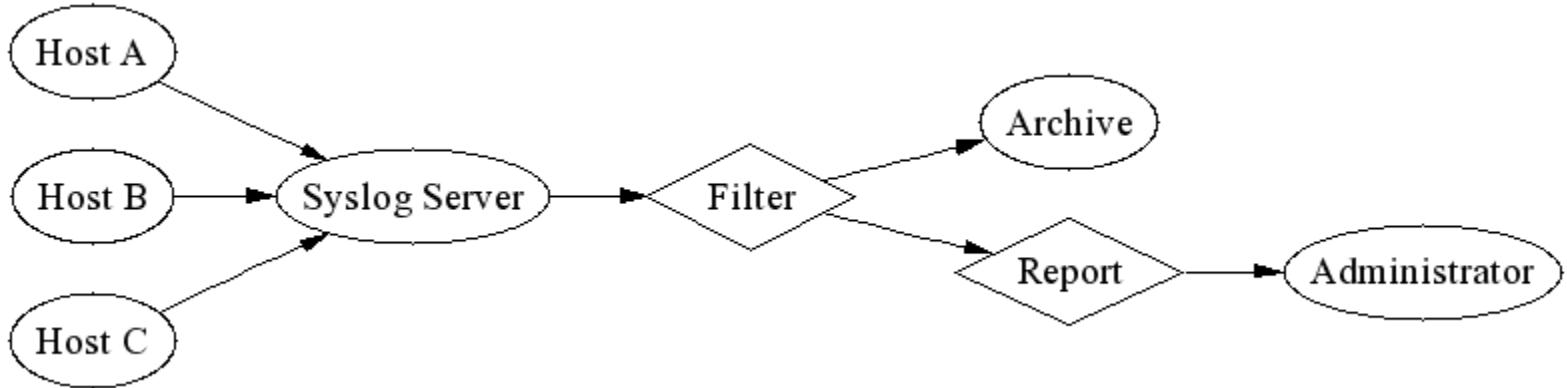
You want me to review all of that?!

- Overcome Administrator Apathy
- Automation
- Centralization
- Filtering
- Reporting
- Rotation
- Archival

Oh cool! Tell me more!

- Centralized Log Servers
- Prevent Tampering
- Single Point of Administration
- Correlate Events between Hosts
- Simplify Reporting / Filtering
- Organized by Host, Date, Type

Syslog Server Illustration



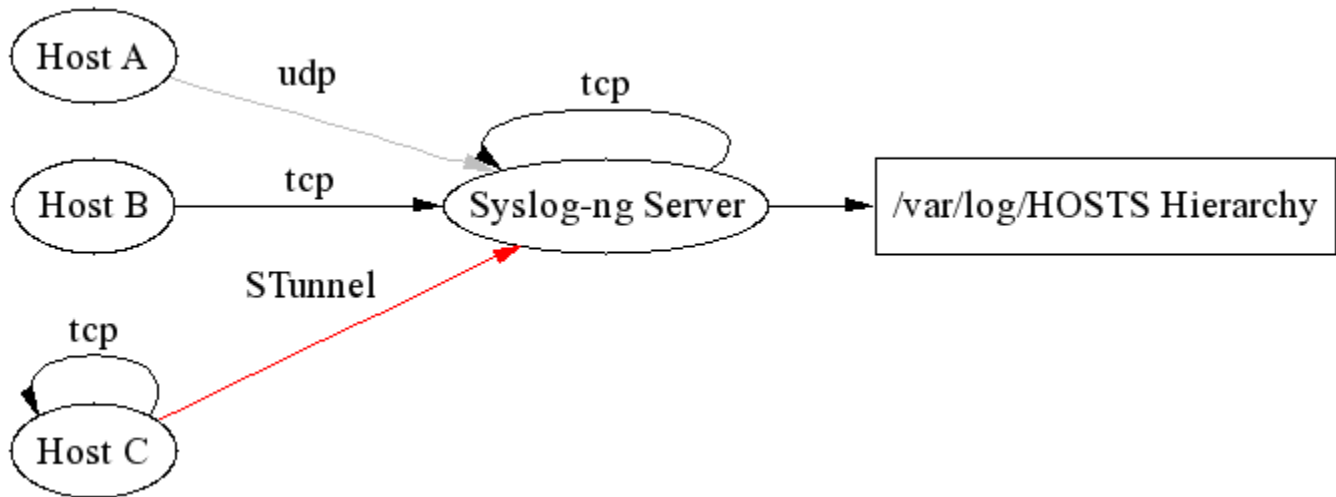
So what software should I use?

- Centralize Syslog with Syslog-ng by Balazs Scheidler
- Supports any Syslog client
 - ◆ Linux, *nix, Cisco, Windows...
- Logs over Network
 - ◆ TCP or UDP
 - ◆ STunnel
- Future Plans for Signed Logs and Encryption

So what software should I use?

- Centralize Syslog with Syslog-ng by Balazs Scheidler
- Logs Organized in a Hierarchy
 - ◆ Host
 - ◆ Date (Year, Month, Day)
 - ◆ Loglevel
 - ◆ `/var/log/HOSTS/host/YYYY/MM/DD/loglevelYYYYMMDD`
 - ◆ Kudos to the Syslog-ng FAQ at <http://www.campin.net/>
- Automatic Rotation with Hierarchy
- External Archival Script Prunes Hierarchy

Syslog Server Illustration



Syslog-ng Server Configuration Sample

```
options { long_hostnames(off); sync(0); };

source src { unix-stream("/dev/log");
             internal();
             file("/proc/kmsg");
             tcp( max-connections(100) );
             udp(); };

destination hosts {
    file("/var/log/HOSTS/$HOST/$YEAR/$MONTH\
        /$DAY/$FACILITY$YEAR$MONTH$DAY"
        owner(root)
        group(root)
        perm(0600)
        dir_perm(0700)
        create_dirs(yes) );
};

log { source(src);
      destination(hosts); };
```

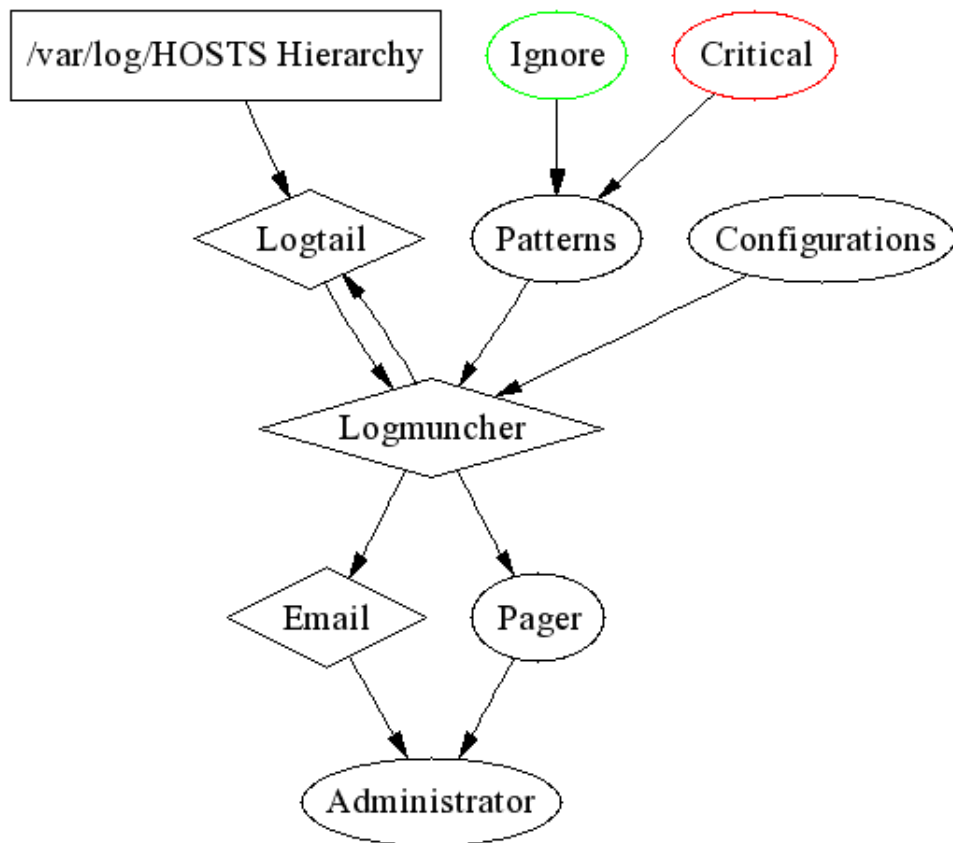
Syslog-ng Client Configuration Sample

```
options { long_hostnames(off);  
          sync(0);  
          log_fifo_size(1000); };  
  
source src { unix-stream("/dev/log");  
             internal();  
             file("/proc/kmsg"); };  
  
destination loghost { tcp("mysyslogserver.mydomain.com."); };  
  
log { source(src); destination(loghost); };
```

I meant for the automated reporting.

- Reporting done with Logmuncher by Geoff Kuenning
- Notification via E-mail, Pager, or Phone
- Ignore Common / Unimportant Log Messages
- Report Important Log Messages
- Yell If A Critical Log Message Occurs
- Gracefully Handle Unknown Log Messages
- Easily Configurable Reg-Exp Filters
- Flexible Reporting Formats

Logmuncher Illustration



Sample Logmuncher Report

- Sanitized messages from a Snort LIDS host

Date: Sat, 17 May 2003 09:25:11 -0500
From: root@logmuncher.mydomain.com
Subject: lids1 05/17/03 09:25:01 Logmuncher Report

***** lids1 Log Entries *****

May 17 09:10:24 lids1 snort: [1:553:4] POLICY FTP
anonymous login attempt [Classification: Misc activity]
[Priority: 3]: {TCP} 80.26.139.84:1558 -> 198.42.129.2:21

May 17 09:10:24 lids1 snort: [1:553:4] POLICY FTP
anonymous login attempt [Classification: Misc activity]
[Priority: 3]: {TCP} 80.26.139.84:1559 -> 198.42.129.3:21

May 17 09:10:24 lids1 snort: [1:553:4] POLICY FTP
anonymous login attempt [Classification: Misc activity]
[Priority: 3]: {TCP} 80.26.139.84:1565 -> 198.42.129.9:21

Sample Logmuncher Host Configuration

```
subject ns2 %d %t Logmuncher Report
header ***** ns2 Log Entries *****
```

```
mtailfile      /var/log/HOSTS/ns2/*/*/*/*
re-ignore      /etc/logmuncher/patterns/common
re-ignore      /etc/logmuncher/patterns/ns2
send-report    administrator@mydomain.com
```

Sample Logmuncher Host Pattern File

```
CROND.*bin.*CMD.*usr/local/sbin/amdump
CROND.*bin.*CMD.*usr/local/sbin/amcheck
CROND.*cricket.*CMD.*home/cricket/cricket/collect-subtrees
CROND.*cricket.*CMD.*usr/bin/find
ftpd.*incoming
ftpd.*FTP session closed
httpd.*No Local authentication done
httpd.*pam_smb.*Configuration Data
httpd.*pam_smb.*Correct NT username/password pair
sendmail.*stat=Sent
sendmail.*relay=.*@localhost
sendmail.*cricket.*forward
sendmail.*relay=ks119is01mail1.ksnet.com
sshd.*Generating new 768 bit RSA key
sshd.*RSA key generation complete
xinetd.*EXIT.*ftp
xinetd.*START.*amanda.*from=192.168.1.12
xinetd.*START.*ftp.*from=192.168.1.13
xinetd.*USERID.*ftp.*USER@HOST
```

Links Page