

Centralized Logging: Syslog

Emmanuel Kwarteng
30/07/2009

What is a Syslog?

Syslog is a standard for forwarding log messages in an IP network. And the term “syslog” is often used for both the actual syslog protocol, as well as the application or library sending syslog messages. The syslog service can operate in a local listening mode which is the default as well as a network listening mode.

So its common features are as below

- * Logging Service
- * Unix based
- * Networkable

Other Characteristics of a syslog server

It run on UDP port 514 and typically limited to 1024 bytes.

- * It follow a FIFO buffers style ie First In First Out
- * Rolling View of Logs
- * Type of Named Pipe

What is Syslog-NG?

Syslog-ng is the new open source implementation of the syslog protocol. It's generally referred to as the System Log Next-Generation since it supports a wide variety of devices, and the format of relayed messages can be customized. Other enhancements include the ability to filter content and it has various methods of storing information including separate files-per-devices, or use of mysql databases. You can install syslog generally from port as below

```
Cd /usr/ports/sysutils/syslog-ng
```

```
Make install clean
```

Other features of Syslog-ng

Syslog-ng can work in network client-server mode, “syslog-ng client” collect the messages from various application's log source then processes logs like compares the message to the filters of the log statement(if any). If the message complies with all filter rules, syslog-ng sends the message to the destination set in the log statement.

Other features of Syslog-ng - continue

Other few important syslog-ng features includes:

- timestamp with millisecond granularity and timezone information
- The addition of the name of relays in the host fields to make it possible to track the path a given message has traversed
- reliable transport using TCP
- TLS encryption
- logging directly into a database etc ...

Reconfiguring Syslog-NG

Configuration depends on network environment.
Example are as below

- * Windows Hosts
- * Cisco Devices
- * Linux Hosts
- * Other Devices and Gear

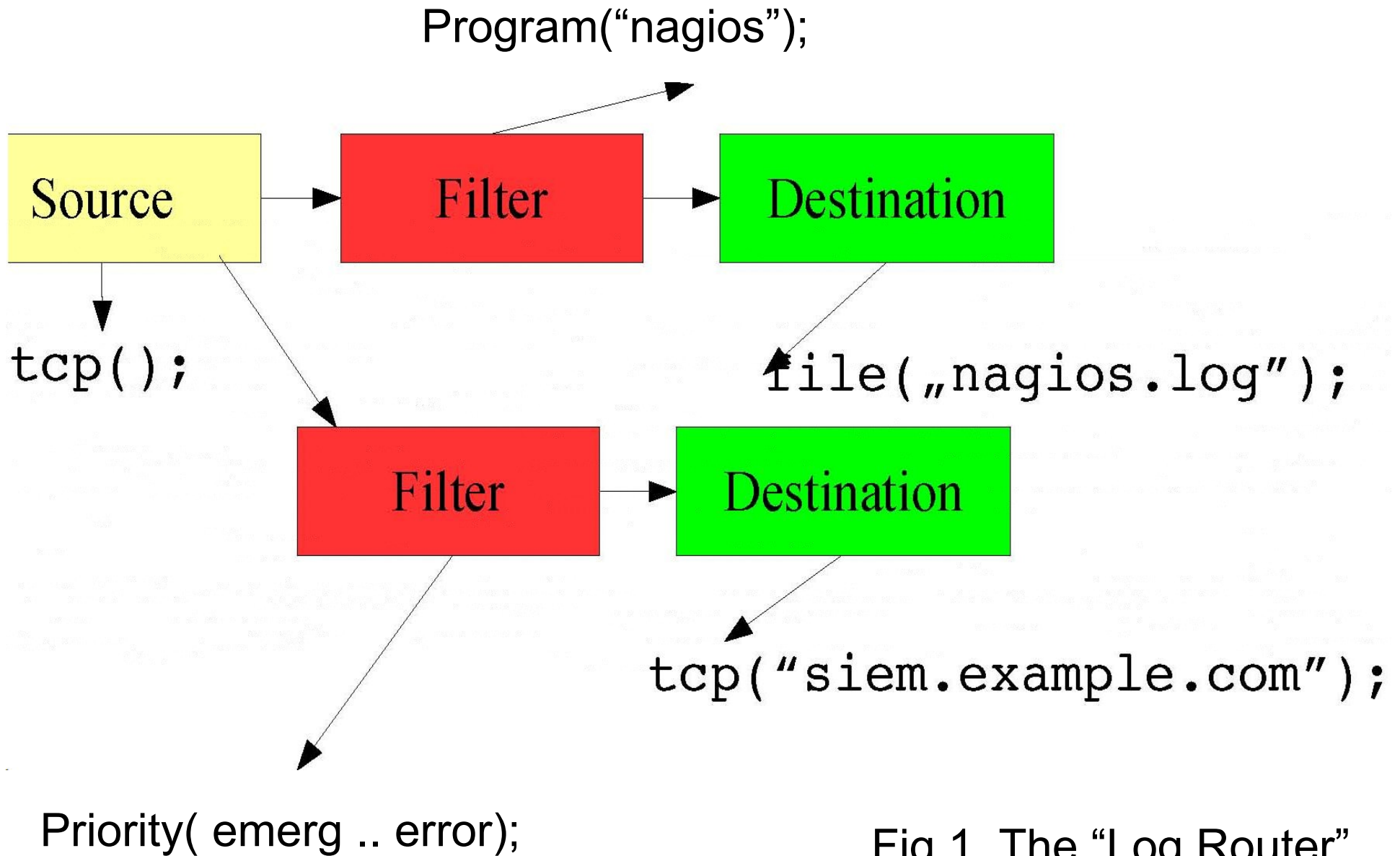


Fig.1 The "Log Router"

Log statement:

Important Syslog-ng configuration options

When modifying the configuration file for syslog-ng (ie. syslog-ng.conf) There are five possible sections to consider:

- options{} : Global options which can be overridden in any of the next four sections.
- source{} : Message sources, such as files, local sockets, or remote hosts
- destination{} : Message destinations, such as files, local sockets, or remote hosts
- filter{} : Filters are powerful and flexible; you can filter on any aspect of log message, such as standard syslogd facility names , log level, hostname, and arbitrary content like words or number strings
- log{} : Log statements connect the source, destination, and filter statements, and tell syslog-ng what to do with them.

For more detail options consult manual using `man syslog-ng.conf`

Global Configuration

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

```
Options {  
    chain_hostnames(0);  
    time_reopen(10);  
    time_reap(360);  
    log_fifo_size(2048);  
    create_dirs(yes);  
    group(admin);  
    Perm(0640);  
    dir_perm(0755);  
    use_dns(no);  
    stats_freq(0);  
};
```

Meaning of Global Configs

- * Disable Hostname Chaining
- * Time to wait before re-establishing a dead connection
- * Time to wait before an idle file is closed
- * FIFO buffer size
- * Create Directories
- * Permissions
- * Disable DNS
- * Disable Statistic Logging

Creating a Source

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

```
Source s_all {  
    Internal();  
    unix-stream("/dev/log");  
    file("/proc/kmsg" log_prefix("kernel: "));  
    Udp();  
};
```

Defining Filters

* Windows Filter

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

```
Filter f_windows {  
    program(MSWinEventLog);  
};
```

* Cisco Filter

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

```
Filter f_cisco_pix {  
    host(IP.OF.PIX.Device);  
};
```

General Filter

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

```
Filter f_not_other {  
    Not host(IP.OF.PIX.Device)  
    And not program(MSWinEventLog);  
};
```

Destinations

- * FIFO Buffers
- * One Large File

→ Windows FIFO
/etc/syslog-ng/syslog-ng.conf

```
Destination d_windows {  
    pipe("/var/log/buffers/windows");  
};
```

→ Cisco FIFO
/etc/syslog-ng/syslog-ng.conf

```
Destination d_cisco {  
    pipe("/var/log/buffers/cisco");  
};
```

Destination - Continued

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

```
Destinatin d_gen_fifo {  
    pipe("/var/log/buffers/syslog");  
};
```

* For archiving purposes, you can do as below
/etc/syslog-ng/syslog-ng.conf

```
Destination d_all {  
    file("/var/log/arch/$MONTH$DAY$YEAR");  
};
```

Tying it all Together !

Now we can tell syslog to handle the configs. ;))

→ Windows Log

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

```
Log {  
    source(s_all);  
    filter(f_windows);  
    destination(d_windows);  
};
```

Tying All Together -continue

→ Cisco Log

```
/etc/syslog-ng/sylog-ng.conf
```

```
Log {  
    source(s_all);  
    filter(f_cisco_pix);  
    destination(d_cisco);  
};
```

General FIFO

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

```
Log {  
    Source(s_all);  
    filter(f_not_others);  
    destination(d_gen_fifo);  
};
```

* Configuration for archive logs is as below

```
Log {  
    source(s_all);  
    destination(d_all);  
};
```

Finishing Up...

- * Making the FIFO buffers
- * Creating the directory structure

```
# mkdir /var/log/arch
```

```
# mkdir /var/log/buffers
```

```
# mkfifo /var/log/buffers/windows
```

```
# mkfifo /var/log/buffers/cisco
```

```
# mkfifo /var/log/buffers/syslog
```

```
# /usr/local/etc/rc.d/syslog.sh restart
```

Check if Everything is Okay

- * Check your Logfiles (/var/log/arch/*)
- * Check your FIFO Buffers
 - cat /var/log/buffers/windows
 - cat /var/log/buffers/cisco
 - cat /var/log/buffers/syslog

A web interface tool with indexing capability as well as reporting and search feature.

Eg. Splunk, php-syslog-ng

Conclusion

System logger is one of the most important feature in operating system which provide users the capability for auditing, security etc. the stock unix standard syslogd suffers from a number of deficiencies (limited configuration options, using UDP protocol to transfer data , etc) , and is best replaced with a newer daemon such as syslog-ng.

Syslog-ng have many nice features to improve our ability to manage our log messages. And a better log reporting system will give us a good monitoring system.

Questions?