|  |  |
| --- | --- |
|  | **2014** |
|  | The Company  Martien Huijsmans |

|  |
| --- |
| **[rsyslog and family]** |
| Todo |

Inhoud

[Rsyslog 1](#_Toc413018405)

[Fedora 20, version rsyslog 1](#_Toc413018406)

[Modules: 2](#_Toc413018407)

[Forward 2](#_Toc413018408)

[Use case: Multiple source connecting to same ip-port 2](#_Toc413018409)

[Capabilities 2](#_Toc413018410)

[Max message size can be 20k 2](#_Toc413018411)

[Features 2](#_Toc413018412)

[Filters 2](#_Toc413018413)

[Filters: examples 2](#_Toc413018414)

[TCP 3](#_Toc413018415)

[Queues 3](#_Toc413018416)

[Throttling 3](#_Toc413018417)

[Configuration 3](#_Toc413018418)

[Config files 3](#_Toc413018419)

[Ruleset 3](#_Toc413018420)

[Templates 3](#_Toc413018421)

[Properties used in Templates and Rules 3](#_Toc413018422)

[Guides 3](#_Toc413018423)

[Logrotate 3](#_Toc413018424)

[Logger 4](#_Toc413018425)

# Rsyslog

## Fedora 20, version rsyslog

[wizard@localhost ~]$ rsyslogd –version  
rsyslogd 7.4.8, compiled with:  
 FEATURE\_REGEXP: Yes  
 FEATURE\_LARGEFILE: No  
 GSSAPI Kerberos 5 support: Yes  
 FEATURE\_DEBUG (debug build, slow code): No  
 32bit Atomic operations supported: Yes  
 64bit Atomic operations supported: Yes  
 Runtime Instrumentation (slow code): No  
 uuid support: Yes  
See http://www.rsyslog.com for more information.

## Modules:

### Forward

<http://www.rsyslog.com/doc/omfwd.html>

## Use case: Multiple source connecting to same ip-port

Are end-ofline preserved?

## Capabilities

### Max message size can be 20k

<http://stackoverflow.com/questions/18619933/centralized-rsyslog-max-size-of-message>

## Features

### Filters

Rsyslog offers three different types "filter conditions":

* RainerScript-based filters
* "traditional" severity and facility based selectors
* property-based filters

ref: <http://www.rsyslog.com/doc/rsyslog_conf_filter.html>

### Filters: examples

Filter by tag  
<http://serverfault.com/questions/514901/how-to-filer-rsyslog-messages-by-tags>

Filter on remote IP-address, store data in certain file  
<http://www.rsyslog.com/newbie-guide-to-rsyslog/>   
Next link describes a template for automatic creation of logfiles  
<http://www.rsyslog.com/storing-messages-from-a-remote-system-into-a-specific-file/>

Filter on message content  
<http://www.rsyslog.com/writing-specific-messages-to-a-file-and-discarding-them/>

### TCP

Supported: <http://www.rsyslog.com/doc/imtcp.html>

Ruleset can be bound to specific listening port.  
Source: above link

### Queues

Default exist for default ruleset. Others can be configured  
<http://www.rsyslog.com/doc/master/rainerscript/queue_parameters.html>

### Throttling

Can be turned on/off (globally or per something ?)  
If on, can increase delay.

## Configuration

### Config files

General  
/etc/rsyslog.conf  
This will also load the application specific config files.  
  
Application specific configurations reside in directory  
/etc/rsyslog.d/

### Ruleset

Ruleset info: <http://www.rsyslog.com/doc/multi_ruleset.html>

### Templates

<http://www.rsyslog.com/doc/rsyslog_conf_templates.html>   
(difficult topic).

## Properties used in Templates and Rules

Property-formatter   
<http://www.rsyslog.com/doc/v8-stable/configuration/properties.html>

## Guides

<http://www.rsyslog.com/guides/>

# Logrotate

Fedora 20  
[wizard@localhost ~]$ logrotate –version  
logrotate 3.8.7

Ref: <http://linuxconfig.org/setting-up-logrotate-on-redhat-linux>   
Ref: logrotate manpage: <http://linuxconfig.org/logrotate-8-manual-page>

Properties

* By default logrotate is invoked once a day using a cron scheduler from location /etc/cron.daily/
  + /etc/cron.daily contains shell script for logrotate
    - Of failure that script can log an error, e.g.  
      /usr/bin/logger -t logrotate "ALERT exited abnormally with [$EXITVALUE]"  
      ref: <http://man7.org/linux/man-pages/man1/logger.1.html>
* Has /etc/logrotate.conf
* Has /etc/logrotate.d/ where RPM package can drop log rotate information

There is a risk a log message loss when the current log file is archived.

# Logger

A linux shell command that interfaces to syslog  
<http://linux.about.com/library/cmd/blcmdl1_logger.htm>

Features

* posix syslog, UDP & TCP.
* supports tags.
* Program name can be specified.  
  e.g. logger -t PROGNAME This is a message to be logged