

SECTION 7 Use Syslog Daemon syslog-ng

Up to SUSE Linux Enterprise Server 9, `syslogd` was used to log system events. With SUSE Linux Enterprise Server 10 these events are logged by `syslog-ng`, the new generation `syslogd`.

The main advantage of `syslog-ng` over `syslogd` is its capability to filter messages not only based on facilities and priorities, but also based on the content of each message.

Objectives

1. Use Syslog Daemon `syslog-ng`

Objective 1 Use Syslog Daemon `syslog-ng`

The syslog daemon **syslog-ng** is used by many services to log system events. The advantage in using a single service for logging is that all logging can be managed from one configuration file.

The syslog daemon accepts messages from system services, and, depending on its configuration, other hosts, and logs them based on settings in the configuration files **/etc/sysconfig/syslog** and **/etc/syslog-ng/syslog-ng.conf**. The file `/etc/syslog-ng/syslog-ng.conf` is generated by SuSEconfig from `/etc/syslog-ng/syslog-ng.conf.in`. Both files share the same syntax.

The configuration of `syslog-ng` is distributed across three files:

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

/etc/sysconfig/syslog

The file ***/etc/sysconfig/syslog*** contains general parameters applicable to syslog-ng as well as syslogd.

Parameters set in this file include switches passed to syslogd or syslog-ng, kernel log level, parameters for klogd, and which syslog daemon is to be used.

```

...
## Type:                string
## Default:             " "
## Config:              " "
## ServiceRestart:     syslog
#
# if not empty: parameters for syslogd
# for example SYSLOGD_PARAMS="-r -s my.dom.ain"
#
SYSLOGD_PARAMS=" "

## Type:                string
## Default:             -x
## Config:              " "
## ServiceRestart:     syslog
#
# if not empty: parameters for klogd
# for example KLOGD_PARAMS="-x" to avoid (duplicate) symbol
resolution
#
KLOGD_PARAMS="-x"

## Type:                list(syslogd,syslog-ng)
## Default:             syslogd
## Config:              syslog-ng
## Command:             /sbin/rcsyslog restart
## PreSaveCommand:     /sbin/rcsyslog status &&
/sbin/rcsyslog stop
#
# The name of the syslog daemon used as
# syslog service: "syslogd", "syslog-ng"
#
SYSLOG_DAEMON="syslog-ng"
...

```

Parameters set in `/etc/sysconfig/syslog` are evaluated by the start script `/etc/init.d/syslog`. Furthermore, `SuSEconfig` uses `/etc/sysconfig/syslog` to add log sockets to the file `/etc/syslog-ng/syslog-ng.conf` when generating this file from `/etc/syslog-ng/syslog-ng.conf.in`.

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

`/etc/syslog-ng/syslog-ng.conf.in` is the template used to create the configuration file **`/etc/syslog-ng/syslog-ng.conf`**, which is the configuration file actually used by `syslog-ng`. Both files have the same syntax.

However, unless you turn off generation of `/etc/syslog-ng/syslog-ng.conf` in `/etc/sysconfig/syslog`, any manual changes to this file will be overwritten when `SuSEconfig` is executed.

Therefore, changes to the configuration of `syslog-ng` should be made in this file.

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

`syslogd` and `syslog-ng` share two concepts that you have to understand to be able to configure either one:

- Facilities
- Priorities

The configuration of `syslog-ng` consists of several parts which are then combined to configure which information is logged where.

These are:

- Sources
- Filters
- Destinations
- Log Paths

Facilities

The facility refers to the subsystem that provides the corresponding message. Each program that uses syslog for logging is assigned such a facility, usually by its developer.

The following describes these facilities:

Table 7-1

Facility	Description
authpriv	Used by all services that have anything to do with system security or authorization. All PAM messages use this facility. The ssh daemon uses the auth facility.
cron	Accepts messages from the cron and at daemons.
daemon	Used by various daemons that do not have their own facility, such as the ppp daemon.
kern	All kernel messages.
lpr	Messages from the printer system.
mail	Messages from the mail system. This is important because many messages can arrive very quickly.
news	Messages from the news system. As with the mail system, many messages might need to be logged in a short time.

Table 7-1 *(continued)*

Facility	Description
syslog	Internal messages of the syslog daemon.
user	A general facility for messages on a user level. For example, It is used by login to log failed login attempts.
uucp	Messages from the uucp system.
local0 – local7	These 8 facilities are available for your own configuration. All of the local categories can be used in your own programs. By configuring one of these facilities, messages from your own programs can be administered individually through entries in the file <code>/etc/syslog-ng/syslog-ng.conf</code> .

Priorities

The priority gives details about the urgency of the message. The following priorities are available (listed in increasing degree of urgency):

Table 7-2

Priority	Description
debug	Should only be used for debugging purposes, since all messages of this category and higher are logged.
info	Used for messages that are purely informative.
notice	Used for messages that describe normal system states that should be noted.
warning	Used for messages displaying deviations from the normal state.
err	Used for messages displaying errors.

Table 7-2 (continued)

Priority	Description
crit	Used for messages on critical conditions for the specified program.
alert	Used for messages that inform the system administrator that immediate action is required to keep the system functioning.
emerg	Used for messages that warn you that the system is no longer usable.

Sources

A source is a collection of source drivers, which collect messages using a given method. These sources are used to gather log messages. The general syntax is as follows:

```
source <identifier> { source-driver(params); source-driver(params); ... };
```

The respective section in `/etc/syslog-ng/syslog-ng.conf` looks like this:

```
source src {
    # include internal syslog-ng messages
    # note: the internal() source is required!
    internal();

    # the following line will be replaced by the
    # socket list generated by SuSEconfig using
    # variables from /etc/sysconfig/syslog:
    unix-dgram("/dev/log");

    # uncomment to process log messages from network:
    #udp(ip("0.0.0.0") port(514));
};
```

In this example, one source for internal messages of syslog-ng and the socket `/dev/log` are defined.

Filters

Filters are boolean expressions that are applied to messages and are evaluated as either true or false. The general syntax is as follows:

```
filter <identifier> { expression; };
```

The identifier has to be unique within the configuration and is used later to configure the actual logging.

The following excerpt of `/etc/syslog-ng/syslog-ng.conf` shows some filters used in SUSE Linux Enterprise Server 10:

```
#
# Filter definitions
#
filter f_iptables { facility(kern) and match("IN=") and match("OUT=");
};

filter f_console { level(warn) and facility(kern) and not
    filter(f_iptables) or level(err) and not facility(authpriv); };

filter f_newsnotice { level(notice) and facility(news); };
filter f_newscrit { level(crit) and facility(news); };
filter f_newserr { level(err) and facility(news); };
filter f_news { facility(news); };
...
filter f_messages { not facility(news, mail)
    and not filter(f_iptables); };
...
```

As you can see, facility and priority (level) can be used within filters. However, it is also possible to filter according to the content of a line being logged, as in the `f_iptables` filter above.

Combining the expressions with “and”, “or”, or “and not” allows you to create very specific filters.

Destinations

Destinations defines where messages can be logged. The general syntax is as follows:

```
destination <identifier> {  
  destination-driver(params);  
  destination-driver(params); ... };
```

Possible destinations are files, fifos, sockets, ttys of certain users, programs, or other hosts.

A sample from `/etc/syslog-ng/syslog-ng.conf` looks like this:

```
destination console { file("/dev/tty10"    group(tty) perm(0620)); };  
destination messages { file("/var/log/messages"); };
```

Log Paths

Log paths are the point where it all comes together. They define which messages are logged where, depending on source, filter, and destination. The general syntax is as follows:

```
log { source(s1); source(s2); ...  
      filter(f1); filter(f2); ...  
      destination(d1); destination(d2); ...  
      flags(flag1[, flag2...]); };
```

The following entries in `/etc/syslog-ng/syslog-ng.conf` for instance are responsible for logging to `/dev/tty10` and `/var/log/messages`:

```
log { source(src); filter(f_console); destination(console); };  
log { source(src); filter(f_messages); destination(messages); };
```

In the first line, log messages that come in through sources defined in source `src` are logged to `tty10` if they match the filter `f_console`. In line two, messages that come in through sources defined in source `src` are logged to `/var/log/messages` if they match the filter `f_messages`.



For further details on the `syslog-ng.conf` file, enter **man 5 syslog-ng.conf**. The documentation in `/usr/share/doc/packages/syslog-ng/html/book1.html` gives a general overview of `syslog-ng` as well as details on the configuration.

Summary

Objective	Summary
1. Use Syslog Daemon syslog-ng	In a Linux system, there are many logs that track various aspects of system operation. Many services log their activities to their own log files, and the level of detail can be set on a per-service basis. In addition, system logs in <code>/var/log/</code> track system-level events. logrotate is the utility to archive log files.
