NAME

syslogd - log system messages

SYNOPSIS

/usr/sbin/syslogd [**-a**] [**-d**] [**-D**] [**-f** *configfile*] [**-m** *markinterval*] [**-N**] [**-p** *logfile*] [**-r**] [**-s**] [**-v**]

DESCRIPTION

The **syslogd** command reads and logs messages into a set of files described by the configuration file **/etc/syslog.conf**.

Options

syslogd recognizes the following options:

-a	Allows all messages except consecutive duplicate messages without reordering them.
-d	Turn on debugging.
-D	Prevent the kernel from directly printing its messages on the system console. In this case, **syslogd** is responsible for routing all kernel messages to their proper destination.
-f *configfile*	Use *configfile* instead of **/etc/syslog.conf**.
-m *markinterval*	Wait *markinterval* minutes between mark messages, instead of 20 minutes.
-N	Don't listen to socket.
-p *logfile*	Use *logfile* instead of **/dev/log**.
-r	Don't suppress duplicate messages.
-s	While logging the messages coming from remote system, IP address will be logged instead of the hostname.
-v	Add priority and facility encoded code at the second field of the message line. Refer to *syslog*(3C) manpage for these priority and facility encoding codes.

syslogd creates the file **/var/run/syslog.pid**, if possible, containing a single line with its process ID. This can be used to kill or reconfigure **syslogd**.

To kill **syslogd**, send it a terminate signal:

```
kill `cat /var/run/syslog.pid`
```

To make **syslogd**, re-read its configuration file, send it a **HANGUP** signal:

```
kill -HUP `cat /var/run/syslog.pid`
```

S

syslogd collects messages from the UNIX domain socket **/dev/log.un**, an Internet domain socket specified in **/etc/services**, the named pipe **/dev/log**, and from the kernel log device **/dev/klog**. By default, local programs calling **syslog()** send log messages to the UNIX domain socket (see *syslog*(3C)). If UNIX domain sockets are not configured on the system, they write to the named pipe instead. If INET domain sockets are not configured, **syslogd** does not receive messages forwarded from other hosts, nor does it forward messages (see below).

Each message is one line. A message can contain a priority code and facility code as the second field of the line. Priorities and Facilities are defined in the header file **<syslog.h>**.

When **syslogd** is invoked using **/sbin/init.d/syslogd** script, user can update the required options in **/etc/rc.config.d/syslogd** file. By default **/etc/rc.config.d/syslogd** contains **-D** option. Before starting the **syslogd** command, the **/sbin/init.d/syslogd** script recreates **/var/adm/syslog/syslog.log** after putting the contents into the file **/var/adm/syslog/OLDsyslog.log**. By default, **OLDsyslog.log** is overwritten by the contents of **syslog.log**. If you want to retain the contents of the previous **OLDsyslog.log** file, configure **PREV_OLDSYSLOG_LINES** in **/etc/rc.config.d/syslogd**. You can set the parameter to the number of lines (in thousands) to be retained from the previous **OLDsyslog.log** file. For example, to retain 20,000 lines from the previous **OLDsyslog.log** file along with the contents of the previous **syslog.log** in the present **OLDsyslog.log**, put **PREV_OLDSYSLOG_LINES=20** in **/etc/rc.config.d/syslogd**. By default **PREV_OLDSYSLOG_LINES** is set to 0.

syslogd configures itself when it starts up and whenever it receives a hangup signal. Lines in the configuration file consist of a **selector** to determine the message priorities to which the line applies and an **action**. The *action* field is separated from the selector by one or more tabs.

Selectors are semicolon separated lists of priority specifiers. Each priority has a **facility** indicating the subsystem that generated the message, a dot, and a **level** indicating the severity of the message. Symbolic names can be used. An asterisk selects all facilities. All messages of the specified level or higher (greater severity) are selected. More than one facility can be selected, using commas to separate them. For example:

```
*.emerg;mail,daemon.crit
```

selects all facilities at the **emerg** level and the **mail** and **daemon** facilities at the **crit** level.

The known facilities and levels recognized by **syslogd** are those listed in *syslog*(3C) converted to lowercase without the leading **LOG_**. The additional facility **mark** has a message at priority **LOG_INFO** sent to it every 20 minutes (this can be changed with the **-m** flag). The **mark** facility is not enabled by a facility field containing an asterisk. The level **none** can be used to disable a particular facility. For example,

```
*.debug;mail.none
```

selects all messages except **mail** messages.

The second part of each line describes where the message is to be logged if this line is selected. There are four forms:

- A file name (beginning with a leading slash). The file is opened in append mode. If the file does not exist, it is created.
- A host name preceded by an **@** character. Selected messages are forwarded to the **syslogd** on the named host.
- A comma-separated list of users. Selected messages are written to those users' terminals if they are logged in.
- An asterisk. Selected messages are written to the terminals of all logged-in users.

Blank lines and lines beginning with a **#** character are ignored.

For example, the configuration file:

```
kern,mark.debug   /dev/console
mail.debug        /var/adm/syslog/mail.log
*.info;mail.none  /var/adm/syslog/syslog.log
*.alert           /dev/console
*.alert           root,eric,kridle
*.emerg           *
*.emerg           @admin
```

S

logs all kernel messages and 20 minute marks onto the system console, all mail system messages to **/var/adm/syslog/mail.log**, and all messages at **info** and above, except mail messages, to the file **/var/adm/syslog/syslog.log**. Messages at **alert** and above are logged to the console and to the users **root**, **eric**, and **kridle** if they are logged in. **emerg** messages are written to all logged-in users' terminals, and forwarded to the host **admin**.

Only a superuser can invoke **syslogd**.

Notes

syslogd logs messages into a set of files. Once the size of a log file reaches 2 GB, **syslogd** stops logging to that file. You can configure the maximum size of **syslogd** log files by setting the variable **LOG_SIZE** in **/etc/default/syslogd**. The values of **LOG_SIZE** can be any positive integer greater than 2, representing the maximum size of the file in GB. When **LOG_SIZE=NOLIMIT**, **syslogd** uses the limit imposed by the file system on file size.

syslogd logs messages in a locale-independent fashion as a stream of bytes and will replace each newline character in the message with a blank space except for the last newline character. Applications using the services of **syslogd** can log messages in different locales. However, be careful when configuring **syslogd** so that messages from different locales do not get logged to the same log file.

WARNINGS

A configuration file selector selects all messages at the specified level *or higher*. The configuration lines:

```
user.debug          /tmp/logfile
user.info           /tmp/logfile
```

cause the logfile to get *two* copies of all **user** messages at level **info** and above.

Kernel panic messages are not sent to **syslogd**.

All HP-UX kernel messages are treated as if they had the **crit** priority level.

If **syslogd** is invoked with the **-D** option and **syslogd** terminates abnormally, kernel messages will not appear on the system console. In that case, reinvoke **syslogd** without the **-D** option to enable the kernel to send its messages to the system console.

syslogd does not support logging to **named pipes**. Therefore, if a named pipe is specified in the configuration file, the behavior of **syslogd** is undefined, and **syslogd** may lose messages if blocked or terminated on a **SIGPIPE**.

syslogd does not support long user and group names on the current release, HP-UX 11i V3.

syslogd logs messages in a locale-independent fashion.

- **syslogd** assumes that ASCII control characters do not form intermediate bytes of the characters of a multibyte locale.
- **syslogd** truncates the last character when the maximum length of the message **LINE_MAX** is reached, even though it is a valid multibyte character.

AUTHOR

syslogd was developed by the University of California, Berkeley.

FILES

/dev/klog	The kernel log device
/dev/log	The named pipe on which **syslogd** reads log messages
/dev/log.un	The UNIX domain socket on which **syslogd** reads log messages
/etc/syslog.conf	Configuration file
/etc/default/syslogd	Configuration file for maximum log size
/var/run/syslog.pid	Process ID

SEE ALSO

logger(1), syslog(3C).

S

S