NAME

syslogd - log systems messages

SYNOPSIS

syslogd [**-468ACcdFHkNnosTuv**] [**-a** *allowed_peer*] [**-b** *bind_address*] [**-f** *config_file*] [**-l** [*mode*:]*path*] [**-M** *fwd_length*] [**-m** *mark_interval*] [**-O** *format*] [**-P** *pid_file*] [**-p** *log_socket*] [**-S** *logpriv_socket*]

DESCRIPTION

The **syslogd** utility reads and logs messages to the system console, log files, other machines and/or users as specified by its configuration file.

The options are as follows:

-4 Force **syslogd** to use IPv4 addresses only.

-6 Force **syslogd** to use IPv6 addresses only.

-8 Tells **syslogd** not to interfere with 8-bit data. Normally **syslogd** will replace C1 control characters (ISO 8859 and Unicode characters) with their "M-*x*" equivalent. Note, this option does not change the way **syslogd** alters control characters (see iscntrl(3)). They will always be replaced with their "^*x*" equivalent.

-A Ordinarily, **syslogd** tries to send the message to only one address even if the host has more than one A or AAAA record. If this option is specified, **syslogd** tries to send the message to all addresses.

-a *allowed_peer*

Allow *allowed_peer* to log to this **syslogd** using UDP datagrams. Multiple **-a** options may be specified.

The *allowed_peer* option may be any of the following:

ipaddr[/*masklen*][:*service*]
ipaddr[/*prefixlen*][:*service*] Accept datagrams from *ipaddr*, *ipaddr* can be specified as an IPv4 address or as an IPv6 address enclosed with '[' and ']'. If specified, *service* is the name or number of an UDP service (see services(5)) the source packet must belong to. A *service* of '*' accepts UDP packets from any source port. The default *service* is 'syslog'. If *ipaddr* is IPv4 address, a missing *masklen* will be

substituted by the historic class A or class B netmasks if *ipaddr* belongs into the address range of class A or B, respectively, or by 24 otherwise. If *ipaddr* is IPv6 address, a missing *masklen* will be substituted by 128.

domainname[:*service*] Accept datagrams where the reverse address lookup yields *domainname* for the sender address. The meaning of *service* is as explained above. *domainname* can contain special characters of a shell-style pattern such as '*'.

The **-a** options are ignored if the **-s** option is also specified.

-b *bind_address*[:*service*]

-b :*service*

Bind to a specific address and/or port. The address can be specified as a hostname, and the port as a service name. If an IPv6 address is specified, it should be enclosed with '[' and ']'. The default *service* is 'syslog'. This option can be specified multiple times to bind to multiple addresses and/or ports.

-C Create log files that do not exist (permission is set to '0600').

-c Disable the compression of repeated instances of the same line into a single line of the form "last message repeated N times" when the output is a pipe to another program. If specified twice, disable this compression in all cases.

-d Put **syslogd** into debugging mode. This is probably only of use to developers working on **syslogd**.

-f *config_file*

Specify the pathname of an alternate configuration file; the default is */etc/syslog.conf*.

-F Run **syslogd** in the foreground, rather than going into daemon mode. This is useful if some other process uses fork(2) and exec(3) to run **syslogd**, and wants to monitor when and how it exits.

-H When logging remote messages use hostname from the message (if supplied) instead of using address from which the message was received.

-k Disable the translation of messages received with facility "kern" to facility "user". Usually the "kern" facility is reserved for messages read directly from */dev/klog*.

-M *fwd_length*

Set the limit on the length of forwarded messages. The minimum is 480 octets. The maximum for RFC 3164 output format is 1024 octets. The default is 1024 octets.

-m *mark_interval*

Select the number of minutes between "mark" messages; the default is 20 minutes.

-N Disable binding on UDP sockets. RFC 3164 recommends that outgoing **syslogd** messages should originate from the privileged port, this option *disables* the recommended behavior. This option inherits **-s**.

-n Disable DNS query for every request.

-O *format*

Select the output format of generated log messages. The values *bsd* and *rfc3164* are used to generate RFC 3164 log messages. The values *syslog* and *rfc5424* are used to generate RFC 5424 log messages, having RFC 3339 timestamps with microsecond precision. The default is to generate RFC 3164 log messages.

-o Prefix kernel messages with the full kernel boot file as determined by getbootfile(3). Without this, the kernel message prefix is always "kernel:".

-p *log_socket*

Specify the pathname of an alternate log socket to be used instead; the default is */var/run/log*. When a single **-p** option is specified, the default pathname is replaced with the specified one. When two or more **-p** options are specified, the remaining pathnames are treated as additional log sockets.

-P *pid_file*

Specify an alternative file in which to store the process ID. The default is */var/run/syslog.pid*.

-S *logpriv_socket*

Specify the pathname of an alternate log socket for privileged applications to be used instead; the default is */var/run/logpriv*. When a single **-S** option is specified, the default pathname is replaced with the specified one. When two or more **-S** options are specified, the remaining pathnames are treated as additional log sockets.

-l [*mode*:]*path*

Specify a location where **syslogd** should place an additional log socket. The primary use for this is to place additional log sockets in */var/run/log* of various chroot filespaces. File permissions

for socket can be specified in octal representation in *mode*, delimited with a colon. The socket location must be specified as an absolute pathname in *path*.

-s Operate in secure mode. Do not log messages from remote machines. If specified twice, no network socket will be opened at all, which also disables logging to remote machines.

-T Always use the local time and date for messages received from the network, instead of the timestamp field supplied in the message by the remote host. This is useful if some of the originating hosts cannot keep time properly or are unable to generate a correct timestamp.

-u Unique priority logging. Only log messages at the specified priority. Without this option, messages at the stated priority or higher are logged. This option changes the default comparison from "=>" to "=".

-v Verbose logging. If specified once, the numeric facility and priority are logged with each locally-written message. If specified more than once, the names of the facility and priority are logged with each locally-written message.

This option only affects the formatting of RFC 3164 messages. Messages formatted according to RFC 5424 always include a facility/priority number.

The **syslogd** utility reads its configuration file when it starts up and whenever it receives a hangup signal. For information on the format of the configuration file, see syslog.conf(5).

The **syslogd** utility reads messages from the UNIX domain sockets */var/run/log* and */var/run/logpriv*, from an Internet domain socket specified in */etc/services*, and from the special device */dev/klog* (to read kernel messages).

The **syslogd** utility creates its process ID file, by default */var/run/syslog.pid*, and stores its process ID there. This can be used to kill or reconfigure **syslogd**.

The message sent to **syslogd** should consist of a single line. The message can contain a priority code, which should be a preceding decimal number in angle braces, for example, '<5>'. This priority code should map into the priorities defined in the include file <*sys/syslog.h*>.

For security reasons, **syslogd** will not append to log files that do not exist (unless **-C** option is specified); therefore, they must be created manually before running **syslogd**.

The date and time are taken from the received message. If the format of the timestamp field is incorrect, time obtained from the local host is used instead. This can be overridden by the **-T** flag.

FILES

/etc/syslog.conf	configuration file
/var/run/syslog.pid	default process ID file
/var/run/log	name of the UNIX domain datagram log socket
/var/run/logpriv	UNIX socket for privileged applications
/dev/klog	kernel log device

SEE ALSO

logger(1), syslog(3), services(5), syslog.conf(5), newsyslog(8)

HISTORY

The **syslogd** utility appeared in 4.3BSD.

The **-a**, **-s**, **-u**, and **-v** options are FreeBSD 2.2 extensions.

BUGS

The ability to log messages received in UDP packets is equivalent to an unauthenticated remote disk-filling service, and should probably be disabled by default. Some sort of inter-**syslogd** authentication mechanism ought to be worked out. To prevent the worst abuse, use of the **-a** option is therefore highly recommended.

The **-a** matching algorithm does not pretend to be very efficient; use of numeric IP addresses is faster than domain name comparison. Since the allowed peer list is being walked linearly, peer groups where frequent messages are being anticipated from should be put early into the **-a** list.

The log socket was moved from */dev* to ease the use of a read-only root file system. This may confuse some old binaries so that a symbolic link might be used for a transitional period.