NAME

lsyslog − Capture, process, and redirect syslog messages.

SYNOPSIS

lsyslog [[-r]|[-k]] [-f <config_file>] | [-h]

DESCRIPTION

lsyslog is a syslog daemon that listens for remote syslog messages and then applies a ruleset to those incomming messages. It will act as a syslog "router" that channels messages based upon the ruleset you define. The rules will determine if the incomming message is sent onto another destination or will be dropped.

Messages can be forwarded onto HP´s ITO console, a web page, or to a flat file. (The primary design was to send the syslog message to an ITO server.)

Rules for processing messages are read in order from a rules file. Each rule can be a combination of tests for hostname, priority, facility, and string match.

USAGE

To utilize the service, all servers should point thier syslog at the host running lsyslog. Each server should have a line similar to following in their syslog.conf:

```
*.*                          @lsysloghost.domain.com
```

This line will send ALL messages regardless of facility and priority to the lsyslog server. Here they will be processed based upon the rules defined in the lsyslog.rules file.

RULES

Rules are read, in order, one per line from a rules file. The rules have the syntax of: if <test> and <test> then <action>

The tests take the form of item=value. Such as facility=SYSLOG, hostname=server1, or string="core dump".

The action is one of the ITO message priroty levels or the word drop. This is the action to perform on the message if this rule is triggerd. If the action is drop then it will be dropped. If it is one of the priority levels then it will be forwarded on with that priority.

If no rule is matched, then the message "falls through" and is dropped by default. It is not necessary to explicitly drop messages but it may be advantageous to insert drop rules at the top of the ruleset so that each rule does not need to be applied to frequently recieved messages.

Example 1:

This rule will drop all mail messages. This rule would most likely be used near the top of the ruleset to explicitly drop all mail related messages if there are a significant number of mail related messages recieved and they need to be dropped early in a complex ruleset to conserve processing power.

```
if facility=mail then drop
```

Example 2:

This rule will forward on messages from server1´s kernel that contain the word failure as critical messages.

if hostname=server1 and string=failure and facility=kernel then critical

Example 3:

This rule will drop all cron.info messages.

if facility=cron and priority=info then drop

Example 4:

This rule will look for a specific string. Note here that quotes are allowed to include white-space in the search. Also note that the search is case-insensitive.

if string="synchronisation lost" then warning

The rules are read from a file specified in the *RULES_FILE* option in the config file.

The options for facility are AUTH, AUTHPRIV, CRON, DAEMON, FTP, KERN, LOCAL0 - LOCAL7, LPR, MAIL, NEWS, SYSLOG, USER, and UUCP.

The options for priority are EMERG, ALERT, CRIT, ERR, WARNING, NOTICE, INFO, and DEBUG.

The actions take two forms, either drop or forward on with a specific level of priority. The valid action names are drop, critical, major, minor, warning, and normal.

Comments (lines beginning with # characters) and blank lines are ignored in the rules file. Test phrases, such as priority=ALERT, must not contain white space. Only one rule is allowed per line.

When setting up a rule file it is recommended to enable the **PARSED_RULES_FILE** option to verify that the rules are read as expected.

OPTIONS

−r Reload ruleset for the currently running daemon. The config options are NOT reloaded.

The config file can be passed with the -f option to specify an alternate config file. The only purpose of the -f option would be to specify a different **PID_FILE** as this is the only config file option used with the -r or -k parameters.

−h Display help and usage information.

−k Kill the currently running daemon.

The config file can be passed with the -f option to specify an alternate config file. The only purpose of the -f option would be to specify a different **PID_FILE** as this is the only config file option used with the -r or -k parameters.

−f Load from an alternate config file.

MAIN CONFIG FILE OPTIONS

MAX_HTML_MESSAGES

(integer) Default: 100

This is the maximum number of messages will be kept in the html page. As new messages are appended to the page, older messages will be pushed off the page.

HTTP_REFRESH_INTERVAL
(integer) Default: 60

If the messages are sent to a HTML page then the resulting page will have a meta-refresh tag with the timer in this many seconds.

PID_FILE
(string) Default: /var/run/lsyslog

This is the file that will hold the pid of lsyslog when it runs as a daemon.

RULE_FILE
(string) Default: /etc/lsyslog.rules

This is the (input) file of rules that will become the ruleset. See the **RULES** section for a description of the format of this file.

REJECT_FILE
(string) Default: None - This is required if **LOG_REJECTS** is enabled.

This is the name of the file that will recieve all rejects (messages that have been dropped.) This must be set if **LOG_REJECTS** is used.

This file is typically used to debug your rule set to insure that important messages are not dropped. A tail can be placed on this file so the user can see what messages are dropped by the current rule set.

MESSAGE_FILE
(string) Default: None - This is required if **MESSAGE_DESTINATION** uses a file.

This is the recipient file of every message that passes a rule and is not rejected.

ITO_GROUP
(string) Default: None - This is required if **MESSAGE_DESTINATION** is set to ITO.

This is also read as **SOC_GROUP** and works the same for ITO and SOC.

This is the ITO / SOC group of messages sent to ITO (via the ITO api) or SOC.

ITO_APP
(string) Default: lsyslog

This is also read as **SOC_APP** and works the same for ITO and SOC.

This is the application name of messages sent to ITO (via the ITO api) or SOC.

ITO_OBJ

(string) Default: syslog

This is also read as **SOC_SECTION** and works the same for ITO and SOC.

This is the object name of messages sent to ITO (via the ITO api) or the section name for messages sent to SOC.

PARSED_RULES_FILE

(string) Default: None

If this value is set, the rules will be dumped (after they are parsed) to this file. This has several benifits in that it verifies the rules have been read, it tells what rules lsyslog is currently running under, and it is useful for debugging if **INCLUDE_RULE_NUMBER** is enabled.

LOG_REJECTS

(enum: TO_FILE ON AS_HTML OFF) Default: OFF

Enable **LOG_REJECTS** to see what messages are dropped by the current ruleset. This should be enabled when the system is first set up to test the rules. If the ruleset is not set up correctly, important messages could be lost. This serves to prevent this problem.

MESSAGE_DESTINATION

(enum: ITO ITO_FILE SOC FILE AS_HTML SYSLOG RSYSLOG) Default: ITO_FILE

Set this value to the desired recipeint of messages that have passed a rule. The possible values are:

ITO - Send directly to ITO console using ITO API. This requires the ITO agent be installed on the system and that the lsyslog binary was compiled and linked against this package.

ITO_FILE - This appends the message to a file that can be parsed by an ITO agent. Use this if you prefer to have a more permenant log on the local system. (If the message is sent directly to ITO via the API there is no guarentee of delivery.)

SOC - Send to a socndp (Systems Operations Console Notification Delivery point) daemon. The **SOC_NDP_HOST** parameter must be set to use this.

FILE - This appends the message to a file. It differs slightly from ITO_FILE in that it is not formatted the same.

AS_HTML - Send messages to a HTML formatted file. Old messages fall off the list as new messages are appended.

SYSLOG - Send to the local syslog daemon.

RSYSLOG - Send to a remote syslog daemon or another lsyslog daemon. Requires the **REMOTE_SYSLOG** parameter to be set.

ALT_MSG_DEST

This is the same as **MESSAGE_DESTINATION** but is an alternate, or second, location for messages. If it is omitted then an alternate location is not used. This parameter uses the same values for other settings as does **MESSAGE_DESTINATION** so they are shared between the two. (A second set of config options for things like group and object do not exist for this target.)

HTML_WRAPPER

(enum: ON OFF) Default: ON

If this is enabled, HTML output to **MESSAGE_DESTINATION** is wrapped in a HTML header and footer. If it is turned off the file must be used as a server side include or used in a similar fasion.

INCLUDE_RULE_NUMBER

(enum: ON OFF) Default: OFF

Turn this on to include the rule number of the pass or drop in the output. This should be used in conjunction with **PARSED_RULES_FILE** to determine what the rule numbers are.

SOC_NDP_HOST

(string) Default: none

This is a required hostame parameter of the SOC NDP daemon if the **MESSAGE_DESTINATION** is set to SOC.

SOC_NDP_PORT

(integer) Default: 5140

This is an optional port parameter of the SOC NDP daemon if the **MESSAGE_DESTINATION** is set to SOC.

SOC_UID

(integer) Default: 0

This is an optional SOC UID (Unique message ID) for the SOC message destination.

LOCAL_HOSTNAME

(string) Default: The local hostname as returned by the gethostname() funciton.

Set this to an alternate hostname if you wish to act as someone else or use a CNAME.

REMOTE_SYSLOG

(string) Default: None

This is a required parameter if one of the destinations is set to RSYSLOG. This is the name of a host that is running a syslog daemon listening on port 514 (or another lsyslog daemon).

FORMAT_REMOTE_SYSLOG

(boolean: true false) Default: false

Enable (set this to true) to add formatting to the packet before it is sent to the next syslog server. This will include the formatting that is seen in many of the messages in ITO, SOC, or the file based options. If it is set to false then messages that pass the rulesets will be forwarded exactly as they were recieved.

RULE_ZERO

(enum: drop critical major minor warning normal) Default: drop

Set this as the default behavior when all rules have been exhausted. The options for this value are the same as the ruleset actions.

DEFAULT_FORMAT_STRING

(string) Default: lsyslog

This is the format string that is prepended to the output messages that show up in the various destinations.

BUGS

LOG_REJECTS=AS_HTML is currently not supported. No work is underway to add this capability as it does not seem to be terribly valuable.

The remote syslog functionality only sends to port 514.