Log Management

Document revision 2.3 (Mon Jul 19 07:23:35 GMT 2004)
This document applies to V2.9

Table of Contents

General Information

Summary

Various system events and status information can be logged. Logs can be saved in local routers file, displayed in console, sent to an email or to a remote server running a syslog daemon. MikroTik provides a shareware Windows Syslog daemon, which can be downloaded from www.mikrotik.com

Specifications

Packages required: ***system***
License required: ***level1***
Home menu level: ***/system logging, /log***
Standards and Technologies: ***Syslog***
Hardware usage: ***Not significant***

Related Documents

- Package Management

Description

Logs have different groups or topics. Logs from each topic can be configured to be discarded, logged locally

or remotely. Locally log files can be stored in memory (default; logs are lost on reboot) or on hard drive (not enabled by default as is harmful for flash disks).

General Settings

Home menu level: ***/system logging***

Property Description

topics (*info* | *critical* | *firewall* | *keepalive* | *packet* | *read* | *timer* | *write* | *ddns* | *hotspot* | *l2tp* | *ppp* | *route* | *update* | *account* | *debug* | *ike* | *manager* | *pppoe* | *script* | *warning* | *async* | *dhcp* | *info* | *notification* | *pptp* | *state* | *watchdog* | *bgp* | *error* | *ipsec* | *open* | *radius* | *system* | *web-proxy* | *calc* | *event* | *isdn* | *ospf* | *raw* | *telephony* | *wireless*; default: **info**) - specifies log group or log message type

action (*disk* | *echo* | *memory* | *remote*; default: **memory**) - specifies one of the system actions or user specified action listed in /system logging action

prefix (*name*) - local log prefix

Example

To logg messages that are generated by firewall by saving them in local buffer

```
[admin@MikroTik] system logging> add topics=firewall action=memory
[admin@MikroTik] system logging> print
 Flags: X - disabled, I - invalid
 #   TOPICS                                             ACTION PREFIX
 0   info                                               memory
 1   error                                              memory
 2   warning                                            memory
 3   critical                                           echo
 4   firewall                                           memory
[admin@MikroTik] system logging>
```

Actions

Home menu level: ***/system logging action***

Property Description

disk-lines (*integer*; default: **100**) - Used when target is set to type disk. Specifies the number of records in log file

disk-stop-on-full (yes | no; default: **no**) - Used when target is set to type disk. Specifies whether to stop to save log messages on disk after the specified disk-lines number is reached

email-to (*name*) - Used when target is set to type email, sets email address logs are sent to

memory-lines (*integer*; default: **100**) - Used when target is set to type memory. Specifies the number of records in local buffer.

memory-stop-on-full (yes | no; default: **no**) - Used when target is set to type memory. Specifies whether to stop to save log messages in local buffer after the specified memory-lines number is reached

name (*name*) - name of an action

remember (yes | no; default: **yes**) - Used when target is set to type echo. Specifies whether to keep log messages, which have not yet been displayed in console

remote (*IP address* | *port* | *IP address* | *integer*: 0..65535; default: **0.0.0.0:514**) - Used when target is set to type remote. Remote log server's IP address and UDP port

target (*disk* | *echo* | *email* | *memory* | *remote*; default: **memory**) - Specifies how to treat logs

- **disk** - logs are saved to hard drive
- **echo** - logs are displayed in console
- **email** - logs are sent by email
- **memory** - logs are saved to local buffer. They can be viewed using the '/log print' command
- **remote** - logs are sent to remote host

Notes

You cannot delete or rename default actions.

Example

To add a new action with name short, that will save logs in local buffer, if number of records in buffer are less than 50:

```
[admin@MikroTik] system logging action> add name=short \
\... target=memory memory-lines=50 memory-stop-on-full=yes
[admin@MikroTik] system logging action> print
 # FACILITY       LOCAL  REMOTE PREFIX         REMOTE-ADDRESS  REMOTE-PORT ECHO
 Flags: * - default
 #   NAME                              TARGET REMOTE
 0 * memory                            memory
 1 * disk                              disk
 2 * echo                              echo
 3 * remote                            remote 0.0.0.0:514
 4   short                             memory
[admin@MikroTik] system logging action>
```

Log Messages

Home menu level: ***/log***

Description

Displays locally stored log messages

Property Description

message (*text*) - message text

time (*text*) - date and time of the event

Command Description

print - shows log messages

- **buffer** - prints log messages that were saved in specified local buffer

- **follow** - monitor system logs
- **without-paging** - prints logs without paging
- **file** - saves the log information on local ftp server with a specified file name

Example

To view the local logs:

```
[admin@MikroTik] > log print
 TIME                 MESSAGE
 dec/24/2003 08:20:36 log configuration changed by admin
 dec/24/2003 08:20:36 log configuration changed by admin
 dec/24/2003 08:20:36 log configuration changed by admin
 dec/24/2003 08:20:36 log configuration changed by admin
 dec/24/2003 08:20:36 log configuration changed by admin
 dec/24/2003 08:20:36 log configuration changed by admin
-- [Q quit|D dump]
```

To monitor the system log:

```
[admin@MikroTik] > log print follow
 TIME                 MESSAGE
 dec/24/2003 08:20:36 log configuration changed by admin
 dec/24/2003 08:24:34 log configuration changed by admin
 dec/24/2003 08:24:51 log configuration changed by admin
 dec/24/2003 08:25:59 log configuration changed by admin
 dec/24/2003 08:25:59 log configuration changed by admin
 dec/24/2003 08:30:05 log configuration changed by admin
 dec/24/2003 08:30:05 log configuration changed by admin
 dec/24/2003 08:35:56 system started
 dec/24/2003 08:35:57 isdn-out1: initializing...
 dec/24/2003 08:35:57 isdn-out1: dialing...
 dec/24/2003 08:35:58 Prism firmware loading: OK
 dec/24/2003 08:37:48 user admin logged in from 10.1.0.60 via telnet
-- Ctrl-C to quit. New entries will appear at bottom.
```