Log Management

Document revision 2.3 (Mon Jul 19 07:23:35 GMT 2004)
This document applies to MikroTik RouterOS V2.8

Table of Contents

General Information

Summary

Various system events and status information can be logged. Logs can be saved in a file on the router, or sent 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

The logging feature sends all of your actions on the router to a log file or to a logging daemon.

Router has several global configuration settings that are applied to logging. Logs have different facilities. Logs from each facility can be configured to be discarded, logged locally or remotely. 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

default-remote-address (*IP address*; default: **0.0.0.0**) - remote log server IP address. Used when remote logging is enabled but no IP address of the remote server is specified

default-remote-port (*integer*; default: **0**) - remote log server UDP port. Used when remote logging is enabled but no UDP port of the remote server is specified

disk-buffer-lines (*integer*; default: **100**) - number of lines kept on hard drive

memory-buffer-lines (*integer*; default: **100**) - number of lines kept in memory

Example

To use the **10.5.13.11** host, listening on **514** port, as the default remote system-log server:

```
[admin@MikroTik] system logging> set default-remote-address=10.5.13.11
default-remote-port=514
[admin@MikroTik] system logging> print
    default-remote-address: 10.5.13.11
       default-remote-port: 514
         disk-buffer-lines: 100
       memory-buffer-lines: 100
[admin@MikroTik] system logging>
```

Log Classification

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

Property Description

echo (*yes* | *no*; default: **no**) - whether to echo the message of this type to the active (logged-in) consoles

facility (*name*) - name of the log group, message type

local (*disk* | *memory* | *none*; default: **memory**) - how to treat local logs

- **disk** - logs are saved to hard drive
- **memory** - logs are saved to local buffer. They can be viewed using the '/log print' command
- **none** - logs from this source are discarded

prefix (*text*; default: **""**) - local log prefix

remote (*none* | *syslog*; default: **none**) - how to treat logs that are sent to remote host

- **none** - do not send logs to a remote host
- **syslog** - send logs to remote syslog daemon

remote-address (*IP address*; default: "") - remote log server's IP address. Used when logging type is remote. If not set, default log server's IP address is used

remote-port (*integer*; default: **0**) - remote log server UDP port. Used when logging type is remote. If not set, default log server UDP port is used

Notes

You cannot add, delete or rename the facilities: they are added and removed with the packages they are associated with.

System-Echo facility has its default **echo** property set to **yes**.

Example

To force the router to send **Firewall-Log** to the 10.5.13.11 server:

```
[admin@MikroTik] system logging facility> set Firewall-Log remote=syslog \
\... remote-address=10.5.13.11  remote-port=514
[admin@MikroTik] system logging facility> print
 # FACILITY       LOCAL  REMOTE PREFIX         REMOTE-ADDRESS  REMOTE-PORT ECHO
 0 Firewall-Log   memory syslog                10.5.13.11      514         no
 1 PPP-Account    memory none                  0.0.0.0         0           no
 2 PPP-Info       memory none                  0.0.0.0         0           no
 3 PPP-Error      memory none                  0.0.0.0         0           no
 4 System-Info    memory none                  0.0.0.0         0           no
 5 System-Error   memory none                  0.0.0.0         0           no
 6 System-Warning memory none                  0.0.0.0         0           no
 7 Telephony-Info memory none                  0.0.0.0         0           no
 8 Telephony-E... memory none                  0.0.0.0         0           no
 9 Prism-Info     memory none                  0.0.0.0         0           no
10 Web-Proxy-A... memory none                  0.0.0.0         0           no
11 ISDN-Info      memory none                  0.0.0.0         0           no
12 Hotspot-Acc... memory none                  0.0.0.0         0           no
13 Hotspot-Info   memory none                  0.0.0.0         0           no
14 Hotspot-Error  memory none                  0.0.0.0         0           no
15 IPsec-Event    memory none                  0.0.0.0         0           no
16 IKE-Event      memory none                  0.0.0.0         0           no
17 IPsec-Warning  memory none                  0.0.0.0         0           no
18 System-Echo    memory none                  0.0.0.0         0           yes
[admin@MikroTik] system logging facility>
```

Log Messages

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

Description

Some log entries, like those containing information about user logout event, contain additional information about connection. These entries have the following format: `<time> <user> logged out, <connection-time-in-seconds> <bytes-in> <bytes-out> <packets-in> <packets-out>`

Property Description

message (*text*) - message text

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

Notes

print command has the following arguments:

- **follow** - monitor system logs
- **without-paging** - print the log without paging
- **file** - saves the log information to ftp 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.
```