

NMIS9 - How to Configure High Volume SNMPTRAPS

- [Introduction](#)
- [Step-by-Step How to Configure the SNMPTRAPS to Forward Traps to Syslog](#)
 - [RHEL/CENTOS Linux](#)
 - [Debian/Ubuntu Linux](#)

Introduction

Configure SNMPTRAPS to scale up to 300 traps per second. The purpose of this article is to show how to configure the SNMPTRAPD to pull data from the devices to rsyslog. Then, the rsyslog collects the logs into a file to be processed by opEvents. Eventually, the opEvents will apply the filters, parsers, and actions to better use the system management, analysis, and troubleshooting based on the events.

Testing SNMPTRAPS:

```
snmptranslate -m ALL -M /usr/local/nmis9/mibs/traps 1.3.6.1.4.1.9.9.43.1.1.6.1.5.34
```

```
*****
```

RESULT: CISCO-CONFIG-MAN-MIB::ccmHistoryEventConfigDestination.34

```
*****
```

```
sudo snmptrap -v 2c -c public 127.0.0.1 80000 1.3.6.1.4.1.4818 1.3.6.1.4.1.4818.1 s Event
```

```
192.168.0.111 x
[omkadmin@omk-vm9-centos7 logs]$
[omkadmin@omk-vm9-centos7 logs]$
[omkadmin@omk-vm9-centos7 logs]$ pwd
/usr/local/nmis9/logs
[omkadmin@omk-vm9-centos7 logs]$ snmptranslate -m ALL -M /usr/local/nmis9/mibs/traps 1.3.6.1.4.1.9.9.43.1.1.6.1.5.34
CISCO-CONFIG-MAN-MIB::ccmHistoryEventConfigDestination.34
[omkadmin@omk-vm9-centos7 logs]$ sudo snmptrap -v 2c -c public 127.0.0.1 80000 1.3.6.1.4.1.4818 1.3.6.1.4.1.4818.1 s Event_gladston
[sudo] password for omkadmin:
[omkadmin@omk-vm9-centos7 logs]$ tail -f trap.log
2023-03-22T10:29:34 localhost: UDP: [127.0.0.1]:52139->[127.0.0.1]:162 RFC1213-MIB::sysUpTime.0=0:0:13:20.00 SNMPv2
-MIB::snmpTrapOID.0=OPMANTEK-MIB::opmantek OPMANTEK-MIB::omkNotifications="Event"
2023-03-22T10:29:36 localhost: UDP: [127.0.0.1]:36863->[127.0.0.1]:162 RFC1213-MIB::sysUpTime.0=0:0:13:20.00 SNMPv2
-MIB::snmpTrapOID.0=OPMANTEK-MIB::opmantek OPMANTEK-MIB::omkNotifications="Event"
2023-03-22T10:33:33 localhost: UDP: [127.0.0.1]:40169->[127.0.0.1]:162 RFC1213-MIB::sysUpTime.0=0:0:13:20.00 SNMPv2
-MIB::snmpTrapOID.0=OPMANTEK-MIB::opmantek OPMANTEK-MIB::omkNotifications="Event"
2023-03-22T10:33:53 localhost: UDP: [127.0.0.1]:41828->[127.0.0.1]:162 RFC1213-MIB::sysUpTime.0=0:0:13:20.00 SNMPv2
-MIB::snmpTrapOID.0=OPMANTEK-MIB::opmantek OPMANTEK-MIB::omkNotifications="Event"
2023-03-22T10:34:17 localhost: UDP: [127.0.0.1]:41872->[127.0.0.1]:162 RFC1213-MIB::sysUpTime.0=0:0:13:20.00 SNMPv2
-MIB::snmpTrapOID.0=OPMANTEK-MIB::opmantek OPMANTEK-MIB::omkNotifications="Gladston"
2023-03-22T10:35:05 localhost: UDP: [127.0.0.1]:39421->[127.0.0.1]:162 RFC1213-MIB::sysUpTime.0=0:0:13:20.00 SNMPv2
-MIB::snmpTrapOID.0=OPMANTEK-MIB::opmantek OPMANTEK-MIB::omkNotifications="Event_gladston"
```

Step-by-Step How to Configure the SNMPTRAPS to Forward Traps to Syslog

OBSERVATION: The "Ls" option will configure snmptrapd to send logs to syslog. So, "Ls2" specifically configures snmptrapd to send logs from the local2 facility. The facility is a value that indicates which process on the device generated the message.

STEP 1

RHEL/CENTOS Linux

```
cd /etc/sysconfig/
```

```
vim snmptrapd
```

```
192.168.0.111 x
[omkadmin@omk-vm9-centos7 /]$
[omkadmin@omk-vm9-centos7 /]$
[omkadmin@omk-vm9-centos7 /]$
[omkadmin@omk-vm9-centos7 /]$ cd /etc/sysconfig/
[omkadmin@omk-vm9-centos7 sysconfig]$ vim snmptrapd
```

[illegible]

```
root@nmis-primary-1:/#  
root@nmis-primary-1:/#  
root@nmis-primary-1:/#  
root@nmis-primary-1:/# cd /etc/default/  
root@nmis-primary-1:/etc/default# ll | grep -i snmptrapd  
-rw-r--r--  1 root root  332 Jun 23  2020 snmptrapd  
root@nmis-primary-1:/etc/default# vim snmptrapd
```

```
ExecStart=/usr/sbin/snmptrapd -n -OQ -Ls2 -p /var/run/snmptrapd.pid -m ALL -M /usr/local/nmis9/mibs/traps
```

root@opmantek-la-poller: /etc/default

```
# This file controls the behaviour of /etc/init.d/snmptrapd
# but not of the corresponding systemd service file.
# If needed, create an override file in
# /etc/systemd/system/snmptrapd.service.d/local.conf
# see man 5 systemd.unit and man 5 systemd.service

# snmptrapd options (use syslog).
TRAPDOPTS='-n -OQ -Ls2 -p /var/run/snmptrapd.pid -m ALL -M /usr/local/nmis9/mibs/traps'
[service]
ExecStart=
ExecStart=/usr/sbin/snmptrapd -n -OQ -Ls2 -p /var/run/snmptrapd.pid -m ALL -M /usr/local/nmis9/mibs/traps
```

STEP 2

We need to configure the traps to go to a specific log file for opEvents to process them. In this case, all messages that come from facility local2 will be collected into /usr/local/nmis9/logs/snmptrap.log file.

cd /etc/rsyslog.d

touch nmis.conf

192.168.0.111 x

```
[root@omk-vm9-centos7 /]#
[root@omk-vm9-centos7 /]#
[root@omk-vm9-centos7 /]# cd /etc/rsyslog.d
[root@omk-vm9-centos7 rsyslog.d]# touch nmis.conf
[root@omk-vm9-centos7 rsyslog.d]# ll
total 4
-rw-r--r--. 1 root root 49 Jan 13 2022 listen.conf
-rw-r--r--. 1 root root  0 Mar 22 14:13 nmis.conf
[root@omk-vm9-centos7 rsyslog.d]#
```

vim nmis.conf

local2.* /usr/local/nmis9/logs/snmptrap.log

192.168.0.111 x

```
local2.* /usr/local/nmis9/logs/snmptrap.log

"nmis.conf" 3L, 61C
```

cd /etc

vim rsyslog.conf

```
192.168.0.111 x
[root@omk-vm9-centos7 ~]#
[root@omk-vm9-centos7 ~]#
[root@omk-vm9-centos7 ~]#
[root@omk-vm9-centos7 ~]# cd /etc
[root@omk-vm9-centos7 etc]# vim rsyslog.conf
```

*.info;mail.none;authpriv.none;cron.none;local2.none /var/log/messages

```
192.168.0.111 x
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.* /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none;local2.none /var/log/messages

# The authpriv file has restricted access.
authpriv.* /var/log/secure

# Log all the mail messages in one place.
mail.* -/var/log/maillog

# Log cron stuff
cron.* /var/log/cron

# Everybody gets emergency messages
*.emerg *

# Save news errors of level crit and higher in a special file.
uucp,news.crit /var/log/spooler

# Save boot messages also to boot.log
local7.* /var/log/boot.log
local3.* /usr/local/nmis9/logs/cisco.log
local1.* /usr/local/nmis9/logs/poller_event.log
local4.* /usr/local/nmis9/logs/apc.log
local5.* /usr/local/nmis9/logs/cyber.log

### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
```

STEP 3

Now, we need to inform OpEvents where the snmptrap comes from. So, we do so, informing the path where the snmptrap.log is on the /usr/local/omk/conf /opCommon.json.

Be careful with this opCommon.json file. It is a Perl hash, so any syntax error will render the OMK Server to stop working properly.

We recommend always creating a backup of this file before any changes.

cd /usr/local/omk/conf/

vim opCommon.json

```
192.168.0.111 x
[root@omk-vm9-centos7 ~]#
[root@omk-vm9-centos7 ~]#
[root@omk-vm9-centos7 ~]# cd /usr/local/omk/conf/
[root@omk-vm9-centos7 conf]# vim opCommon.json
```

```

192.168.0.111 x
"opevents_import_nodes_activated" : "true",
"opevents_associate_outage_term" : "planned_outage",
"opevents_gui_current_events_priorities_lower" : 3,
"opevents_realtime_push_on_key" : [],
"opevents_no_action_on_flap" : "true",
"opevents_event_status_enabled" : "false",
"opevents_auto_acknowledge" : "true",
"opevents_logs" : {
  "tivoli_log" : [
    "omis9_logs>/tivoli.log"
  ],
  "cisco_compatible" : [
    "omis9_logs>/cisco.log"
  ],
  "omis_eventlog" : [
    "omis9_logs>/event.log"
  ],
  "winlogd" : [
    "omis9_logs>/winlogd.log"
  ],
  "cyber_log" : [
    "omis9_logs>/cyber.log"
  ],
  "traplog" : [
    "omis9_logs>/trap.log"
  ],
  "snmptraps" : [
    "omis9_logs>/snmptrap.log"
  ],
  "apc_log" : [
    "omis9_logs>/apc.log"
  ]
},
"opevents_hostname" : "",

```

STEP 4

The parser is made on the EventParserRules.json file. In this case, we are sending to an opEvents plugin to do the syntax translation.

```
cd /usr/local/omk/conf/
```

```
vim EventParserRules.json
```

```

192.168.0.111 x
[root@omk-vm9-centos7 ~]#
[root@omk-vm9-centos7 ~]#
[root@omk-vm9-centos7 ~]#
[root@omk-vm9-centos7 ~]# cd /usr/local/omk/conf/
[root@omk-vm9-centos7 conf]# vim EventParserRules.json

```

```

192.168.0.111 x
{
  "snmptraps" : {
    "1" : {
      "IF" : 1
      "THEN" : ["plugin(snmpTrap)"]
    },
  },
  "winlogd" : {
    "1" : {
      "IF" : "\\w+\\\\[\\d+\\\\]",
      "THEN" : {
        "30" : {
          "IF" : "The\\s+(.)\\\\s+service",
          "DESCRIPTION" : "The Microsoft .NET Framework NGEN v4.0.30319_x86 service entered the running state.",
          "THEN" : [
            "capture(element)"
          ]
        },
        "31" : {
          "IF" : "service entered the running state",
          "THEN" : [
            "set.state(up)",
            "set.stateful(Service)",
            "set.priority(0)"
          ]
        },
        "21" : {
          "THEN" : [
            "capture(category,user,details)"
          ],
          "IF" : "Category:[\\\\w\\\\ ]{0,256}); User:[\\\\w\\\\ ]{0,256}); (.+)$"
        },
        "32" : {
          "THEN" : [
            "capture(category,user,details)"
          ]
        }
      ]
    },
  },
  "EventParserRules.json" 677L, 23897C
34,1

```

STEP 5

In step 4, you added the snmptraps plugin parser rules in the EventParserRules.json file. Now, we need to copy the snmpTrap.pm file on the /usr/local/omk/conf/parser_plugins/ directory. This file is the OpEvents parser plugin. The plugin is not always needed. The traps can be collected using the event handler nmis traplog. However, the plugin can parse more complex SNMP traps.

```
cd /usr/local/omk/conf/parser_plugins/
```

```
vim snmpTrap.pm
```

```

192.168.0.111 x
[root@omk-vm9-centos7 /]#
[root@omk-vm9-centos7 /]#
[root@omk-vm9-centos7 /]# cd /usr/local/omk/conf/parser_plugins/
[root@omk-vm9-centos7 parser_plugins]# ll
total 8
-rw-rw-r--. 1 root root 2316 Apr 29 2021 README
-rw-rw-r--. 1 root root 755 Apr 29 2021 TestPlugin.pm
[root@omk-vm9-centos7 parser_plugins]# vim snmpTrap.pm

```

snmpTrap.pm file [Download here: snmpTrap.pm](#)

STEP 6

Restart the daemons associated.

```
systemctl restart rsyslog
```

```
systemctl restart opeventsd
```

```
systemctl restart snmptrapd
```

✓ 192.168.0.111 x

```
[root@omk-vm9-centos7 /]#  
[root@omk-vm9-centos7 /]#  
[root@omk-vm9-centos7 /]#  
[root@omk-vm9-centos7 /]# systemctl restart rsyslog  
[root@omk-vm9-centos7 /]# systemctl restart opeventsd  
[root@omk-vm9-centos7 /]# systemctl restart snmptrapd
```