opEvents - Syslog Handling - Adding a New Vendor

Purpose

This page will explain how to add a new node vendor in the event the default settings are not handling the syslog traps properly.

For this discussion we'll use the term 'newVendor' to be the variable that represents the new vendor we want opEvents to handle.

Steps

- Choose a unique syslog facility for the newVendor.
- Provision rsyslog to handle the traps appropriately.
- Provision opEvents to parse and process the traps.

rsyslog Provisioning

Determine what facility level these syslog traps should be stamped with. The syslog server will key on this facility level in order to send the syslog trap to the proper file. If the device syslog is very similar to Cisco then you may want to simply use the local7 facility and the syslog traps will be sent to /usr/local/nmis8/logs/cisco.log. Configure the nodes in question to send syslog to NMIS at the proper facility level. For this example we will use local6 for newVendor. Typically facilities local0 through local7 are used for processing syslog from external nodes.

Ensure the syslog server is provisioned to received traps (udp & tcp). This configuration is below and can be made on the /etc/rsyslog.conf file.

```
### /etc/rsyslog.conf

# enable network sources
module(load="imudp")
input(type="imudp" port="514")

module(load="imtcp" MaxSessions="1000" MaxListeners="50")
input(type="imtcp" port="514"

# and handle inbound/poller NMIS syslogs
local7.*                /usr/local/nmis8/logs/cisco.log
local1.*                /usr/local/nmis8/logs/poller_event.log
```

Next we'll tell rsyslog where to file messages that arrive with the facility local6.

```
### /etc/rsyslog.conf

# and handle inbound/poller NMIS syslogs
local7.*                /usr/local/nmis8/logs/cisco.log
local6.*                /usr/local/nmis8/logs/newVendor.log
local1.*                /usr/local/nmis8/logs/poller_event.log
```

After modifying /etc/rsyslog.conf the syslog daemon must be restarted.

```
[root@opmantek rsyslog.d]# service rsyslog restart
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
```

Now when syslog traps are received with facility level local6 we will see them in the /user/local/nmis8/logs/newVendor.log file. If this file does not exist it will be created automatically.

opEvents Provisioning

For the sake of this discussion let's assume the new vendor can be parsed with the existing cisco_alternate rules found in /usr/local/omk/conf/EventParserRules.nmis.

Here is a list of current vendor's in the EventParserRules.nmis

- winlogd
- junos
- cisco_compatible
- nxlog
- JuniperSyslog
- HuwaeiSylog

If need additional parsers please open a support case, you will need a sample of the syslog in order to proceed

We need to tell opEvents which parser rules to use for the new device /usr/local/nmis9/logs/newVendor.log. (or what log name that you entered in the rsyslog.conf for the new Device or new Vendor)

This is done by modifying /usr/local/omk/conf/opCommon.nmis.

Find the 'opevents_logs section and add the 'cisco_alternate', '<nmis_logs>/newVendor' relationship.

Just copy one of the examples:

Add the following lines:

'cisco_alternate' => ['<nmis_logs>/newVendor.log'],

```
### /usr/local/omk/conf/opCommon.nmis

    'opevents_logs' => {
      'cisco_alternate' => [
        '<nmis_logs>/newVendor.log'
      ],
      'cisco_syslog' => [
        '<nmis_logs>/cisco.log'
      ],
      'nmis_eventlog' => [
        '<nmis_logs>/event.log'
      ],
```

After modifying opCommon.nmis the opEvents daemon must be restarted.

```
[root@opmantek ~]# service opeventsd restart
Restarting opevents daemon opeventsd                       [  OK  ]
[root@opmantek ~]#
```

At this point you should be able to go to the Gui > Raw Logs This will allow you to verified you see the logs coming in

Create an event action policy as described here: Event Actions and Escalation

Once these actions are complete the syslog traps from newVendor should be seen in opEvents.

Related Topics

- opEvents - Syslog Handling - Adding a New Format
- opEvents - Centralized Logging Solution
- SNMP Traps with Cisco and Other devices
- High Volume SNMP Trap Processing