Interface Utilisation Alerting to IBM Tivoli NetCool using syslog

Table of contents

Summary

The NOC team of a service provider needed to get very specific alerts sent to their instance of NetCool from NMIS.

This solution leverages the nocSyslog.nmis from the NMIS Events sent to IBM Tivoli Netcool using syslog solution.

Requirement

- every X period of time, 5-15 minutes they want to collect the average interface utilisation for every interface being collected
- the average input and output interface utilisation will be calculated for the last X period of time 5 mins to X hours
- the highest utilisation of input or output will be selected, this is the interface utilisation
- the interface utilisation will be compared to a threshold level (should this be static or multi-level, e.g. just use the existing NMIS threshold values or other values)
- if the interface utilisation exceeds the threshold a special NOC event will be created.
- this can be the same as the existing NMIS events, but it needs to include the group name for the node
- all the regular features of NMIS interface alerts are excepted, which would include adding the interface description, bandwidth of the interface and the values of the threshold.

Sample event.
1388903720,NODENAME,Proactive Interface Utilisation,Critical,INTERFACENAME,INTERFACE DESCRIPTION Bandwidth=7168000: Value=93.17 Threshold=93,GROUPNAME

This event will either be sent as a syslog or logged to a file, either of which will be processed by NetCool.

Solution

An NMIS utility script which finds all the interfaces on all the nodes, performs the calculation on the interfaces and sends events to the configured syslog server.

For testing a local syslog server can be used and the facility could be local3 (configurable).

In production the syslog should be sent using TCP to ensure it arrives. The NetCool team would then process the received syslog event into NetCool.

Example syslog

```
Aug 25 17:55:01 volla interface_util_alerts.pl[4264]: NMIS_Event::volla::1661414101,asgard-pphh,Proactive
Interface Utilisation,Fatal,FastEthernet0/0,123 -- Opmantek LAN -- Bandwidth=100000000 -- Value=11.95
Threshold=10
Aug 25 17:55:01 volla interface_util_alerts.pl[4264]: NMIS_Event::volla::1661414101,asgard-pphh,Proactive
Interface Utilisation,Fatal,FastEthernet0/1,123 -- WAN -- Bandwidth=100000000 -- Value=11.92 Threshold=10
Aug 25 18:23:06 volla interface_util_alerts.pl[7621]: NMIS_Event::volla::1661415786,asgard-pphh,Proactive
Interface Utilisation,Fatal,FastEthernet0/0,123 -- Opmantek LAN -- Bandwidth=100000000 -- Value=6.48 Threshold=5
Aug 25 18:23:06 volla interface_util_alerts.pl[7621]: NMIS_Event::volla::1661415786,asgard-pphh,Proactive
Interface Utilisation,Fatal,FastEthernet0/1,123 -- WAN -- Bandwidth=100000000 -- Value=6.45 Threshold=5
```

Installation

The code for this solution is included in the NMIS9 contrib folder which is available in the installation or from NMIS9@GitHub, it will be in the folder nmis9 /contrib/interface_util_alerts

A good option to install is to create a util folder e.g. /usr/local/nmis9/util and then create a symbolic link so the file will run with the correct paths, and copy the nocSyslog.nmis to the NMIS9 conf folder

Some handy commands (sudo might be required):

```
sudo mkdir /usr/local/nmis9/util
sudo ln -s /usr/local/nmis9/contrib/interface_util_alerts/interface_util_alerts.pl /usr/local/nmis9/util
/interface_util_alerts.pl
sudo cp /usr/local/nmis9/contrib/noc_netcool_syslog/nocSyslog.nmis /usr/local/nmis9/conf
sudo /usr/local/nmis9/bin/nmis-cli act=fixperms
```

Update nocSyslog.nmis with your needed config, the options should be self explanatory except for extra_logging, which if enabled will give you some logging to nmis.log with when events are sent over syslog to NetCool.

```
%hash = (
  'syslog' => {
    'syslog_facility' => 'local3',
    'syslog_server' => 'localhost:udp:514',
    'extra_logging' => 1,
  }
);
```

Run it

To run it on a single node.

```
/usr/local/nmis9/util/interface_util_alerts.pl node=YOURNODENAME info=true
```

To run on all nodes, just run the script.

To put into production, set a cron.d file, e.g. /etc/cron.d/interface_util_alerts

```
sudo cp /usr/local/nmis9/contrib/interface_util_alerts/interface_util_alerts.crond /etc/cron.d
/interface_util_alerts
```

Check the nmis.log for debug and info messages, check the configured syslog target to see the events.

Local Syslog Testing

To test locally, add the following to /etc/rsyslog.conf for testing and restart syslogd.

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

local3.*                /usr/local/nmis9/logs/noc.log
```