Envío de eventos del Servidor Poller al Servidor Primario

En el siguiente apartado se describen las configuraciones que se han realizado para que los eventos se envíen del servidor Poller al servidor Primario, también se realizar una comprobación para validar el funcionamiento.

Configuración en el Servidor Primario

A continuación se describen los archivos que se deben considerar del lado del servidor primario. Es importante realizar un BK de los archivo que se modifican para restablecerlos si es necesario.

Se abre el siguiente archivo para editarlo.

```
vi /etc/rsyslog.conf
```

La siguiente sección debe quedar de la siguiente forma.

```
# Provides UDP syslog reception
$ModLoad imudp.so
$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp.so
$InputTCPServerRun 514

#poller NMIS servers use local1 by default, capture that into poller_event.log
local1.*                                                /usr/local/nmis8/logs/poller_event.log
```

```
# rsyslog configuration file

# For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
# If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html

#### MODULES ####

# The imjournal module bellow is now used as a message source instead of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
#$ModLoad immark  # provides --MARK-- message capability

# Provides UDP syslog reception
#$ModLoad imudp
#$UDPServerRun 514

# Provides TCP syslog reception
#$ModLoad imtcp
#$InputTCPServerRun 514


#### GLOBAL DIRECTIVES ####

# Where to place auxiliary files
$WorkDirectory /var/lib/rsyslog

# Use default timestamp format
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# File syncing capability is disabled by default. This feature is usually not required,
# not useful and an extreme performance hit
#$ActionFileEnableSync on

# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf
```

Se reinicia el servicio

```
service rsyslog restart
```

Configuración en el Servidor Poller

A continuación se describen los archivos que se deben considerar del lado del servidor poller. Es importante realizar un BK de los archivo que se modifican para restablecerlos si es necesario.

Se abre el siguiente archivo para editarlo.

```
vi /usr/local/nmis9/conf/Config.nmis
```

La siguiente sección debe quedar de la siguiente forma.

```
'syslog' => {
'syslog_events' => 'true',
'syslog_facility' => 'local1',
'syslog_server' => 'MASTER.IP.ADDRESS:tcp:514', #Se agrega la IP del Server Primario
'syslog_use_escalation' => 'false'
},

'syslog_use_escalation' => 'false' ##### envío de logs directamente #El parámetro debe estar en false
```

```
  },
  'sound' => {
    'sound_critical' => '/nmis9/events/critical.wav',
    'sound_fatal' => '/nmis9/events/critical.wav',
    'sound_levels' => '',
    'sound_major' => '/nmis9/events/major.wav',
    'sound_minor' => undef,
    'sound_normal' => undef,
    'sound_type' => 'audio/wav',
    'sound_warning' => undef
  },
  'syslog' => {
    'syslog_events' => 'true',
    'syslog_facility' => 'local1',
    'syslog_server' => '10.109.185.38:tcp:514',
    'syslog_use_escalation' => 'false'
  },
  'system' => {
    'auto_expand_more_graphs' => 'true',
    'backup_node_on_delete' => 'true',
    'buttons_in_logs' => 'false',
    'cache_summary_tables' => 'true',
```

Se abre el siguiente archivo para editarlo.

```
vi /usr/local/omk/conf/opCommon.json
```

La siguiente sección debe quedar de la siguiente forma.

```
   "opevents_logs" : {

         "nmis_pollerlog" : [
            "<nmis9_logs>/poller_event.log"
         ],
```

```
"opevents_emails" : "<omk_conf>/EventEmails.json",
"opevents_weekly_report_title" : "Weekly Summary Report",
"opevents_logs" : {
   "winlogd" : [
      "<nmis9_logs>/winlogd.log"
   ],
   "tivoli_log" : [
      "<nmis9_logs>/tivoli.log"
   ],
   "nmis_eventlog" : [
      "<nmis9_logs>/event.log"
   ],
   "traplog" : [
      "<nmis9_logs>/trap.log"
   ],
   "cisco_compatible" : [
      "<nmis9_logs>/cisco.log"
   ]
},
"opevents_reports_purge_older_than" : "730d",
"opevents_gui_default_period" : "2h",
"log_archive_enabled" : "true",
"opevents_gui_console_pagination" : [
   10,
```

Realizar el reinicio de servicios

```
service opeventsd rsyslogd nmis9d omkd restart
```

Prueba

Se realiza un prueba de envío de eventos ejecutando un tcpdump desde el Servidor Poller hacia el Servidor Primario.

```
tcpdump -s0 -A -nni eth0 host MASTER.IP.ADDRESS and port 514
```

Los resultados de la prueba se muestran como la siguiente imagen

```
m.&....G............>.....
o.^.....
13:08:46.109993 IP 10.109.210.[illegible].59786 > 10.109.185.[illegible]: Flags [P.], seq 1:274, ack 1, win 229, options [nop,nop,TS val 1878613675 ec
r 3770057411], length 273
E..E..@.@...[illegible]
m..
m.&....G............O.....
o.^.....<140>Apr 14 13:08:46 omk-vm9-centos7 nmisd worker collect Organo_Judicial_VSAT-Juzgado_Municipal_de_Besiko_PAENT037[9020]: NMIS_
Event::Poller_3::1618423725,Organo_Judicial_VSAT-Juzgado_Municipal_de_Besiko_PAENT037,Node Reset,Warning,,Old_sysUpTime=0:00:58 New_sysU
pTime=6
.
13:08:46.110056 IP 10.109.210.[illegible].59786 > 10.109.185.[illegible].514: Flags [F.], seq 274, ack 1, win 229, options [nop,nop,TS val 1878613675 ecr
3770057411], length 0
E..4..@.@...
m..
m.&....G............>.....
o.^.....
13:08:46.222559 IP 10.109.185.[illegible].514 > 10.109.210.[illegible].59786: Flags [.], ack 274, win 235, options [nop,nop,TS val 3770057525 ecr 18786136
75], length 0
E..49.@.7.i.
m.&
m..........G.......r......
...5o.^.
13:08:46.222620 IP 10.109.185.[illegible].514 > 10.109.210.[illegible].59786: Flags [F.], seq 1, ack 275, win 235, options [nop,nop,TS val 3770057525 ecr
1878613675], length 0
E..49.@.7.i.
m.&
m..........G.......r......
...5o.^.
13:08:46.222633 IP 10.109.210.[illegible].59786 > 10.109.185.[illegible].514: Flags [.], ack 2, win 229, options [nop,nop,TS val 1878613787 ecr 3770057525
], length 0
E..4..@.@...
m..
m.&....G............>.....
o._....5
^C
323 packets captured
323 packets received by filter
0 packets dropped by kernel
[root@omk-vm9-centos7 omkadmin]# tcpdump -s0 -A -nni eth0 host 10.109.185.[illegible] and port 514
```