IHV Audit Trail - Linux

- 2018-02-21 - Industrial HiVision

As of v6.0 IHV logs events to the Linux SysLog.
The events include:

- Log in and out of Industrial HiVision
- Any action which results in an SNMP Set Request being sent to a device, including the MIB variable that was set, and the new value
- Any actions from HiDiscovery within Industrial HiVision
- Start of external applications
- All actions for which the "Edit Mode" is needed

Edit syslog.conf

```
#  /etc/rsyslog.conf    Configuration file for rsyslog.
#
#                       For more information see
#                       /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html


#################
#### MODULES ####
#################

$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog   # provides kernel logging support
#$ModLoad immark  # provides --MARK-- message capability

# provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

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


"/etc/rsyslog.conf" 121 lines, 2630 characters
```
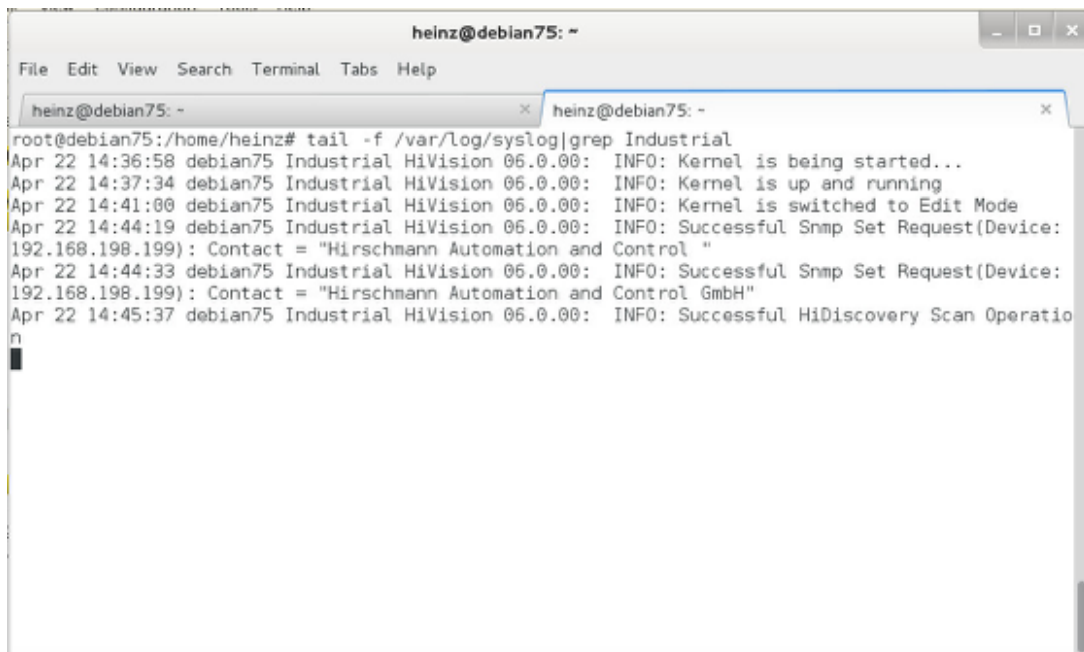
In this example it is rsyslog.conf file present in /etc/ folder

Edit/uncomment the following lines:

1. provides UDP syslog reception
   $ModLoad imudp
   $UDPServerRun 514

Restart rsyslogd in order to apply the changes

SysLog File

```
root@debian75:/home/heinz# tail -f /var/log/syslog|grep Industrial
Apr 22 14:36:58 debian75 Industrial HiVision 06.0.00:  INFO: Kernel is being started...
Apr 22 14:37:34 debian75 Industrial HiVision 06.0.00:  INFO: Kernel is up and running
Apr 22 14:41:00 debian75 Industrial HiVision 06.0.00:  INFO: Kernel is switched to Edit Mode
Apr 22 14:44:19 debian75 Industrial HiVision 06.0.00:  INFO: Successful Snmp Set Request(Device:
192.168.198.199): Contact = "Hirschmann Automation and Control "
Apr 22 14:44:33 debian75 Industrial HiVision 06.0.00:  INFO: Successful Snmp Set Request(Device:
192.168.198.199): Contact = "Hirschmann Automation and Control GmbH"
Apr 22 14:45:37 debian75 Industrial HiVision 06.0.00:  INFO: Successful HiDiscovery Scan Operatio
n
```

tail -f /var/log/syslog |grep Industrial