CPLogToSyslog processes stop running after a few minutes

Solution ID	sk109016
Product	Security Management, Multi-Domain Management / Provider-1
Version	R77, R77.10, R77.20, R77.30
OS	Gaia, SecurePlatform 2.6
Date Created	09-dic-2015
Last Modified	14-giu-2017

Symptoms

- CPLogToSyslog processes stop running after a few minutes for each Domain
- The CPLogToSyslog policy filename *$FWDIR/state/SEAM/local.cplogtosyslog_policy.C* was **not** renamed to *$FWDIR/state/SEAM/local.cplogtosyslog_policy.err*
- Debug of CPLogToSyslog process shows the following before the processes stops running:

  ```
  Error: No field was found
  Error: Failed to read value of 'Origin' field
  Error: Failed to resolve 'Origin' field
  ```

- Traffic capture and output of "`netstat -anp | grep -E "PID|CPLogToSyslog"`" command on the Security Management Server / Multi-Domain Security Management Server show the connection to the Syslog server is over UDP and not TCP.
- Logs sent by the CPLogToSyslog to Syslog server are missing the 'Origin' field.

Cause

CPLogToSyslog process defaults to TCP instead of UDP even when `$FWDIR/state/SEAM/local.cplogtosyslog_policy.C` file is configured for UDP.

Currently, TCP is the only supported protocol for CPLogToSyslog (refer to the CPLogToSyslog Administration Guide).

Solution

Follow these steps if you wish the *CPLogToSyslog* process to work over UDP instead of TCP:

1. Connect to the command line on the Security Management Server / Multi-Domain Security Management Server.
2. Log in to the Expert mode.
3. Backup the current shell script:
   - On Security Management Server:

     `[Expert@HostName:0]# cp $FWDIR/bin/fwstart $FWDIR/bin/fwstart_ORIGINAL`
   - On Multi-Domain Security Management Server:

     `[Expert@HostName:0]# cp $MDSDIR/scripts/mdsstart_customer $MDSDIR/scripts/mdsstart_customer_ORIGINAL`
4. Edit the current shell script:
   - On Security Management Server:

     `[Expert@HostName:0]# vi $FWDIR/bin/fwstart`
   - On Multi-Domain Security Management Server:

     `[Expert@HostName:0]# vi $MDSDIR/scripts/mdsstart_customer`
5. Search for the **`CPLOGTOSYSLOG`**.

   Add the "**`udp`**" argument in the following lines:

```
# start cplogtosyslog
set actCPLogToSysLog = `$CPDIR/bin/cpprod_util CPPROD_GetValue "fw1" "CPLogToSysLog" 1`
if ("$actCPLogToSysLog" == "1") then
  # Check for MDSDIR environment vaiable
  if (! $?MSP_SOMEIP_ADDR && -f $FWDIR/bin/CPLogToSyslog) then
        $CPDIR/bin/cpwd_admin start -name CPLOGTOSYSLOG -path $FWDIR/bin/CPLogToSyslog -command "CPLogToSyslog -udp" >& /dev/nul
  else
    $FWDIR/bin/CPLogToSyslog -udp &
  endif
  if ($status) then
    echo 'Failed to start CPLogToSyslog'
  else
    echo "CPLogToSyslog is starting"
  endif
endif
```

6. Save the changes and exit from Vi editor.
7. Restart Check Point services:
   - On Security Management Server:

     [Expert@HostName:0]# cpstop ; cpstart

   - On Multi-Domain Security Management Server:

     [Expert@HostName:0]# mdsstop_customer <Name of Domain Management Server>
     [Expert@HostName:0]# mdsstart_customer <Name of Domain Management Server>