How To Add ESP Log File Monitoring

This process will monitor the files for specific strings that are known to represent a possible error and send an email to the specified recipients with the line from the log file that triggered the error.

When an error message is received, the recipient should access the full log file for more details and information as only a snippet of the error message may be received.

Mail Prerequisite

Please note that your ESP server must be configured and capable of sending email. Prior to following the setup instructions, you should verify that the server is configured with a mail program. If it isn't, you will need to do this or reach out to your IT staff for assistance.

One way to test this is by issuing the following from the command line (replace the email address with a valid email address):

```
mail -s "This is a test mail" myname@mycompany.com
This is a test
```

When you have finished composing the e-mail enter `<CTL>-D` on a new line to send it. Verify that the email is received.

Installation and Configuration

The process should be initiated from the ESP application server where the ESP log files reside. Commands should be executed as the root or esp user (via sudo).

Instructions are provided for both Ubuntu and RHEL.
When 2 alternate commends are presented, the first command applies to Ubuntu.

1. **Install swatch**

   ```
   sudo apt-get install swatch
   or
   sudo yum install swatch
   ```

2. **Install xtail**

```
sudo apt-get install xtail
```
or
```
sudo yum install xtail
```

or
```
sudo wget http://www.unicom.com/files/xtail-2.1.tar.gz
gunzip xtail-2.1.tar.gz
tar -xvf xtail-2.1.tar
cd xtail-2.1
sudo sh configure
sudo sh make
sudo sh make install
```
(you can ignore any errors about creating the man file)

3. **Create the esp.log conf file**

```
cd /etc
sudo vi swatch_esp.conf
```

Add the following: (customize email addresses as appropriate – separated by a colon)

```
watchfor /CRITICAL/
    mail addresses=testemail1\@test.org:testemail2\@test.org,
subject=CRITICAL_Error_In_ESP_Log_File
    threshold track_by=CRITICAL, type=limit, count=1, seconds=60
```

4. **Create the cron log conf file**
   (Note: this will monitor all files in the ESP cron log directory.)

```
cd /etc
sudo vi swatch_cron.conf
```

Add the following: (customize email addresses as appropriate – separated by a colon)

```
ignore /spiffymcgee|records with 0 errors|Errors:/
watchfor /ERROR|error|Error|No such file|Permission denied|Traceback/
    mail addresses=testemail1\@test.org:testemail2\@test.org,
subject=ERROR_Found_In_Cron_Log_File_Directory
    threshold track_by=ERROR, type=limit, count=1, seconds=60
```


5. **Create the esp startup script.**

   You must customize the file for the following: (the parameters are highlighted below):
   1. The location of the esp.log files
   2. The path to xtail
        a. Use the command: `which xtail` to confirm the path
   3. Name of the swatch process. Swatch had to change its name so depending on the OS you are running the package may be installed as swatch or swatchdog.
        a. Use the commands `which swatch` and `which swatchdog` to determine which process name to use. The one that returns a path is the correct one.

```
        cd /etc/init.d
        sudo vi swatch_esp
```

Add the following as the contents of the file:

```
#!/bin/sh
# chkconfig: 2345 80 20
# Simple Log Watcher Program

case "$1" in 'start')
        /usr/bin/swatchdog --daemon --config-file=/etc/swatch_esp.conf --
tail-file='/var/log/esp.log' --pid-file=/var/run/swatch_esp.pid --tail-
program-name /usr/bin/xtail

        ;;
'stop')
        PID=`cat /var/run/swatch_esp.pid`
        kill $PID
        ;;
*)
        echo "Usage: $0 { start | stop }"
        ;;
esac
exit 0
```

Set the Permissions:

```
sudo chmod 755 swatch_esp
```

6. **Create the cron startup script.**

You must customize the file for the following: (the parameters are highlighted below):
   1. The DIRECTORY of the ESP cron logs
   2. The path to xtail
        a. Use the command: `which xtail` to confirm the path
   3. Name of the swatch process. Swatch had to change its name so depending on the OS you are running the package may be installed as swatch or swatchdog.
        a. Use the commands `which swatch` and `which swatchdog` to determine which process name to use. The one that returns a path is the correct one.

```
cd /etc/init.d
sudo vi swatch_cron
```

Add the following as the contents of the file:

```
#!/bin/sh
# chkconfig: 2345 80 20
# Simple Log Watcher Program

case "$1" in 'start')
        sudo /usr/bin/swatchdog --daemon --config-file=/etc/swatch_cron.conf
--tail-file='/srv/esp/log/' --pid-file=/var/run/swatch_cron.pid --tail-
program-name /usr/bin/xtail

        ;;
'stop')
        PID=`cat /var/run/swatch_cron.pid`
        kill $PID
        ;;
*)
        echo "Usage: $0 { start | stop }"
        ;;
esac
exit 0
```

Set the Permissions:

```
sudo chmod 755 swatch_cron
```

7. **Start the monitors**
   ```
   sudo /etc/init.d/swatch_esp start
   sudo /etc/init.d/swatch_cron start
   ```

8. **Test it out.**
   (NOTE: update file names and locations as appropriate)
   1. `sudo su esp`
   2. `echo "CRITICAL This is just a test. If this was a real error you would see it here" >> /var/log/esp.log`
   3. `echo "ERROR This is just a test. If this was a real error you would see it here" >> /srv/esp/log/daily_log_cron.test`

   `You should receive an email with the errors above.`

9. **Add it to system startup**

Ubuntu:
```
cd /etc/init.d
sudo update-rc.d swatch_esp defaults 98 02
sudo update-rc.d swatch_cron defaults 98 02
```

RedHat:
```
cd /etc/init.d
sudo chkconfig --add swatch_esp
sudo chkconfig --add swatch_cron
```