

```
#!/bin/bash
#
#####
#
#   Name:           PSAD.sh
#   Author:         Chris Fedun 03/28/2017
#   Description:     PSAD Config
#
#   Copyright (C) 2017 Christopher Fedun
#
#   This program is free software: you can redistribute it and/or modify
#   it under the terms of the GNU General Public License as published by
#   the Free Software Foundation, either version 3 of the License, or
#   (at your option) any later version.
#
#   This program is distributed in the hope that it will be useful,
#   but WITHOUT ANY WARRANTY; without even the implied warranty of
#   MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
#   GNU General Public License for more details.
#
#   You should have received a copy of the GNU General Public License
#   along with this program. If not, see <http://www.gnu.org/licenses/>.
#####
##### Parameters #####
```

```
host_name=$2
```

```
domain_name=$1
```

```
##### Variables #####
```

```
MY_IP=$( curl http://checkip.amazonaws.com )
```

```
##### Functions #####
```

```
function save_orig
```

```
{
    cp /etc/psad/auto_dl /etc/psad/auto_dl.orig
    cp /etc/psad/psad.conf /etc/psad/psad.conf.orig
}
```

```
function configure_PSAD
```

```
{
sed -i "s|EMAIL_ADDRESSES                root@localhost;|EMAIL_ADDRESSES
root@$domain_name;|" /etc/psad/psad.conf

sed -i "s|HOSTNAME                        _CHANGEME_;|HOSTNAME                $host_name;|" /etc
/psad/psad.conf

sed -i "s|IPT_SYSLOG_FILE                  /var/log/messages;|IPT_SYSLOG_FILE
/var/log/syslog;|" /etc/psad/psad.conf
sed -i "s|MIN_DANGER_LEVEL                  1;|MIN_DANGER_LEVEL                2;|" /etc/psad/psad.conf
sed -i "s|EMAIL_ALERT_DANGER_LEVEL          1;|EMAIL_ALERT_DANGER_LEVEL        3;|" /etc/psad/psad.conf

sed -i "s|ENABLE_AUTO_IDS                  N;|ENABLE_AUTO_IDS                    Y;|" /etc/psad/psad.conf
sed -i "s|AUTO_IDS_DANGER_LEVEL              5;|AUTO_IDS_DANGER_LEVEL            3;|" /etc/psad/psad.conf
#echo " $MY_IP          0;" >> /etc/psad/auto_dl
psad --sig-update
service psad restart
service psad enable

}
```

```
##### Main #####
```

```
save_orig
```

```
configure_PSAD
```

```
exit
```

##### END :) #####