Commonwealth Informatics
a genpact company

ESP Docs

How to add ESP system Login Auditing

1 Revision History

Version Number	Modification Date	by	Description of Changes
1.0	22 Feb 2019	J. Miller	Initial Creation

This document covers the Redhat and Ubuntu linux Operating Systems
Written for ESP version 3.x

Commonwealth Informatics
a genpact company

Contents

Commonwealth Informatics
a genpact company

2 Overview

The purpose of this document is to list the installation steps to enable basic Auditing for the ESP system.
This Document currently covers Database and Operating System failed login attempts
This script can be found in the 3.4.10 build under the share/ folder

3 Auditing PostreSQL Database logins

The script referenced in Appendix A can be used to search the postgreSQL log to identify failed login attempts.
Installation steps are described here

1 – copy the file script audit_postgresql_logins.sh to the esp scripts directory
the default scripts directory is **/srv/esp/prod/scripts/**
please update *installdir* below
Note: this file is included with version 3.4.10 and later

```
sudo cp /srv/esp/installdir/share/audit_postgresql_logins.sh
/srv/esp/installdir/scripts/audit_postgresql_logins.sh
```

2 – chmod the file so it is executable by root and not readable by anyone

```
sudo chmod 700 /srv/esp/installdir/scripts/audit_postgresql_logins.sh
```

3 – update the following variables in the audit_postgresql_logins.sh script

GREPFORLIST - list used by grep to search file
LOGDATE – the date you are searching the postgres log for (yesterday or today)
PLOGDIR – the location of where the postgreSQL logs is
MAILLIST - list of people/groups to get the daily email
AUDITLOG – a local log that will contain the results of the report/search

4 - create a root crontab entry for the script to run daily
Always a good idea to first backup the current root crontab file

```
sudo su -
crontab -l > /tmp/root.cron.backup
```

Option 1:
Edit the crontab manually as root
sudo su –
crontab -e
add this entry to run the job daily at 12:05 and look at the log for yesterday
05 00 * * * /srv/esp/*installdir*/scripts/audit_postgresql_logins.sh
save and exit

or **Option 2:**

```
sudo su -
(crontab -l; echo "05 00 * * * /srv/esp/installdir/scripts/audit_postgresql_logins.sh" | crontab –
```

Then run crontab -l again to verify the new entry is there along with the previous ones.

Commonwealth Informatics
a genpact company

4 Auditing System SSH logins

The script referenced in Appendix B can be used to search the system Audit/Auth log to identify failed login attempts
Installation steps are described here

1 – copy the file script audit_ssh_logins.sh to the esp scripts directory
the default scripts directory is **/srv/esp/prod/scripts/**
please update *installdir* below
Note: this file is included with version 3.4.10 and later

```
sudo cp /srv/esp/installdir/share/audit_ssh_logins.sh  /srv/esp/installdir/scripts/audit_ssh_logins.sh
```

2 – chmod the file so it is executable by root and not readable by anyone

```
sudo chmod 700 /srv/esp/installdir/scripts/audit_ssh_logins.sh
```

3 – update the variables in the audit_postgresql_logins.sh script

3 – update the following variables in the audit_postgresql_logins.sh script

GREPFORLIST - list used by grep to search file
LOGDATE – the date you are running the search for (yesterday or today)
SYSLOG – the location of the system audit log(redaht) or the system auth log (ubuntu)
PLOGDIR – the location of where to store the daily audit log (same as Postgres logs above)
MAILLIST - list of people/groups to get the daily email
AUDITLOG – a local log that will contain the results of the report/search

NOTE: depending on when the auth/audit logs is rotated,
you may see the same failures for previous days, for up to a week.

4 - create a root crontab entry for the script to run daily
Always a good idea to first backup the current root crontab file

```
sudo su -
crontab -l > /tmp/root.cron.backup
```

Option 1:
Edit the crontab manually as root
sudo su –
crontab -e
add this entry to run the job daily at 12:05 and look at the log for yesterday
05 00 * * * /srv/*installdir*/scripts/audit_ssh_logins.sh
save and exit

or **Option 2:**

sudo su -
(crontab -l; echo "**05 00 * * * /srv/*installdir*/scripts/audit_ssh_logins.sh**" | crontab –

Then run crontab -l again to verify the new entry is there along with the previous ones

5 APPENDIX A- PostgreSQL script

audit_postgresql_logins.sh version 1.0.1

```
#!/bin/bash
#####################################################################
## This script checks PostreSQL logs for failed logins based on the
## GREPFORLIST and sends an email to the MAILLIST
##
## Please update values for:
## GREPFORLIST, LOGDATE, PLOGDIR, MAILLIST & AUDITLOG
## Version 1.03  -  03-04-2019 J Miller
#####################################################################
## sample Cron entry for "yesterday" - run at 12:05AM every day (default)
## 05 00 * * * /srv/esp30/scripts/audit_postgresql_logins.sh
## sample Cron entry for "today" - run at 11:59PM every day
## 23 59 * * * /srv/esp30/scripts/audit_postgresql_logins.sh
#####################################################################
## GREPVLIST OPTION - to exclued text - use GREPVLIST VAR
## set GREPVLIST then run the command - verify your results!
## GREPVLIST=`cat /srv/esp30/scripts/.goodlist_postgres`
## GREPVLIST="(connection authorized|connection received)"
## grep -E $GREPFORLIST" $PLOGDIR/postgresql-$LOGDATE.log | grep -Ev "$GREPVLIST" >> $AUDITLOG
#####################################################################################
##
## 1 - UPDATE GREPFORLIST varable below to add to intial search if required
## note there is a space in front of " connection" below.. this is needed!
GREPFORLIST="(failed|FATAL)"
##
## 2 - UPDATE LOGDATE to correspond to date in cron job - today or yesterday
## Ex. LOGDATE="`date +%F`"
LOGDATE="`date --date='yesterday' +%F`"
##
## 3 - UPDATE PLOGDIR with the location to store logs from this script
## when possible use the same directory as the Postgres Audit logs
PLOGDIR="/var/lib/pgsql/9.2/data/pg_log"
##
## 4 - UPDATE MAILLIST to send daily email to appropriate support personnel
#MAILLIST="esp_support@commoninf.com,jmiller@commoninf.com"
MAILLIST="jmiller@commoninf.com"
##
## AUDITLOG - should not need to change this - it will roll monthly
AUDITLOG="$PLOGDIR/PostrgreSQLAudit.`date --date='yesterday' +%b%Y`.log"
##
## Create the AUDITLOG if its not there, echo startline into the local log
if [ -a $AUDITLOG ]
then
echo "Running Postres Login check for $LOGDATE" >> $AUDITLOG
else
touch $AUDITLOG
echo " Running Postres Login check for $LOGDATE" >> $AUDITLOG
fi
##DEBUG echo "PLOGDIR =$PLOGDIR - LOGDATE =$LOGDATE - AUDITLOG =$AUDITLOG"
##DEBUG echo "grep -EB 1 $GREPFORLIST $PLOGDIR/postgresql-$LOGDATE.log | tee -a $AUDITLOG | mailx -s Atrius Daily
Postgres Login Audit $MAILLIST "
## run the command and append it to local log and mail the results
grep -EB 1 "$GREPFORLIST" $PLOGDIR/postgresql-$LOGDATE.log | tee -a $AUDITLOG | mailx -s "Atrius Daily Postgres Login
Audit" $MAILLIST
echo "##" >> $AUDITLOG
```

6 APPENDDIX B – System/OS script

```
#!/bin/bash
#############################################################################
##  This script checks System Logs for failed logins and sends an email to the MAILLIST
##
##   Please update the MAILLIST as needed
##     set LOGDATE if needed, by default it will look at yesterdays logs
##
##   The GREPVLIST option described below can be used to filter the output
##
## Version 1.01 3-02-2019  JMiller
#############################################################################
## sample Cron entry for "yesterday" - run at 12:05AM every day (default)
## 05 00 * * * ausearch -ts yesterday -te yesterday --message USER_LOGIN --success no -I  | mailx -s “subj” $MAILLIST
## sample Cron entry for "today" - run at 11:59PM every day
## 23 59 * * * ausearch -ts today -te today --message USER_LOGIN --success no -I | mailx -s “subj” $MAILLIST
#############################################################################
## GREPVLIST OPTION - to exclude text - use GREPVLIST VAR
##     this is not used today - be careful with this option!
## set GREPVLIST then run the command - verify your results!
## GREPVLIST="(esp30|jmiller)"
## ausearch -ts yesterday -te yesterday --message USER_LOGIN --success no -I grep -v $GREPVLIST | mailx -s “subj” $MAILLIST
#############################################################################
## UPDATE LOGDATE to correspond to date in cron job - today or yesterday
#LOGDATE="`date +%F`"
LOGDATE="`date --date='yesterday' +%F`"
## LOG for this script - will roll monthly - should also match above
AUDITLOG="$PLOGDIR/ESPSytemAudit.`date --date='yesterday' +%b%Y`.log"
## UPDATE MAILLIST to send daily email to appropriate support personnel
MAILLIST="jmiller\@commoninf.com,jmiller\@commoninf.com"
## Create the AUDITLOG if its not there, echo startline into the local log
if [ -a $AUDITLOG ]
then
echo "Running System Audit check for $LOGDATE" >> $AUDITLOG
else
touch $AUDITLOG
echo " Running System Audit check for $LOGDATE" >> $AUDITLOG
fi
#DEBUG echo "LOGDATE =$LOGDATE - AUDITLOG =$AUDITLOG"
## run the command and append it to local log
ausearch -ts yesterday -te yesterday --message USER_LOGIN --success no >> $AUDITLOG
## run the command and mail the output
ausearch -ts yesterday -te yesterday --message USER_LOGIN --success no | mailx -s "Atrius Daily System Audit" $MAILLIST
echo "##" >> $AUDITLOG
```