Linux - Upgrading (old pre v1.3.1)

Prerequisites

The individual performing this installation has some Linux experience.

Root level server access.

An existing (working) Open-AudIT installation.

NOTE - This guide is for upgrading an existing Linux installation to Open-AudIT 1.2. If you wish to install onto a clean server, use the prerequisites and installation guides.

NOTE - Open-AudIT 1.2 has some additional prerequisites. Please ensure you install screen, ssh-pass and samba-client via your package manager. Please also install winexe via the Suse Build Service. Details are on the prerequisites pages for RedHat/CentOS and Debian/Ubuntu.

Backup Your Existing Install

Backup your database. Substitute your actual username for USER (likely openaudituser), password for PASSWORD (likely openaudituserpassword), your database name (likely openaudit) for DATABASE_NAME and a suitable path and filename for BACKUP_FILE_NAME in the command below.

```
mysqldump -u USER -pPASSWORD DATABASE_NAME > BACKUP_FILE_NAME.sql
```

Backup your files by copying your existing files to a backup directory.

```
cp -R /usr/local/open-audit /usr/local/open-audit_backup
```

If the omkd daemon is installed, stop the daemon and backup the /usr/local/omk directory.

```
service stop omkd

cp -R /usr/local/omk /usr/local/omk_backup
```

Copy the Open-AudIT tarball to the server (OAE-Linux-x86_64-1.2.tar.gz).

You may need to use SCP or FTP to get the file onto the server.

The file will now likely be in the users home directory.

Change into the /usr/local directory.

```
cd /usr/local
```

Untar the file.

```
tar xvf ~/OAE-Linux-x86_64-1.0.4.tar.gz
```

Fix the file ownership and permissions.

```
chown -R root:root omk

chmod -R 775 omk

chmod -R 770 /usr/local/open-audit

chmod -R 777 /usr/local/open-audit/code_igniter/application/views/lang

chmod -R 777 /usr/local/open-audit/code_igniter/application/uploads

chmod 770 /usr/local/open-audit/other/audit_linux.sh

chmod 770 /usr/local/open-audit/other/audit_subnet.sh

chmod 660 /usr/local/open-audit/other/open-audit.log

chmod 770 /usr/local/open-audit/other/discover_subnet.sh
```

Change permissions for Debian / Ubuntu

```
chown -R root:www-data /usr/local/open-audit
```

Change permissions for RedHat / CentOS

```
chown -R root:apache /usr/local/open-audit
```

Change into the omk directory

```
cd omk
```

Install the omkd Daemon (if not installed)

Copy the daemon startup script.

```
cp /usr/local/omk/install/omkd.init.d /etc/init.d/omkd
```

Adjust the startup script for your flavor of Linux distribution

for Debian / Ubuntu

You need to comment out the lines (nano /etc/init.d/omkd)

```
. /etc/init.d/functions             #
RedHat/CentOS only

lockfile=/var/lock/subsys/$prog     #
RedHat/CentOS only

killproc $prog                      #
Redhat/CentOS only
```

and uncomment (remove the # from the front of the line) the lines below them

```
# . /lib/lsb/init-functions          #
Debian/Ubuntu only

# lockfile=/var/lock/$prog           #
Debian/Ubuntu only

# pkill $prog                        #
Debian/Ubuntu only
```

for RedHat / CentOS - nothing required.

Add the daemon to the startup sequence

For Debian / Ubuntu

```
update-rc.d omkd start 20 2 3 4 5 . stop
20 0 1 6 .
```

For RedHat / CentOS

```
chkconfig --add omkd
```

Copy the config files.

```
cp install/users.dat conf/

cp install/oae_reports.json conf/

cp install/opCommon.nmis conf/
```

Edit the config files.

```
nano conf/opCommon.nmis
```

OAE_SERVER variable - By default this should be "http://127.0.0.1/open-audit/". You should not need to change this. If you do, insert the ip address of the server (127.0.0.1 or localhost are also fine) in to the oae_server variable (along with http:// and don't forget the trailing /). If you have Open-AudIT installed into a sub-directory in your web root, be sure to add that to the end of the oae_server variable above. On the Opmantek virtual appliance (for example) it would be http://<SERVER_IP>/open-audit/

OAE_LINK variable - By default this should be "/open-audit/". You should not need to change this. If you have Open-AudIT installed into a sub-directory in your web root, be sure to add that to the end of the oae_link variable above. On the Opmantek virtual appliance (for example) it would be "/open-audit/"
NOTE - If your Open-AudIT Enterprise and Open-AudIT installations are on the same machine, the oae_link variable should be set to only the directory of Open-AudIT. IE - if you have an Open-AudIT install in the root of your web directory, you can set the variable to "/". On the Opmantek virtual appliance it would be set to "/open-audit/".

If you have other Opmantek software installed (NMIS, opMaps, etc) you can also edit the module_configs -> module_host variable in opCommon.nmis. Replace http://localhost with the address of the server.

If you do not have NMIS installed on the same server, set the variable omkd_require_nmis => "false" (it's in the omkd section of the config).

The email section is described in the Open-AudIT Enterprise - Configuration Guide document.

If the omkd daemon is installed, merge the config files with those from your backed up directory. This should be done manually as new configuration items may have been added to the new file. If any items are not as per the defaults in the backed up file, copy them across.

If the omkd daemon is not installed, create the nmis user.

```
useradd nmis
```

Integrate the omkd daemon with Apache

To make the Opmantek applications accessible via the web the omkd needs to be integrated with your Apache webserver, so that the Apache serving as a front-end knows how to reach the omkd-provided applications.

You need to copy the apache proxy config file to the correct location and restart apache.

Please note that it is essential that you perform the following step and replace any existing proxy config files from older Open-AudIT Enterprise installations! Release 1.2.1 corrects a security issue with the proxy configuration which could have been abused for denial-of-service attacks if Open-AudIT Enterprise was installed with unrestricted inbound access from the Internet.

For Debian / Ubuntu:

```
cp /usr/local/omk/install/04omk-proxy.conf /etc/apache2/conf.d/
```

service apache2 restart

For RedHat / CentOS:

```
cp /usr/local/omk/install/04omk-proxy.conf /etc/httpd/conf.d/
```

service httpd restart

Start the daemon.

```
service omkd start
```

Edit the Open-AudIT scripts (if using a web root subdirectory)

If you have your web root in a subdirectory, you will need to edit the "url" variable in the various script files. These files can be found in /usr/local/open-audit /other/ The files you will need to edit all begin with audit_ They include audit_linux.sh, audit_subnet.sh, audit_windows.vbs, etc, etc. The URL variable can usually be found at the top of the file.

Delete the old web files

The new web files should live in the subdirectory /open-audit/. We should remove the existing web files.

For Debian / Ubuntu (prior to 14.04)

```
rm -rf /var/www/open-audit

rm -rf /var/www/device_images

rm -rf /var/www/theme-tango

rm /var/www/index.php

rm /var/www/favicon.png
```

For RedHat / CentOS / Ubuntu 14.04

```
rm -rf /var/www/html/open-audit

rm -rf /var/www/html/device_images

rm -rf /var/www/html/theme-tango

rm /var/www/html/index.php

rm /var/www/html/favicon.png
```

Copy new web files

If your Open-AudIT install is into a subdirectory of your webroot, be sure to add that to the end of the destination of the cp command below.

For Debian / Ubuntu (prior to 14.04)

```
cp -Rf /usr/local/open-audit/www/* /var/www/
```

For RedHat / CentOS / Ubuntu 14.04

```
cp -Rf /usr/local/open-audit/www/* /var/www/html/
```

Fix the file permissions

For Debian / Ubuntu (prior to 14.04)

```
chmod -R 775 /var/www
```

For RedHat / CentOS / Ubuntu 14.04

```
chmod -R 775 /var/www/html
```

Restore old files (if required)

Copy any attachment files from your old to the new install.

```
cp /usr/local/open-audit_backup/code_igniter/application/attachments/* /usr/local/open-audit/code_igniter
/application/attachments/
```

If you have any Groups or Report files saved in /usr/local/open-audit_backup/code_igniter/application/controllers/(groups or reports)/ that have been custom written, you may wish to copy them to the new install. If they are already activated in the database, there should be no need.

Log in to Open-AudIT at **http://SERVER/open-audit/index.php/main/list_groups** and go to Help -> About to verify that the installation status is ok; if a database upgrade is required, that page will display all relevant instructions for performing the database upgrade.

If you do not see the Open-AudIT logon page in your browser, you may need to reload the Apache config.

For Debian / Ubuntu

```
service apache2 reload
```

for RedHat / CentOS

```
service httpd reload
```

In the Open-AudIT web interface, go to Menu -> Admin -> Config and set the URLs for opMaps, Dashboard and NMIS. These will likely be:

For opMaps - /omk/oae/map

For Dashboard - /omk/oae

For NMIS - /cgi-nmis8/nmiscgi.pl

Check your Groups and Reports are functional. If you have some standard Groups and Reports activated, you may wish to deactivate them (Menu -> Admin -> Groups -> List Groups -> delete icon) and activate new ones (Menu -> Admin -> Groups -> Activate Group). Most Group and Report definitions have been updated. Do not deactivate Network Groups. These are created dynamically and if you deactivate them, you will either have to wait until a new computer is audited on the subnet in question (and hence the Group is recreated) or manually input a Group definition.

Ensure you copy the new audit scripts to any hosts that use them - these are usually updated.

Enjoy Open-AudIT 🙂