Release Notes for Open-AudIT v1.2

LINUX UPGRADERS - PLEASE NOTE. There are now some additional dependencies you will need to install using your package manager. These are screen, ssh-pass and smb-client. Details are in the pre-requisites pages. We also need to install winexe. It is not in repositories, but available for most distributions via the SuSe Build Service. Go to the URL http://download.opensuse.org/repositories/home:/ahajda:/winexe/ and download the relevant package for your distribution. Install it using "sudo dpkg -i PACKAGENAME" (Debian/Ubuntu) or "yum install PACKAGENAME" (RedHat/CentOS) and you should be good to go.

Discovery on a linux based Open-AudIT server will not work without these packages installed.

The big new feature in 1.2 is the new discovery engine. From the web interface, regardless of running Open-AudIT on Windows or Linux, you can audit Windows, audit an Active Directory Domain, audit Linux and SNMP query and nmap discover devices. Discovery will create a Network Group if you provide it a slash separated subnet (ie - 192.168.0.0/24) and that Network Group does not already exist.

Discovery works by:

1. Accept the required items via the Discovery web form at Menu -> Admin -> Discovery -> Discover Subnet. The items also in that menu for Discover SNMP, Windows and Linux all use the same functionality as below, but are designed for a single device.
2. Run a script and Nmap the target subnet to ping scan all ip addresses. For any responding ip addresses, nmap it and test for ports open for WMI, SNMP, SSH, Telnet, HHTP and HTTPS (only SNMP, WMI and SSH are currently actually used). Return the result to Open-AudIT.
3. Open-AudIT server accepts the result (for an individual ip address). If SNMP is running on the target it will attempt:

    a - To connect using any device specific credentials already stored in Open-AudIT (if they exist).
    b - To connect using the credentials provided via the Discovery web form.
    c - To connect using the default Open-AudIT credentials stored via Menu -> Admin -> Config.
4. If Open-AudIT can connect via SNMP it will gather what information it can about the device.
5. Open-AudIT determines if it has the device in it's database. If not insert it, if so update it. Store the credentials used (if any worked) to access SNMP against the individual device.
6. If WMI is open and the Open-AudIT server is Windows. Run the audit_windows script against the target.
7. If WMI is open and the Open-AudIT server is Linux, copy the script to the target and start it.
8. If Windows audit is successfully started, store credentials used against the individual device.
9. If SSH is open, copy the script to the target (Linux targets only at the moment) and start it.
10. If SSH audit is successfully started, store credentials used against the individual device.
11. Done.

NOTE - Some Linux distributions will not allow (by default) an SSH command to be sent that uses sudo. We rely on the linux audit script being run with root (or sudo) level access. At the present time, the script should still actually run and complete but you will not retrieve all details as you would if you had root (or sudo) access. If you provide the root user, it will work. If you provide a user with sudo access, it will work on Debian/Ubuntu. If you provide a non-root user (even if they have sudo) on RedHat/CentOS, you will receive a reduced audit result (but you should still receive one).

NOTE - On the Discovery web form is a check box to run using "debug". This should only be used to troubleshoot an individual device (or very small subnet - say a device or two) and the web interface will hang until such time as the discovery process is complete. Do not use this in normal operation. It is provided as a convenience only.

Discovery is quite verbose and creates quite a few log lines in (linux) /usr/local/open-audit/other/open-audit.log or (windows) c:\xampplite\open-audit\other\open-audit.log. In order to have "some" management over this file, a new menu item is provided at Menu -> Admin -> Logs -> Purge Log to simply delete the contents of that file. If you find you need to view more lines than are shown in the web interface, simply add /#LINES (ie - /50) to the end of the URL.

You should first setup the default credentials for Open-AudIT in Menu -> Admin -> Config, but you can also provide these on a per Discovery basis.

Please ensure you (at least) put your Open-AudIT server's ip address in the default_network_address config item. This is required for several audit types. When we push a script to a target device, it needs to know where to return the result to. We considered auto-populating this field, but there is simply too much scope to get this incorrect. Better to have you, the user, put in the correct address (once).

You will also see config options to display (or hide) passwords in the web interface.

AIX audit processing is also now available. The AIX audit script is available from Opmantek as part of the Open-AudIT Enterprise licensed suite.

We have moved the default location for the web files into the /open-audit/ subdirectory. Subsequently, if you have bookmarked (say) the logon page, you will need to update your bookmark.

The individual details of changes are below.

FIX - audit_linux, in network card section of audit_linux script, model and description fields were reversed.

FIX - audit_windows, correctly retrieve the bios asset tag as per reported in the forums.

FIX - Group definition, fixed the group category for the Windows Workstations group definition. Was in 'device' but should have been in 'os'.

FIX - processing, Windows discovery scripts function now writing correctly to log file. Needed to close file before submitting data to Open-AudIT Server, then reopen the file to write the final entry to it.

FIX - SNMP discovery, Correctly parse a hostname from a FQDN when returning info in SNMP.

FIX - SNMP discovery, stopped SNMP discovery from over writing man_ fields.

FIX - SNMP discovery, uptime should now be reported correctly.

FIX - Web interface, code cleanup for adding and editing Groups. If an added Group does not contain the required SQL (or SQL attributes), we now show an error page. Added code to clean up and format both SQL attributes when editing or exporting.

IMPROVE - audit_linux, added a check when submit_online=y to test ping the server before running the audit (think VPNs with no return route).

IMPROVE - audit_osx, fixed processor speed, added network domain, added parsing for command line arguements.

IMPROVE - audit_osx, removed unrequired 'sudo' from processor detail retrieval section.

IMPROVE - audit_windows, added a default to retrieve the current domain if no domain is specified.

IMPROVE - audit_windows, added a function to force the script to use cscript (even if double clicked and using wscript).

IMPROVE - audit_windows, better and additional checks for NULL. Better domain detection.

IMPROVE - audit_windows, enabled feedback that something is happening when user clicks 'Audit My PC' on the web interface.

IMPROVE - Config variable, added default credentials for Windows, SSH, etc.

IMPROVE - Config variable, added show_passwords, show_snmp_community. Set to "y" by default. Enables password masks on Windows/SSH and SNMP sensitive strings in the GUI.

IMPROVE - Config variable, name changed from snmp_default_community to default_snmp_community (to align with the other new config items for windows, ssh, etc).

IMPROVE - Group definition for Virtual Systems now examines man_manufacturer, not manufacturer.

IMPROVE - Group definition, added the Non Production Devices group to be activated by default.

IMPROVE - Group definition, revised some Group definitions to exclude system.type and only work from system.man_type.

IMPROVE - Open-AudIT Enterprise, now has icons and shortcuts in the Start Menu on Windows.

IMPROVE - Open-AudIT Enterprise, added search functionality for name or ip address into web interface.

IMPROVE - Open-AudIT Enterprise, send default location and 'Devices: none' data when nothing in database for Open-AudIT Enterprise Maps.

IMPROVE - Open-AudIT Enterprise, send some (blank) data to Open-AudIT Enterprise when nothing in Open-AudIT so graphs render (even though they show nothing).

IMPROVE - processing, added a device type called specialized (and an icon). Possible return of device type from Nmap.

IMPROVE - processing, included in the SQL the activation of some Groups and Reports so by default a new install will contain them.

IMPROVE - processing, patch to remove the date_default_timezone_get function. It causes PHP warnings. We now get the date.timezone from the php.ini so please ensure this is set correctly.

IMPROVE - processing, small alteration to the 'allowed characters' in the config file.

IMPROVE - processing, when an SNMP probe or audit script is processed, if the man_icon field is blank or 'unknown' it is updated with man_icon, icon or type.

IMPROVE - Report definition for Software Keys updated as per forum post.

IMPROVE - SNMP discovery, added Microsoft vendor SNMP helper file.

IMPROVE - SNMP discovery, added QNAP NAS OID's.

IMPROVE - SNMP discovery, cleanup of operating system names for 8072 (generic computers) and VMware.

IMPROVE - SNMP discovery, extended the timeout value.

IMPROVE - Web interface, added a dash for occasions when the hostname is blank in Search results.

IMPROVE - Web interface, added a note on the config screen about inserting a dash to remove the value of an item.

IMPROVE - Web interface, added "head office" to list of location types.

IMPROVE - Web interface, added better error message when requesting a report that does not exist.

IMPROVE - Web interface, added data to the default location. Added in the SQL creation script and the admin->upgrade php. Allowed it to be viewed in Locations list. Added and activated the corresponding Group. All devices if not already assigned a location, now get assigned the Default Location.

IMPROVE - Web interface, added extra text to the list groups page when no devices present in database (ie - after a new install).

IMPROVE - Web interface, added the function name into the html page title.

IMPROVE - Web interface, Adjust the CSS alignment on form fields.

IMPROVE - Web interface, default web directory is now /open-audit/. All scripts changed.

IMPROVE - Web interface, force upgrade when logging on.

IMPROVE - Web interface, provide links to online documentation via Menu -> Help.

IMPROVE - Web interface, provide list of "types" instead of a text field.

IMPROVE - Web interface, revised logon page. If no device present, pre-fill the default logon credentials.

IMPROVE - Web interface, show Last Seen and Last Seen By in OAE.

IMPROVE - Web interface, update credentials per device. Provide defaults if not set on specific device.

IMPROVE - Windows installer, changes made to ensure port and subdirectory of Open-AudIT install, on the webserver, should 'just work' without configuring anything as far as Open-AudIT itself is concerned.

NEW - All Opmantek files now include a standard header.

NEW - audit_aix, added functionality for AIX audit processing and display. (AIX audit script available separatley for Open-AudIT Enterprise licensed users).

NEW - audit_linux, extra attempts to retrieve fields when running audit_linucx.sh as a non-root user.

NEW - Discovery, ability to audit Active Directory from the web interface.

NEW - Discovery. System_id. Create network group if it does not exist.

NEW - Web interface, summary menu in Device Details is expanded by default.