Release Notes for Open-AudIT v3.2.0

Released 2019-09-06

Linux SHA256: bbb32cbcd517471b86518fa580d367c0f246190220d2800aa7ec0f6678a12973

Linux md5sum: e36410b059eb9e6fb9009ed2b9ad367d

NOTE - Re-released on 2019-09-06 to fix a task bug.

Open-AudIT 3.2.0 see's a major new feature incorporated - **Rules**. Rules allow you to manage properties for discovered devices. Think of it as ***"If This, Then That"*** for Open-AudIT. More details can be found on the **Rules** page and a new **Blog Post**. The affected files (in case you have made any customisations) are mostly within the SNMP helpers. A full list is at the bottom of the page, but the main files are:

Linux - /usr/local/open-audit/code_igniter/application/helpers/snmp_*_helper.php

Windows - c:\xampp\open-audit\code_igniter\application\helpers\snmp_*_helper.php

NOTE - Minor API change. We have replaced the attribute=inText setting to now use attribute=in(Text) in URLs and API requests. If you are using attribute=inText, you will need to refactor your calls. Apologies for any inconvenience caused. This was to better service requests like system.manufacturer=intel without having to code exceptions for every permutation we come across.

Old - http://server/open-audit/index.php/devices?system.status=inproduction,testing

New - http://server/open-audit/index.php/devices?system.status=in(production,testing)

Version	Type	Collection	Description
Open-AudIT Community	Bug	discoveries	Security issue reported and rectified. See Errata - 3.1.2 Security issue, September 2019 CVE-2019-16293
Open-AudIT Community	New Feature	rules	Rules
Open-AudIT Community	Change	API	Replace attribute=inText with attribute=in(Text)
Open-AudIT Community	Improvement	scripts	Enable running audit_windows.vbs without Admin rights. Admin required for policy reading.
Open-AudIT Community	Improvement	discoveries	If we're running under Windows AND the default Apache service user AND have a failed 'net use' in the discovery log, show a warning.
Open-AudIT Community	Improvement	discoveries	Provide warning when Windows Apache running as Local System and we have failed audit script copies in the discovery log.
Open-AudIT Community	Bug	credentials	When retrieving credentials for a device::read, if they no longer exist, do not try to merge them into the response.
Open-AudIT Community	Bug	scripts	Remove unnecessary wscript.quit in policy auditing (left from debugging).
Open-AudIT Community	Improvement	input	Revise 'in' operator to require opening and closing round braces in URL.
Open-AudIT Community	Improvement	queries	Fix parsing queries to use case-insensitive where (as opposed to case sensitive WHERE) when executing.
Open-AudIT Community	Improvement	discoveries	Allow the user to supply an ID when creating Discoveries. This enables the Server and Collector to use the same discovery ID so logs will align.
Open-AudIT Community	Improvement	credentials, locations, orgs	As per discoveries, allow ID for Orgs, Locations and Credentials so they're in sync between Server and Collector.
Open-AudIT Community	Improvement	discoveries	Remove $device->id from log messages. We have $device-IP and we use that. Removing the ID (still stored in discovery_log.system_id) removes confusion when reading Collector vs Server discovery logs.
Open-AudIT Community	Improvement	locations, orgs	Add reset function to Orgs and Locations controllers.
Open-AudIT Community	Improvement	discoveries	Set the local IP for a log entry (when status = complete). Only log discovery retrieved if we are given an IP (end of discover subnet script causes this.
Open-AudIT Community	Improvement	input, logs	Allow input/logs from localhost AND any IP of a Collector.

Open-AudIT Community	Improvement	users, orgs	Don't log in m_users::get_org as this is called repeatedly.
Open-AudIT Community	Improvement	scripts	Eliminate loop disks (mounted by Snaps) from linux audit.
Open-AudIT Community	Improvement	rules	Set the PHP memory limit to 1024 the input controller. Discovery now regularly uses > 500MB because of the Rules matching.
Open-AudIT Community	Improvement	discoveries	Add another match test, for dns_hostname.
Open-AudIT Community	Improvement	scripts	Remove the DirectX software entry as the registry cannot provide the correct version above 11.
Open-AudIT Community	Improvement	discoveries	Show the name as it is always present, rather than the hostname, in the log.
Open-AudIT Community	Improvement	discoveries	Add the peak memory use to the last log line in discoveries.
Open-AudIT Community	Improvement	users	Disable the NMIS user (null password) by default.
Open-AudIT Community	Bug	discoveries	Fix non-updating status for discovery on single device discovery.
Open-AudIT Community	Bug	users	Fix bug in m_logon when testing for multiple LDAP servers. Allow for user.name@domain.com and parse to user.name when searching for a user or logging on using headers. Full user.name@domain.com is sent from Enterprise.
Open-AudIT Community	Improvement	scripts	Only show 'Audit My PC' on the logon screen if default network address is set and not to localhost.
Open-AudIT Community	Bug	discoveries	Validate network address when discovery submitted and also when generating the command to be run.
Open-AudIT Community	Improvement	discoveries	Set discovery status, duration, etc on logs received for more accurate display in GUI.
Open-AudIT Community	Bug	discoveries	Do not attempt to SCP audit file from target if not in returned array of audit script output.
Open-AudIT Community	Improvement	database	Schema changes to ensure defaults for all coluins that are not TEXT type.
Open-AudIT Community	Improvement	database	New function to derive SQL schema columns. Replaces functions in m_collection and include_dictionary. Use new function in collections helper for columns.
Open-AudIT Community	Improvement	database, groups	Remove GROUP BY name on groups collection for Strict MySQL compliance.
Open-AudIT Community	Improvement	groups	Enable 'expose' in groups create form.
Open-AudIT Enterprise	Improvement	collectors	Forward all discovery logs from Collector to Server.
Open-AudIT Enterprise	Improvement	clouds	Ability to inventory and audit Google Compute cloud servers.
Open-AudIT Professional	Improvement	networks	Add Cloud Network as a type of network.
Open-AudIT Enterprise	Improvement	collectors	Store the Collectors OS.
Open-AudIT Enterprise	Improvement	files	Address issue when declaring a Unix style filepath containing a *. This breaks the Windows audit. If a path now starts with a /, exclude it from the Windows audit script.
Open-AudIT Enterprise	Improvement	collectors	Set default collector interval to 5 minutes.
Open-AudIT Professional	Improvement	discoveries	Revise warning message for Centos/Redhat 6 for discovery create form.
Open-AudIT Professional	Improvement	logs	New "summary" logs page. Group all logs for an individual request. From Professional / Enterprise, there will still be multiple as a single web browser request can generate several calls to the Community API.
Open-AudIT Professional	Improvement	API	Only load dictionary in include_read when format is screen. When reading a discovery, load org, assigned org and assigned location in the includes array.
Open-AudIT Professional	Improvement	credentials	Remove menu entry for Default Credentials (we no longer ship SNMP public).
Open-AudIT Professional	Bug	devices	Sort device types ignoring case in drop down on devices::read template.
Open-AudIT Professional	Improvement	discoveries	Revise the status naming on discoveries::collection and discoveries::read.

Open-AudIT Enterprise	Bug	dashboards	Allow all dashboards on Cloud.
Open-AudIT Enterprise	Improvement	discoveries	Do not flag SNMP status as true when cloud auditing.
Open-AudIT Professional	Improvement	networks	Add the new network type and sort alpha on networks::read template.
Open-AudIT Professional	Improvement	networks	Add a Refine button on networks::collection template (Show all /24 networks, for example).
Open-AudIT Enterprise	Bug	discoveries	Enable edit discovery options in Cloud.
Open-AudIT Professional	Improvement	discoveries	Show warning for Discovery Apache Service user under Windows.
Open-AudIT Enterprise	Bug	tasks	Show Collector on tasks:read when type == discoveries.
Open-AudIT Enterprise	Improvement	collectors	Add OS to the collector details when registering.
Open-AudIT Professional	Improvement	tasks	For the tasks::create and tasks::read templates, only allow intervals of 5 minutes.
Open-AudIT Professional	Bug	tasks	specify the correct type on tasks::create template form (tasks, not scripts).
Open-AudIT Enterprise	Improvement	discoveries	Discovery Execute button on Server should create a task for Collector.
Open-AudIT Professional	Improvement	GUI	All ? buttons should go to Documentation, not the Feature page.
Open-AudIT Professional	Improvement	credentials, discoveries	Add wizard buttons on Discovery and Cloud pages.
Open-AudIT Enterprise	Improvement	collectors	Sync Orgs and Locations to Collector.
Open-AudIT Professional	Improvement	GUI	Add Get Support to Help menu.
Open-AudIT Professional	Task	installer	New package requirement for Ubuntu/Debian only - php-curl. Centos/RedHat ship with this, as does our Xampp install for Windows.
Open-AudIT Enterprise	Improvement	collectors	Allow credentials and discoveries when in Collector mode.
Open-AudIT Enterprise	Improvement	collectors, discoveries	Delete the discovery logs on the server when a Collector discovery runs.
Open-AudIT Professional	Bug	installer	Parse database.php config correctly so we can back it up in the installer.
Open-AudIT Professional	Improvement	discoveries	On discoveries::read template, insert a BR where we have a new line int he logs.
Open-AudIT Enterprise	Bug	discoveries	If we are Cloud or have Collectors, disable Run Discovery on Bulk Edit template. If we run Discovery from Bulk Edit, redirect upon completion to Dashboard with success or fail flash. Allow for new id=in() format in URL.
Open-AudIT Professional	Improvement	devices	Remove the sortable attribute from Bulk Edit (in table header) on devices::collection template.
Open-AudIT Professional	Improvement	GUI	Only populate debug panel if $response is set.
Open-AudIT Enterprise	Improvement	GUI	Do not allow 'discover this device' when running Cloud.
Open-AudIT Enterprise	Improvement	logs	Revised log severity from error to debug on collector request with no discoveries returned.
Open-AudIT Professional	Bug	LDAP	Fix logging on to Professional / Enterprise using LDAP, verified by Community using full user.name@domain.com format.
Open-AudIT Professional	Improvement	networks	Use ip_padded for table display to enable sort on networks::read template.
Open-AudIT Enterprise	Improvement	collectors	Populate the Collectors discovery response with the config match items from the local (Server) install.
Open-AudIT Professional	Improvement	GUI	On all individual item pages make the tab title $collection - $name.
Open-AudIT Enterprise	Bug	collectors, networks	Collector Register should not create multiple entries in /networks (each time one is registered from the same subnet).

Open-AudIT Enterprise	Bug	collectors	Change Collector status to approved once a collector requests is received.
Open-AudIT Professional	Improvement	discoveries	Links on Discoveries::Read::Summary now directly show devices audited or not audited, rather than link to the devices:: collection template, hence show what the user expects to see.
Open-AudIT Professional	New Feature	GUI	Export & Import. On each details page (for all collections except devices, so Credentials, Locations, Rules, etc), there is now an "Export" button. This will provide a JSON object of the item in question, minus it's ID and edited_date, edited_by fields. On each list page (again, except devices) there is a new button called "Import". The JSON from the aforementioned Export can be copied here and a new item created. This ties in nicely to let users share queries, rules or anything else they would like to. NOTE - It does include credentials. If you want to remove those from being included, set the configuration item "decrypt_credentials" to 'n'.

---

snmp_850_helper.php
snmp_838_helper.php
snmp_81_helper.php
snmp_818_helper.php
snmp_8072_helper.php
snmp_800_helper.php
snmp_7571_helper.php
snmp_7309_helper.php
snmp_7262_helper.php
snmp_705_helper.php
snmp_6889_helper.php
snmp_683_helper.php
snmp_6527_helper.php
snmp_6486_helper.php
snmp_641_helper.php
snmp_637_helper.php
snmp_6027_helper.php
snmp_5776_helper.php
snmp_5624_helper.php
snmp_5596_helper.php
snmp_5567_helper.php
snmp_52_helper.php
snmp_5227_helper.php
snmp_4900_helper.php
snmp_47196_helper.php
snmp_46242_helper.php
snmp_429_helper.php
snmp_3873_helper.php
snmp_3833_helper.php
snmp_36_helper.php
snmp_3607_helper.php
snmp_3417_helper.php
snmp_3375_helper.php
snmp_3347_helper.php
snmp_31926_helper.php
snmp_3097_helper.php
snmp_30065_helper.php
snmp_3003_helper.php
snmp_2_helper.php
snmp_29999_helper.php
snmp_297_helper.php
snmp_2971_helper.php
snmp_278_helper.php
snmp_253_helper.php
snmp_248_helper.php
snmp_2435_helper.php
snmp_2352_helper.php
snmp_2334_helper.php
snmp_232_helper.php
snmp_2281_helper.php
snmp_2272_helper.php
snmp_22610_helper.php
snmp_21671_helper.php
snmp_20916_helper.php
snmp_1981_helper.php
snmp_19746_helper.php
snmp_1916_helper.php
snmp_1896_helper.php
snmp_18334_helper.php
snmp_17453_helper.php
snmp_1723_helper.php
snmp_171_helper.php
snmp_1713_helper.php
snmp_1588_helper.php
snmp_12532_helper.php
snmp_1230_helper.php
snmp_12140_helper.php
snmp_1139_helper.php
snmp_10418_helper.php