Release Notes for Open-AudIT v3.3.0

Released 2020-04-06

~~Linux SHA256: 7c24df67b08c0993c60d5f07c83ca64e397e5b5ba41137ac225f615ff4daac8b~~

~~Linux md5sum: 6db64aab17965480ceff52bbc988db09~~

Linux SHA256: 25bac7c8698a9d4087ebced1998e0529a44224f4ee924d0a61889d12b0e4e073

Linux md5sum: 540762d5250f9b497a4ff66c06b1a365

Items highlighted I think deserve a special mention.

Don't forget :

- Professional gets all Community features
- Enterprise get all Professional and Community features.

NOTE - 3.3.0 breaks backwards compatibility with releases prior to 1.14.04. If you need to upgrade from a release earlier than 1.14.04, first upgrade to 2.0.1, then to 3.4.0. You can find 2.0.1 here - https://dl-openaudit.opmantek.com/OAE-Linux-x86_64-release_2.0.1.run

Version	Type	Collection	Description
Enterprise	Improvement	Baselines	Move baselines definition into the database. Results are still stored as JSON files on disk due to database size.
Enterprise	Improvement	Baselines	Make Baselines templates look as per other endpoint templates.
Community	Improvement	Groups	Allow for 'normal' /groups/<id>?action=execute URL as per other endpoints.
Professional	Improvement	Database	New menu option. Admin Database Schema Compare. Checks the schema of the in-use database against the definition supplied as a file and highlights differences.
Professional	Improvement	All	Add the name of the object to the title bar if we're viewing an execute or read template.
Cloud	Improvement	Tasks	Implement working tasks for all customers for Cloud.
Professional	Improvement	Discoveries	Change the Export Logs icon to avoid a clash with the Export icon implemented for all collections::read templates.
Professional	Improvement	Discoveries	New menu items under Discoveries.
Professional	Improvement	Devices	New menu items under Devices..
Professional	Improvement	Devices	Provide a global ***default columns retrieval*** list and ***default columns show*** list. Default columns show can be overwritten per user. Allow on the /devices page to show/hide columns and save as the users default columns list.
Professional	Improvement	Devices	Refine the devices collection template to hide/show the sub_resource items. Refine the sub_resource templates and add another for viewing a single sub_resource entry.
Professional	Improvement	Devices	Add task to the device display left side menu.
Enterprise	Improvement	Integrations	Add Last Run to Integrations Collection template.
Community	Improvement	Discoveries	Add sudo password on credentials templates. Use new 'sudo_password' when using ssh_key credentials, if populated. Revise SSH timeouts when using sudo. The old "password" field, on a credentials entry for an SSH Key, was used both for the key itself (if encrypted) and also for the sudo password. This didn't work when they we different (ie, most of the time). If the SSH Key had no password, it worked as expected.
Professional	Improvement	Configuration	Remove oae_password from being used. Set password to '', effectively barring logon (new installs only).
Community	Improvement	Devices	Only allow JPG, PNG and SVG files to be uploaded as device images.
Professional	Bug	Devices	Fix displayed text for Audit My PC link on Linux.
Community	Improvement	LDAP Servers	Add new attribute for ldap_servers - use_auth.

Professional	Improvement	Discoveries	Minor refinements to the discoveries_read template.
Professional	Improvement	Discoveries	Add open|filtered to the discovery scan options with a default of 'n'. Previously we used the "filtered" column to check for open|filtered. This change aligns the discovery scan options with Nmap return strings.
Professional	Bug	Racks	System detail button on rack visualization does not work in Firefox.
Professional	Improvement	Discoveries	Add time for Scanning for Nmap response to discoveries::read template.
Professional	Improvement	Clusters	Add clusters endpoint.
Professional	Improvement	Devices	Buttons to clear change logs and audit logs for a device.
Professional	Improvement	All	Warn if deleting a collection item, that it will also delete any associated tasks.
Professional	Improvement	Devices	Show processor hyperthreading, socket and architecture on devices read template.
Community	Improvement	Discoveries	Remove network address, add open|filtered to discoveries create and read templates.
Community	Improvement	Devices	Implement code to delete a device from the database when config item set and status changed to deleted.
Community	Improvement	Devices	Add nmis_customer to integrations (and database).
Professional	Improvement	Devices	Un-managed Devices Menu Entry and Edit.
Community	Improvement	Devices	Retrieve more linux user information (home, shell, ssh Keys).
Community	Improvement	All	A large amount of code formatting to adhere to the include code sniffer (see /other/PHPCS_Coding_Standard).
Community	Improvement	Devices	Add deprecation notice to devices::collection template for running a Query based on a Group.
Community	Improvement	Configuration	Allow filters in /configuration (particularly for configuration.name), mostly for the API.
Professional	Improvement	Widgets	Add server.edition to Server Types summary.
Community	Improvement	Devices	Remove the 'default' route (for 0.0.0.0) as it already shows in 'ip r' and it also may have more than one for 0.0.0.0 with different weights, think VPN.
Community	Improvement	Devices	Add Seagate identifier for Manufacturer to linux disks.
Community	Improvement	Discoveries	Don't use the timeout (2m), hard set to 10 seconds for SSH login.
Community	Improvement	All	Sort the meta->data order.
Community	Improvement	Discoveries	Mac Models added.
Community	Improvement	Discoveries	Revise SSH timeouts when using sudo. Only use configured limit for the audit script (otherwise a simple delete file has to timeout). Timeout was defaulting to 10mins, regardless of setting. I had to explicitly set this for each ssh->read command. Discovery using this went from 365 seconds to 165 seconds for a single host.
Community	Improvement	Discoveries	Use self-delete on SSH audit scripts running via discovery.
Community	Improvement	Users	Accept username and password via request headers in m_logon.
Community	Improvement	Configuration	Code added to check_defaults to set default_network_address based on determined server IP, if not already set by the user.
Community	Improvement	All	Massive (code) shake up of how we do Collections (and a bit of READ, too). No more m_collections::collection or My_Model::collection_sql used. Each collection now responsible for it's own items. Every model has a collection function that takes either a user or response. We can now call each for either a straight list of items the user can see or a full response with column list, exclusions, et al as per the API.
Community	Improvement	Users	Remove nmis user from default user list.
Community	Bug	Discoveries	Use correct argument order in explode function for UUID retrieval via SSH.

Community	Improvement	Discoveries	New discovery routine using the queue. We now have a "discovery queue". Each IP is scanned NOT by discover_subnet.vbs||sh, now it's directly in PHP. We have effectively deprecated the discover_subnet scripts as at 3.3.0. We create a new entry per IP in a queue and loop over those, with a default number of spawned processes set to 20 (configurable). Discovery times have again sped up by a large amount and if your network and Open-AudIT server allow it, you can increase the default queue limit and gain even more.
Community	Bug	Discoveries	For service items, include the 'port' in the match. We were matching on name + type only, which failed when we have multiple websites, same names, different ports (80 + 443).
Community	Improvement	Discoveries	Remove 'manufacturer' from discover_subnet.sh as we don't use it and when it contains an ampersand, it seems to fail validations - even if we enclose it in CDATA.
Community	Improvement	Devices	Automatically filter any devices without oae_manage = 'y' when requesting from Enterprise.
Community	Bug	Discoveries	Fix bug in audit_linux.sh relating to Docker machine detection (thanks David).
Community	Improvement	Discoveries	Add config option called match_ip_no_data. If we discover a device and that IP is already in the database AND we have no audit data about that device, assuming it is the same device, do not create another (usually duplicate) device.
Community	Improvement	Discoveries	For service items, include the 'port' in the match. We were matching on name + type only, which failed when we have multiple websites, same names, different ports (80 + 443).
Community	Improvement	Devices	Add processor.hyperthreading to DB schema.
Community	Bug	Discoveries	Linux audit fix for log size from danf0x. Thanks Dan.
Community	Improvement	Discoveries	Improved IIS 7 and above enumeration. Only for local audit.
Community	Improvement	Discoveries	ESXi audit script - fix memory_count, domain and format os_installation_date as a date, not a timestamp. Correctly format manufacurer name for VMware, Inc. SSH Helper, better attribute retrieval to match the audit script for ESXi.
Community	Improvement	Discoveries	After SSH attribute retrieval, if populated, use these in preference to previously obtained values (SNMP, Nmap, etc.)
Community	Bug	Discoveries	Correct argument order to split FQDN into hostname and domain.
Community	Improvement	Discoveries	When running an audit script via discovery using sudo, no longer timeout to discovery_ssh_timeout, parse, then wait for the respone until we see 'Audit Completed' in the output - or wait for the timeout. Output the script output to the discovery_log if log_level = 7.
Community	Improvement	Discoveries	Retrieve routes via SNMP if count is below config item discovery_route_retrieve_limit.
Community	Improvement	All	Improve input helper for better user input validation. Provide a list of valid sub_resources and validate request against it. Ensure valid groupby provided. Improve setting IDs. Ensure integers and comma's only. Improve setting properties. Improve setting sort. Force sub_resource_id to an integer type.
Community	Improvement	Devices	Add memory.manufacturer to SQL schema, retrieve on Linux.
Community	Change	All	Remove 'group' from the list of properties for input and use.
Community	Improvement	All	Add option of properties=all or properties=* for all endpoints, which provides all SQL columns, the output of which is fully qualified name in the JSON.
Community	Improvement	All	Include log in debug output if meta->debug is true and set log_level to 7.
Community	Improvement	Discoveries	In m_device::match, provide an array of ignored strings. Eg - 'To be filled by O.E.M.', which in a serial number frequently causes a false positive match.
Community	Improvement	Discoveries	Remove a lot of added text from attributes in order to match ssh with ssh_audit values. Make some attributes in audit linx script, identical to those retrieved from in-app discovery.
Community	Bug	NMIS	Fix nmis import. Set org_id and location_id and redirect to a valid URL.
Community	Improvement	Rules	Add two new rules (HP -> Hewlett Packard) and (innotek GmbH -> Virtual).
Community	Improvement	Groups	Improve Group definitions for Printers, Debian Computers and Public IP Devices
Professional	Improvement	Devices	Provide a DHCP section on devices_read template
All	Improvement	All	Requesting create_form in JSON now provides everything required to build a suitable POST request. New function in all models called dictionary (used by controller/create_form and util/dictionary).

Community	Improvement	Database	Add errors, warnings and notices to DB upgrade output screen.
Professional	Improvement	Logs	Refine the View Logs by Summary to only show create, update or delete actions by default (data altering requests).
Community	Improvement	All	PHPDocs for most functions added.
Professional	Improvement	Discoveries	Randomly discoveries will take ~60 seconds to start. Add a notice if status not empty and logs empty on discoveries read template.