Release Notes for Open-AudIT v4.1.0

Released 2021-04-15

Linux SHA256: a804adcf5e11f5d9e77b8ff1d856f42e5ee0c9936362887cc9c8339ac39cb435

Linux md5sum: da3513028d8d9b01f743dbb37829dbf5

As at 2021-04-15, this release is Linux only. A Windows release is coming ASAP.

New Feature - Device Seed Discoveries. Linked article - Device Seed Discoveries.

New Feature - OKTA OpenID for authentication. Linked article - OKTA OpenID authentication and Configuration.

From 4.1.0 onward we allow more flexibility when creating a discovery regarding setting individual discovery scan options. You can now change individual options without having to create a "custom" discovery scan options entry. The Discovery Scan Options for a given discovery now function as the match rules. You choose an option set, but you can override individual options. They'll default to the discovery scan option chosen, if not explicitly set. Much more flexible and intuitive. These are still restricted to Enterprise licensed customers.

Small reminder that Open-AudIT Community is still at version 3.5.3, not 4.1.0. This will be updated in a future release.

Database Schema Change - For 4.1.0, we have changed the schema for the discoveries table, see below. Essentially, we have broken out some attributes from the 'other' JSON field and moved them to full columns (subnet, ad_domain, ad_server). We have also changed to use scan_options and match_options for those items, instead of again embedding them in 'other'. There are also a few new columns, mostly to do with the new 'seed' discovery type. We have left 'other' in the table for now, but it is not used in the application from 4.1.0 onward.

Old	New

```
CREATE TABLE `discoveries` (

`id` int(10) unsigned NOT NULL AUTO_INCREMENT,

`name` varchar(200) NOT NULL DEFAULT '',

`org_id` int(10) unsigned NOT NULL DEFAULT '1',

`description` text NOT NULL,

`type` varchar(100) NOT NULL DEFAULT '',

`devices_assigned_to_org` int(10) unsigned DEFAULT
NULL,

`devices_assigned_to_location` int(10) unsigned
DEFAULT NULL,

`network_address` varchar(100) NOT NULL DEFAULT '',

`system_id` int(10) unsigned NOT NULL DEFAULT '0',

`other` text NOT NULL,

`options` text NOT NULL,

`discard` enum('y','n') NOT NULL DEFAULT 'n',

`last_run` datetime NOT NULL DEFAULT '2000-01-01 00:00:
00',

`last_finished` datetime NOT NULL DEFAULT '2000-01-01
00:00:00',

`duration` time NOT NULL DEFAULT '00:00:00',

`status` varchar(20) NOT NULL DEFAULT '',

`ip_all_count` int(10) unsigned NOT NULL DEFAULT '0',

`ip_responding_count` int(10) unsigned NOT NULL
DEFAULT '0',

`ip_scanned_count` int(10) unsigned NOT NULL DEFAULT
'0',

`ip_discovered_count` int(10) unsigned NOT NULL
DEFAULT '0',

`ip_audited_count` int(10) unsigned NOT NULL DEFAULT
'0',

`edited_by` varchar(200) NOT NULL DEFAULT '',

`edited_date` datetime NOT NULL DEFAULT '2000-01-01 00:
00:00',

PRIMARY KEY (`id`)

) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

```
CREATE TABLE `discoveries` (

`id` int(10) unsigned NOT NULL AUTO_INCREMENT,

`name` varchar(200) NOT NULL DEFAULT '',

`org_id` int(10) unsigned NOT NULL DEFAULT '1',

`description` text NOT NULL,

`type` varchar(100) NOT NULL DEFAULT '',

`subnet` varchar(45) NOT NULL DEFAULT '',

`seed_ip` varchar(45) NOT NULL DEFAULT '',

`seed_restrict_to_subnet` enum('y','n') NOT NULL
DEFAULT 'y',

`seed_restrict_to_private` enum('y','n') NOT NULL
DEFAULT 'y',

`seed_ping` enum('y','n') NOT NULL DEFAULT 'y',

`ad_domain` varchar(200) NOT NULL DEFAULT '',

`ad_server` varchar(45) NOT NULL DEFAULT '',

`devices_assigned_to_org` int(10) unsigned DEFAULT
NULL,

`devices_assigned_to_location` int(10) unsigned
DEFAULT NULL,

`network_address` varchar(100) NOT NULL DEFAULT '',

`system_id` int(10) unsigned NOT NULL DEFAULT '0',

`other` text NOT NULL,

`scan_options` text NOT NULL,

`match_options` text NOT NULL,

`command_options` text NOT NULL,

`discard` enum('y','n') NOT NULL DEFAULT 'n',

`last_run` datetime NOT NULL DEFAULT '2000-01-01 00:00:
00',

`last_finished` datetime NOT NULL DEFAULT '2000-01-01
00:00:00',

`duration` time NOT NULL DEFAULT '00:00:00',

`status` varchar(20) NOT NULL DEFAULT '',

`ip_all_count` int(10) unsigned NOT NULL DEFAULT '0',

`ip_responding_count` int(10) unsigned NOT NULL
DEFAULT '0',

`ip_scanned_count` int(10) unsigned NOT NULL DEFAULT
'0',

`ip_discovered_count` int(10) unsigned NOT NULL
DEFAULT '0',

`ip_audited_count` int(10) unsigned NOT NULL DEFAULT
'0',

`edited_by` varchar(200) NOT NULL DEFAULT '',

`edited_date` datetime NOT NULL DEFAULT '2000-01-01 00:
00:00',

PRIMARY KEY (`id`)

) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Version	Type	Collection	Description
Professional	New Feature	All	OKTA OpenID implemented for authentication. See OKTA OpenID authentication and Configuration.
Professional	Bug	All	Modal for Help -> About not firing.
Community	Bug	Devices	Audit Results Overwriting attributes. In some cases, if an audit is processed, a change made using the GUI and another audit then processed, the change made by the GUI was being reverted. Bug in SQL when updating a device and determining if to set an attribute in the system table, by weight.
Professional	Bug	All	Some templates (discoveries, credentials, clouds) had a JS issue and were not removing the edit buttons.
Community	Improvement	All	Replace all passwords with ****** in interface (irrespective of using the html 'password' type).
Enterprise	Bug	Racks	Populate system.type correct on racks and rack devices read templates.
Enterprise	Improvement	All	Evaluation and Trial Licenses should enable all Enterprise features.
Professional	Improvement	Devices	Improve SAN disks on devices read template.
Professional	Improvement	Devices	Improve display of discovery error logs on device details template.
Professional	Improvement	Queries	Add an 'All Queries' item to the report menu.
Professional	Improvement	All	Use striped rows in tables for improved readability.
Enterprise	New Feature	Discoveries	New type of discovery - Device Seed. Provide a starting IP and add detected IPs/MACs to the discovery as we query devices. SNMP, Linux, Windows ARP tables, routes, etc. Enterprise only. Can restrict to a given subnet. Can restrict to private IPs only. See Device Seed Discoveries.
Professional	Bug	All	On the VersionCheck from JS, only check for Open-AudIT, as opposed to Open-AudIT Pro, Ent, et al.
Professional	Improvement	Devices	Add the change_log.id on the devices_read template (helpful when sorting).
Community	Improvement	All	Code review of all input and output to minimise XSS attacks.
Community	Bug	Devices	Fix a bug preventing auditing Debian in audit_linux script (software and other sections).
Community	Improvement	Devices	Add os_arch (x86_64, for example) to the DB schema and audit scripts.
Community	Improvement	Discoveries	In ssh_helper, do not set type if manufacturer === Ubiquiti.
Community	Improvement	Devices	Silence warnings when processing SAN due to uninitialised object.
Community	New Feature	Discoveries	Add support for radio stats retrieval from Cambium devices. New DB table - radio. Used when interface model = radio and OID is Cambium, via SNMP. Displayed in Professional / Enterprise.
Community	Improvement	Devices	For Windows targets, retrieve user password last changed and last logon timestamps.
Community	Improvement	Devices	Disabled SVG uploading for device images because of XSS issues when requesting the direct image. Actual image display in the web pages is fine.
Community	Improvement	Devices	Set to '*' (all columns) if we're not passed a property list when reading a device sub_component.
Community	Improvement	Discoveries	Include Nmap results of port scans in log->command_output.
Community	Bug	All	Fix incorrect variable name in request helper for access token.
Community	Improvement	All	Improve Nmap version detection.
Community	Improvement	All	Add extra headers to template recommended by OWASP Zap.
Community	Improvement	All	Upgrade jQuery to 3.6.0. Upgrade Bootstrap to 3.4.1.
Professional	Improvement	All	Upgrade jQuery to 3.6.0. Upgrade Bootstrap to 3.4.1.
Professional	Bug	Locations	Fix populating lat/long and GeoCode on locations read template. Also fix link in No API Key warning in alert on same template.

Professional	Improvement	Discoveries	Disable attributes for discoveries and discovery scan options for excluding ports when Nmap <7 detected.
Professional	Bug	Devices	Template fix on devices_read for policies section.
Community	Improvement	Networks	Assign networks.org_id to discoveries.org_id or discoveries.devices_assigned_to_org (if set) if network is created via discovery.
Community	Improvement	Networks	Assign networks.location_id to discoveries.devices_assigned_to_location (if set) if network is created via discovery.
Professional	Improvement	Networks	Add networks.environment attribute.