

Release Notes for Open-Audit v2.3.2

Released 2019-02-04

Linux md5sum: b8f7b940820c088c429196a28739170b

Linux SHA256: 3f94938134c147998f7aa28a1c56af38204ef27fbce5a3c379953413eeeb813f

Introduction

With Open-Audit 2.3.2 we have introduced the ability to customise both the scanning options for Nmap and the device matching rules - per discovery.

The Nmap scanning options are contained in a new endpoint (or collection) named `nmap_scan_options`. You can create your specific options and save them as an item, then use them in your discoveries.

Community users have the ability to select one of the supplied discovery scan options and use it as the default for all scans. Community users will use the default configured matching rules in the configuration as per previous releases for all scans.

Professional users can select an individual discovery scan options entry per scan. Professional users will use the default configured matching rules in the configuration as per previous releases for all scans.

Enterprise users can CRUD (create, read, update, delete) individual discovery scan options as well as customise individual attributes per discovery. Enterprise users can customise the matching rules per scan.

Discovery Scan Options

For more detailed information, go to the [Discovery Scan Options](#) page.

The options contained within a discovery scan options entry are as below.

| | |
|-------------------------------|--|
| | |
| Must Respond To Ping | If set, Nmap will first attempt to send and listen for an ICMP response. If the device does not respond, no further scanning will occur. Previously a device did not have to respond to a ping for Open-Audit to continue scanning. |
| Use Service Version Detection | When a detected port is detected as open, if set to 'y', Nmap will query the target device in an attempt to determine the version of the service running on this port. This can be useful when identifying unclassified devices. This was not previously used. |
| Consider Filtered Ports Open | Previously, Open-Audit considered an Nmap response of "open filtered" as a device responding on this port. This has caused some customer issues where firewalls respond on behalf of a non-existing device, and hence cause false positive device detection. We now have this attribute available to set per scan. |
| Timing | The standard Nmap timing options. Previously set at T4 (aggressive). |
| Top Nmap TCP Ports | The top 10, 100, 1000 ports to scan as per Nmap's "top ports" options. Previously we scanned the Top 1000 ports (the Nmap standard). |
| Top Nmap UDP Ports | The top 10, 100, 1000 ports to scan as per Nmap's "top ports" options. Previously we scanned UDP 161 (snmp) only. |
| Custom TCP Ports | Any specific ports we would like scanned in addition to the Top TCP Ports. Comma separated, no spaces. |
| Custom UDP Ports | Any specific ports we would like scanned in addition to the Top UDP Ports. Comma separated, no spaces. |
| Timeout per Target | Wait for X seconds for a target response. |
| Exclude TCP Ports | Exclude any ports listed from being scanned. Comma separated, no spaces. |
| Exclude UDP Ports | Exclude any ports listed from being scanned. Comma separated, no spaces. |
| Exclude IP Addresses | Exclude IP Addresses (individual IP - 192.168.1.20, ranges - 192.168.1.30-40 or subnets - 192.168.1.100/30) listed from being scanned. Comma separated, no spaces. |

| | |
|----------|--|
| SSH Port | Scan for this port and if detected open, use this port for SSH communication. This is added to the list of Custom TCP PORTs above, so there is no need to include it in that list as well. |
|----------|--|

When creating a discovery in Enterprise, the screen now looks as below (after Advanced has been clicked).

As always, you can simply set the name and subnet to be scanned and the defaults (as per the configuration) will be used and you're off and running. If you want to change individual items per scan, click the Advanced button and you have full access to all fields.

Professional users are able to select the Discovery Options from the dropdown, but not customise individual attributes.

Click for larger image.

Discoveries

Name: My Discovery Name ?

Subnet: 192.168.1.0/24 ?

Network Address: http://127.0.0.1/open-audit/ ?

General Options

Organisation: Default Organisation ?

Type: Subnet ?

Devices Assigned to Org: ?

Devices Assigned to Location: ?

Nmap Discovery Options

Discovery Options: UltraFast

Resulting Nmap Command(s):

```
nmap -n -T4 -ss -p 22,135,62078,21 [ip]
nmap -n -T4 -sU -p 161 [ip]
```

Must Respond to Ping: Yes ?

Use Service Version Detection: No ?

Consider Filtered Ports Open: No ?

Timing: Aggressive ?

Top Nmap TCP Ports: None ?

Top Nmap UDP Ports: None ?

Custom TCP Ports: 22,135,62078,21 ?

Custom UDP Ports: 161 ?

The below attributes of timeout, excluding TCP, UDP & IPs and ssh port detection can be set below and will overwrite the given Discovery Scan Option.

Timeout Per Target (Seconds): ?

Exclude TCP Ports: ?

Exclude UDP Ports: ?

Exclude IP Addresses: ?

SSH Running on Ports: 22 ?

Device Matching Rules

Match Dbus: Yes ?

Match FQDN: Yes ?

Match Hostname: Yes ?

Match Hostname Dbus: Yes ?

Match Hostname Serial: Yes ?

Match Hostname Uuid: Yes ?

Match IP: Yes ?

Match Mac: Yes ?

Match Mac Vmware: No ?

Match Serial: Yes ?

Match Serial Type: Yes ?

Match Uuid: Yes ?

About

Discoveries are at the very heart of what Open-Audit does.

How else would you know "What is on my network?"

Discoveries are preprepared data items that enable you to run a discovery upon a network in a single click, without entering the details of that network each and every time.

For more detailed information, check the [Open-Audit Knowledge Base](#).

Notes

Some examples of valid Subnet attributes are: 192.168.1.1 (a single IP address), 192.168.1.0/24 (a subnet), 192.168.1-31-20 (a range of IP addresses).

NOTE - Only a subnet (as per the examples - 192.168.1.0/24) will be able to automatically create a valid network for Open-Audit. If you use a single IP or a range, please ensure that before you run the Discovery you have added a corresponding network so Open-Audit will accept audit results from those targets.

As at Open-Audit 2.3.1, the network address should be set to localhost for Linux and the server's IP for Windows. Only use https if you have configured and enabled HTTPS on this server and HTTP has been disabled from localhost.

Discovery Options

Discovery preset details are as follows (including an indicative time to scan an individual IP):

UltraFast: 1 second. Scan only the ports that Open-Audit needs to use to talk to the device and detect an IOS device (WMI, SSH, SNMP, Apple Sync). A "filtered" port is not considered open. Device must respond to an Nmap ping. Use aggressive timing.

SuperFast: 5 seconds. Scan the top 10 TCP and UDP ports, as well as port 62078 (Apple IOS detection). A "filtered" port is not considered open. Device must respond to an Nmap ping. Use aggressive timing.

Fast: 40 seconds. Scan the top 100 TCP and UDP ports, as well as port 62078 (Apple IOS detection). A "filtered" port is not considered open. Device must respond to an Nmap ping. Use aggressive timing.

Medium (Classic): 90 seconds. As close to a traditional Open-Audit scan as we can make it. Scan the top 1000 TCP ports, as well as 62078 (Apple IOS detection) and UDP 161 (SNMP). A "filtered" port is considered open (and will trigger device detection). Devices are scanned regardless of a response to an Nmap ping. Use aggressive timing.

Medium: 100 seconds. Scan the top 1000 TCP and top 100 UDP ports, as well as port 62078 (Apple IOS detection). A "filtered" port is not considered open. Device must respond to an Nmap ping. Use aggressive timing.

Slow: 4 minutes. Scan the top 1000 TCP and top 100 UDP ports, as well as port 62078 (Apple IOS detection). Version detection enabled. A "filtered" port is considered open (and will trigger device detection). Device must respond to an Nmap ping. Use normal timing.

UltraSlow: 20 minutes. Not recommended. Scan the top 1000 TCP and UDP ports, as well as port 62078 (Apple IOS detection). Devices are scanned regardless of a response to an Nmap ping. Version detection enabled. A "filtered" port is considered open (and will trigger device detection). Use polite timing.

Custom: Unknown time. When options other than as set by a standard discovery preset are altered.

Nmap Timing Options

Nmap timing details are found on the bottom of this linked page <https://nmap.org/book/inan-performance.html>. From that page:

If you are on a decent broadband or ethernet connection, I would recommend always using -T4 (Aggressive). Some people love -T5 (Insane) though it is too aggressive for my taste. People sometimes specify -T2 (Polite) because they think it is less likely to crash hosts or because they consider themselves to be polite in general. They often don't realize just how slow -T2 really is. Their scan may take ten times longer than a default scan. Machine crashes and bandwidth problems are rare with the default timing options -T3 (Normal) and so I normally recommend that for cautious scanners. Omitting version detection is far more effective than playing with timing values at reducing these problems.

— Gordon Fyodor Lyon

Open-Audit Enterprise 2.0.0 is licensed to Opmartek for 12345 Nodes - Expires 18-Jul-2019
 Purchase a license for more nodes by clicking [here](#)

Powered by Opmartek

| | | |
|-------------------------|-------------|--|
| Open-AudIT Enterprise | New Feature | Discovery specific scan and match options. |
| Open-AudIT | Improvement | Add a 5 second delay for invalid logon attempts. |
| Open-AudIT Professional | New Feature | Add "Debug" under the users name (top left) which shows JSON output similar to what COmmunity has had for some time. |
| Open-AudIT Community | New Feature | Add timings for major sections of the response to the META sections of the output (visible using Debug). |
| Open-AudIT Community | Improvement | Refine processing a device. Do NOT populate "hostname" with "dns_hostname". Populate name with hostname, sysName, dns hostname then IP in that order. |
| Open-AudIT Community | Improvement | Add a new column - system.identification. Populate upon scan or audit processing. |
| Open-AudIT Professional | Improvement | Display the "identification" column in the default list when showing the device list. |
| Open-AudIT Community | Improvement | Improve discovery logging. Log at severity 5 when no working credentials are found or no management protocols (WMI, SSH, SNMP) are returned. |
| Open-AudIT Community | Improvement | Do not unset the device type if all we have is an Nmap result (ie, MAC manufacturer = Apple or port 62078 is open and device name contains iphone, set device even with just an Nmap scan to iphone). |
| Open-AudIT Community | Improvement | Use Sodium Compat and Random Compat PHP libraries to enable PHP > 7.2 compatibility. Updated version of phpSecLib installed. |
| Open-AudIT Community | Improvement | Audit code (in audit_windows.vbs and audit_linux.sh) that correctly parses and inserts as XML the devices open netstat ports. Correspondingly, process this data as per other data with no requirement to parse the raw netstat data within the Open-AudIT server. |
| Open-AudIT Community | Bug | NMIS export now renders correctly and does not error out. |
| Open-AudIT Community | Bug | Add the discovery data to the response so when requested from OAP/E, we don't produce an error because of a GET but no data returned. |
| Open-AudIT Community | Improvement | Remove discovery logs from a JSON read request to discoveries. We should now use the /discovery_log endpoint. |
| Open-AudIT Professional | New Feature | Add a button on the discoveries_read template to enable use to export all relevant discovery information. |
| Open-AudIT Community | Improvement | In audit_windows.vbs, wrap attempt to talk to domain in an on error resume next to prevent breakage when talking to an openLDAP domain. |
| Open-AudIT Community | Bug | Fix broken service, user, route sections on device details page. |
| Open-AudIT Community | Improvement | Add a new device type of Unclassified. If we have limited information about a device, but Do have something lile a manufacturer derived from a MAC or a port is open, then the device is now classes as Unclassified, not Unknown. |

| | | |
|-------------------------|-------------|---|
| Open-Audit Community | Improvement | New icon for Unknown devices (warning road sign with exclamation mark). Reuse old unknown icon for Unclassified devices (blue circle with question mark). |
| Open-Audit Professional | Improvement | Show different colours for an unknown or unclassified device. |
| Open-Audit Enterprise | Improvement | Added more items to clouds::read template. |
| Open-Audit Enterprise | Improvement | AutoRefresh clouds::read template if status not completed. |
| Open-Audit Professional | Improvement | AutoRefresh discoveries::read template if status not completed. |
| Open-Audit Professional | Improvement | Improve design of discoveries::read template for devices and logs. |
| Open-Audit Professional | Bug | On the discoveries::create form, fix the tour for the missing tour_name class. |
| Open-Audit Professional | Bug | Provide bulk edit on queries_execute and reports_execute templates. |
| Open-Audit Professional | Bug | Restore Support -> Export button on template. Force download instead of display output. |
| Open-Audit Professional | Improvement | Added pagination and summary to top of dataTables for discoveries::read template for logs, devices and IPs. |
| Open-Audit Professional | Improvement | Add a button that links to credentials create on discoveries devices when discovery log shows no XXX type of credentials. |
| Open-Audit Professional | Improvement | Add buildings, floors, rooms and rows to sub menus under Locations. |
| Open-Audit Professional | Improvement | Check and automatically fix the Nmap SetUID issue on Linux. |
| Open-Audit Professional | Improvement | Add the Nmap Program detected to the Nmap Ports section on the device details template. |
| | | |