Qualys 8.9.3 Release Notes

This new release of the Qualys Cloud Suite of Security and Compliance Applications includes the following improvement.

Qualys Cloud Platform

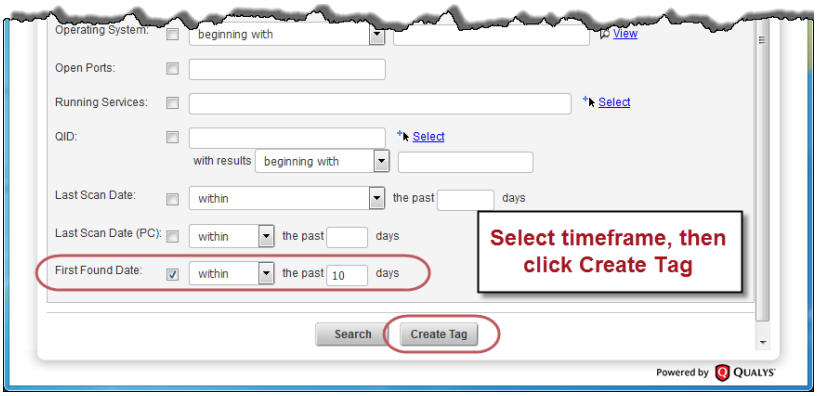
Asset Search – Create Tags based on First Found Date
EC2 Scans – Exclude Terminated Instances

Qualys 8.9.3 brings you many more Improvements and updates! Learn more

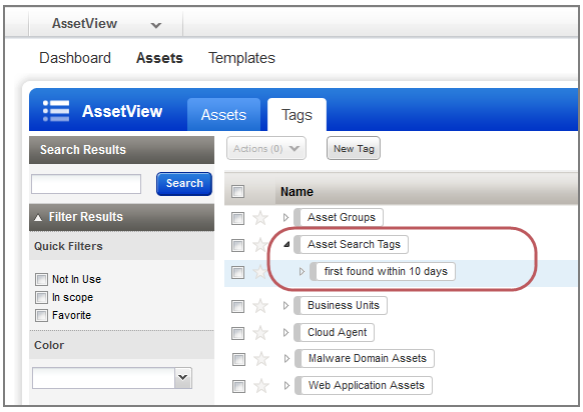
---

Asset Search – Create Tags based on First Found Date

You can now create dynamic asset tags based on the First Found Date attribute in Asset Search. Go to Assets > Asset Search. Add the hosts you want to search by specifying IPs/Ranges (do not use asset groups because they are ignored during tag creation). Then select First Found Date within (or not within) the past N days, e.g. within the past 10 days. Click Create Tag and give your tag a name.



Tip - Want to see the results first? Click Search and then click Create Tag from within your report.



Your new tag appears in the AssetView module, below Asset Search Tags. It's automatically assigned to all scanned hosts in your account that match your search criteria.

What is the First Found date?
This is the date when a host was first successfully scanned for VM or PC – either by a regular scan or Cloud Agent assessment. For PC, you must have OS CPE enabled (under PC > Reports > Setup) to capture this date.

EC2 Scans – Exclude Terminated Instances

We'll automatically filter out all EC2 instances with a Terminated status from your EC2 scans (on demand and scheduled), removing the dead EC2 instances from the scans. Note that the Launch EC2 Scan Preview – which appears after you launch an on demand EC2 scan – will continue to list Terminated instances. The filtering happens after the scan job is submitted to the scanner.

Issues Addressed

- When an OS change is detected, we now correctly display the NetBIOS Hostname in the General Information panel of the Host Information page.
- We now display the last scan date when the scan was launched on the host in Last Vulnerability Scan information for the host.
- Policy Compliance dashboard now shows the failing percentage as 1% for a policy with minimal failure, for the Top 5 failing policies.
- When you relaunch an EC2 policy scan, we now display the correct window with correctly populated fields related to EC2 scan (and not regular policy scan).
- Previously, when you relaunched an EC2 vulnerability scan, the drop-down for scanner appliances > build my list > available appliances was being displayed by default. This is fixed, and the drop-down is now displayed only when you click the corresponding down arrow.
- The scanner appliances drop-down for EC2 vulnerability scan now displays the appliances in a specific order, starting from the alphabetically sorted scanner appliances in selected VPC and then scanners in other VPCs in the same region. For EC2-Classic, EC2-All VPC and EC2-Selected VPC options, the connected appliances are listed above the disconnected ones for any VPC / Region."
- Previously, a scanner assigned to a custom network was scanning assets of the Global Default Network as well. Now this issue is fixed, and the scanner assigned to a custom network will scan assets from that custom network only.
- While editing a scanner appliance, the Protocol value under Proxy Settings, is now fixed to HTTP. The option to select HTTPS is now removed, as connecting the scanner to EC2 through proxy servers via HTTPS is not supported. Existing HTTPS protocols are automatically converted to HTTP.
- You can now provide a longer name (maximum 32 characters) for virtual scanner appliances.
- An email is sent to the user when a scan/map is trying to execute on a scanner appliance that is either offline or unavailable. We've improved the text in this email for better understanding and clarity.
- CSV report with merged agent data now shows the tracking method for agents.
- Users are now able to see the Cloud agent URL in VM > Help > About (General Information tab)
- When using the option profile setting Close Vulnerabilities on Dead Hosts, we'll now mark Vulnerabilities (QIDs) associated with a dead host as Fixed even if there are no remediation tickets associated with those vulnerabilities. You need to get this feature enabled in the subscription before you can use it.

- VM Scan API /api/2.0/fo/schedule/scan/ now accepts maximum 255 characters for the parameter connector_name.
- Previously, the Update Asset IP API /api/2.0/fo/asset/ip/?action=update displayed the "invalid identifier" error while updating a large number of IP address at a time. Now this issue is fixed and the update happens successfully.
- Fixed an issue with the online help search on the Contact Support page (Help > Contact Support).
- Updated the documentation for the Asset Group API V2 (/api/2.0/fo/asset/group/) to remove inaccurate note about IPs being ignored when added to an asset group.