Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.21.1

January 2, 2023

What's New

This new release of the Qualys Cloud Platform (VM, PC) includes improvements to Vulnerability Management and Policy Compliance.

Qualys Cloud Platform

Privileges added to Administrator user role to "manage user account" permission.

New Technology Support: Neo4j Database for Instant Data Collection using an OS Auth Record

Qualys Policy Compliance (PC/SCAP/SCA)

New Technology Support: MongoDB 5.x

Qualys 10.21.1 brings you many more improvements and updates! Learn more

Priviliges added to Administrator user role to “manage user account” permission.

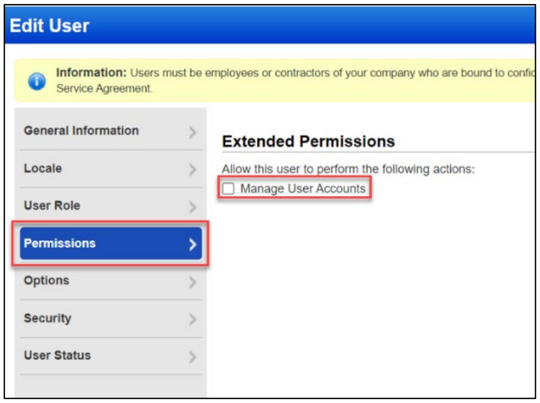
With this release, the Administrator user role can "manage user account" permission of the Manager/Unit Manager/Administrator role in the subscription except for the POC user. The Administrator user role will be able to create/edit Users and the User Administrator user, can enable/disable the “**Manager User Account**” permission of the Manager/Unit Manager role. The “Manager User Account” permission value will be enabled by default.

Pre-requisites

Contact Qualys support or TAMs to get this option available in your subscription.

Perform the following steps if you are in need to manage specific user permissions:

1. Log in through the Administrator user.
2. Navigate to **Users** > **Users**, and select the user.
3. Click the **Edit** option from the Quick actions menu.
4. Go to the **Permissions** tab and select/deselect the "**Manage User Accounts**" checkbox for the Manager/Unit Manager role.


Edit User

Information: Users must be employees or contractors of your company who are bound to confid
Service Agreement.

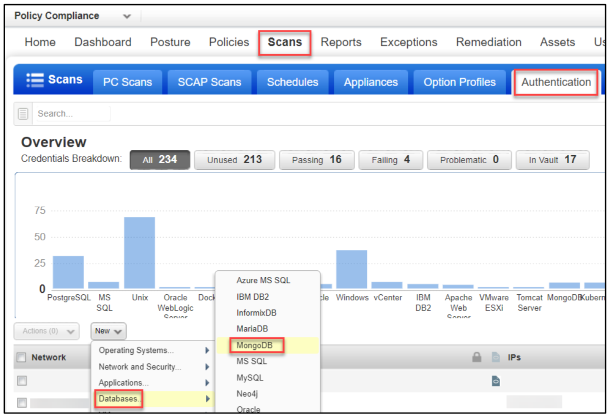
Extended Permissions

Allow this user to perform the following actions:

□ Manage User Accounts

New Technology Support: MongoDB 5.x

We have extended our support for database level checks for MongoDB Authentication to include MongoDB 5.x. Now when the user uses the MongoDB authentication record for scanning, they can now scan MongoDB 5.x databases and perform database level checks. Go to **Scans > Authentication > Databases > MongoDB.**


Overview

Credentials Breakdown: All 234 | Unused 213 | Passing 16 | Failing 4 | Problematic 0 | In Vault 17

New Technology Support: Neo4j Database for Instant Data Collection using an OS Auth Record

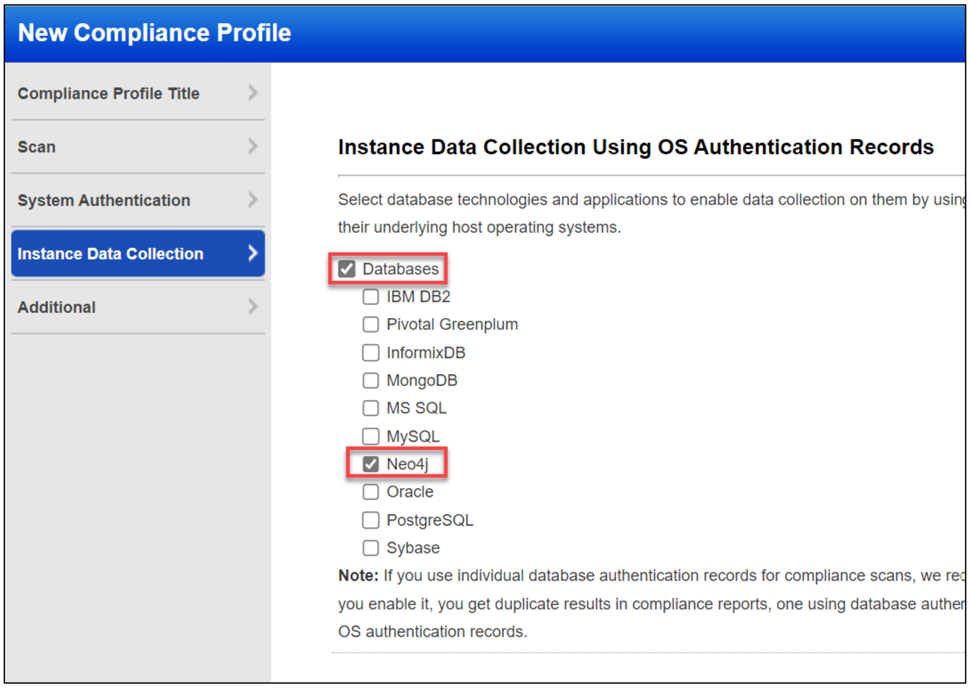
We've added a new technology support Neo4j to collect an OS-based instance data for Neo4j DB technology using an OS auth record. You can generate the policy report, authentication report, and compliance results for the Neo4j database.

Enabling OS Authentication-Based Data Collection for Neo4j Database Instances

Go to **Scans** > **Options Profile** > **New** > **Compliance Profile** > **Instance Data Collection** and select the **Neo4j** checkbox under the **Databases** section.

After you save your changes, the settings in the profile are used in the next compliance scan. You can always go back and review your compliance profile information and edit it if required.

Once you save your Neo4j DB instance details, they will appear in compliance results, policy reports, and authentication reports.



Instance Data Collection Using OS Authentication Records

Select database technologies and applications to enable data collection on them by usin
their underlying host operating systems.

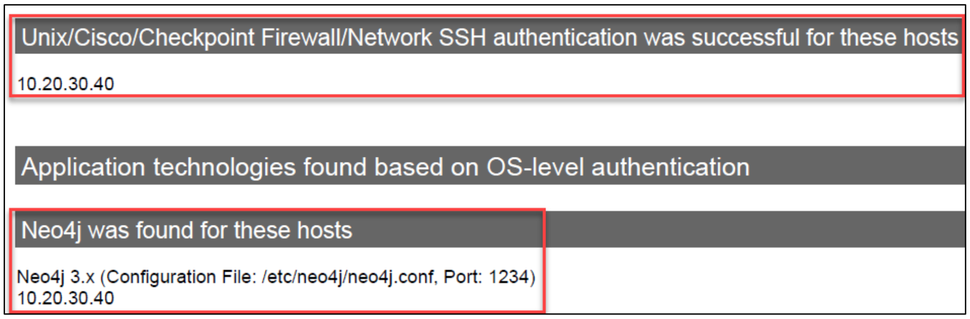
☑ Databases
- ☐ IBM DB2
- ☐ Pivotal Greenplum
- ☐ InformixDB
- ☐ MongoDB
- ☐ MS SQL
- ☐ MySQL
- ☑ Neo4j
- ☐ Oracle
- ☐ PostgreSQL
- ☐ Sybase

Note: If you use individual database authentication records for compliance scans, we rec
you enable it, you get duplicate results in compliance reports, one using database authen
OS authentication records.

Sample Reports: Compliance Scan Result

Note: If you have run the host scans using Unix, you will find the details under the Unix section, if not, the field will be empty. In Compliance scan result report, you will find the **Neo4j** details under **Application technologies found based on OS-level authentication.**

Here's a sample report where you'll see the compliance scan results for the **Neo4j database.**



Unix/Cisco/Checkpoint Firewall/Network SSH authentication was successful for these hosts

10.20.30.40

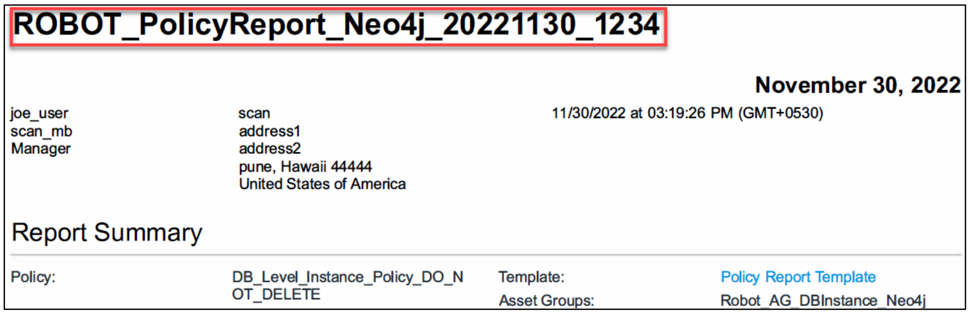
Application technologies found based on OS-level authentication

Neo4j was found for these hosts

Neo4j 3.x (Configuration File: /etc/neo4j/neo4j.conf, Port: 1234)
10.20.30.40

Sample Reports: Policy Report

Here's a sample policy report where you can check the policy status of the **Neo4j** instances that are scanned by using the underlying OS authentication records.



ROBOT_PolicyReport_Neo4j_20221130_1234

November 30, 2022

joe_user
scan_mb
Manager

scan
address1
address2
pune, Hawaii 44444
United States of America

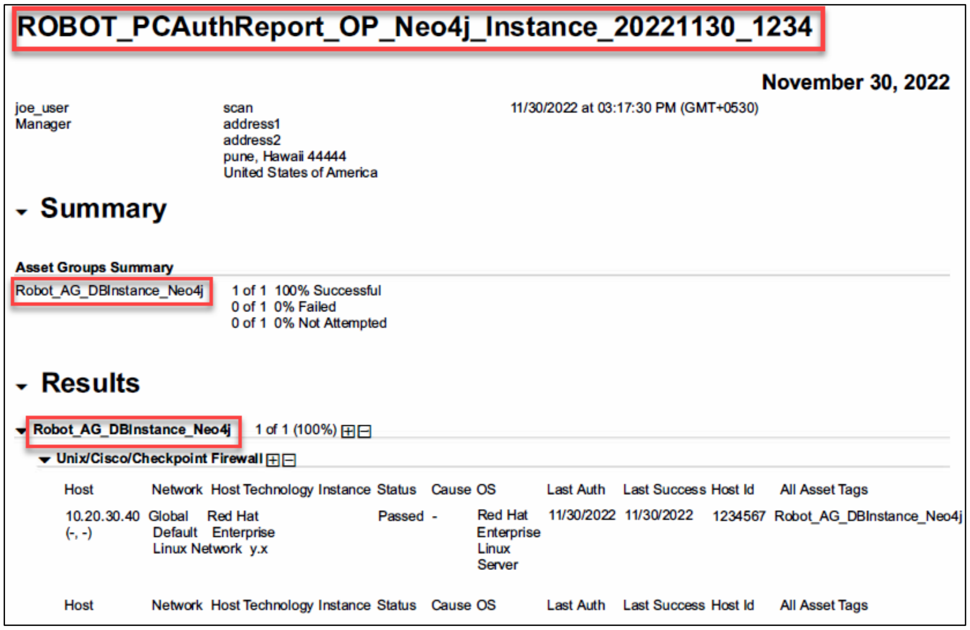
11/30/2022 at 03:19:26 PM (GMT+0530)

Report Summary

Policy:	DB_Level_Instance_Policy_DO_NOT_DELETE	Template:	Policy Report Template
		Asset Groups:	Robot_AG_DBInstance_Neo4j

Sample Reports: Authentication Report

Here's a sample authentication report where you can check the authentication status of the **Neo4j** instances that are scanned by using the underlying OS authentication records.



ROBOT_PCAuthReport_OP_Neo4j_Instance_20221130_1234

November 30, 2022

joe_user
Manager

scan
address1
address2
pune, Hawaii 44444
United States of America

11/30/2022 at 03:17:30 PM (GMT+0530)

Summary

Asset Groups Summary

Robot_AG_DBInstance_Neo4j	1 of 1 100% Successful 0 of 1 0% Failed 0 of 1 0% Not Attempted

Results

Robot_AG_DBInstance_Neo4j 1 of 1 (100%) ⊞⊟

Unix/Cisco/Checkpoint Firewall ⊞⊟

Host	Network	Host Technology	Instance	Status	Cause	OS	Last Auth	Last Success	Host Id	All Asset Tags
10.20.30.40 (-, -)	Global Default Linux Network	Red Hat Enterprise y.x		Passed	-	Red Hat Enterprise Linux Server	11/30/2022	11/30/2022	1234567	Robot_AG_DBInstance_Neo4j
Host	Network	Host Technology	Instance	Status	Cause	OS	Last Auth	Last Success	Host Id	All Asset Tags

Issues Addressed

- We fixed an issue where the used report storage size was not getting correctly updated in a few cases.
- We fixed an issue where the remediation tickets were not getting created from the Unit manager's account for the remediation policies created by the manager.
- The following issue was observed regarding running the scan-based report in the case of a user with the Unit Manager role. When the user opened the 'Select Scan Results' page, a particular number of scan results were shown on that page. Upon simply closing and opening that page again, a different number of scan results were shown. We have now fixed this issue about the discrepancy in the number of scan results shown on the 'Select Scan Results' page.
- From Vulnerability Management, while searching for tags from the 'Asset Search' tab, no tags were shown though the tags were available. Also, the same issue was observed in the case of the user with the Manager Account role. We have fixed this issue now.
- We have resolved an error that the customer encountered after launching an encrypted patch report in PDF format.
- We fixed an issue where the customer was facing an issue uploading a csv file for the vCenter-vmware map due to blank/empty rows at the end. Now empty rows in csv are handled.
- We have fixed an issue where the Asset Group name in the CVSS Environment column was not generated in the downloaded scan report.
- We have fixed an issue where user was unable to edit existing report template where Report Template Title is exceeding char limits set and getting "Unknown Error has Occurred" error status.
- We fixed an issue where the sub-users encountered HTTP ERROR 500 while checking the summary and information of scheduled scans created by other users for the in-scope and out-of-scope asset groups.
- For subscriptions with AGMS enabled, we fixed an issue where the Associated Ags column did not display asset group data in a report for Reader user.
- Previously, the consultant report excluded all operating systems irrespective of the exclusions specified in the template. The report now displays the operating systems correctly as specified in the template.
- The vulnerability scorecard report failed when users tried generating it with the All Asset Groups option selected. The report is now generated correctly.
- We have introduced an error message to display when sub-users try to launch patch reports with Asset Group/IP and Asset Tag together. Sub-users can select either Asset Tag or Asset Group/IP.
- We fixed an issue where the 'next launch' field displayed incorrect time for Schedule scan or Schedule report when the selected Time Zone is of <America/North_Dakota/New_Salem> and when Daylight Saving is enabled.
- We fixed an issue where the customer encountered that the API for Ignoring QID with asset groups parameter ignores QID in all the assets in which QID was flagged. We have fixed the API call to ignore requested QID's from mentioned Asset group only in API call.

- We have fixed an issue, where when we download Scanner appliances list from Scan/Appliances Tab UI, it contains the platform provider column information when selected from the UI.
- When a user triggers a map scan and configures/approves hosts, the map scan result was displayed empty. Now, we have fixed this issue so that the map scan result is correctly displayed while approving the hosts.
- We have now improved the error message for Reader user. The error message is displayed when a Reader user is trying to generate the report on the assets which are not in his scope (for AGMS accounts only).
- We fixed an issue to run the VMDR bundle successfully without having to change the ITAM license type to Free.
- While extending the prospect account, we were getting the blank and incorrect info. This issue is fixed for the prospect account.
- We fixed an issue where sales role user is now able to extend prospect account and update it into VMDR Trial.
- We fixed an issue where CloudView Free is now processed correctly. Now, the expiration date is set correctly for CloudView.
- We fixed an issue of scans that are getting stuck in the uploading state when a user, who owns any offline scanner, is deleted. The scans are now being uploaded without any issues.
- We fixed an issue for the manager users to successfully create the remediation tickets from 'Host_info page' for AGMS enabled accounts in VMDR.
- We fixed an issue to make sure that the Unit Manager users do not see the “Scheduled Scan and Scheduled Maps” of IPs that are not assigned to them in VM and PC. Users must select the checkbox of “Restrict view of scheduled tasks on unassigned assets” option to restrict the Unit Manager’s access.
- We fixed an issue to start the Scheduled Map scan at the scheduled time in custom network.
- We fixed an issue of Activity logs getting updated with unknown user when Assets/Domain are updated in VM and PC.
- We fixed an issue where customers were able to create exceptions for SCA-only assets or agents, and these exceptions were automatically getting removed when the next pc scan processing was triggered which will not happen as we are not allowing customers to create the exception for SCA-only accounts.
- We fixed an issue for scan processing, where the data for inactive instances are getting deleted from the table which was not happening earlier.
- We fixed an issue for compliance scan processing, where the policy compliance report results are shown/displayed as blank even though the data exists.