Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.21.3

February 7, 2023

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

Qualys Policy Compliance (PC/SCAP/SCA)

MongoDB Instance Discovery and System Record Creation

Configure Oracle System Record Template for Multitenant Container Database

Qualys 10.21.3 brings you many more improvements and updates! Learn more

MongoDB Instance Discovery and System Record Creation

This release introduces instance discovery and auto record creation for MongoDB authentication. This functionality is already available for other technologies like Apache Web Server, IBM WebSphere, Jboss, Tomcat and Oracle. There are a few notable differences for MongoDB though. When we auto discover MongoDB instances, we'll discover the target configuration for each instance but not the login credentials. We've introduced a new configuration called "MongoDB System Record Template" that you'll use to provide MongoDB login credentials for system created records. You'll create the system record template and then select it in the option profile used for discovery scans. The template is linked automatically to the system created records created as a result of the scan.

Benefits

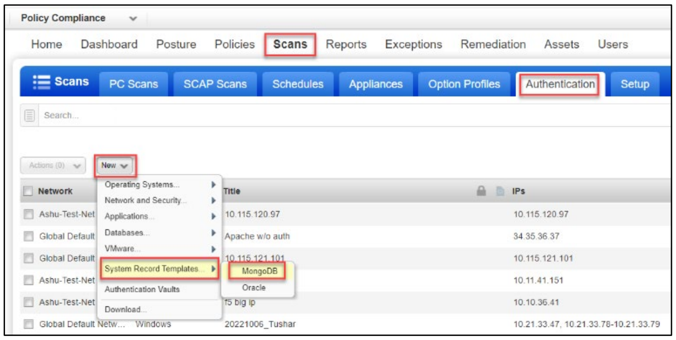
- We'll auto discover MongoDB instances on each scanned host and create authentication records for those instances. We support auto-discovery and system record creation for MongoDB instances running on Unix platforms. Make sure you have Unix authentication records in your account for hosts running MongoDB.
- When we create MongoDB authentication records for discovered instances, we'll insert the credentials from the MongoDB system record template you selected in the option profile.
- You can easily rotate MongoDB passwords. Edit the credentials in the MongoDB system record template and all MongoDB records linked to the template will be updated to use the new credentials with no additional scan or action by you.
- You can edit individual MongoDB system-created records and save them as user-created. This allows you to change the credentials for individual records without changing the credentials for all records associated with a template.

How it works

Here's the basic flow for MongoDB instance discovery and auto record creation.

1. Create a MongoDB system record template and enter the login credentials you want to use for system-created records.
2. Select the MongoDB system record template in the compliance option profile you want to use for discovery scans.
3. Launch your discovery scan. Your scan results will list the auto-discovered instances.
4. In the authentication list you'll see newly created MongoDB records. For each system-created record, you'll see the template associated with the record.

Go to **Scans** > **Authentication** > **New** > **System Record Templates** > **MongoDB**.



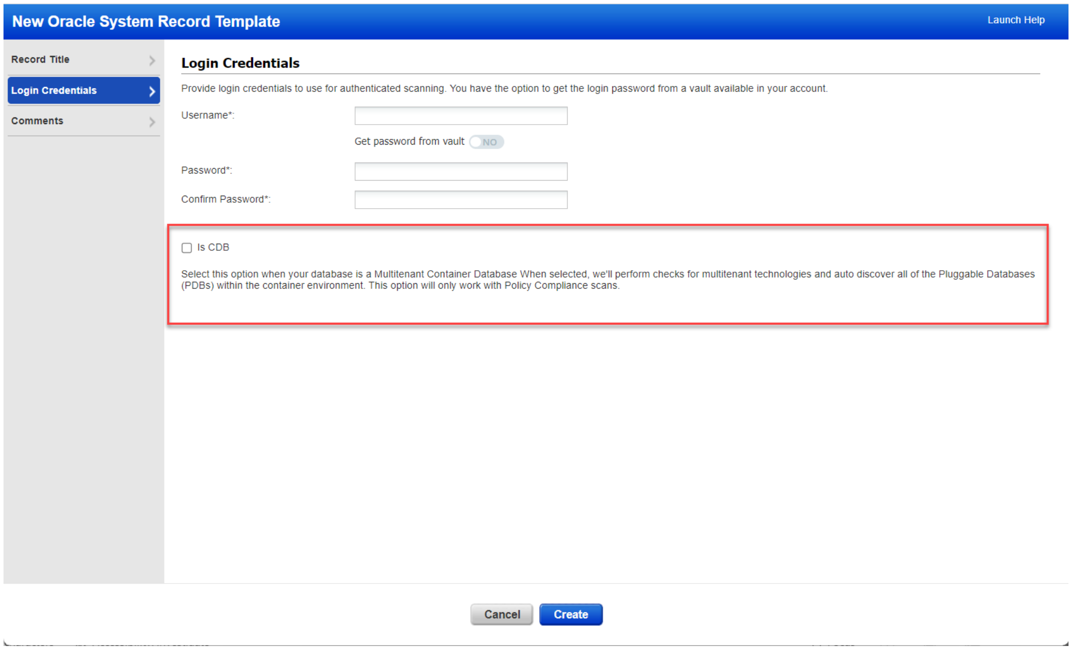
Network		Title	IPs
Ashu-Test-Net		10.115.120.97	10.115.120.97
Global Default		Apache w/o auth	34.35.36.37
Global Default		10.115.121.101	10.115.121.101
Ashu-Test-Net			10.11.41.151
Ashu-Test-Net		f5 big ip	10.10.36.41
Global Default Netw...	Windows	20221006_Tushar	10.21.33.47, 10.21.33.78-10.21.33.79

For details, refer to online help.

Configure Oracle System Record Template for Multitenant Container Database

We added a new option in the Oracle system record template record called “Is CDB” to support this feature. There is no longer a need for customers to create individual template records for each pluggable database in the CDB. Customers can select this new option in the Oracle system record template.

Note: This option is supported for Policy Compliance scans only.



Login Credentials

Provide login credentials to use for authenticated scanning. You have the option to get the login password from a vault available in your account.

Username*:

Get password from vault NO

Password*:

Confirm Password*:

□ Is CDB

Select this option when your database is a Multitenant Container Database When selected, we'll perform checks for multitenant technologies and auto discover all of the Pluggable Databases (PDBs) within the container environment. This option will only work with Policy Compliance scans.

For details, refer to Online help.

Issues Addressed

- We fixed an issue where the users were getting scan status as "Failed" instead of "No Host Alive." Now users will see the "No Host Alive" status for the host scan result for which all hosts are not alive.
- With this release, we have improvised our database query to handle large data in the scorecard report stats. Earlier user was facing a "Snapshot too old" error for large data, This has been fixed now.
- We fixed an issue where the users having AG's in the policy without any error could not fetch Policy List using an API call for a Non-AGMS account.
- Fixed the issue where the customer could not launch & download compliance reports for PC/SCA. Now users can launch reports and download them in all formats.
- We fixed an issue where the launch scan page remained in a loading state for a long time. We improved the scan launch workflow.
- We fixed an issue where the user was not able to launch the Scheduled Vulnerability Scan on new assets due to the restriction of the number of characters in the Asset Groups field.
- When user selected All scanners in Tagset option for the Scanners Appliance field while launching the scan, the user was not able to exclude the IP network range tags. We fixed this issue by improving the scan launch workflow.
- We have fixed an issue where different First Found dates were shown in the Asset Search Report and the Host Information page.
- We have fixed an issue where the "Tags are unavailable at this time" error was shown in the Scan Status for a scheduled scan.
- We have fixed an issue where the colon symbol next to the "Network" option was missing in the details shown by clicking the Asset Groups tab.
- We have fixed an issue wherein the user was unable to run a VM scan with the following specification in the option profile:
  - Vulnerability Detection: Complete
  - Include: Oval Checks or QRDI checks
- We have fixed an issue where TrueRisk details (Asset Risk Score (ARS), Asset Criticality Score (ACS), and Qualys Detection Score (QDS)) did not populate in vulnerability reports.
- We have fixed an issue where the name of the user who launched a scan for external sites in CertView and VMDR did not appear correctly; the username of the POC Manager appeared instead. This issue is now fixed, and the name of the user launching the scan is now correctly displayed.
- We have fixed an issue for AGMS-enabled accounts where the default scanner appliance while editing an asset group changed automatically upon saving.
- Previously, users encounter delays in the loading of the Remediation tab from the VMDR UI due to a high remediation ticket count. With this release, we have improved the navigation speed.
- We have fixed an issue where the downloading of the PDF report would stuck during the process.
- Previously, when users generated the scan report for PDF format they would encounter PHP fatal error. This issue is now resolved and the scan reports can be successfully generated in PDF format.
- Fixed an issue wherein the PC Posture Steaming API failed with a time-out error. The "evidenceTruncationLimit" parameter has been introduced in this release to enable you to truncate current and unexpected values from evidence data.

  Use **evidenceTruncationLimit=0** if you do not want your evidence data to be truncated.
  Use **evidenceTruncationLimit=1** to fetch evidence data, which includes 100 lines by default.