# Qualys Cloud Platform (VM, PC) 10.x

## Release Notes

Version 10.20.4
October 13, 2022

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

### Qualys Policy Compliance (PC/SCAP/SCA)

New Technology Support: Red Hat OpenShift Container Platform 4.x (Scanner)

**Qualys 10.20.4 brings you many more improvements and updates!** Learn more

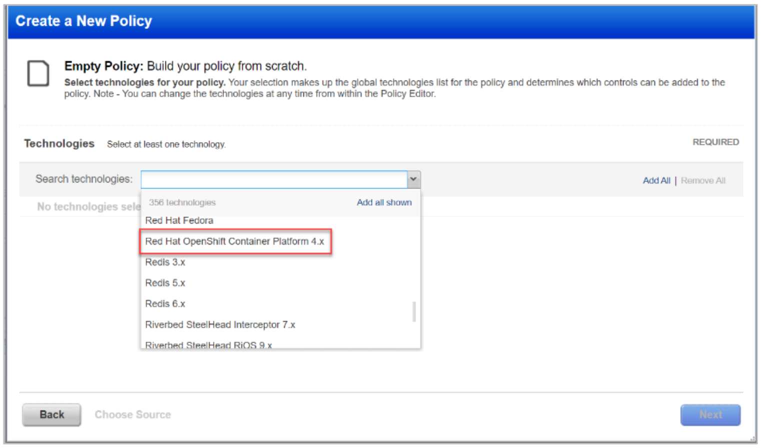
## New Technology Support: Red Hat OpenShift Container Platform 4.x (Scanner)

We’ve added support for Red Hat OpenShift Container Platform 4.x on Unix hosts. This technology is supported for authenticated scans using a scanner.

You’ll need a Unix record defined for the host running the server. Go to **Scans** > **Authentication** > **New** to create new authentication records for Unix.

### Policies and Controls

You’ll see **Red Hat OpenShift Container Platform 4.x** in the **Technologies** list when creating new policies and when searching controls by technology.


Create a New Policy

**Empty Policy:** Build your policy from scratch.
**Select technologies for your policy.** Your selection makes up the global technologies list for the policy and determines which controls can be added to the policy. Note - You can change the technologies at any time from within the Policy Editor.

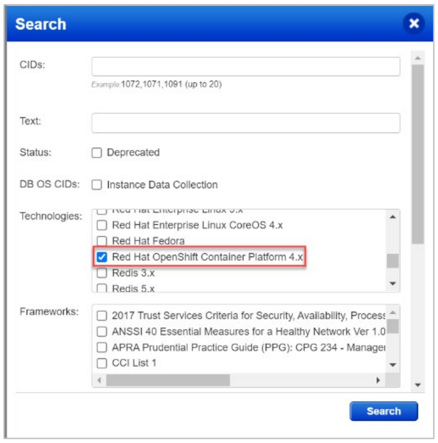
Technologies Select at least one technology. REQUIRED

Search technologies:

No technologies sele

356 technologies

- Red Hat Fedora
- Red Hat OpenShift Container Platform 4.x
- Redis 3.x
- Redis 5.x
- Redis 6.x
- Riverbed SteelHead Interceptor 7.x
- Riverbed SteelHead RiOS 9.x


Search

CIDs:
Example 1072,1071,1091 (up to 20)

Text:

Status: □ Deprecated

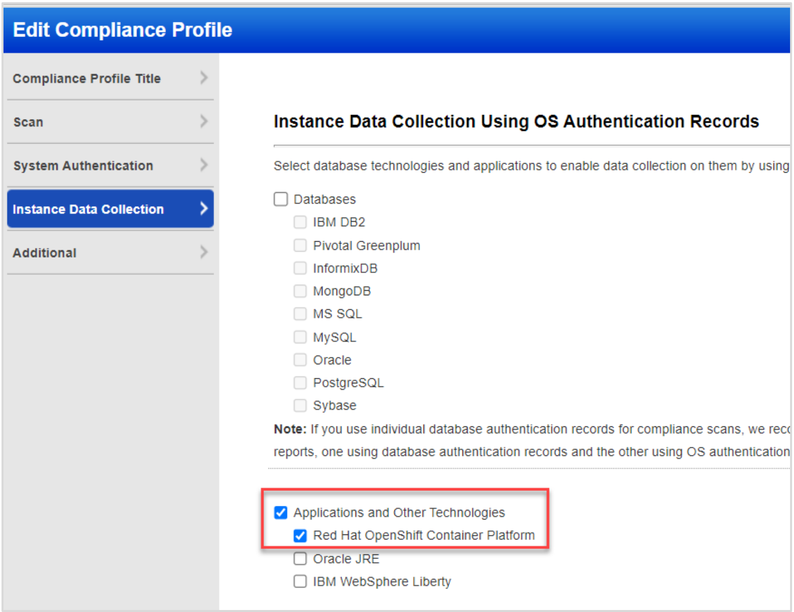
DB OS CIDs: □ Instance Data Collection

Technologies:
□ Red Hat Enterprise Linux CoreOS 4.x
□ Red Hat Fedora
☑ Red Hat OpenShift Container Platform 4.x
□ Redis 3.x
□ Redis 5.x

Frameworks:
□ 2017 Trust Services Criteria for Security, Availability, Process
□ ANSSI 40 Essential Measures for a Healthy Network Ver 1.0
□ APRA Prudential Practice Guide (PPG): CPG 234 - Managei
□ CCI List 1

### Enabling OS Authentication-Based Data Collection for Red Hat OpenShift Container Platform Instances

Go to **Scans** > **Options Profile** > **New** > **Compliance Profile** > **Instance Data Collection** and select the **Red Hat OpenShift Container Platform** checkbox under the **Applications and Other Technologies** section.



Instance Data Collection Using OS Authentication Records

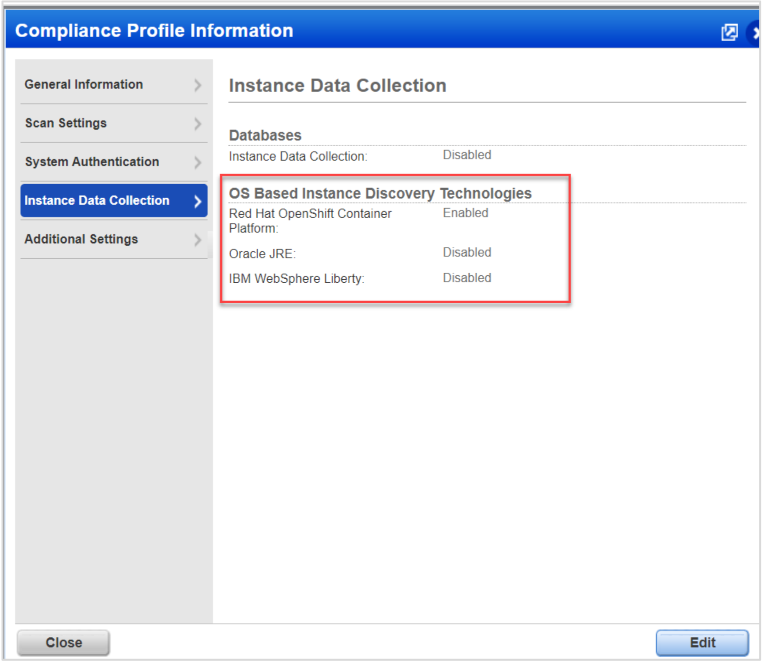
Select database technologies and applications to enable data collection on them by using

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

**Note:** If you use individual database authentication records for compliance scans, we rec
reports, one using database authentication records and the other using OS authentication

- ☑ Applications and Other Technologies
  - ☑ Red Hat OpenShift Container Platform
  - ☐ Oracle JRE
  - ☐ IBM WebSphere Liberty

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.



Instance Data Collection

Databases

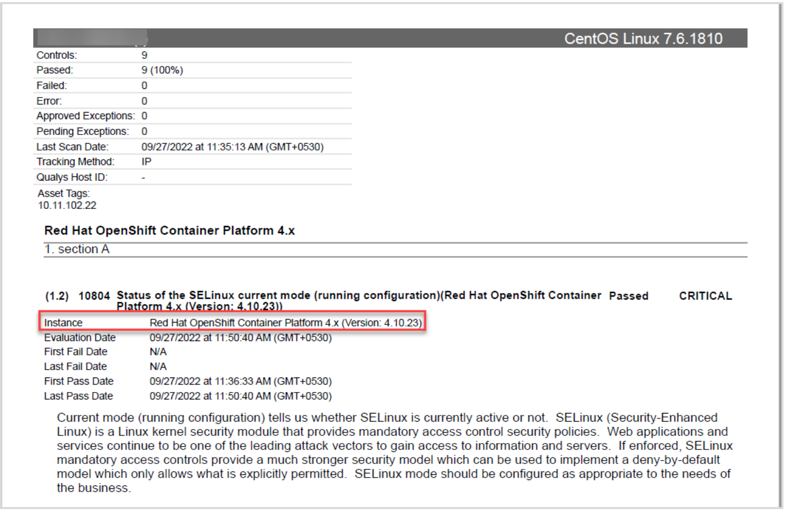
| | |
|---|---|
| Instance Data Collection: | Disabled |

OS Based Instance Discovery Technologies

| | |
|---|---|
| Red Hat OpenShift Container Platform: | Enabled |
| Oracle JRE: | Disabled |
| IBM WebSphere Liberty: | Disabled |

## Sample Report

Here’s a sample report where you’ll see the **Red Hat OpenShift Container Platform 4.x** instance for scanned hosts.



[redacted] CentOS Linux 7.6.1810

|  |  |
|---|---|
| Controls: | 9 |
| Passed: | 9 (100%) |
| Failed: | 0 |
| Error: | 0 |
| Approved Exceptions: | 0 |
| Pending Exceptions: | 0 |
| Last Scan Date: | 09/27/2022 at 11:35:13 AM (GMT+0530) |
| Tracking Method: | IP |
| Qualys Host ID: | - |

Asset Tags:
10.11.102.22

**Red Hat OpenShift Container Platform 4.x**

1. section A

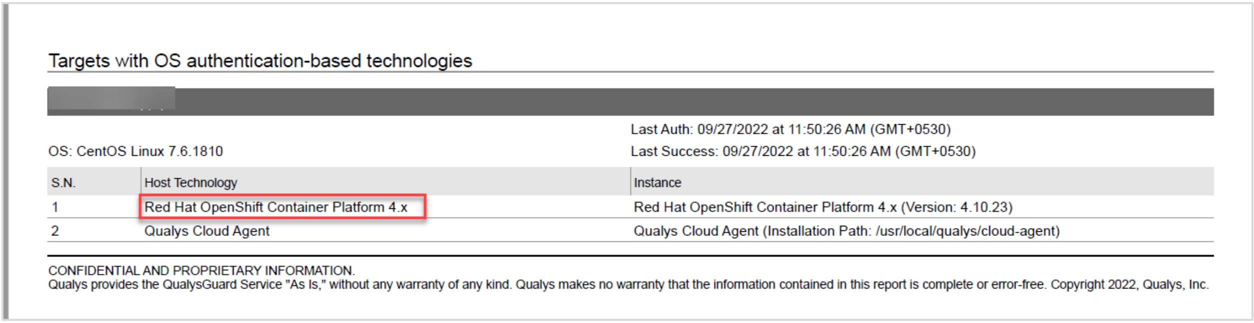
**(1.2) 10804 Status of the SELinux current mode (running configuration)(Red Hat OpenShift Container Platform 4.x (Version: 4.10.23)) Passed CRITICAL**

|  |  |
|---|---|
| Instance | Red Hat OpenShift Container Platform 4.x (Version: 4.10.23) |
| Evaluation Date | 09/27/2022 at 11:50:40 AM (GMT+0530) |
| First Fail Date | N/A |
| Last Fail Date | N/A |
| First Pass Date | 09/27/2022 at 11:36:33 AM (GMT+0530) |
| Last Pass Date | 09/27/2022 at 11:50:40 AM (GMT+0530) |

Current mode (running configuration) tells us whether SELinux is currently active or not. SELinux (Security-Enhanced Linux) is a Linux kernel security module that provides mandatory access control security policies. Web applications and services continue to be one of the leading attack vectors to gain access to information and servers. If enforced, SELinux mandatory access controls provide a much stronger security model which can be used to implement a deny-by-default model which only allows what is explicitly permitted. SELinux mode should be configured as appropriate to the needs of the business.

## Sample Authentication Report

Here’s a sample authentication report where you can check the authentication status of the **Red Hat OpenShift Container Platform 4.x** instances that are scanned by using the underlying OS authentication records.



Targets with OS authentication-based technologies

[redacted]

OS: CentOS Linux 7.6.1810

Last Auth: 09/27/2022 at 11:50:26 AM (GMT+0530)
Last Success: 09/27/2022 at 11:50:26 AM (GMT+0530)

| S.N. | Host Technology | Instance |
|---|---|---|
| 1 | Red Hat OpenShift Container Platform 4.x | Red Hat OpenShift Container Platform 4.x (Version: 4.10.23) |
| 2 | Qualys Cloud Agent | Qualys Cloud Agent (Installation Path: /usr/local/qualys/cloud-agent) |

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2022, Qualys, Inc.

## Issues Addressed

- We fixed a performance issue when processing PC scan results for scans launched on asset groups that contain DNS hosts. This performance issue also had an impact on VM report generation where users got reports with no Hosts Matching Filters.
- Applicable to CSV reports generated in subscriptions with Policy Compliance Reporting Service (PCRS) enabled. The values that appeared in the various date columns in the CSV reports contained an extra space just before the timestamp. We fixed this issue by removing the extra space in all date columns.
- Applicable to CSV reports generated in subscriptions with Policy Compliance Reporting Service (PCRS) enabled. We fixed an issue with the calculation used for the percentage value that appears in the Percentage column under Host Statistics (Percentage of Controls Passed per Host). The calculation didn't consider controls with a status of Error that had an approved exception that would change the status to Passed.
- Applicable to CSV reports generated in subscriptions with Policy Compliance Reporting Service (PCRS) enabled. We fixed an issue where the CSV report did not show the updated remediation value in the case where the remediation value had been updated at the policy level.
- Applicable to CSV reports generated in subscriptions with Policy Compliance Reporting Service (PCRS) enabled. We fixed an issue where Policy Reports included Remediation Info sections (For Failed Controls, For Passed Controls, For Error Controls) even when the Policy Report Template did not have these sections selected on the Layout tab. Now these sections will only appear when selected in the report template.
- Applicable to CSV reports generated in subscriptions with Policy Compliance Reporting Service (PCRS) enabled. We fixed an issue with downloading reports where the download completed but the status did not update to Finished, making the report unavailable.