Qualys Cloud Platform (VM, PC) v10.x

Release Notes

Version 10.9

March 26, 2021 (Updated May 12, 2021)

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

Qualys Cloud Platform

Asset Tag Support for Windows and Unix Authentication Records

Qualys Policy Compliance (PC/SCAP/SCA)

Perform Compliance Assessment of Oracle Multitenant Databases via Container Database
New Oracle Multitenant Technologies
Configure Auto Update Activity Logs
Support for OS authentication-based data collection in Compliance Option Profile
Support to Exclude Asset Tags from Policy Compliance Assessment
Support for New OCA Technology

Qualys Vulnerability Management (VM)

Whole Number CVSS Scores Now Appear with Decimal Point

Qualys 10.9 brings you more improvements and updates! **Learn more**

Qualys Cloud Platform

Asset Tag Support for Windows and Unix Authentication Records

We're excited to introduce asset tag support for Windows and Unix authentication records. With this support, you have the option to define target hosts in your authentication record using asset tags instead of adding IP addresses/ranges to the record. At scan time, we'll resolve the asset tags in the record to IP addresses in your account and scan them using the login credentials defined in the record. The tag selection is similar to other existing workflows with tag support.

Prerequisites

Please reach out to your Technical Account Manager or Qualys Support to enable these features:

- Asset Tagging must be enabled for your subscription

- Tag Support for Authentication Records must be enabled for your subscription

Some considerations and limitations for Initial Release

Please note the following for the initial release of Tag Support for Authentication Records:

- Asset tags are supported in Unix and Windows authentication records only.

- Asset tags are resolved at scan launch time and this could result in performance degradation.

- You cannot search for authentication records by asset tag.

- You cannot remove hosts from authentication records with tags using the "Remove Hosts" workflow from the Actions menu.

- Certain application and database authentication records require a Windows or Unix record with the same IP address(es) defined. In this case, you must create a Windows/Unix record with IPs/ranges. We cannot compare IP addresses in the application/database record against asset tags in the Windows/Unix record because tag resolution does not happen until scan launch time.

- Be careful not to save multiple records for the same type with the same tag included. The tag will be resolved to an IP address at scan time, and it will match multiple records in your account. If those records have different login credentials defined, then authentication could fail depending on which record is used by the scanner. We do not prevent you from adding an individual tag to a record that is already used in another record of the same type.

- When adding tags to a record using the API, we only validate whether the tags specified in your request are valid. We do not filter out system root level tags, such as Asset Group and Business Unit. We also do not check that the tags selected for a record with asset type "IP Range in Tag Rule" are valid for this asset type. Be mindful when making your tag selection.

- You'll see a new system root level tag called "Tag Set" in AssetView (under Assets > Tags) when you have authentication records with tags. It's important that you do not set this system root level tag as the parent to other tags in your account.

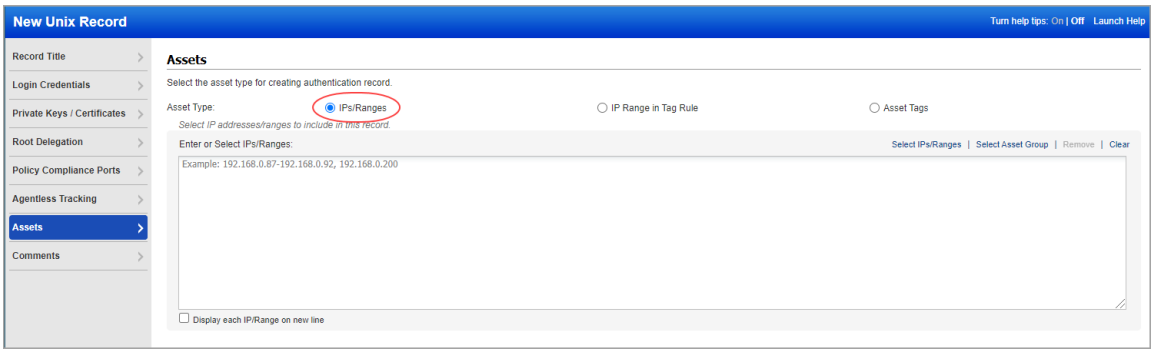
Changes in Windows and Unix Authentication Records

When configuring a Windows or Unix record, you'll notice that the **IPs** tab has been renamed **Assets**, and you'll be required to choose an asset type for the record. You'll see these asset type options: IPs/Ranges, IP Range in Tag Rule and Asset Tags. Your selection will determine the type of assets you'll add to the record.

For Windows records with domain level authentication, please note that you can only add assets when domain type is "NetBIOS, User-Selected IPs". The **Assets** section is disabled when domain type is "NetBIOS, Service-Selected IPs" or "Active Directory". This is the same as existing behavior where you can't add IPs to a record with these domain types.

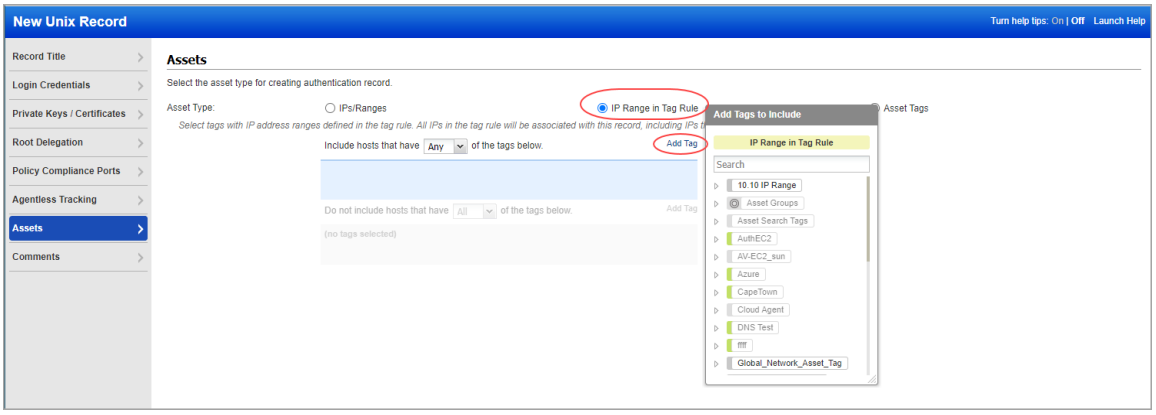
Asset Type: IPs/Ranges

Use this option to add IP addresses/ranges to the record. Enter the IP addresses/ranges in the field provided. (Same as in previous releases.)



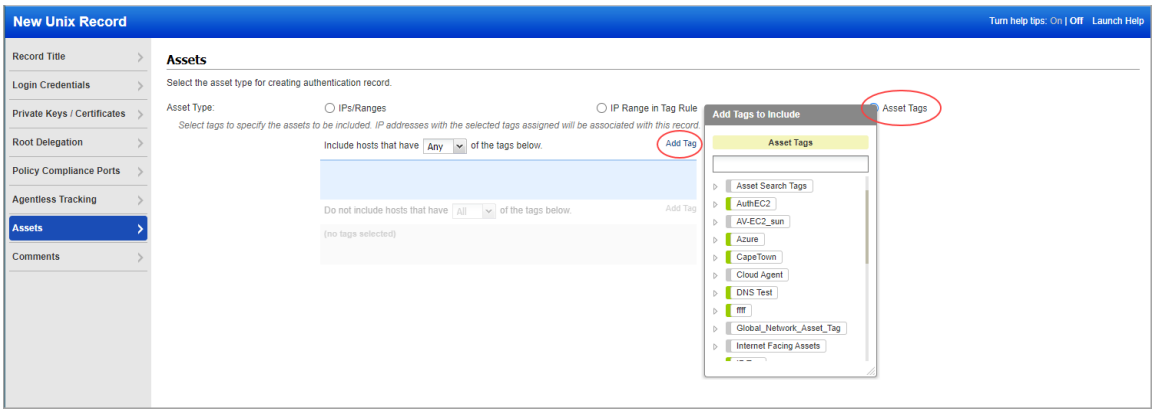
Asset Type: IP Range in Tag Rule

Use this option to add tags that have IP address ranges defined in the tag rule. All IP addresses defined in the tag rule will be associated with the record, including IPs that don't already have the tag assigned. Click Add Tag to pick tags to include or exclude. Note that only tags with the dynamic tag rule "IP Address in Range(s)" will be available in the tag selector.



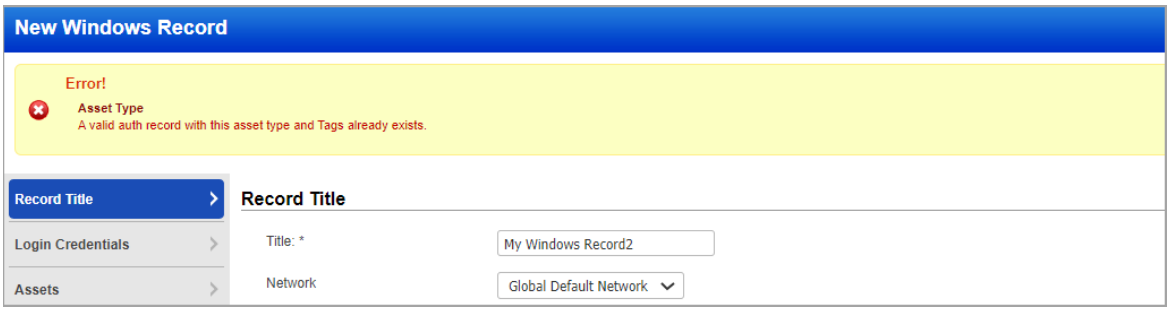
Asset Type: Asset Tags

Use this option to add tags to the record for the assets you want included. IP addresses with the selected tags already assigned will be associated with the record. Click Add Tag to pick tags to include or exclude.



Multiple records of same type with same Tag Set cannot be saved

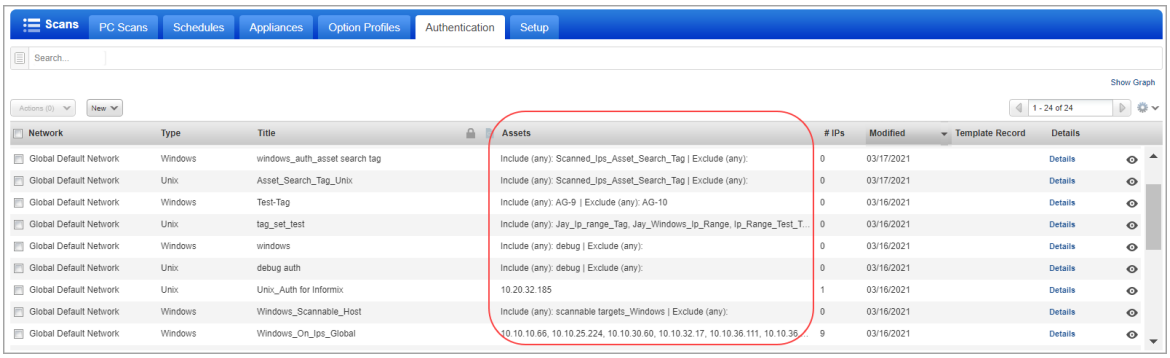
When you save a record with asset tags, we look at the combination tag settings, including the asset type ("IP Range in Tag Rule" or "Asset Tags"), the Included tags and tag scope (any, all), and the Excluded tags and tag scope. The combination of these settings create a single Tag Set tag on the backend. If you try to create another record of the same type with the same Tag Set, then an error will appear (as shown below). If any of the settings are different, then a new Tag Set tag is created and you will be allowed to save the record.



Change to Authentication Records List

On the **Authentication** tab you'll notice that the **IPs** column has been renamed **Assets**. In this column, you'll see the assets defined for each record – IP addresses or tags. For tags, we'll show tags that are Included with the any/all tag scope, and tags that are Excluded with the any/all tag scope. If no tags are excluded then no tags will be listed after the Exclude label. Also, the **#IPs** column will have a value of 0 for records with tags.

Here's a sample authentication records list. Note that when there are several tags in the record or tag names are long, the list of tags will be truncated.



Qualys Policy Compliance (PC/SCAP/SCA)

Perform Compliance Assessment of Oracle Multitenant Databases via Container Database

Now customers have the option to assess their Oracle multitenant databases for compliance via the container database (CDB). We added a new option in the Oracle record called "Is CDB" to support this feature. Customers simply select the new option in the Oracle record. There is no longer a need for customers to create individual records for each pluggable database in the CDB. Note that this option is supported for Policy Compliance scans only.

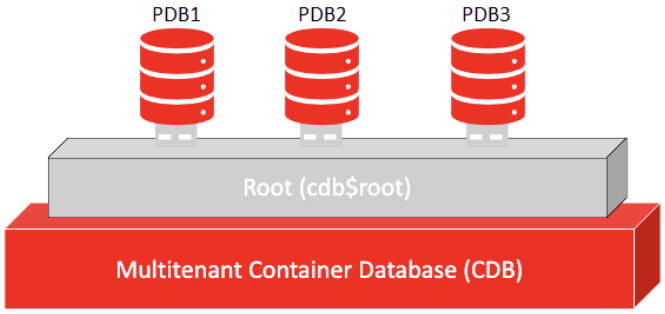
How it works

When "Is CDB" is selected in the Oracle record, the compliance scan will auto discover and assess all accessible Pluggable Databases (PDBs) within the container database (CDB). The assessment is performed through the CDB, which means there is no need for the scanner to connect directly to individual PDBs. This saves customers from having to create separate Oracle records for each PDB instance.

Identifying the Oracle database as a CDB in the Oracle record also ensures the right compliance checks are performed for multitenant technologies. We've introduced 3 new multitenant technologies in this release (Oracle 12c/18c/19c Multitenant) and we've rewritten compliance controls in order to assess the pluggable databases via the CDB.

Multitenant Container Database Architecture

Here's a sample container database with 3 pluggable databases. You'll create one record for the entire CDB. In previous releases, you had to create separate records for each database instance.



In this sample:

IP address = 10.10.10.1

CDB instance = ORCL

PDB instances = PDB1, PDB2, PDB3

Create an Oracle record with these settings: IP=10.10.10.1, service name=ORCL, Is CDB=enabled

We'll assess the CDB plus the 3 PDBs within the container database. Compliance evaluation data is collected across all of the database instances to determine the final posture. The data we collect across the instances is combined into a single Actual value that gets compared to the Expected value for the control to determine the Pass or Fail posture. See Sample Policy Report.

What are the steps?

Follow these steps to perform compliance assessment of your container database.

1) Set up a scan user account and privileges in the container database you want to scan with authentication. See Oracle Authentication (PC) for a set of scripts we've provided to help you set up the account and privileges for a multitenant container database scan.

2) Create an Oracle authentication record. In the record, you'll specify the scan user account from the first step, identify the target CDB (by SID or Service Name), select the "Is CDB" option, and add the IP address for the CDB. See Your Oracle Record.

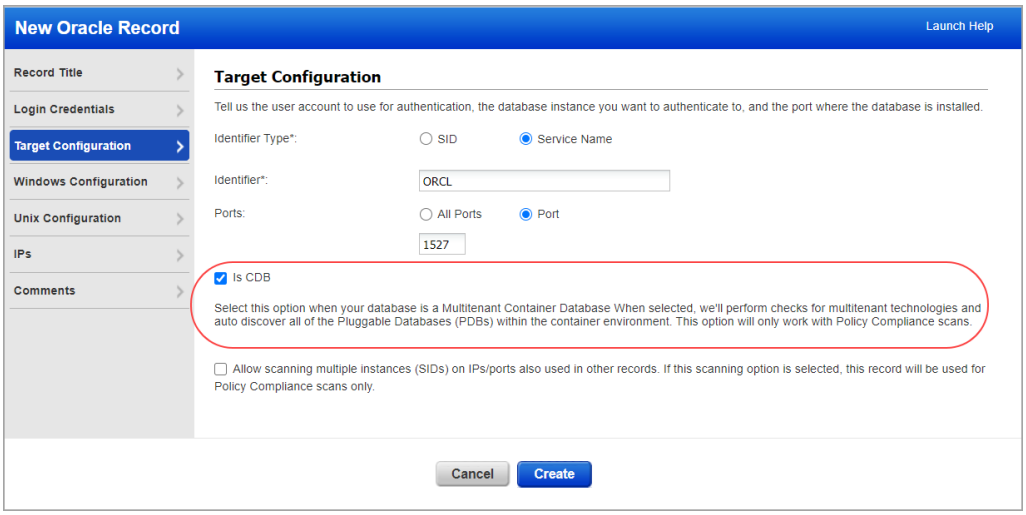
3) Start a new compliance scan. When the Oracle record has the "Is CDB" option enabled, the scanner will auto discover and assess all accessible Pluggable Databases (PDBs) within the container database at scan time. The assessment is performed through the CDB; we will not connect directly to individual PDBs. The Appendix section of your compliance scan results will show successful Oracle authentication. See Sample Scan Results.

4) Create a compliance policy with the new Oracle Multitenant technologies, the controls you want to assess on your CDB and PDBs, and an asset group containing the CDB IP address.

5) Run Policy Reports on your container database. The Evidence and Extended Evidence sections for each control will show the data collected on the CDB and across the PDBs within the container database. See Sample Policy Report.

Your Oracle Record

You'll see the new "Is CDB" option on the Target Configuration tab in your Oracle record.



What happens if the option "Is CDB" is selected for a non-Multitenant database instance?

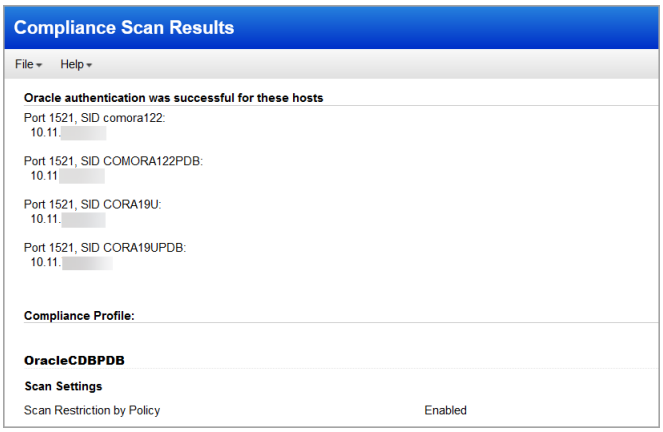
This depends on whether the necessary privileges required for CDB assessment are granted to the scan user account defined in the record. If the necessary privileges are granted, then assessment will still happen and will be reported under the Oracle Multitenant technology, however no PDBs will be enumerated in a non-Multitenant database instance. If the necessary privileges are not granted, then scan authentication will fail with insufficient privileges, highlighting which tables are lacking in privileges. The data reported will be the same for a non-Multitenant database instance whether "Is CDB" is selected or not. The only difference is the source of the retrieved data.

About system created authentication records

Please note that we cannot auto create Oracle authentication records for the CDB at this time. You can edit system records after they've been created to set the Is CDB option.

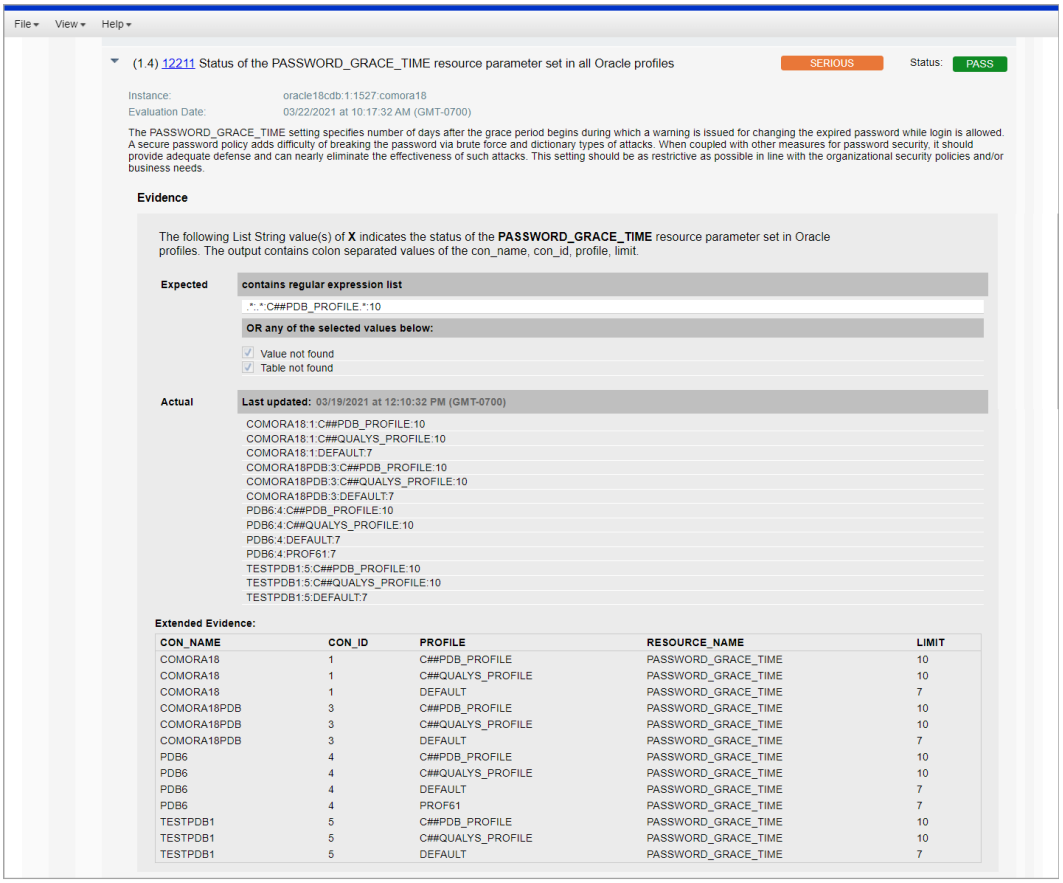
Sample Scan Results

The Appendix section of your Compliance Scan Results will indicate whether authentication was successful or not, under Oracle authentication.



Sample Policy Report

In the sample below, the control shows the PASSWORD_GRACE_TIME for the CDB as well as all the accessible pluggable databases within the CDB. With this feature, the CDB and the PDBs are assessed together with the same control. The Actual value for the control will list the PASSWORD_GRACE_TIME setting collected for the CDB and the PDBs that were assessed.



Extended Evidence

The Extended Evidence section will list the CDB and PDBs included in the control evaluation. The information shown in this section depends on the type of control being evaluated. For some controls, you'll see all the PDBs discovered in the CDB. For other controls, you'll see the CDB plus the PDBs that had a different setting than the CDB. For example, let's say there are 5 PDBs discovered in a CDB but only 2 had a different setting than the CDB. In this case, the Extended Evidence will include 3 lines – one for the CDB and one for each PDB with a different setting. If all the PDBs have the same setting as the CDB, then only 1 line will appear in the Extended Evidence section for the CDB.

The column CON_NAME shows the name for each container database and the column CON_ID shows the container database ID. Here's a look at CON_ID values:

- A value of 0 means the data pertains to the entire CDB.
- A value of 1 means the data pertains to the root.
- A value of 2 means the data pertains to the seed.
- A value of 3-254 means the data pertains to a PDB. Each PDB has its own container ID.

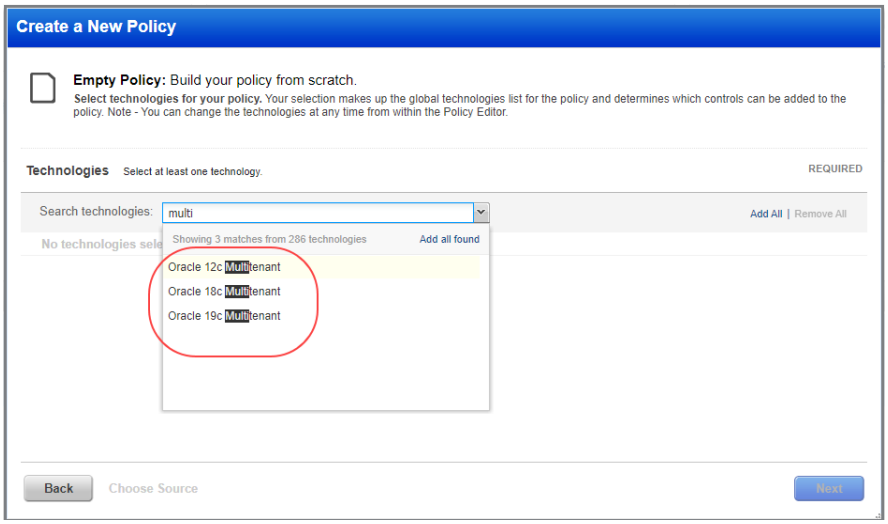
New Oracle Multitenant Technologies

To support the Oracle Multitenant Container Database (CDB) feature, we added support for these Oracle Multitenant database technologies:

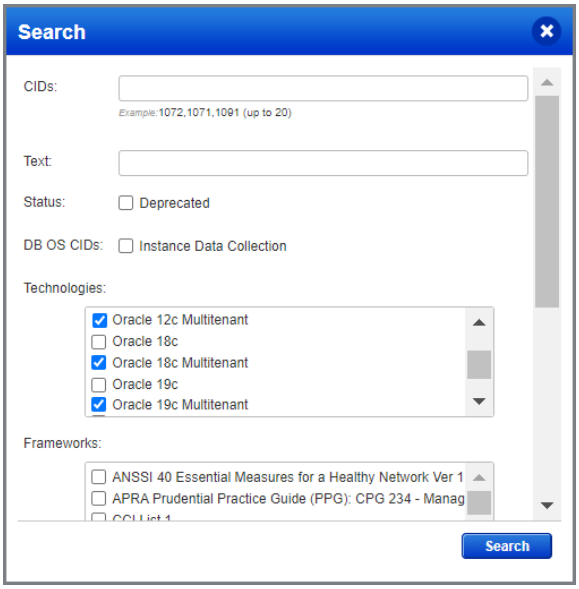
- Oracle 12c Multitenant
- Oracle 18c Multitenant
- Oracle 19c Multitenant

Policies and Controls

You'll see the Oracle Multitenant technologies when creating a new policy.



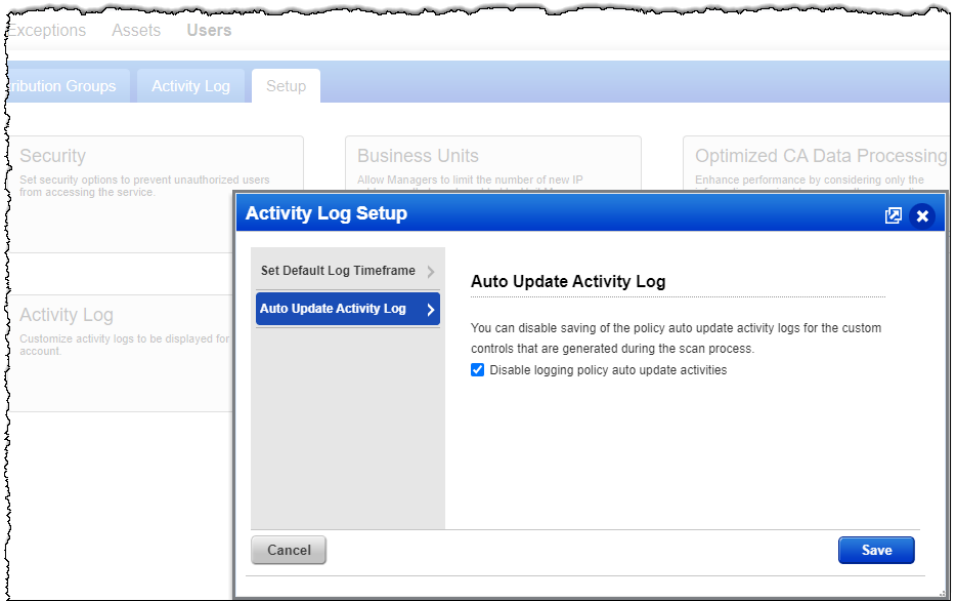
You'll also see the Oracle Multitenant technologies when searching controls by technologies.



Configure Auto Update Activity Logs

You can now disable logging policy auto update activities for the custom controls that are generated during the scan process.

Simply navigate to Users > Setup > Activity Log, and in the Activity Log Setup, select the Disable logging policy auto update activities option. By default, all activity logs are saved.



Support for OS authentication-based data collection in Compliance Option Profile

Now, we have added the **Instance Data Collection** tab in the compliance option profile. On this tab, you can enable data collection on the supported database as well as other OS-based instance discovery technologies by using underlying OS-based authentication records. This means if you have an authentication record for the underlying operating system, you don't need individual authentication records for the databases and instance technologies that you select on this tab. You can use these settings while creating or editing an option profile.

Supported Databases

Currently, we support the following database versions for this feature:

Database	Supported Versions
MongoDB	MongoDB 3.x, MongoDB 4.x
Oracle	Oracle 12c, Oracle 18c, Oracle 19c
MySQL	MySQL 5.x, MySQL 8.x
Microsoft SQL Server	MSSQL 2012, MSSQL 2014, MSSQL 2016, MSSQL 2017, MSSQL 2019

You need a Unix authentication record for the hosts running MongoDB, Oracle, and MySQL instances. For data collection on MSSQL instances, you need a Windows authentication record.

Supported OS-based Instance Discovery Technologies

Currently, we support Oracle JRE 8 as the OS-based instance discovery technology.

If you are using Cloud Agent for Policy Compliance (PC), these database and OS-based instance technologies are auto-discovered by the agent. To know more, see the online help topic "Middleware Technologies Auto-discovered by Cloud Agents for PC".

What are the steps?

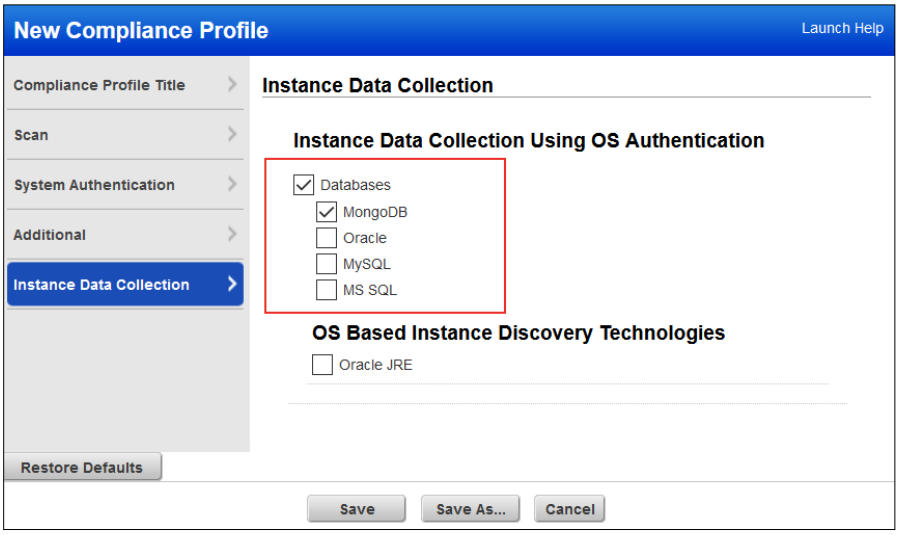
Learn how to use this feature:

Enabling OS-auth-based data collection for database instances

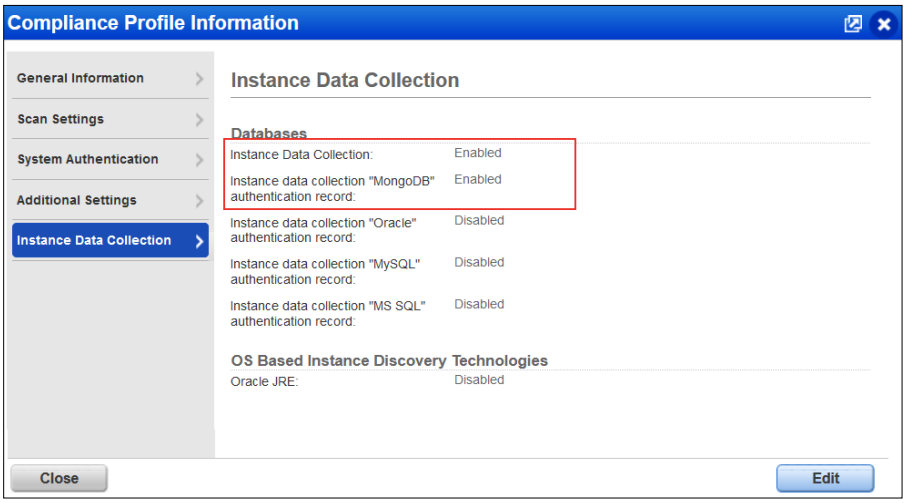
Enabling OS-auth-based data collection for Oracle JRE

Enabling OS-Auth-based Data Collection for Database Instances

To enable database instance data collection by using underlying OS authentication record, you must select the **Databases** checkbox. Only then can you select the database technologies from the available options.

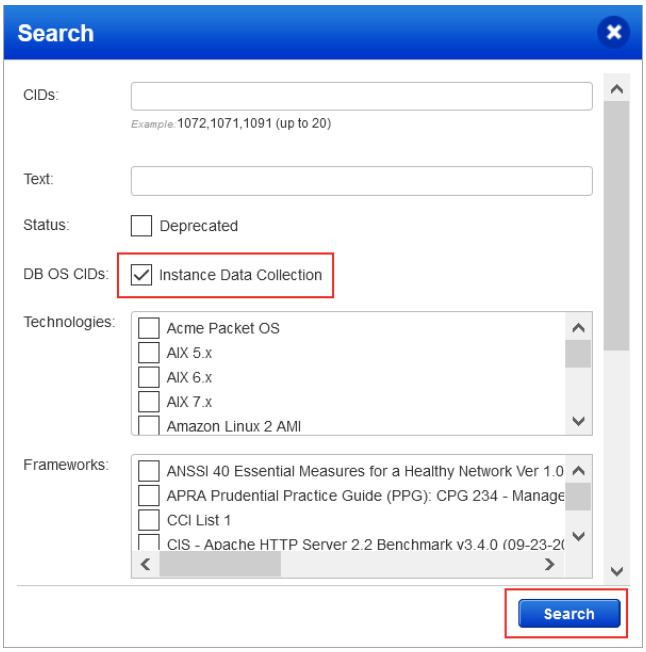


After you save your changes, the settings in the option profile are used in the next compliance scan. You can always go back and review your compliance profile information and edit it if required.



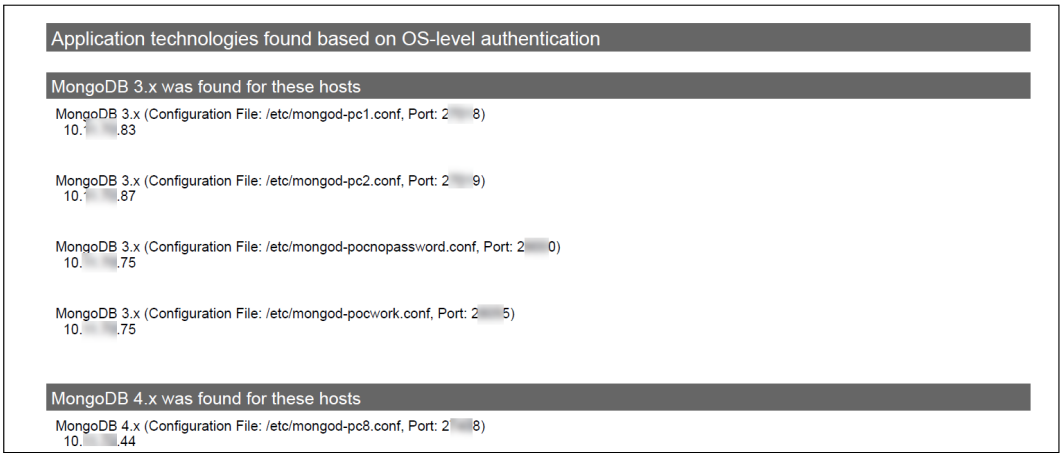
Searching for OS-Dependent Database Controls

Only system-defined OS-dependent database controls are used in data collection and evaluation of database technology instances. To see the list of OS-dependent database controls (SDCs only), go to **Policies** > **Controls** > **Search**, in the Search dialog box, select the **Instance Data Collection** box for DB OS CIDs, and click **Search**.



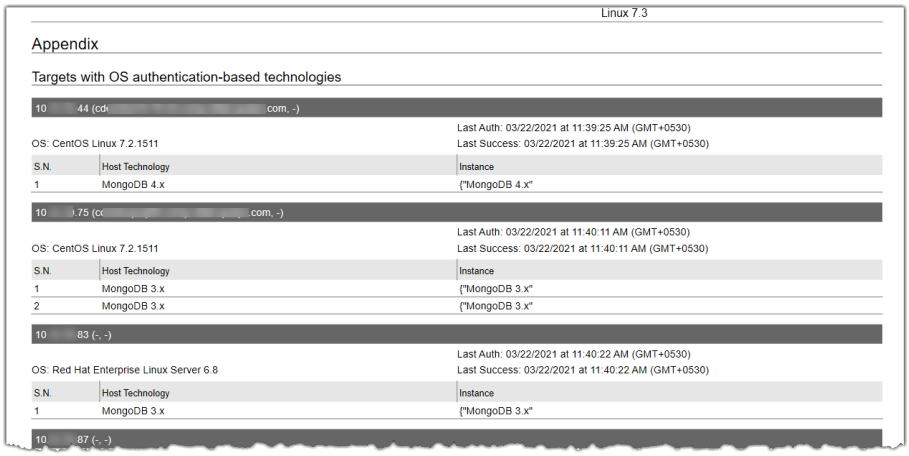
Sample Compliance Scan Result

Here's a sample compliance scan result where, in the **Application technologies found based on OS-level authentication** section, you can see the hosts on which database instances are identified.



Sample Authentication Report

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



Linux 7.3

Appendix

Targets with OS authentication-based technologies

10 44 (cd com, -)

Last Auth: 03/22/2021 at 11:39:25 AM (GMT+0530)
OS: CentOS Linux 7.2.1511 Last Success: 03/22/2021 at 11:39:25 AM (GMT+0530)

S.N.	Host Technology	Instance
1	MongoDB 4.x	{"MongoDB 4.x"

10 .75 (c com, -)

Last Auth: 03/22/2021 at 11:40:11 AM (GMT+0530)
OS: CentOS Linux 7.2.1511 Last Success: 03/22/2021 at 11:40:11 AM (GMT+0530)

S.N.	Host Technology	Instance
1	MongoDB 3.x	{"MongoDB 3.x"
2	MongoDB 3.x	{"MongoDB 3.x"

10 83 (-, -)

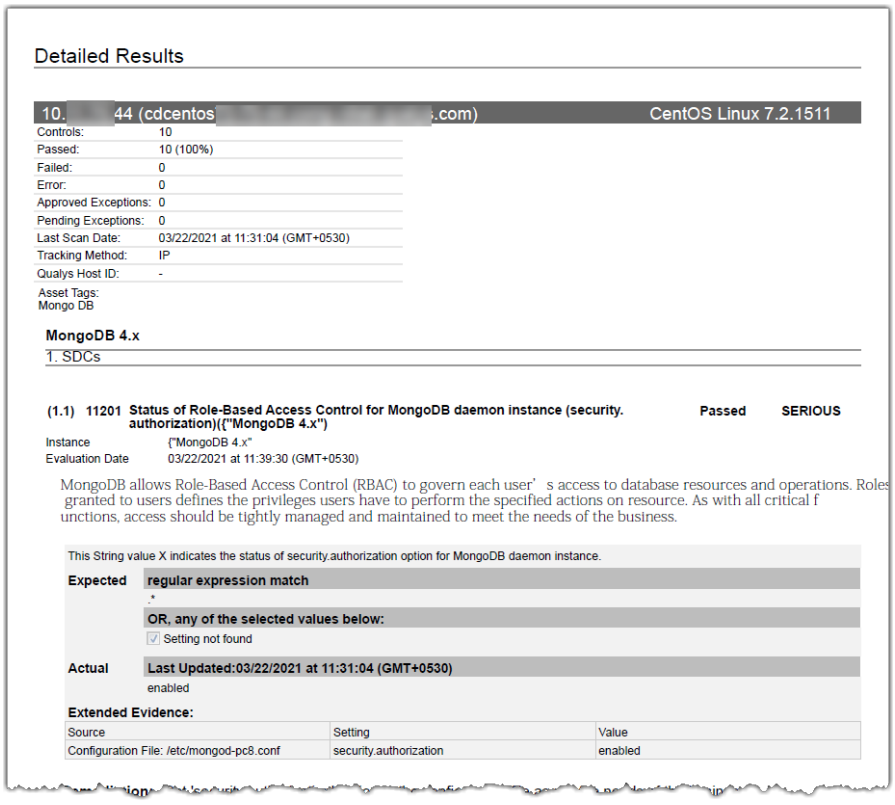
Last Auth: 03/22/2021 at 11:40:22 AM (GMT+0530)
OS: Red Hat Enterprise Linux Server 6.8 Last Success: 03/22/2021 at 11:40:22 AM (GMT+0530)

S.N.	Host Technology	Instance
1	MongoDB 3.x	{"MongoDB 3.x"

10 87 (-, -)

Sample Policy Report

And here's a sample policy report where you can check the detailed results for each database instance that is scanned against a policy.



Detailed Results

10. 44 (cdcentos .com) CentOS Linux 7.2.1511

Controls:	10
Passed:	10 (100%)
Failed:	0
Error:	0
Approved Exceptions:	0
Pending Exceptions:	0
Last Scan Date:	03/22/2021 at 11:31:04 (GMT+0530)
Tracking Method:	IP
Qualys Host ID:	-

Asset Tags:
Mongo DB

MongoDB 4.x

1. SDCs

(1.1) 11201 Status of Role-Based Access Control for MongoDB daemon instance (security. authorization)({"MongoDB 4.x") Passed SERIOUS

Instance {"MongoDB 4.x"
Evaluation Date 03/22/2021 at 11:39:30 (GMT+0530)

MongoDB allows Role-Based Access Control (RBAC) to govern each user' s access to database resources and operations. Roles granted to users defines the privileges users have to perform the specified actions on resource. As with all critical f unctions, access should be tightly managed and maintained to meet the needs of the business.

This String value X indicates the status of security.authorization option for MongoDB daemon instance.

Expected **regular expression match**
.*
OR, any of the selected values below:
Setting not found

Actual **Last Updated:03/22/2021 at 11:31:04 (GMT+0530)**
enabled

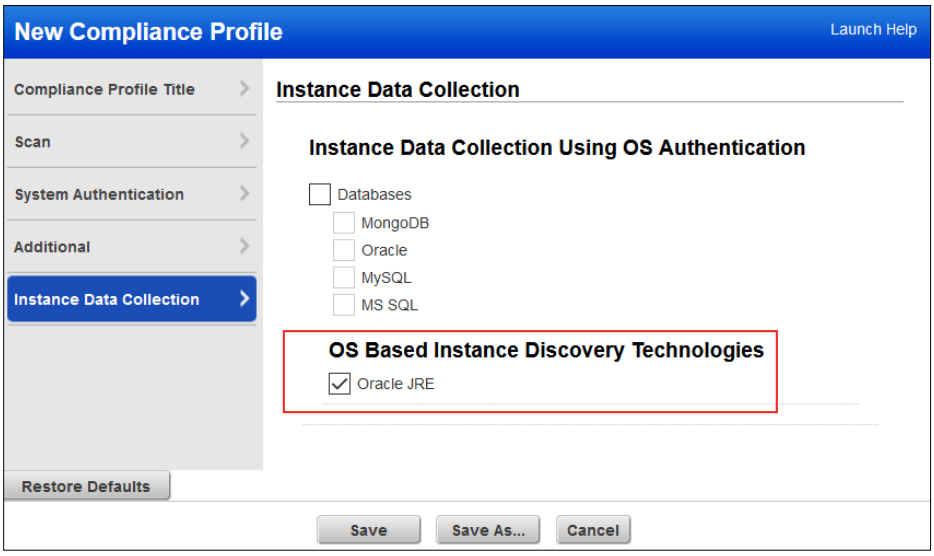
Extended Evidence:

Source	Setting	Value
Configuration File: /etc/mongod-pc8.conf	security.authorization	enabled

See Supported Databases.

Enabling OS-Auth-based Data Collection for Oracle JRE

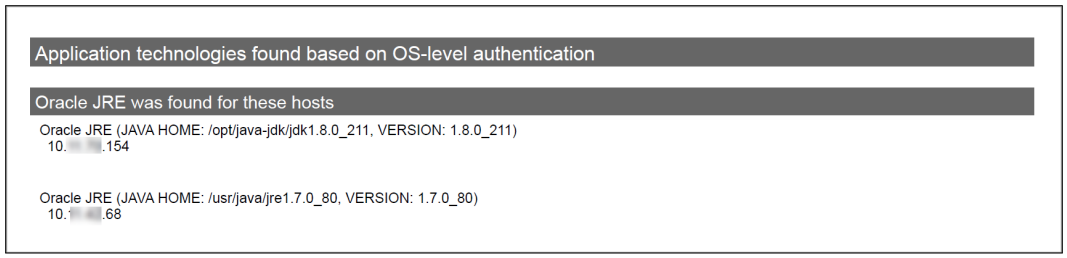
To enable Oracle JRE data collection using underlying OS authentication record, you must select the **Oracle JRE** checkbox.



The data collection and reporting workflow remains unchanged.

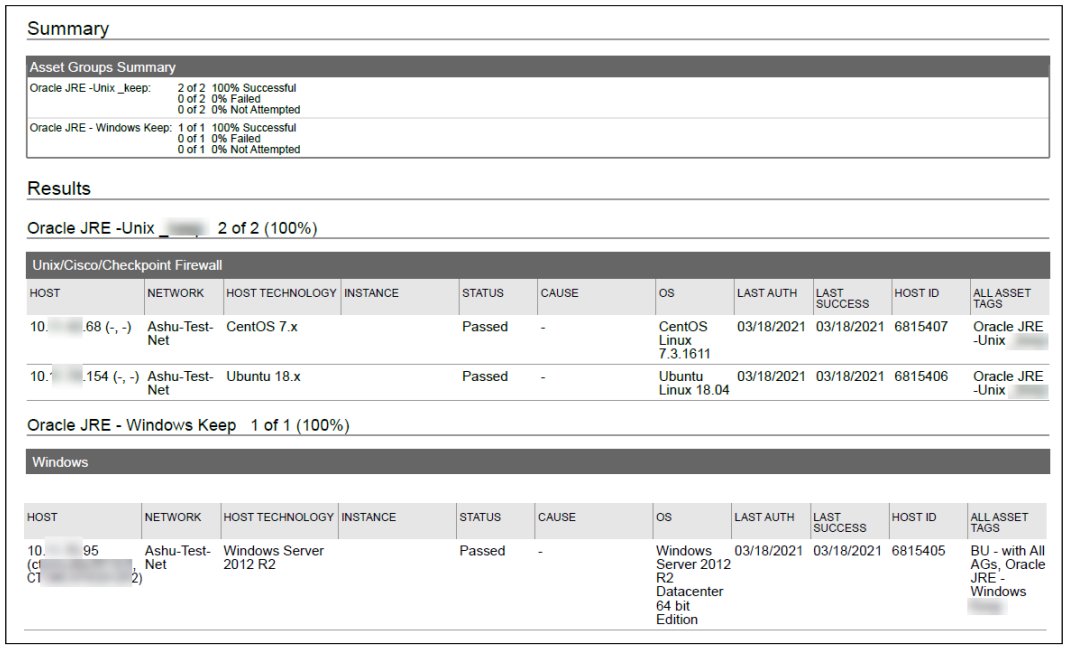
Sample Compliance Scan Result

Here's a sample compliance scan result where, in the **Application technologies found based on OS-level authentication** section, you can see the hosts on which Oracle JRE instances are identified.



Sample Authentication Report

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



Summary

Asset Groups Summary

Oracle JRE -Unix _keep:	2 of 2 100% Successful 0 of 2 0% Failed 0 of 2 0% Not Attempted
Oracle JRE - Windows Keep:	1 of 1 100% Successful 0 of 1 0% Failed 0 of 1 0% Not Attempted

Results

Oracle JRE -Unix _ 2 of 2 (100%)

Unix/Cisco/Checkpoint Firewall

HOST	NETWORK	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS	LAST AUTH	LAST SUCCESS	HOST ID	ALL ASSET TAGS
10. .68 (-, -)	Ashu-Test-Net	CentOS 7.x		Passed	-	CentOS Linux 7.3.1611	03/18/2021	03/18/2021	6815407	Oracle JRE -Unix
10. .154 (-, -)	Ashu-Test-Net	Ubuntu 18.x		Passed	-	Ubuntu Linux 18.04	03/18/2021	03/18/2021	6815406	Oracle JRE -Unix

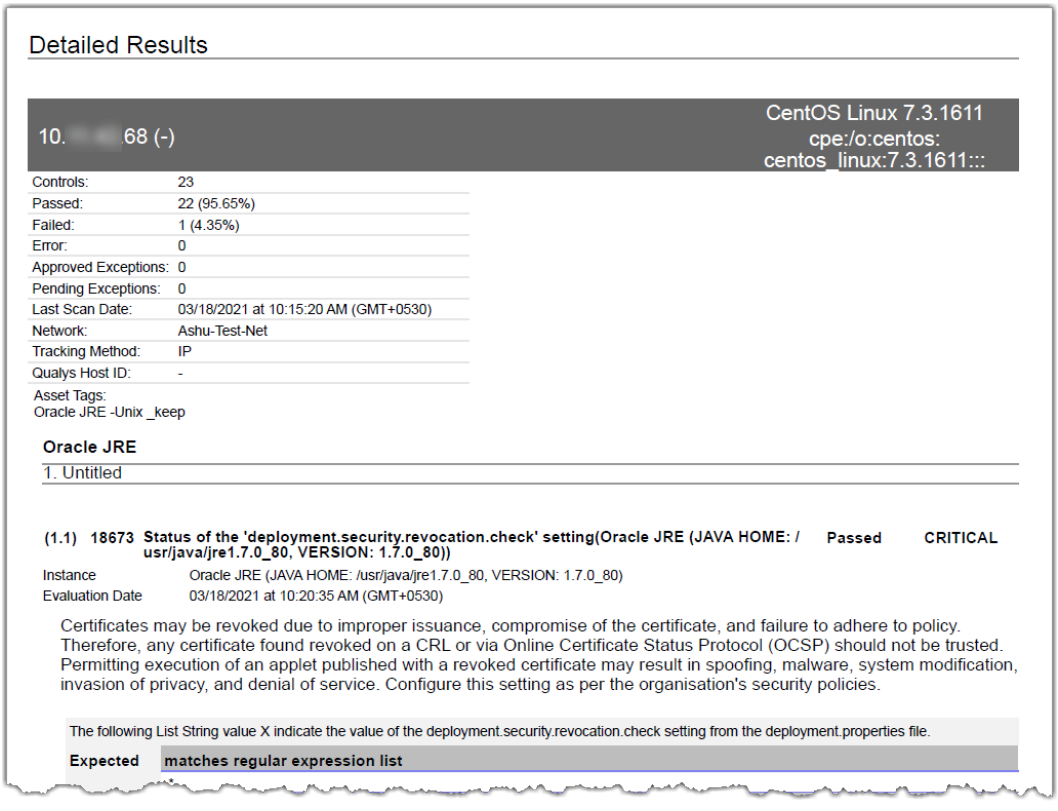
Oracle JRE - Windows Keep 1 of 1 (100%)

Windows

HOST	NETWORK	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS	LAST AUTH	LAST SUCCESS	HOST ID	ALL ASSET TAGS
10. 95 (cl CT 2)	Ashu-Test-Net	Windows Server 2012 R2		Passed	-	Windows Server 2012 R2 Datacenter 64 bit Edition	03/18/2021	03/18/2021	6815405	BU - with All AGs, Oracle JRE - Windows

Sample Policy Report

And here's a sample policy report where you can check the detailed results for each Oracle JRE instance that is scanned against a policy.



Detailed Results

10. 68 (-) — CentOS Linux 7.3.1611 cpe:/o:centos:centos_linux:7.3.1611:::

Controls:	23
Passed:	22 (95.65%)
Failed:	1 (4.35%)
Error:	0
Approved Exceptions:	0
Pending Exceptions:	0
Last Scan Date:	03/18/2021 at 10:15:20 AM (GMT+0530)
Network:	Ashu-Test-Net
Tracking Method:	IP
Qualys Host ID:	-

Asset Tags:
Oracle JRE -Unix _keep

Oracle JRE

1. Untitled

(1.1) 18673 Status of the 'deployment.security.revocation.check' setting(Oracle JRE (JAVA HOME: / usr/java/jre1.7.0_80, VERSION: 1.7.0_80)) **Passed** **CRITICAL**

Instance Oracle JRE (JAVA HOME: /usr/java/jre1.7.0_80, VERSION: 1.7.0_80)
Evaluation Date 03/18/2021 at 10:20:35 AM (GMT+0530)

Certificates may be revoked due to improper issuance, compromise of the certificate, and failure to adhere to policy. Therefore, any certificate found revoked on a CRL or via Online Certificate Status Protocol (OCSP) should not be trusted. Permitting execution of an applet published with a revoked certificate may result in spoofing, malware, system modification, invasion of privacy, and denial of service. Configure this setting as per the organisation's security policies.

The following List String value X indicate the value of the deployment.security.revocation.check setting from the deployment.properties file.

Expected **matches regular expression list**

See Enabling OS-Auth-based Data Collection for Database Instances.

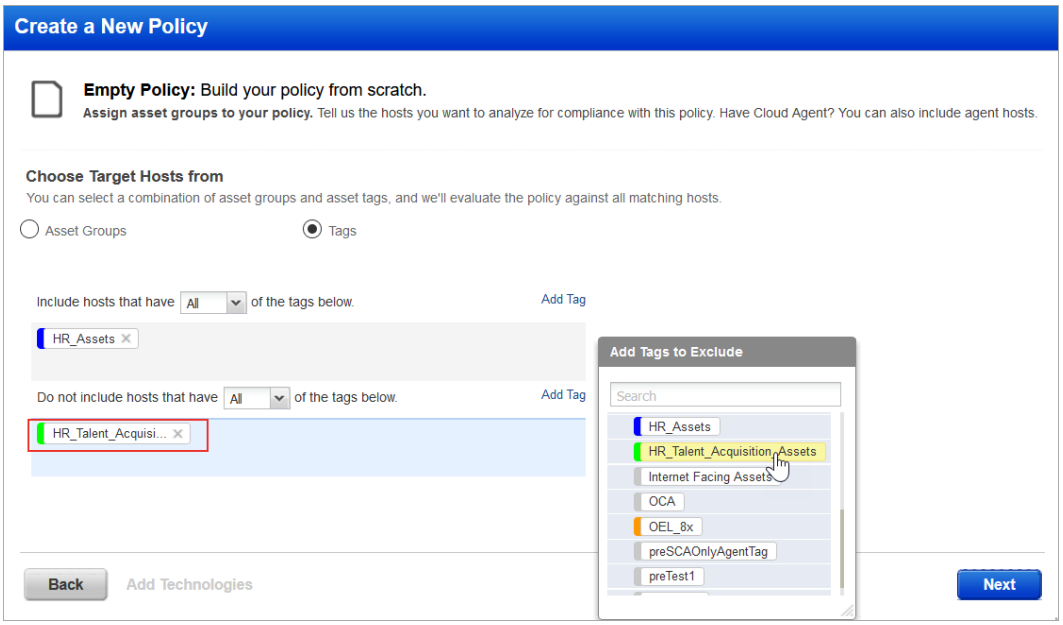
Support to Exclude Asset Tags from Policy Compliance Assessment

In the Policy Editor, you already have an option to add asset tags to the include list. Depending on the condition you set, host assets that match any or all of the specified tags are included in policy compliance assessment.

However, there might be a situation where you want to exclude some assets that have the tags specified in the include list, and untagging those hosts may not be a smart option.
As a solution, starting with this release, you can further filter out the host assets having the tags in your include list. All you need to do is, identify the asset tags that you want to exclude, and add them to the exclude list in the Policy Editor. Assets having the tags in the exclude list are excluded from policy compliance assessment.

The option to add tags to the exclude list is enabled only after you add at least one tag to the include list.

Consider a scenario where you want to apply a policy to the host assets in your Human Resource (HR) department. The Talent Acquisition (TA) team is also a part of the HR department. You do not want to apply that policy to the assets owned by the TA team. All the HR host assets (which also include TA assets) are grouped under the HR_Assets tag. You have added the HR_Assets tag to the include list. In this case, you must group the TA assets under a separate tag, say HR_Talent_Acquisition_Assets, and add this tag to the exclude list.



Let's take another example. Suppose you want to evaluate your Windows 2019 assets against a policy. You've assigned the Win_2k19 tag to all of them, and you have added this tag to the include list in the Policy Editor. Out of these Windows 2019 assets, you want to exclude Windows 2019 AD Servers from the assessment. You simply assign them the Win_2k19_AD_Servers tag, and add this tag to the exclude list. That's it!

Depending on the condition you set, host assets that match any or all of the specified tags are excluded from policy compliance assessment. This gives you more control over which assets must be evaluated. Excluding unwanted assets from the assessment saves time and helps you get compliance results quicker.

Support for New OCA Technology

Compliance assessment support for Cisco ISE is now available on assets for which data is collected by using Out-of-Band Configuration Assessment (OCA) tracking. We support the following versions of Cisco ISE:

- Cisco ISE 2.x
- Cisco ISE 3.x

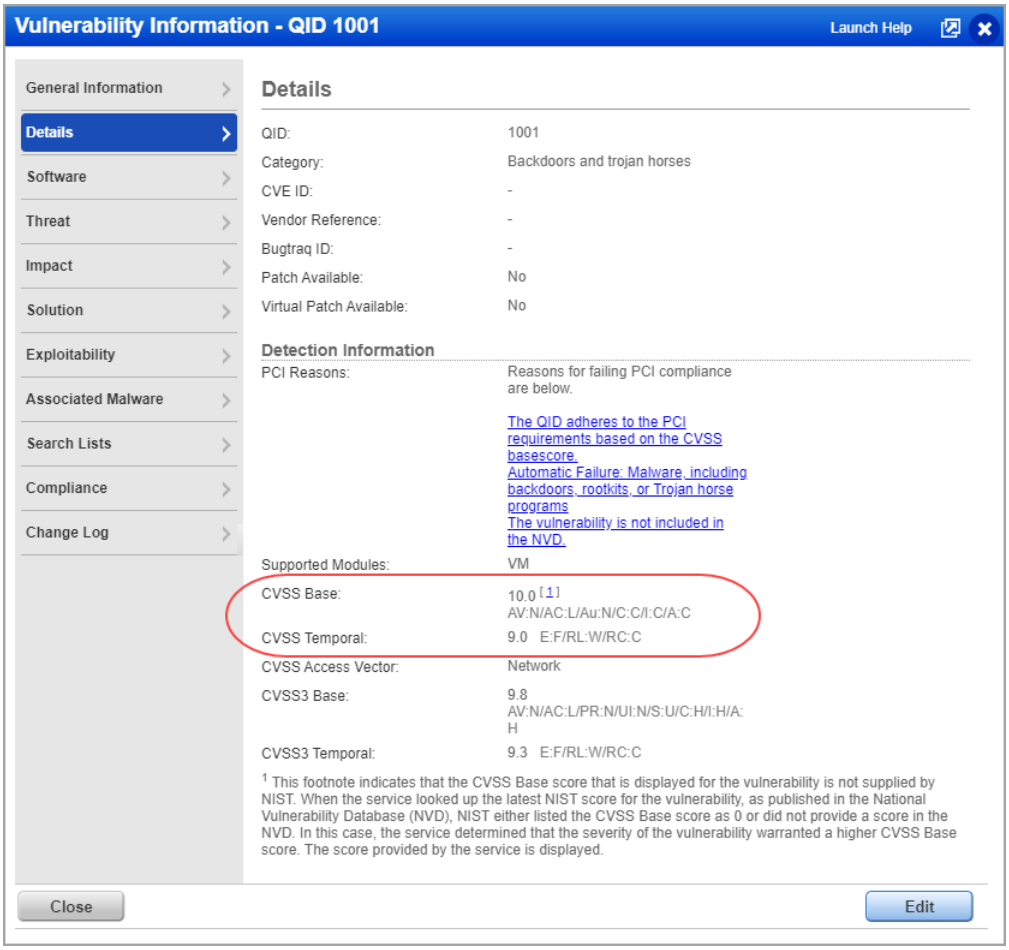
Using the **OCA** module, upload the corresponding configuration or command output for the assets. Then, navigate to **Policy Compliance** > **Reports** tab to run the Policy Compliance Report for these technologies to view the compliance posture of the corresponding assets.

Qualys Vulnerability Management (VM)

Whole Number CVSS Scores Now Appear with Decimal Point

Any CVSS score which is a whole number will now appear with a decimal point. For example, a score of 9 will now appear as 9.0, and a score of 10 will now appear as 10.0. This change applies to CVSS and CVSS3 Base and Temporal scores. You'll see the updated format wherever CVSS scores appear in the UI and API, such as on the Vulnerability Information page, on the KnowledgeBase list, and in the KnowledgeBase API output. Note that other CVSS scores that are not whole numbers are already represented with a decimal point, such as 5.8, 9.7, etc.

In this example, QID 1001 has a CVSS Base score of 10.0 and a CVSS Temporal score of 9.0.



Issues Addressed

- We have fixed the issue, where even if the “Include all hosts with PC agents” option is not selected, the policy is evaluated on the host if the IP is part of the selected asset group or the asset group tags.
- Fixed an issue where pdf format of the Patch Report was showing improper and unusable links.
- Fixed an issue where the user was getting an error while creating a ticket from the host info page.
- Fixed an issue where XML format of reports did not display the complete details of CVSS score. With the fix, XML format of reports displays the complete details of CVSS Temporal score (for both CVSS2 and CVSS3).
- We have now fixed an issue so that if the user selects an internal scanner, the selection is correctly reflected during the scan. Previously, an error with lack of an external scanner was displayed.
- We fixed an issue where we allowed a duplicate Virtual Host entry to be created when it should not have been allowed.
- We have fixed an issue where the Search List tab for any QID in KnowledgeBase was displayed as blank. Now, the correct Search Lists entries are populated.
- We fixed an issue where when a user's role is downgraded from Manager to Unit Manager, the user was able to see the policies created by the user, but cannot edit them. After the fix, the users will be able to edit the policies that they have created when their roles are downgraded.
- We fixed an issue where after the policy compliance scan is launched, the title of the scan in the processing tasks list was shown blank. After the fix, the title is displayed for the processing scan listed in the processing tasks list.
- We have fixed an issue where in certain cases the Scorecard Report was showing more tags than that is defined when generating the report. After the fix, you will see the same tags in the Scorecard Report that were selected for the report.
- We fixed an issue where although the host was scanned successfully, the Policy Compliance report was blank. This issue occurred because the authentication for one of the OS failed due to which the Policy Evaluation was skipped.
- Fixed an issue where customers received errors when trying to save exceptions. The fix now resolves the performance issue in the exception workflow.
- We've added a troubleshooting section for unauth merge scans (Agent Correlation Identifier) to the online help which covers correlation log location, correlation artifact location, and unsupported platforms for Windows and Linux.
- The user was getting an error when trying to retrieve the password from HashiCorp Vault using the vault record in the Unix authentication record. This is because the user was using the Active Directory Secrets Engine instead of Key-Value Secret Engine version 2 in the HashiCorp vault. We have updated the HashiCorp Vault topic in the VM Online Help to inform our customers that we only support Key-Value Secret Engine version 2 to retrieve secrets from the HashiCorp Vault.
- We made an update to the online help for FortiOS scan privileges to include additional commands that are required for scanning. This is to address an issue where some commands for a user on the FortiOS were not executed because of insufficient permissions.