



Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.13

August 19, 2021

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

Qualys Cloud Platform

[Introducing Asset Group Management Service](#)

[Introducing Tag-based User Scoping](#)

[Support for Qualys Solaris Agent in VM and PC Workflows](#)

[Send Notifications if Scheduled Scans are Delayed, Skipped, or Deactivated](#)

Qualys Vulnerability Management (VM)

[Cloud Provider Metadata for AWS added to Patch Reports](#)

[Introducing Data List Set up](#)

[Processing Tasks Filter Renamed to Scan Processing \(VM Scans Only\)](#)

Qualys Policy Compliance (PC/SCAP/SCA)

[IBM DB2 Database User-Defined Control Support](#)

[New Unix Target Types and Technology Support](#)

[Generic Linux Target Type](#)

[New Technology support on VMware vCenter Server](#)

[Disable Case Sensitive Search for Agent Scan](#)

[Control Comments added to CSV, XML Formats of Policy Reports](#)

Qualys 10.13 brings you many more improvements and updates! [Learn more](#)

Qualys Cloud Platform

Introducing Asset Group Management Service

Asset Group Management Service (AGMS) is a new dedicated microservice which offers significant performance improvements for common asset management tasks such as Add, Edit, Delete and Get assets from an asset group.

AGMS Benefits

AGMS offers multiple benefits to our customers. AGMS uses an optimized User Scoping algorithm to find out the affected Asset Groups for the User resulting in efficient Asset Edit operations in Asset Groups and the License Container. AGMS also uses an in-memory data grid which caches all data, reducing the DB calls and network I/O. As a result of this AGMS can handle millions of assets very easily.

Here are some additional highlights:

- Improved performance in Asset Management & Asset Group Management functionality
- Reduces data inconsistencies scenarios from current model and avoids them in the future
- Performance of Asset Tagging functionality improved by 15-20%

Based on insights from our internal benchmarks and feedback from early adopters we have seen performance improvements anywhere from 10x to 30x for common asset group operations, such as adding IPs in bulk, editing Asset Groups and many other common use cases.

These performance improvements are driven by following changes behind the scenes.

- In-memory database
- Distributed processing
- Efficient data structures
- Redesigned database schema
- New APIs optimized for performance.

When will the AGMS functionality rollout begin?

We have already deployed AGMS to 30 plus customer subscriptions across all shared platforms. We will continue to rollout this functionality to more customers over a period of time.

How can I verify AGMS is enabled for my subscription?

After AGMS is enabled, the “Host Assets” tab on the Assets page will appear as “Address Management,” and AGMS Help will display in the online help in your subscription.

Learn more

See this notification: [Asset Group Management Service](#)

See the [AGMS online help](#) for details regarding all the UI and API changes made as part of the new AGMS system.

Introducing Tag-based User Scoping

Tag-based user scoping (TBUS) allows customers to scope a user's asset access via asset tags rather than IP-based methods, such as Asset Groups or Business Units.

This feature will allow for greater flexibility for scoping a user's asset access and will address specific use cases, such as roaming agents with unpredictable IP addresses. Currently, this new model will cover asset access for Reporting and Asset Search. In a future release, it will also cover asset access for Scanning. When enabled, tag-based user scoping is supported in VM/VMDR, PC and SCA.

Some things to consider

- A Manager will assign a set of tags to each user to define the user's scope. This can include all types of tags, including Business Unit Tags, Asset Group Tags, Static Tags, Dynamic Tags, Agent Activation Key Tags. The user's final scope will be derived from all of the assigned tags as a union.
- Dynamic Tags must be managed carefully, as an improperly scoped tag could enable a user to see assets beyond their intended scope. We recommend using a combination of Asset Group Tags, Business Unit Tags, and Agent Activation Key Tags.
- There is no automatic propagation like with Asset Groups. Asset access is managed entirely through tags, and any IP scopes that the user should have access to view must be added as an IP Range Tag to that user's scope. (Note that Asset Group Tags and Business Unit Tags are IP Range Tags and can be used for this purpose.)
- The existing Asset Group model and the new Asset Tag model are both available and they work independently of each other. Both can be used to define a user's scope. If a user is assigned assets via Asset Groups and also via Asset Tags then both options will be available to the user when taking actions like generating reports.

Tag-based user scoping must be enabled

Contact your Technical Account Manager to request tag-based user scoping for your subscription. The following option is currently available.

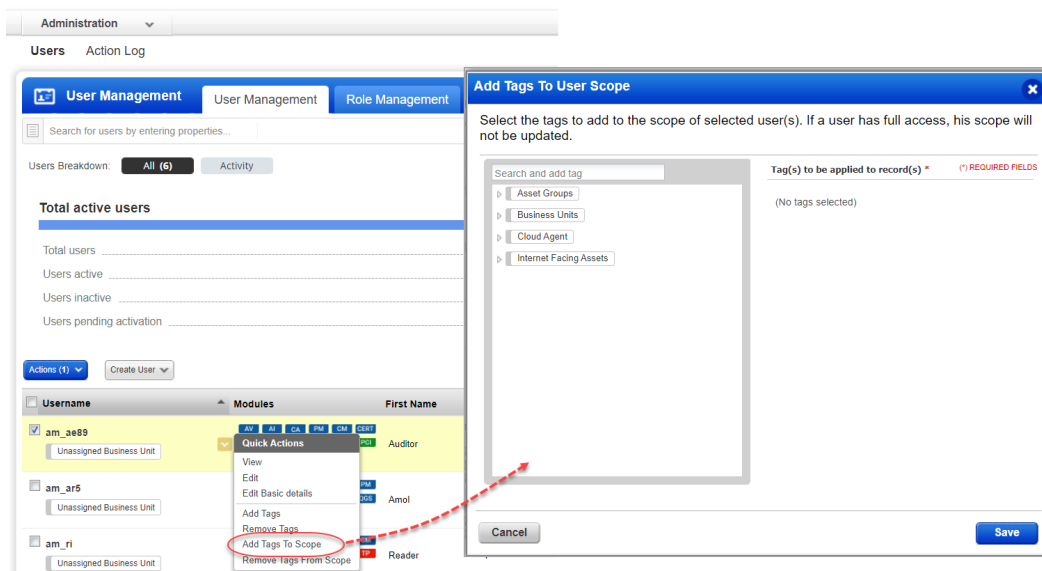
Include all assets from tags in all operations, except scan launch

For Scanning, any IP being scanned must be in the license container (for VM/PC) and the user's All group. This means the IP must be available to the user via Asset Groups or Business Unit assignment. If the IP is not available to the user launching the scan, then it will be ignored.

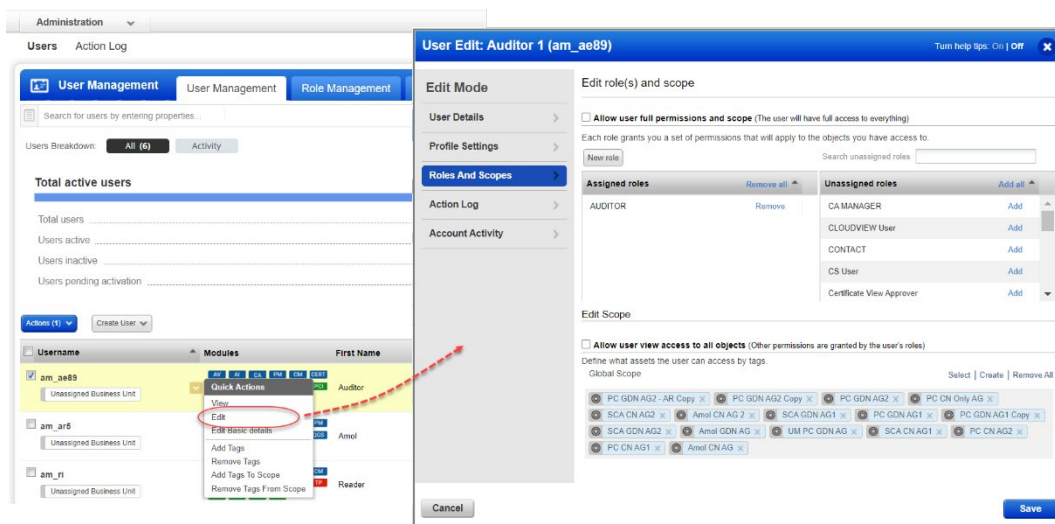
For Reporting, the user can report on any asset tag in their scope even if the tag resolves to an IP address that's not in their All group. In other words, the user can run a report on IPs that they have not been assigned via Asset Groups or Business Unit.

How to assign asset tags to users

Asset tags can be assigned to a user by a Manager from the Administration utility. Choose **Administration** from the module picker. On the **User Management** tab, identify the user you're interested in and choose **Add Tags to Scope** from the Quick Actions menu. Select new tags you want to assign to the user, and click **Save**.



Optionally, if you want to view the tags already assigned to a user before adding tags, then choose **Edit** from the Quick Actions menu. Go to the **Roles And Scopes** tab and you'll see assigned tags under **Edit Scope**. Here you can add/remove tags to define the user's scope.



You'll see these options in the Edit Scope section:

- Select – Select tags to assign to the user.
- Create – Create a new tag and assign it to the user.
- Remove All – Remove all tags already assigned to the user.

Do I also need to assign asset groups to users?

Only if the user will also need to perform scanning. In a future release, when tag-based user scoping is supported for scanning, the user will only need to have asset tags assigned and asset group assignment will not be needed.

Keep in mind that Managers have access to all assets in the subscription, Auditors have access to all assets in PC, and Unit Managers have access to all assets in their assigned business unit.

How to generate reports on asset tags

The steps you take to generate the report are the same whether you have tag-based user scoping enabled or not. You'll go to Reports, and choose the type of report you want to generate from the New menu. Then select the asset tags you want to include in the report source.

The asset tags are resolved to IP addresses at the time of report generation. If tag-based user scoping is enabled, all resolved IP addresses that match the user's tag-based scope will be included in the report. If tag-based user scoping is not enabled, only the resolved IP addresses that match the user's assigned asset groups/business unit will be included in the report.

Example 1

Let's say a user has the following assets assigned:

AG1 with 10.10.10.10-10.10.10.15 – assigned asset group
Tag1 with 10.10.10.10-10.10.10.15 – assigned tag in user scope
Tag2 with 10.10.10.20-10.10.10.30 – assigned tag in user scope

The table below shows the user scope determined with the above assignment.

User Scope Mechanism	User Scope Determined
Asset Group Based	AG1: 10.10.10.10-10.10.10.15
Tag Based	AG1 + Tag1 + Tag2: 10.10.10.10-10.10.10.30

If tag-based user scoping is not enabled and the user runs a report on Tag2, the report will not resolve to any assigned IP addresses. The error "Empty report targets/assets resolved from the tags" will appear and the report cannot be generated. The user can successfully report on Tag1 since the IPs will resolve to IPs that have also been assigned to the user via AG1.

If tag-based user scoping is enabled and the user runs a report on Tag2, then the report will run and the IPs 10.10.10.20-10.10.10.30 will be included in the report even though these IPs have not been assigned to the user via AG1. The user can also report on Tag1 and AG1 since these are also in the user's asset scope.

Example 2

In this example, the user is assigned AG1 and Tag2. The user does NOT have Tag1 assigned to their user scope.

AG1 with 10.10.10.10-10.10.10.15 – assigned asset group
Tag1 with 10.10.10.10-10.10.10.15 – NOT assigned to user
Tag2 with 10.10.10.15-10.10.10.30 – assigned tag in user scope

The table below shows the user scope determined with the above assignment.

User Scope Mechanism	User Scope Determined
Asset Group Based	AG1: 10.10.10.10-10.10.10.15
Tag Based	AG1 + Tag2: 10.10.10.10-10.10.10.15, 10.10.10.15-10.10.10.30

If tag-based user scoping is enabled and the user runs a report on Tag1, the report will not be generated even though the user is assigned the same set of assets through asset group AG1. The report doesn't run because the user selected a tag for the report target that is not in their user scope. The user can run the report by specifying the asset group AG1 for the report target. The user can also report on Tag2 without issue since this tag is in the user's scope.

A few notes on reporting

- Tag-based user scoping is not yet supported for STIG Based Reports or the Compliance Posture Information API (/api/2.0/fo/compliance/posture/info/). The report/API output will not show posture information for assets that match the user's tag-based scope.

- When you run an Interactive Report or Scorecard Report (from PC/SCA) on asset tags, the report displays a union of the assets that match the user's tag-based scope and the assets that match the user's assigned asset groups/business unit.

- If your subscription has both PC and SCA enabled and a sub-user runs an Interactive Report or Scorecard Report (from PC/SCA) on asset tags, the report displays assets from PC and from SCA.

Support for Qualys Solaris Agent in VM and PC Workflows

Qualys Cloud Agent recently added support for Solaris. In VM and PC, you can start evaluating host assets with Solaris agent installed. You'll see Solaris agent host instance information in vulnerability and compliance scan results, and in compliance policy reports. In PC, you can evaluate both System-Defined Controls (SDCs) and User-Defined Controls (UDCs) for your Solaris agent hosts. Please note that for UDCs, the Solaris agent can evaluate controls for Solaris 10.x and 11.x technologies only.

Here's a sample policy report where you can check the detailed results for each Solaris agent instance that is scanned against a policy.

1

8 (comdevsol113)

Passed

Instance

os

Previous Status

Passed

OS:

Solaris 5.11

OS CPE:

-

Last Scan Date:

06/01/2021 at 02:38:09 PM (GMT+0530)

Network:

Global Default Network

Tracking Method:

AGENT

Qualys Host ID:

18

Asset Tags:

Cloud Agent

18

This Integer value X indicates the current status of the svc:/network/dhcp/server:ipv4 service.

Expected

any of the selected values below:

☒ Offline(0)
 ☒ Online(1)
 ☒ Setting not found
 ☒ Disabled(2)
 ☒ Uninitialized(3)
 ☒ Service is incomplete
 ☒ Maintenance(4)
 ☒ Degraded(5)
 ☒ Legacy_run(6)

Actual

Last Updated:06/01/2021 at 02:38:09 PM (GMT+0530)

Setting not found

Extended Evidence:

svcs: Pattern 'svc:/network/dhcp/server:ipv4' doesn't match any instances

Send Notifications if Scheduled Scans are Delayed, Skipped, or Deactivated

You can now send custom notifications to users in case a scheduled scan is delayed, skipped, or deactivated. This is supported for vulnerability and compliance scan schedules.

To enable notifications for delayed, skipped, or deactivated scans, go to **Scans > Schedules > Schedule Scan > Notifications** and select the preferred check boxes. Once you select the check box, you can edit the default message that will appear in the email notification.

The screenshot shows the 'New Scheduled Compliance Scan' configuration window. The 'Notifications' tab is selected in the left sidebar. The main area contains three notification options, each with a checked checkbox and a custom message field. The options are:

- ☐ Send notification after scan completes
Custom message for this notification:
A Qualys scan is finished.
- ☒ Send notification if scan launch is delayed
Custom message for this notification:
The Qualys scan launch has been delayed and will be tried again
- ☒ Send notification if scan launch is skipped
Custom message for this notification:
The Qualys scan launch has been skipped.
- ☒ Send notification if schedule is deactivated by the service
Custom message for this notification:
The Qualys scan has been deactivated by the service.

The window has a 'Cancel' button at the bottom left and a 'Save' button at the bottom right.

Note: For existing scheduled scans, the **Send notification if scan launch is delayed** and the **Send notifications if the scan launch is skipped** options will be enabled by default.

Qualys Vulnerability Management (VM)

Cloud Provider Metadata for AWS added to Patch Reports

We've added a new patch report template option that lets you include cloud provider metadata in patch reports (all supported report formats). Simply select the new template option "Cloud Provider Metadata" when creating or updating a patch report template. When you download or fetch a saved patch report where this option was used, you'll see cloud metadata for each AWS cloud asset in the report.

Good to Know

- Only cloud provider metadata for AWS is supported in the patch report at this time. We will add support for other cloud providers in a future release.
- You can only include cloud metadata when detailed results are grouped by Host.
- You can download saved patch reports in different formats from the UI or fetch saved reports using the API by specifying the report ID.

Patch Report Template

In Vulnerability Management, go to **Reports > Templates > New > Patch Template** (or edit an existing template). Go to the **Display** tab to select the new option **Cloud Provider Metadata**. Note that this option can only be selected by **Group by** is set to **Host**.

The screenshot shows the 'New Patch Template' dialog box with the following configuration:

- Report Title**: (empty)
- Findings**: (empty)
- Display**: (selected tab)
- Filter**: (empty)
- User Access**: (empty)
- Detailed Results**:
 - Sorting and Grouping**:
 - Group by:** * Host (selected)
 - Add the following data to report**:
 - ☐ QIDs that will be fixed by each patch
 - ☐ Available links for each patch
 - ☐ Patches from unspecified vendors
 - Display patch severity by:**
 - ☒ **Assigned Severity:** Assigned to the QID for the patch detection.
 - ☐ **Highest Severity:** Highest across all QIDs found on the host that can be fixed by the patch
 - Display Cloud Related Information**:
 - ☒ **Cloud Provider Metadata**
Include cloud provider information for Cloud instances.
 - Display patch CVSS Base score by:**
 - ☐ **Assigned Score:** Assigned to the QID for the patch detection.
 - ☐ **Highest Score:** Highest across all QIDs found on the host that can be fixed by the patch.
 - ☒ **Do not display CVSS scores**

Buttons at the bottom: Cancel, Test, Save As..., Save.

Sample Patch Report in Online Report Format

When you run the Patch Report in Online Report format, you'll see **AWS** in the **Provider** column for each AWS cloud asset. Click the **AWS** link to get a pop-up showing the cloud related information. See the sample report below.

My Patch Report in Online Format

Report Summary

Company: Sample
Created by: Joe User
Created on: 30/07/2021

Total Patches: 3
Hosts Requiring Patches: 3
Vulnerabilities Addressed: 3

View Report Targets...

IP	Net...	DNS Name	NetBIOS	OS	CPE	Provider	Patch...
10.90...	Glo...	i-0d39e8a57806...				AWS	1
10.90...	Glo...	i-044b22c059c5...		Amazon Linux		AWS	1
10.20...	Glo...	i-01c23af4a567...		Amazon Linux		AWS	1

Cloud Related Information

Cloud Provider: AWS
Cloud Provider's Service: EC2
Cloud Resource Type: Instance
Instance Id: i-01c23af4a5678f910
Account Id: 123456789123
Image Id: ami-01b2e34b5678fa9d1
Group ID: sg-12a3b4e5
Group Name: default
Instance State: RUNNING
Spot Instance: No
Availability Zone: us-east-1a
Private IP Address: ip-10-20-30-40.ec2.internal
Region Code: us-east-1
Public DNS Name: ip-10-20-30-40.ec2.internal
Local Hostname: ip-10-20-30-40.ec2.internal
MAC Address: r-01ca2c34567d891b2
Reservation Id: subnet-1d234567
Subnet ID: vpc-1e23cd45
VPC ID:

Sample Patch Report in PDF Format

When you run the Patch Report in PDF format, you'll see the **Cloud Related Information** section below the IP address for each AWS cloud asset in the report. See the sample report below.

► 10.20.30.40 (i-01c23af4a5678f910,-) - Global EC2 Network

Amazon Linux (1 patches)

Cloud Related Information

Cloud Provider: AWS
Cloud Provider's Service: EC2
Cloud Resource Type: Instance
Instance Id: i-01c23af4a5678f910
VPC ID: vpc-1e23cd45
Image ID: ami-01b2e34b5678fa9d1
Instance Type: t2.medium
Instance State: RUNNING
Public DNS Name: ip-10-20-30-40.ec2.internal
Private DNS Name: ip-10-20-30-40.ec2.internal
Account ID: 123456789123
Region Code: us-east-1
Subnet ID: subnet-1d234567
Availability Zone: us-east-1a
Group ID: sg-12a3b4e5
Group Name: default
Private IP Address: 10.20.30.40
Public IP Address: r-01ca2c34567d891b2
Reservation Id: subnet-1d234567
Spot Instance: No
Local Hostname: ip-10-20-30-40.ec2.internal
MAC Address:

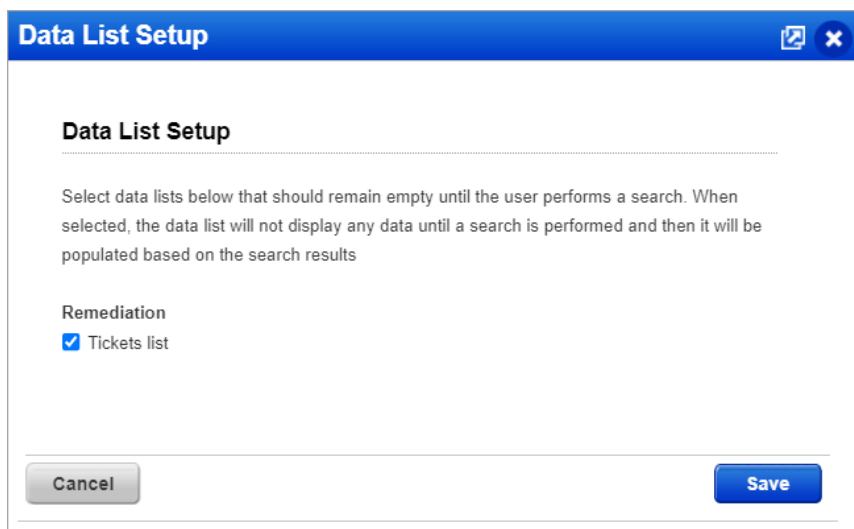
For sample Patch Reports in CSV and XML formats, please refer to the [API Release Notes](#).

Introducing Data List Setup

In this release, we have introduced Data List Setup for tabs that list data. The data list setting is useful if the list data to display for a tab is large and loading of default data in the tab takes time. When you select a data list for a tab, the tab will not display any data when you open the tab until you perform a search. The data will be populated based on the search results. Note that all the users irrespective of their roles can turn on or off data list setting.

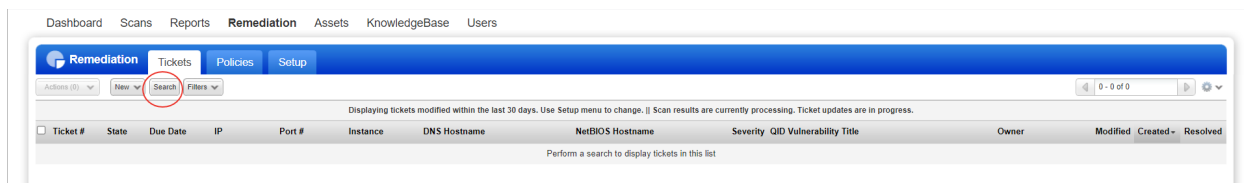
Note that currently, the data list setting is available only for the **Remediation > Tickets** tab.

To set up data list for **Remediation > Tickets** tab, go to **Users > Setup > Data List Setup**. Under **Remediation**, Select **Tickets list** data list and click **Save**.



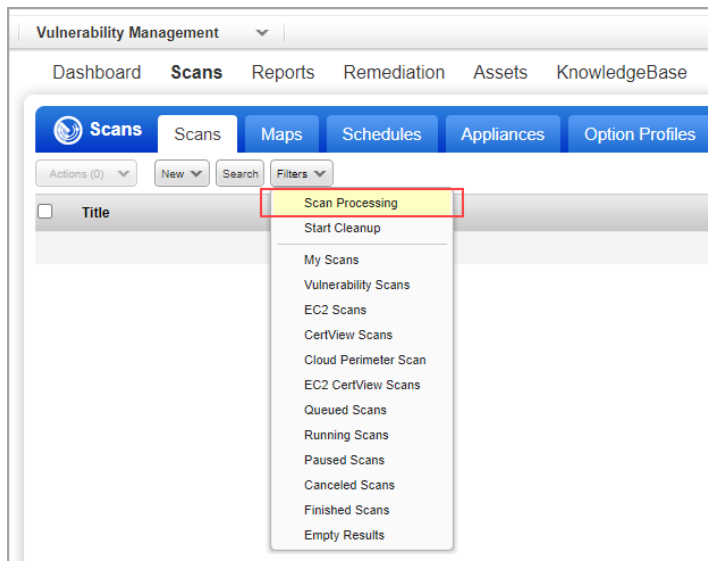
The image shows a 'Data List Setup' dialog box with a blue header bar containing the title and window controls. The main content area has a title 'Data List Setup' followed by an instruction: 'Select data lists below that should remain empty until the user performs a search. When selected, the data list will not display any data until a search is performed and then it will be populated based on the search results'. Under the 'Remediation' section, the 'Tickets list' option is checked with a blue checkbox. At the bottom, there are 'Cancel' and 'Save' buttons.

When selected the **Tickets** tab will not display any tickets. The tickets are populated based on the search results.



Processing Tasks Filter Renamed to Scan Processing (VM Scans Only)

The next time you're on the Scans list in VM/VMDR, you'll notice a small change on the Filters menu. We renamed the filter "Processing Tasks" to "Scan Processing" for better clarity. To see this change, go to **VM/VMDR > Scans > Scans** and click the **Filters** menu.



Qualys Policy Compliance (PC/SCAP/SCA)

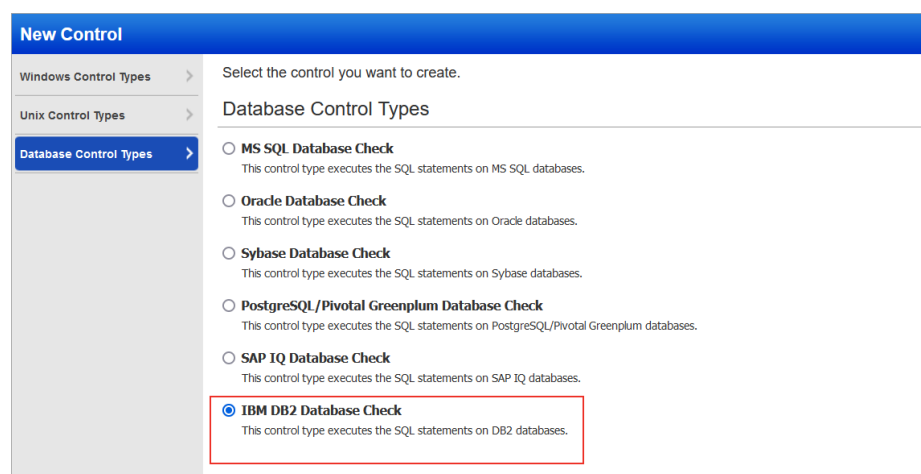
IBM DB2 Database User-Defined Control Support

You can now use IBM DB2 database user-defined controls (UDC) to create custom checks by executing SQL statements on databases. These controls can then be used to generate policy reports on your databases. We're already providing UDC support for MS SQL, Oracle, Sybase, PostgreSQL/ Pivotal Greenplum, and SAP IQ databases.

Follow these steps to create IBM DB2 database controls and generate a report:

Step 1 - Add database controls

In Policy Compliance, go to **Policies > Controls > New > Control**. Click the **Database Control Types** tab and then click **IBM DB2 Database Check**.



In each control you'll define the SQL statement that you want to execute on your database.

Note: Only SELECT statements are supported for the database controls. For example, you can use the following SQL statement to list all fields from "Customers" where country is "Germany" AND city is "Berlin":

```
SELECT * FROM Customers WHERE Country='Germany' AND City='Berlin'
```

See the Help for sample queries and results.

Step 2 - Add database controls to a policy

Create a new compliance policy or edit an existing policy, and add your database controls to the policy. Tip - Make sure your policy has the database technologies selected in the control.

Step 3 - Launch a compliance scan

Launch a compliance scan on the host running the IBM DB2 database. Edit the compliance option profile that you'll use for the scan to set the maximum number of rows you want the check to return. By default, we return up to 256 rows for an IBM DB2 Database Check. To edit

this limit, select the database control type in the compliance option profile and set a new value. The maximum value that you can set for an IBM DB2 check is 5000 rows.

Database Control Types
These settings apply to user-defined database controls. By default, we'll return up to 5000 rows for Oracle and up to 256 rows for all other control types. Select the control type to edit the limit.

- ☐ MS SQL Database Check
Set a limit on the number of rows to be returned per scan for custom MS SQL Database checks (default is 256).
Max rows to return: (limit (1-256))
- ☐ Oracle Database Check
Set a limit on the number of rows to be returned per scan for custom Oracle checks (default is 5000).
Max rows to return: (limit (1-5000))
- ☐ Sybase Database Check
Set a limit on the number of rows to be returned per scan for custom Sybase Database checks (default is 256).
Max rows to return: (limit (1-5000))
- ☐ PostgreSQL/Pivotal Greenplum Database Check
Set a limit on the number of rows to be returned per scan for custom PostgreSQL/Pivotal Greenplum Database checks (default is 256).
Max rows to return: (limit (1-5000))
- ☐ SAP IQ Database Check
Set a limit on the number of rows to be returned per scan for custom SAP IQ Database checks (default is 256).
Max rows to return: (limit (1-10000))
- ☐ IBM DB2 Database Check
Set a limit on the number of rows to be returned per scan for custom DB2 Database checks (default is 256).
Max rows to return: (limit (1-5000))

Step 4 - Return to your policy to set control criteria

Edit your compliance policy by using the policy editor to see the actual data returned by your scan. Select a column and define the expected value. This is how you set the criteria that will determine pass/fail status for the control.

IBM DB2 10.x Remove this technology Copy to Other Technologies

rationale test

deso

☒ Set status to PASS if no data found

Column Filters

Criteria 1

Column name	Data-type	Operator	Operator Criteria	Expected Values
GRANTEE	List String	regular expression list	matches	.*

Add another column

Test Control

Remediation

Click **Add another column** to add more criteria. You can add up to 5 criteria, i.e. Criteria 1, Criteria 2, Criteria 3 and so on. You can choose AND or OR between each criteria. If you choose AND then both criteria must match to Pass. If you choose OR, then at least one criterion must match to Pass. Click Test Control to verify the criteria you set. Then save your policy.

Step 5 - Run a report

You'll see PASS or FAIL status in your report like you do with any control. If the columns returned by the most recent scan are different than previous scans, then you may want to edit your policy to modify the criteria selected for the control. Here's a sample report where the expected value matches the actual value, resulting in a status of Passed.

IBM DB2 10.x

1. Sample IBM DB2 Check

(1.1) 100010 db2 statement(DB2v10:1:50004:sample)

Instance DB2v10:1:50004:sample

Evaluation Date 06/29/2021 at 07:00:10 PM (GMT+0530)

db2 udc rationale

test db2 udc description

Expected any of the selected values below:

☒ Set status to PASS if no data found

Actual Last Updated:06/29/2021 at 01:48:26 PM (GMT+0530)

Failed

SERIOUS

(1.2) 100012 db2 udc statement test(DB2v10:1:50004:sample)

Instance DB2v10:1:50004:sample

Evaluation Date 06/29/2021 at 07:00:10 PM (GMT+0530)

db2 udc test rationale

test description

Expected matches regular expression list

DB Column Name: GRANTOR

*

OR, any of the selected values below:

☒ Set status to PASS if no data found

Actual Last Updated:06/29/2021 at 01:48:26 PM (GMT+0530)

Passed

CRITICAL

GRANTOR	GRANTEE	DBADMAUTH	CREATETAB- AUTH	BINDADDAUTH	CONNECTAUTH	NOFENCEAUTH	GRANTEEType
SYSIBM	DB2INST2	Y	N	N	N	N	U
SYSIBM	PUBLIC	N	Y	Y	Y	N	G

New Unix Target Types and Technology Support

We've added support for several new technologies since the last Qualys PC release.

New Unix Target Types

You'll see more options on the Target Type menu in Unix and Network SSH authentication records, including the following:

- General Linux (Policy Compliance) – [Learn more about this target type](#)
- ArubaOS (Policy Compliance)
- IBM z/OS Security Server RACF (Policy Compliance)

See the online help for privileges required for authenticated scans on these devices.

Additional technology support

We've added PC support for the following technologies:

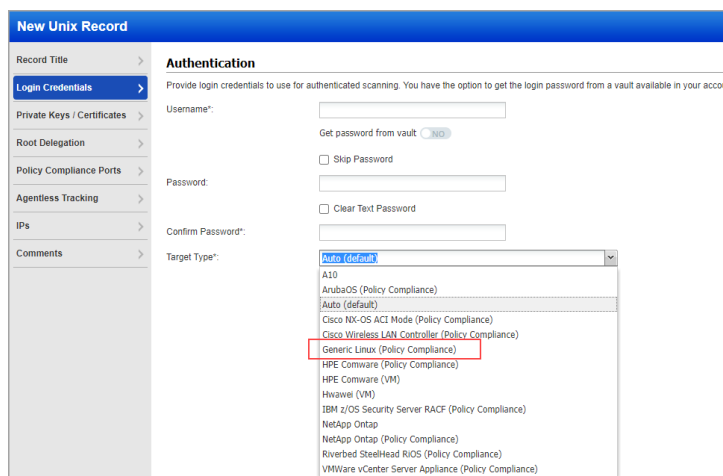
- Cisco SD-WAN 16.x, 17.x, 18.x, 19.x, 20.x and Cisco WLC 8.x
- EulerOS 2.x
- DB2 v11, v12 on IBM z/OS 2.3, 2.4

Generic Linux Target Type

In the Unix and Network SSH authentication records, we now provide a Target Type option called “Generic Linux (Policy Compliance)”. Select this option to perform compliance assessments on Linux OS technologies not yet supported by Qualys Policy Compliance (PC).

This option gives users the ability to scan target hosts with unsupported PC Linux OS technologies. When we later add support for a Linux OS technology, you’ll want to edit the authentication record to remove the Generic Linux target type selection.

Please note that we only recommend using the Generic Linux target type if the Linux technology is not already supported. For example, you can use it for Scientific Linux, NixOS, Deepin, Lunar Linux, VyOS and others.



The screenshot shows the 'New Unix Record' form. On the left is a sidebar with navigation links: Record Title, Login Credentials, Private Keys / Certificates, Root Delegation, Policy Compliance Ports, Agentless Tracking, IPs, and Comments. The main area is titled 'Authentication' and contains fields for Username, Password, and Confirm Password. There are checkboxes for 'Get password from vault', 'Skip Password', and 'Clear Text Password'. The 'Target Type' dropdown is open, displaying a list of target types. 'Generic Linux (Policy Compliance)' is highlighted with a red box. Other target types include AIO, ArubaOS (Policy Compliance), Auto (default), Cisco NX-OS ACI Mode (Policy Compliance), Cisco Wireless LAN Controller (Policy Compliance), HPE Comware (Policy Compliance), HPE Comware (VM), Huawei (VM), IBM z/OS Security Server RACF (Policy Compliance), NetApp Ontap, NetApp Ontap (Policy Compliance), Riverbed SteelHead R/OS (Policy Compliance), and VMware vCenter Server Appliance (Policy Compliance).

What are the benefits?

This new technology enables users to perform a compliance assessment on any new Linux/Unix OS technology that is not widely used and has customer specific use cases.

Whenever any new flavor of Unix OS is released and is not yet supported by Qualys PC, you’ll be able to use the Generic Linux technology to report for compliance.

What user account privileges are needed?

Root privileges are required for successful compliance scans.

Which controls are supported for Generic Linux?

Controls for the Generic Linux technology are limited to checks related to basic Unix/Linux OS settings and Access Control requirements.

What if I select Generic Linux but my target host has a supported technology?

If you select Generic Linux in the authentication record for a target that has a supported technology like RHEL, Ubuntu or CentOS, then we will report compliance data only for the policy controls related to the supported technology on the target.

Is Generic Linux supported by agents?

No. The Generic Linux technology is only supported by scanners.

New Technology support on VMware vCenter Server

We've added PC support for the following technologies on VMware vCenter Server:

- VMware vCenter Server (Windows) 5.x
- VMware vCenter Server (Windows) 6.x

Disable Case Sensitive Search for Agent Scan

We added an option to disable the case-sensitive search in Unix agent Directory Search Check and Directory Integrity Check. Once the **Disable case-sensitive search** check-box is selected, the search result lists all possible combinations in the upper and/or lowercase file name. By default, this option is disabled (unchecked) which returns search result with case-sensitive file name.

Note: The case-sensitive search functionality is applicable to both file/directory and not applicable to base directory.

New Control: Directory Integrity Check Turn help tips: On | **Off** Launch Help

General Information > **Agent Scan Options**

Scan Parameters >

Control Technologies >

References >

Agent Scan >

Use agent scans only

Want to define the Base Directory using wildcards?
This option must be selected and this control will only be evaluated using agent scan data.

☐ Use agent scans only

Disable case-sensitive search

By default, the scanner and agent perform case-sensitive matching for this UDC type. When you disable the case-sensitive search, the agent scan will match any combination of uppercase and lowercase letters (i.e. TEST, test, Test). Not applicable to Base directory value.

☐ Disable case-sensitive search

Auto Update expected value

When enabled, we'll update this control's expected value with the actual value collected from each cloud agent scan. You must also enable "Use scan data as expected value" in this control (under Control Technologies). To create reports reflecting results for each agent scan, schedule your compliance reports to run in between the scan interval defined for your agents.

☐ Auto Update expected value

Cancel **Create**

Control Comments added to CSV, XML Formats of Policy Reports

When creating Policy Compliance Reports, users have the option to include control comments in the report output. The control comments already appear in HTML and PDF formats of the report. Starting in this release, control comments will also appear in CSV and XML formats of the report.

To include control comments in the report output you must select it in the Compliance Policy Report Template. Go to **PC > Reports > Templates** and create a new Policy Template (or edit an existing template). On the **Layout** tab in the template, choose **Group By: Controls** and then make sure **Comments** is selected under **Sections > Controls**.

The screenshot shows the 'New Compliance Policy Report Template' dialog box with the 'Layout' tab selected. The left sidebar contains a navigation menu with 'General Information', 'Layout' (selected), 'Display', 'Trending', 'Frameworks', and 'User Access'. The main content area is divided into three sections: 'Timeframe Selection', 'Report Layout', and 'Sections'. In the 'Timeframe Selection' section, 'Show only hosts that have been scanned during the specified period of time.' is displayed, with 'Timeframe' set to 'No Time Limit' and 'Limit Timeframe' set to 'Select a date'. The 'Report Layout' section prompts the user to 'Choose a grouping method for the report's detailed results section, and select the components to be included in the report.' The 'Group By:' dropdown is set to 'Controls'. Below this, 'Status' is set to 'All' and 'Criticality' is set to 'All'. The 'Sections' section is divided into 'Report' and 'Controls'. Under 'Report', 'Control Statistics' and 'Report Details' are checked. Under 'Controls', 'Control Summary', 'External Mappings', 'Comments' (highlighted with a red box), and 'Control References' are listed. The 'Layout' section shows a preview of the report structure, including 'Report Title', 'Report Summary', 'Percentage of Hosts Passed per Control', 'Detailed Results', 'Control', 'Comments', and 'Technology'. The 'Comments' section in the preview is highlighted with a red box. At the bottom, there are 'Cancel', 'Save As...', and 'Save' buttons.

For sample Policy Reports in CSV and XML formats, please refer to the [API Release Notes](#).

Issues Addressed

- In Qualys 10.12 we made a change to automatically move Closed/Ignored tickets to Closed/Fixed when the vulnerability was no longer detected on the host, but have now reverted this change and restored the original behavior. Now there will be no change to Closed/Ignored tickets.
- When searching for a policy by name, the autofill will now work when you enter any part of the policy name.
- Network id was not sent to the download report page. Manager User is able to successfully download the interactive report for both Global Network and Custom Network assets from host asset list page.
- We fixed an issue where access for Unit Managers was not being handled properly for agent hosts. Users will now be able to see appropriate agent hosts which are allowed through the business unit and see any corresponding remediation tickets.
- We fixed an issue where a subscription with VM only (no PC) could not view vCenter authentication record information.
- We fixed an issue where in certain cases Map Report was failing to generate successfully.
- We fixed an issue where in certain specific cases when Agent was installed on Asset with IPv6 address, the scan data was not updating properly.
- We fixed an issue where the next scheduled launch date for a scheduled scan with DST (daylight saving time) enabled was shown 1 day later than the actual next scheduled date. Now the next scheduled date is shown correctly for the scheduled scans.
- We fixed an issue where the Trending graph on the PC > Reports > Policy Summary tab did not show trending data for policies with only asset tags assigned.
- When editing the Expected Value for a control in the Policy Editor, a negative value can only be entered for: equal to, not equal to, greater than, greater than equal to, less than, less than equal to.
- An issue was reported when an SCA user was unable to select the "Enable the Dissolvable Agent" checkbox in the Compliance Option Profile which the user was able to select during one of the previous sessions due to an issue in the code. We fixed the issue in the code. As per the current design, the PC/SCA users will not be able to select the check box if "Scan by Policy" is enabled in the option profile.
- On the expiration of compliance manager, the user was facing the following issues: 1) although the user selected the SCA module from the module picker, after selection, it displayed policy compliance (and not SCA), and 2) user was unable to edit scheduled scans. We have now fixed the issues so that on the selection of SCA from the module picker, SCA is correctly displayed (and not policy compliance) and the user is able to edit scheduled scans.
- We fixed an issue in the API response for Export Scan Template to XML format where the Info key "host_with_cloud_agents" appeared blank instead of showing the correct template setting.
- We updated the help for VMware ESXi to explain that Unix authentication is also required for scanning some ESXi controls and we list the controls that require Unix authentication.
- We made a fix in the help to add Oracle Database 19c as a supported version for both VM and PC.