



Qualys VM for QRadar - QRadar 7.3.3 FP10+/7.4.3 FP3+/7.5.0 GA+

User Guide

Version 3.1.0

March 01, 2023

Copyright 2021-23 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

| | |
|---|-----------|
| Introduction to Qualys VM for QRadar – 7.3.3 FP10+/7.4.3 FP3+/ | 5 |
| Features..... | 5 |
| Prerequisites..... | 5 |
| Install the App..... | 5 |
| Note: | 5 |
| Validating Dependencies | 6 |
| Log Source Event Mapping | 6 |
| Enable Last Scan Datetime Parsing..... | 7 |
| Log Source..... | 7 |
| Custom Event Properties | 8 |
| Configure the App | 9 |
| Qualys API Configurations..... | 9 |
| Advanced Configurations | 13 |
| Steps to enable indexing for the specific custom event properties:..... | 14 |
| Multi-tenant Environment..... | 15 |
| Achieving Multi-tenancy and Segregating Data into Different Log Sources..... | 15 |
| Creating and Configuring Log Source | 16 |
| Managing Multi-tenant Apps | 17 |
| Configure Instance > Qualys VM App Settings option..... | 19 |
| How Qualys App works? | 20 |
| What happens after configuration? | 20 |
| How does data get into QRadar?..... | 20 |
| Using the Qualys app..... | 21 |
| Summary..... | 21 |
| Knowledgebase | 21 |
| Reports..... | 22 |
| Search..... | 25 |
| Raw Data | 26 |
| Input Logs..... | 27 |
| Uninstalling the app..... | 28 |
| Troubleshooting | 29 |
| If you see no data | 29 |
| If your host detection job is not running..... | 29 |
| If you get “[Errno 111] Connection refused” error..... | 29 |
| Case 1 | 29 |
| Case 2 | 30 |
| If you see “HTTP Error 401: Unauthorized” error..... | 30 |
| If you see the ‘Number of host detections logged = 0’ in host detection | 30 |
| If you see “corresponding record not found in KB” message | 30 |
| If you see “Internal Server Error” while saving settings | 30 |
| If dashboard widgets are not showing data for multi-tenant environment | 31 |
| DSM editor does not show Tags or DNS properties and you cannot add them..... | 31 |
| If you need to delete and recreate Log Source Type “Qualys LEEF” | 31 |
| Helpful AQLs to check VM Detection Logs and Events | 33 |
| Compatibility for Qualys VM app for QRadar v3.1.0+..... | 33 |
| Qualys Support..... | 35 |

Introduction to Qualys VM for QRadar – 7.3.3 FP10+/7.4.3 FP3+/7.5.0 GA+

Use the Qualys VM for QRadar – 7.5.0 GA+, 7.5.0 FP3+, 7.3.3 FP10+ to ingest your Qualys VM detections into QRadar and visualize them on a single page. All you need to do is install the app, configure the app, and schedule the sync. The Qualys VM will continuously pull your detection delta, so you always see updated reports. Want to visualize historical data? Just use date-time pickers given in the Qualys VM and see useful reports.

Features

- Support for multi-tenant environment
- Updates for Summary Tab Widget and Reports / Search Tab
- QRadar authentication token workflow to upgrade existing version of Qualys VM for QRadar - QRadar 7.3.3 FP10+/7.4.3 FP3+/7.5.0 GA+ and for fresh installations
- Advanced tab that shows the success and failure messages for the etls running with process IDs. User can download etl logs from Advanced tab

Prerequisites

Make sure you have:

- A valid Qualys subscription
- API access to Qualys VM module
- Knowledgebase API access, if you want to enable Knowledgebase input
- Internet access and your Qualys API server must be reachable from QRadar

Note: This app is compatible with these versions only- 7.3.3 FP10+/7.4.3 FP3+/7.5.0 GA+

Note: If you are upgrading from Qualys app for QRadar 2.0.1 or earlier version to Qualys VM for QRadar - QRadar 7.3.3 FP10+/7.4.3 FP3+/7.5.0 GA+ Version 3.x.x, ensure to Save the Qualys App Settings again even if you saved them in the earlier version.

Install the App

- 1) Log in to QRadar and go to the **Admin** tab.
- 2) Click **Extensions Management**.
- 3) Click the **Add** button and upload the extensions .zip file.
- 4) Confirm whether you want to replace/skip any existing contents with those coming from the extension and click **Install**.

Note:

Installation of our app can be done considering these two scenarios if the user wants to use the app in multitenant environment-

- If you are installing Qualys VM for QRadar - QRadar 7.3.3 FP10+/7.4.3 FP3+/7.5.0 GA+ by checking “Start default instance for each App” checkbox, it will create shared instances for all the security profiles. In this case, to avoid the case of multiple appearance of our app non-admin profiles you need to delete the shared instance from QRadar Assistant app and manually create separate instances for the desired security profile. For more information, refer [Creating an instance](#).
- If you are installing Qualys VM for QRadar - QRadar 7.3.3 FP10+/7.4.3 FP3+/7.5.0 GA+ by unchecking “Start default instance for each App” checkbox it will install the app without creating any instances for it. In this case, you need to create

instances for desired security profile. For more information, refer [Creating an instance](#).

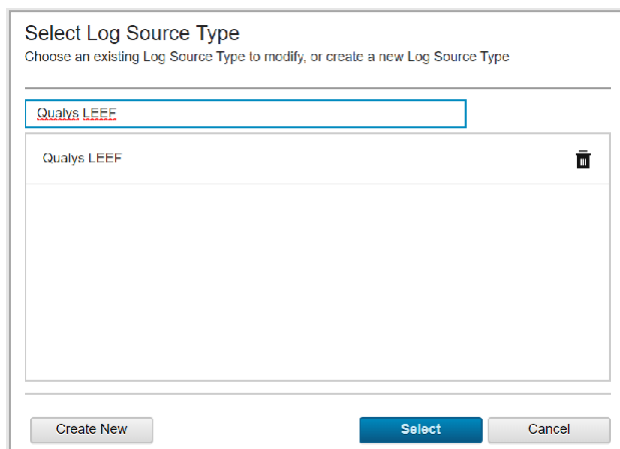
- 5) Once installation is completed, refresh your QRadar user interface.
- 6) You should see the tab **Qualys VM** in the top menu.
- 7) Deploy changes once app installation is completed.

Validating Dependencies

Please go through each of the sections listed below. You need to carry out the following steps manually, right after you install the app and before you start using it. Some sections may not be applicable in your case, and you may need to skip them.

Log Source Event Mapping

- 1) Go to **Admin > DSM Editor**.
- 2) In **Select Log Source Type**, search for “Qualys LEEF” and click **Select**.



- 3) From the Qualys LEEF screen, go to **Event Mappings** tab. The requirement is that there should be mapping for QualysMultiline and if you do not see mapping for QualysMultiline, create new (refer below steps).
- 4) Click + icon to add a new mapping. The “Create a new Event Mapping” pop-up opens. Set **Event ID** as “QualysMultiline” (without quotes) and **Category** as “QualysMultiline” (without quotes).
- 5) Click the **Choose Event** link. In the “Event Categorizations” pop-up that opens, click the **Create New** button. Set the values as follows:
 - Name: QualysMultiline Information
 - Description: QualysMultiline Information
 - Log Source Type: Qualys LEEF
 - High Level Category: System
 - Low Level Category: Information
 - Severity: 2
- 6) Click **Save**. This will take you back to “Event Categorizations”.
- 7) Click and select the newly created entry, which is shown in the “Search Results” table.
- 8) Click **Ok**. This takes you back to “Create a new Event Mapping”.
- 9) Click **Create**. This takes you back to “Qualys LEEF” pop-up - Event Mappings tab.
- 10) Confirm that you now have 3 entries, including Event ID “QualysMultiline” - Category “QualysMultiline”.
- 11) Finally, click **Save** and close the window.

Enable Last Scan Datetime Parsing

- 1) Go to **Admin > DSM Editor**.
- 2) In **Select Log Source Type**, search and select “Qualys LEEF”.
- 3) In the pop-up that opens, go to **Properties**. In the list of properties, search and open “Last Scan Datetime”.
- 4) In the **Property Configuration > Expression** section, click **Edit**.
- 5) Notice the **Enabled** field. This field may be in disabled state (grayed out). If disabled, select the **Enabled** field. It changes color.
- 6) Click **OK** in the Expression section.
- 7) Click **Save** and close the window.

Log Source

When you install app, it will create a new Log Source named “QualysMultiline”. Please check if it is created. You can also create the custom log source for the Qualys app with following steps. Keep the configuration of custom log source same as that mentioned below.

- 1) Qualys VM will send the data to QRadar console only. The user will not be able to use the app for distributed setup.
- 2) On your console UI, go to **Admin > Data Sources > Log Sources** and click the **Add** button.
- 3) Add the details shown below to the form to Create QualysMultiline Log Source. All fields marked with an asterisk (*) are mandatory. Make sure your Log Source Name and Log Source Identifier have same value.

| Property | Value | |
|-----------------------------|---|---|
| Log Source Name | QualysMultiline (Customizable) | * |
| Log Source Description | QualysMultiline | |
| Log Source Type | Qualys LEEF | * |
| Protocol Configuration | TCP Multiline Syslog | * |
| Log Source Identifier | QualysMultiline (Customizable, but same as Log Source Name) | * |
| Listen Port | 12468 (Customizable) | |
| Aggregation Method | Start/End Matching | * |
| Event Start Pattern | [A-Z][a-z][a-z]\s\d\d\s\d\d:\d\d:\d\d\s | * |
| Event End Pattern | qualys_event_ends | * |
| Event Formatter | No Formatting | * |
| Show Advance Option | Yes | * |
| Use Custom Source Name | Unchecked | * |
| Use As a Gateway Log Source | Checked | * |

| | | |
|--|-----------------------|---|
| Flatten Multiline Events into Single Line | Checked | * |
| Retain Entire Lines During Event Aggregation | Checked | * |
| Enabled | Checked | * |
| Credibility | 5 | |
| Target Event Collector | <default/your choice> | |
| Coalescing Events | Unchecked | * |
| Store Event Payload | Checked | * |
| Log Source Extension | QualysLEEFCustom_ext | * |

4) Click **Save**.

If you need to create this new Log Source manually, you must do a full deployment. For that, please go to **Admin > Advance** and click **Deploy Full Configuration**.

Custom Event Properties

- 1) Go to **Admin > Log Sources** and confirm that QualysMultiline Log Source is Enabled. If it is disabled, please enable it.
- 2) Go to **Admin > Custom Event Properties** and confirm that all 25 Qualys related properties are Enabled and are linked to “Qualys LEEF” log source type.

Qualys related properties are:

- App Version
- PCI Flag
- Qualys QID
- Severity Level
- QID Category
- CVE
- Last Fixed Datetime
- Operating System
- Qualys Host ID
- Tracking Method
- First Found Datetime
- Qualys Severity
- Last Scan Datetime
- App ID
- Last Test Datetime
- Detection Type
- Patchable
- Last Update Datetime
- Network ID
- Last Found Datetime

- QID Title
- Host IP
- Status
- DNS
- Tags

For the Qualys related properties, complete these checks:

- 1) If any property is disabled, enable it.
- 2) If any property does not belong to the Qualys LEEF log source type, please open it to edit and select Qualys LEEF as the log source type.
- 3) If any property does not belong to QualysMultiline log source, open it to edit and select QualysMultiline as log source.
- 4) Please check if all Custom Event Properties have Event Name as QualysMultiline Information. If not, select Event Name as QualysMultiline Information.
- 5) Finally, save the properties.

If you do not see the properties, please refer to the [Troubleshooting](#) section in this document to learn how to delete and recreate Log Source Type “Qualys LEEF”.

For any change in Custom Event Properties, it is recommended to do Deploy Full Configuration.

Configure the App

For Single User Instance - If you want to use Qualys VM for QRadar - QRadar 7.3.3 FP10+/7.4.3 FP3+/7.5.0 GA+ as single user instance, you just need to configure the steps mentioned in [Qualys API Configurations](#).

Multi-tenant Environment - If you want to use Qualys VM for QRadar QRadar 7.3.3 FP10+/7.4.3 FP3+/7.5.0 GA+ in multi-tenant environment, you need to configure the steps mentioned in [Multi-tenant Environment](#) section and then the steps mentioned in [Qualys API Configurations](#).

Qualys API Configurations

Complete the following steps once you configure the app.

- 1) Log in to QRadar and go to the **Admin** tab.
- 2) Scroll to “Apps” section and click **Qualys VM App Settings**. A pop-up window opens.

Credentials

QRadar Authorization token is used while interacting securely with QRadar. You can obtain this token from **Admin > User Management > Authorized Service**.

For multi-tenant environment, make sure that you create an authentication token with user role permission specific to the security profile's user and select security profile same as that of the instance is created and configured. For more information, refer [Adding an authorized service](#).

For example, here we have created instance for *Security Profile A* and users that will be using this instance has user role as *User Role A*. Hence, while creating authentication token for the created instance, follow the steps:

- a) Go to **Authorized Services** in Admin tab
- b) Click **Add Authorized Service**.
- c) Enter the desired **Service Name**.
- d) Select **User Role** as *User Role A*.
- e) Select **Security Profile** as *Security Profile A*.
- f) Set the expiry date as required.
- g) Click **Create Service** and then click **Deploy changes**.

To get started, an authorization token of respective user role and security profile is required. Please contact your system administrator to generate an authorization service token.
Note: Deploy changes once the token is created.

QRadar Authorization Token

Log Source Name

Qualys API Server URL

Qualys API Username

Qualys API Password

☐ Use a proxy server for API calls

Proxy Server

Save

Use the **Credentials** tab to configure your Qualys credentials. Enter your Qualys API server, username, and password in the appropriate fields.

QRadar Authorization Token

Log Source Name

Qualys API Server URL

Qualys API Username

Qualys API Password

☒ Use a proxy server for API calls

Proxy Server

Proxy Configuration

If you want Qualys app to use proxy while calling the API, configure proxy details.

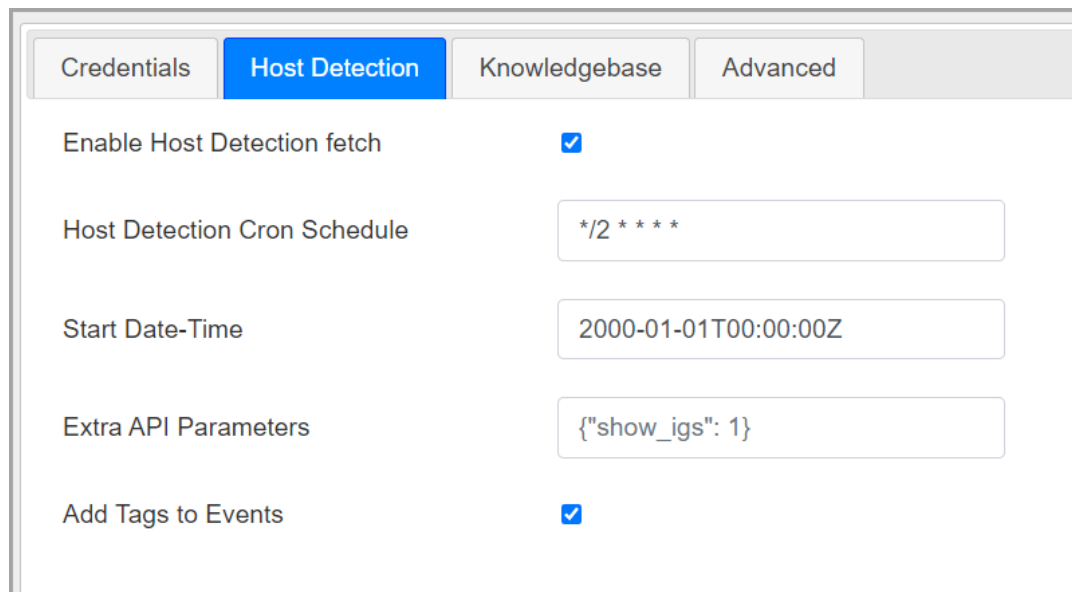
Select the check box to enable proxy.

Add your proxy server and proxy port in <proxy server>:<proxy port> format.

If your proxy needs authentication, add proxy user and proxy password along with server and port, in <proxy user>:<proxy password>@<proxy server>:<proxy port> format.

Host Detection

Use the **Host Detection** tab to configure and enable Host Detection input.



The screenshot shows a configuration window with four tabs: 'Credentials', 'Host Detection' (which is selected and highlighted in blue), 'Knowledgebase', and 'Advanced'. Below the tabs, there are five configuration items:

- Enable Host Detection fetch**: A checkbox that is checked with a blue checkmark.
- Host Detection Cron Schedule**: A text input field containing the cron expression `* / 2 * * * *`.
- Start Date-Time**: A text input field containing the ISO 8601 timestamp `2000-01-01T00:00:00Z`.
- Extra API Parameters**: A text input field containing the JSON object `{"show_igs": 1}`.
- Add Tags to Events**: A checkbox that is checked with a blue checkmark.

You must enable this input to use this extension. To enable this input, select the checkbox in front of **Enable Host Detection fetch**.

In the **Host Detection Cron Schedule** field, write a valid cron entry (time part only). Your input will run according to this schedule. This is a mandatory field. It is advised that you keep the cron schedule coordinated with your scanning schedule. For example, if you run scans once a day, schedule this input to run once a day. [Learn about cron expressions...](#)

(Optional) In the “Start Date-Time” field, enter the date from which you wish to fetch the VM detection data. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2007-01-25T23:12:00Z”. This field is optional and may be left blank. When left blank, it defaults to 1999-01-01T00:00:00Z.

(Optional) If you want to provide any extra parameters for the Host Detection API, set them in the Extra **API Parameters** field, in valid JSON format. Please refer to the [Qualys API \(VM, PC\) User Guide](#) for a list of API input parameters. This field is optional and may be left blank.

(Optional) If you want to get Tags in VM detection data, select the “Add Tags to Events” option.

Knowledgebase

Use Knowledgebase tab to configure and enable Knowledgebase input.

A copy of Qualys knowledgebase is bundled with this extension. To keep it up to date, please enable this input. It is advised that you update your knowledgebase copy at least once a week.

To enable this input, select the checkbox in front of **Enable Knowledgebase fetch**.

In the **Knowledgebase Cron Schedule** field, write a valid cron entry (time part only). Your input will run according to this schedule. This is a mandatory field. You might not want to run this every day. Once a week is also OK. [Learn about cron expressions...](#)

(Optional) If you want to provide any extra parameters for the Knowledgebase API, set them in the **Extra API Parameters** field, in valid JSON format. Please refer to the [Qualys API \(VM, PC\) User Guide](#) for a list of API input parameters. This field is optional and may be left blank.

You can specify **KB table batch size** to define the number of records to be pulled for faster loading.

The screenshot shows the 'Knowledgebase' configuration tab. It has four sub-tabs: 'Credentials', 'Host Detection', 'Knowledgebase' (selected), and 'Advanced'. The 'Knowledgebase' tab contains the following settings:

- Enable Knowledgebase fetch:** A checkbox that is checked.
- Knowledgebase Cron Schedule:** A text input field containing the cron expression `*/* * * * *`.
- Extra API Parameters:** A text input field containing the JSON object `{"is_patchable": 1}`.
- KB table batch size:** A text input field containing the value `1000`.

Advanced

Use Advanced tab to see the last success and last failure for host detection and knowledgebase.

The screenshot shows the 'Advanced' configuration tab. It has four sub-tabs: 'Credentials', 'Host Detection', 'Knowledgebase', and 'Advanced' (selected). The 'Advanced' tab displays the following information:

- Host Detection:** A section with a yellow status indicator and 'Process ID 648'. It shows 'Last Success' as '19 minutes ago' with '3688 host detection(s) logged'. Below it, 'Last Failure' is shown as '2 minutes ago' with the message 'Response Code:401, Got unexpected response from API: ACCESS DENIED'.
- Knowledgebase:** A section with a yellow status indicator and 'Process ID 644'. It shows 'Last Success' as '46 minutes ago' with 'Added 1693 new QID(s) and updated 1022 QID(s)'. Below it, 'Last Failure' is shown as '2 minutes ago' with the message 'Error during request to https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/: API request failed: <?xml version="1.0" encoding="UTF-8" ?>'.
- Download Application Logs:** A section with a blue 'Download' button. It includes the text 'This includes the app.log, startup.log & background job's log files.' and 'Application ID: 1104'.
- Save:** A blue 'Save' button at the bottom right.

Advanced Configurations

These are the advanced and optional configurations which provides you additional benefits while using Qualys VM for QRadar - QRadar 7.3.3 FP10+/7.4.3 FP3+/7.5.0 GA+!

Index Management

From the QRadar Console, you can use the Index Management tool to control database indexing on event and flow properties. By adding an indexed field in your search query, it helps to improve the speed of searches in QRadar by narrowing the overall data. Learn how to modify database indexing in the Index Management tool by making use of statistics before and after you enable or disable indexing on multiple properties.

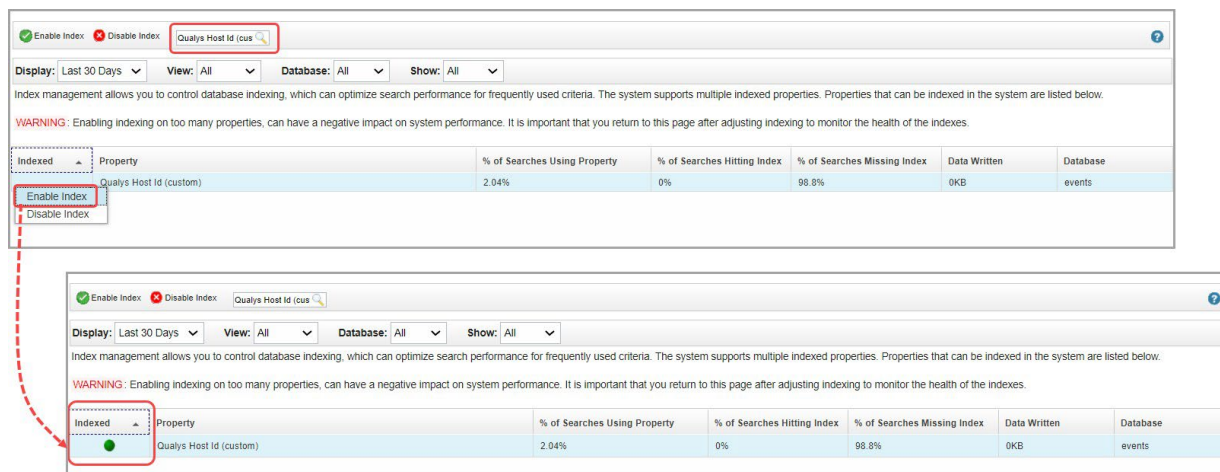
Steps to enable indexing for the specific custom event properties:

1) On the navigation menu, click **Admin** and then click **Index Management** in the **System Configuration** section.

2) Search, select and click **Enable Index** for the below mentioned properties:


- Qualys Host Id (custom)
- Qualys Severity (custom)
- Qualys QID (custom)
- Status (custom)
- Last Scan Date (custom)
- Detection Type (custom)

Once you click **Enable Index**, *Indexed* column shows  (green bubble) for the indexed property.



The screenshots show the Index Management interface in QRadar. The top screenshot shows the 'Qualys Host Id (custom)' property with the 'Enable Index' button highlighted. The bottom screenshot shows the same property with a green bubble in the 'Indexed' column, indicating that indexing has been successfully enabled. A red dashed arrow points from the 'Enable Index' button in the top screenshot to the green bubble in the bottom screenshot.

| Indexed | Property | % of Searches Using Property | % of Searches Hitting Index | % of Searches Missing Index | Data Written | Database |
|-------------------------------|-------------------------|------------------------------|-----------------------------|-----------------------------|--------------|----------|
| Enable Index Disable Index | Qualys Host Id (custom) | 2.04% | 0% | 98.8% | 0KB | events |

| Indexed | Property | % of Searches Using Property | % of Searches Hitting Index | % of Searches Missing Index | Data Written | Database |
|---|-------------------------|------------------------------|-----------------------------|-----------------------------|--------------|----------|
|  | Qualys Host Id (custom) | 2.04% | 0% | 98.8% | 0KB | events |

3) Click **Save**.

For more information, refer [Index management](#).

Multi-tenant Environment

Multitenant environments allow Managed Security Service Providers (MSSPs) and multi-divisional organizations to provide security services to multiple client organizations from a single and shared IBM QRadar deployment. You do not have to deploy a unique QRadar instance for each customer.

In a multitenant deployment, you ensure that customers see only their data by creating domains that are based on their QRadar input sources. Then, use security profiles and user roles to manage privileges for large groups of users within the domain. Security profiles and user roles ensure that users have access to only the authorized information.

Achieving Multi-tenancy and Segregating Data into Different Log Sources

Prerequisites for Setup:

- QRadar Version should be multitenancy supported.
- QRadar Assistant App must be installed with Version 3.1.0 or later
- Qualys VM for QRadar - QRadar 7.3.3 FP10+/7.4.3 FP3+/7.5.0 GA+ should be installed
- QRadar Log Source Management app should be installed

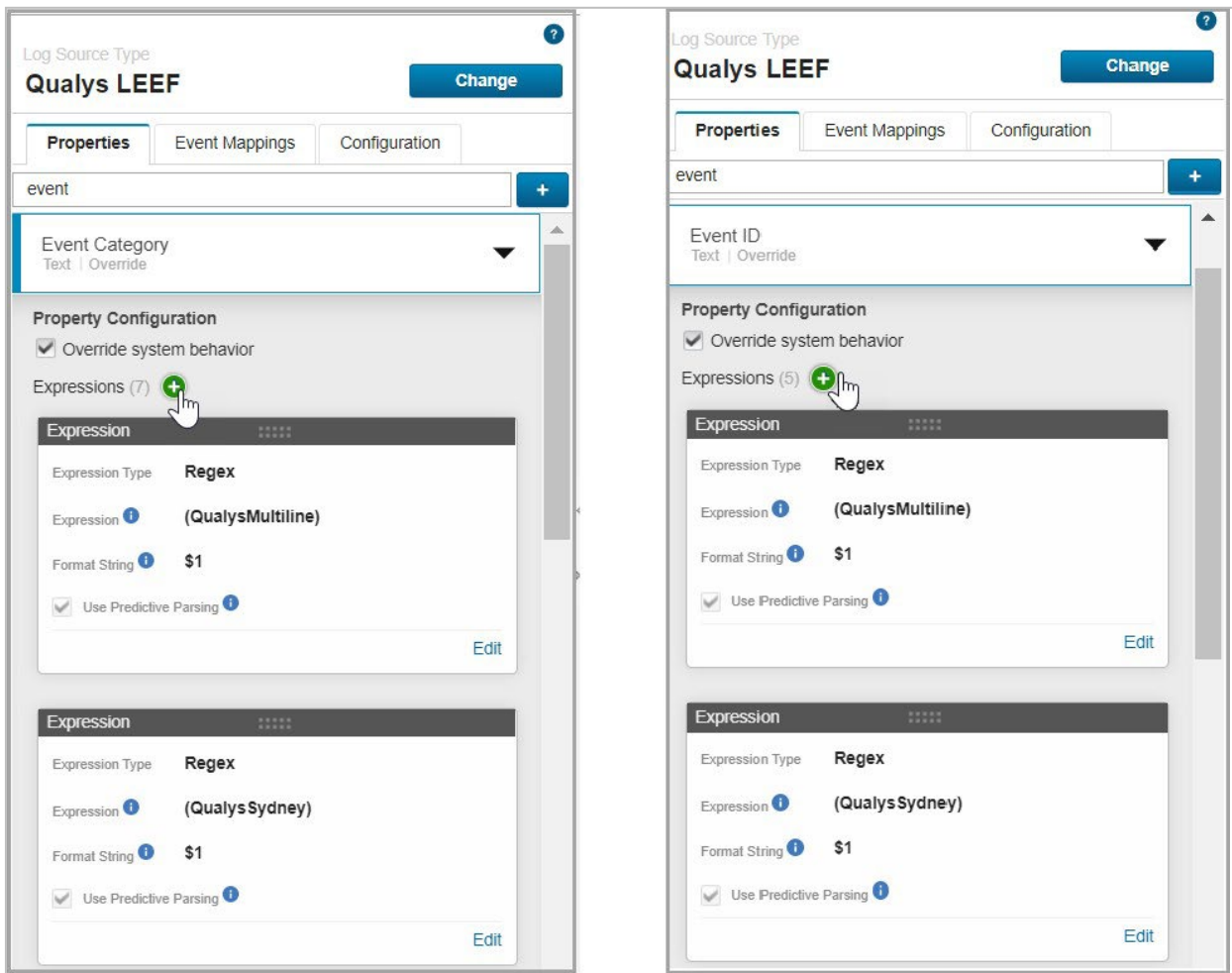
Prerequisites for Configurations:

- [Creating and Configuring Log Sources](#) - Event ID, Event Category and Event Mappings
- [Creating Tenant](#)
- [Creating and assigning a domain to the tenant](#)
- [Creating a Security profile](#) and associating Domains and Log sources to it
- [Creating a user role](#) for Tenant users
- [Create the tenant users](#) with desired User role and Security profile

Creating and Configuring Log Source

User can create custom log sources of "Qualys LEEF" log source type to segregate the data. For more information, see [Log Sources](#).

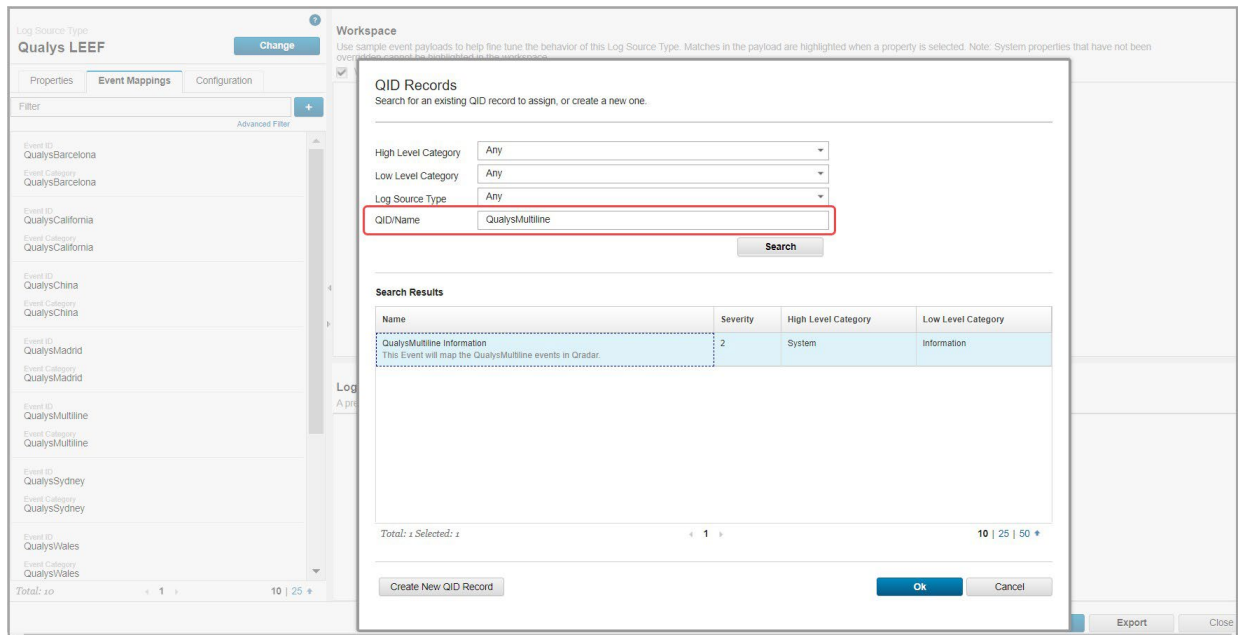
1. After creating Log Sources, go to **DSM Editor** and search for "Qualys LEEF" log source type.
2. Add Event ID and Event Category in Properties tab specific to the log source for which data is to be pulled. In DSM Editor in Qualys LEEF log source 'Properties' tab user will need to create a new Event Id and Event Category like 'QualysMultiline' as per the Log source created, add format string for both Event Id and Event Category then save it.



Note: If the user is upgrading from the Qualys app for QRadar 2.0.1, where **Event ID** and **Event Category** was configured for the required log source, user will need to repeat the Step-2 again after upgrade since the Qualys LEEF Log Source Type properties are replaced with new app on upgrading.

3. Create the event mapper in the "Event Mappings" tab specific for the created log source-
 - User will need to create event mapper in "Event Mappings" tab and choose the already existing QID i.e., 'QualysMultiline'.
 - Enter the same values in "Event ID" and "Event Category" field as per the log source name and then click **Choose QID** and search for "QualysMultiline Information".

Note: This way the user created event mapper will inherit the configurations of the "QualysMultiline" event mapper that comes bundled with app installation.





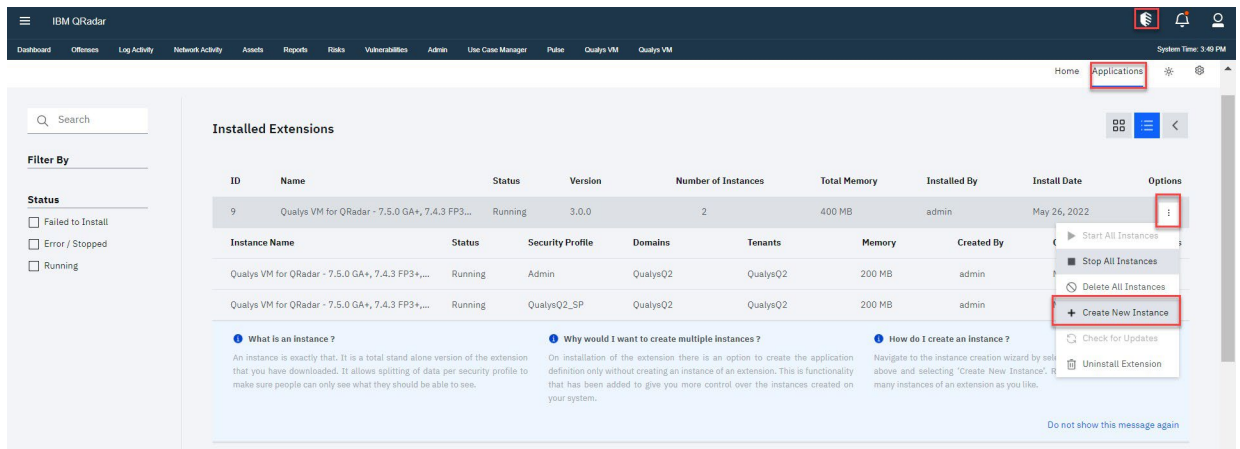
Now, user will be able to pull the data into the desired Log Source by following the above steps and saving the same log source in the Qualys VM App settings.

Managing Multi-tenant Apps

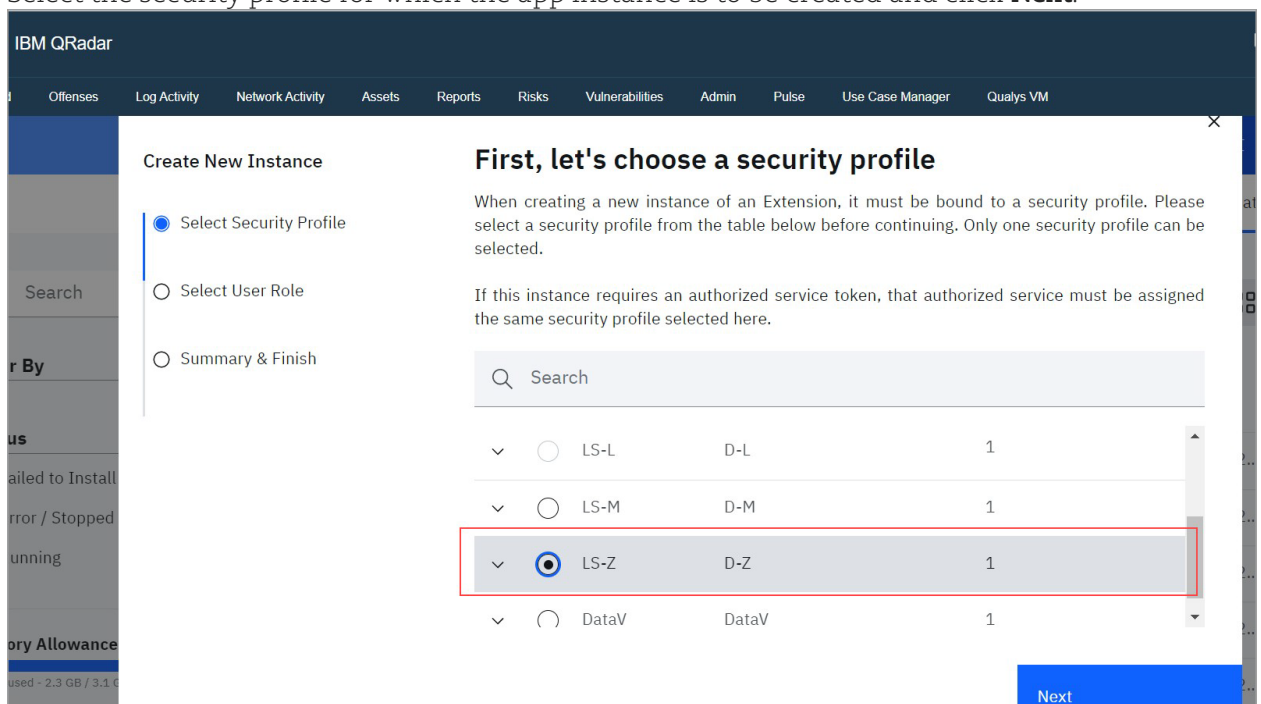
Qualys VM for QRadar - QRadar 7.3.3 FP10+/7.4.3 FP3+/7.5.0 GA+ can now be used in multi-tenant environment for QRadar V 7.4.1 Fix Pack 2, 7.4.2 GA+ or later. When a user installs the app, they are presented with the option to create a default instance. Users can select this option if they only want a single instance of the app, or the app does not need to support multi-tenancy. If a user does not select the Default Instance option, they must create a separate instance and associate each instance with a security profile to keep all your data separate.

Creating an Instance

1. Click the QRadar Assistant app icon (), and then click **Applications**.
2. Ensure you are in the List View (**Manage** > List View option) in Application Manager.
3. In the Installed Extensions section, click the ellipsis icon () in the **Options** column of the extension and then click **Create New Instance**.



- Select the security profile for which the app instance is to be created and click **Next**.



- Select user role shown for the selected security profile and click **Next**.
- Review the summary and click **Confirm & Create** to create an instance.
- Once you confirm the changes, the app will be installed for that security profile and app instance will be created.
Run the following command to check the app ID for the instance:
/opt/qradar/support/recon ps
- Go to Admin tab and click **Deploy Changes**.

Managing Instances

After creating multiple instances, it will be listed as shown below with the total memory consumed and the memory for each instance.

The screenshot shows the IBM QRadar interface. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Risks', 'Vulnerabilities', 'Admin', 'Use Case Manager', 'Pulse', 'Qualys VM', and 'Qualys VM'. The main content area is titled 'Installed Extensions'. On the left, there is a 'Filter By' section with 'Status' options: 'Failed to Install', 'Error / Stopped', and 'Running'. The main table lists installed extensions with columns: ID, Name, Status, Version, Number of Instances, Total Memory, Installed By, Install Date, and Options. A red box highlights the first row of the table, which shows an instance of 'Qualys VM for QRadar - 7.5.0 GA+, 7.4.3 FP3+...' with a status of 'Running', version '3.0.0', 2 instances, and 400 MB of memory. Below the table, there are three informational sections: 'What is an instance?', 'Why would I want to create multiple instances?', and 'How do I create an instance?'. The 'What is an instance?' section explains that an instance is a total stand-alone version of the extension. The 'Why would I want to create multiple instances?' section explains that on installation, there is an option to create the application definition only without creating an instance of an extension. The 'How do I create an instance?' section explains that you can create an instance by selecting the overflow menu (three dots) above and selecting 'Create New Instance'.

| ID | Name | Status | Version | Number of Instances | Total Memory | Installed By | Install Date | Options |
|----|---|---------|---------|---------------------|--------------|--------------|--------------|---------|
| 9 | Qualys VM for QRadar - 7.5.0 GA+, 7.4.3 FP3+... | Running | 3.0.0 | 2 | 400 MB | admin | May 26, 2022 | : |

| Instance Name | Status | Security Profile | Domains | Tenants | Memory | Created By | Creation Date | Options |
|---|---------|------------------|----------|----------|--------|------------|---------------|---------|
| Qualys VM for QRadar - 7.5.0 GA+, 7.4.3 FP3+... | Running | Admin | QualysQ2 | QualysQ2 | 200 MB | admin | May 26, 2022 | : |
| Qualys VM for QRadar - 7.5.0 GA+, 7.4.3 FP3+... | Running | QualysQ2_SP | QualysQ2 | QualysQ2 | 200 MB | admin | May 26, 2022 | : |

What is an instance ?
An instance is exactly that. It is a total stand alone version of the extension that you have downloaded. It allows splitting of data per security profile to make sure people can only see what they should be able to see.

Why would I want to create multiple instances ?
On installation of the extension there is an option to create the application definition only without creating an instance of an extension. This is functionality that has been added to give you more control over the instances created on your system.

How do I create an instance ?
Navigate to the instance creation wizard by selecting the overflow menu (⋮) above and selecting 'Create New Instance'. Remember you can create as many instances of an extension as you like.

Do not show this message again

To configure the Qualys VM App Settings from QRadar Assistant for the created instances, follow the steps mentioned below:

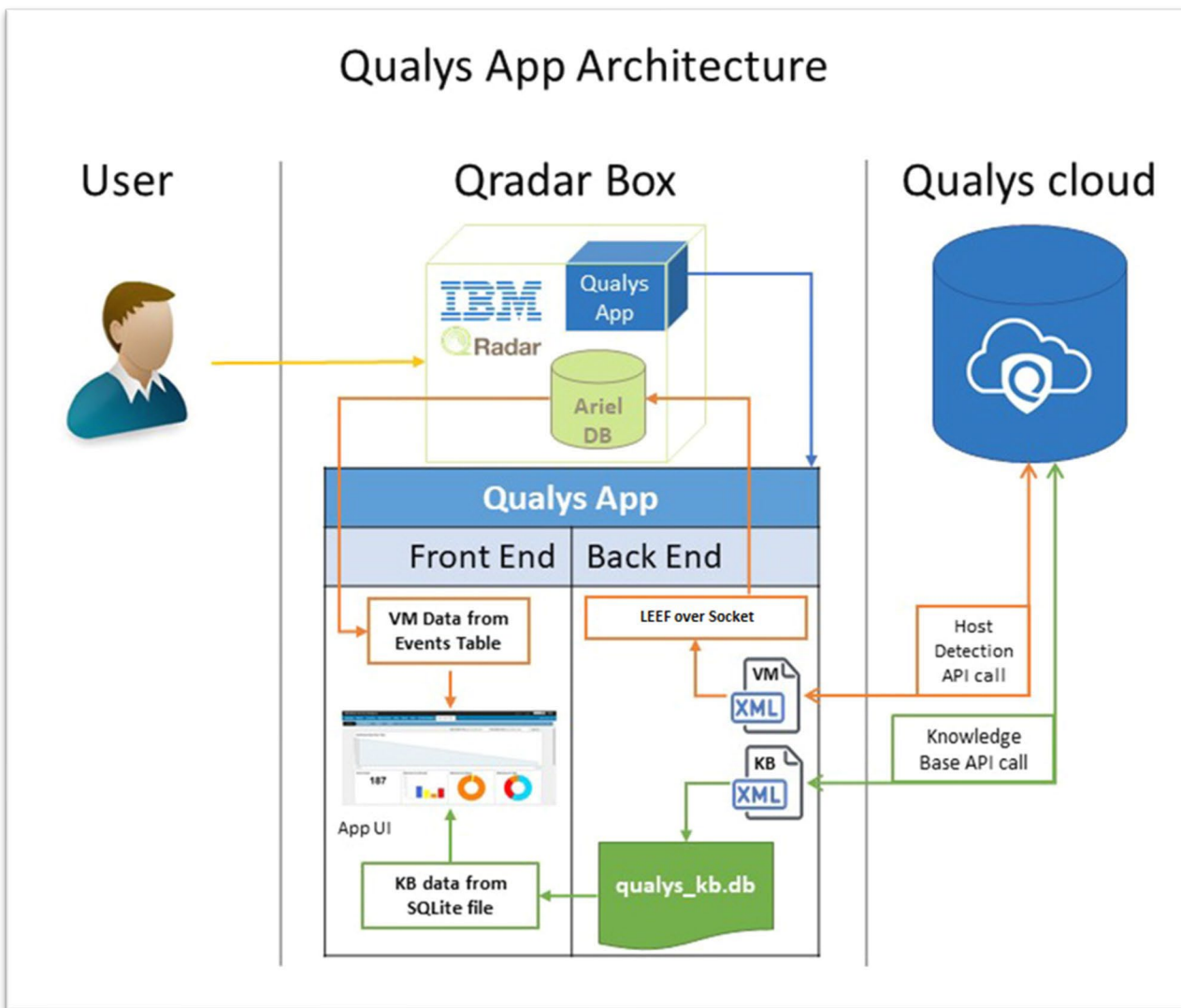
1. Click on the ellipsis icon (⋮) in the **Options** column for the instance and then click **Configure Instance > Qualys VM App Settings** option.
2. Do various configurations on the Configuration Page. For more information, see [Qualys VM App Settings](#).

For more information related to other options, refer [Managing instances](#).

Configuring Instance

For multi-tenant instance, once you complete above configurations, you need to proceed with [Qualys API Configurations](#).

How Qualys App works?



What happens after configuration?

Once you configure and enable Host Detection input, the application bundled with this extension will start fetching your VM detection data. By default, it will pull detection data for 10 hosts at a time. This value is set to such a small number to make sure the app can process your data without hitting the memory limit governed by QRadar. For first run, it might take some time depending on your scan volume. After that, subsequent pulls are incremental ones - fetching only new/changed data.

How does data get into QRadar?

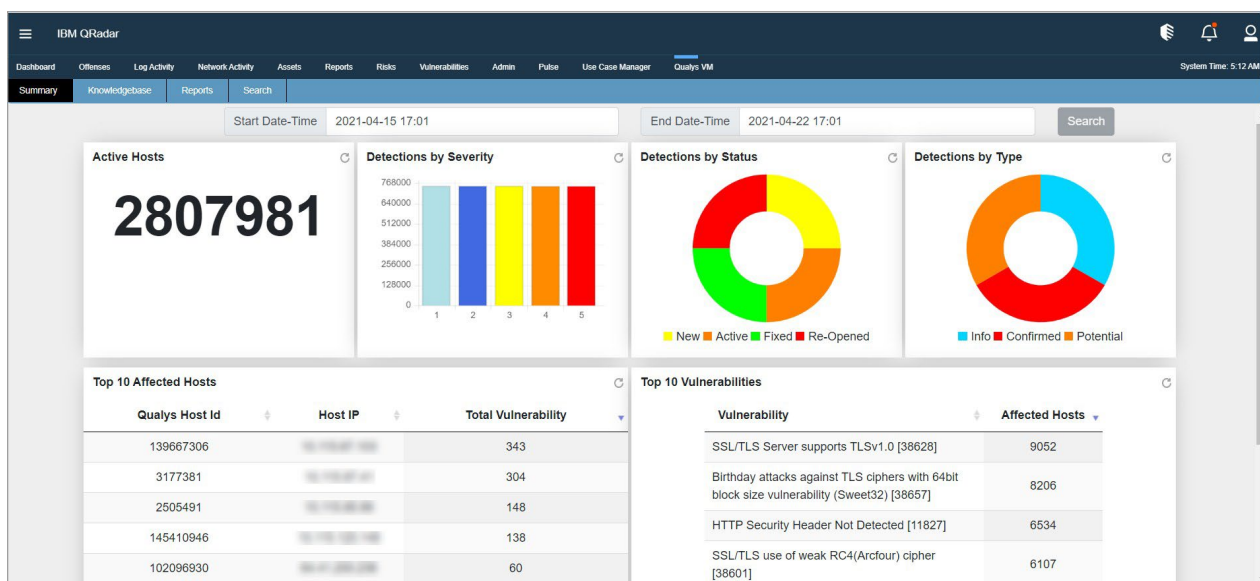
Whenever cron runs any job (based on the cron schedule you defined), it makes outbound API call to Qualys, transforms the XML response it receives into LEEF format and sends it to the QRadar over socket using TCP port configured in "QualysMultiline" Log Source. Using DSM editor and "QualysLEEF" Log Source Type provided with this extension, QRadar then puts this data into the "events" table in Ariel database.

Using the Qualys app

Summary

When you click the **Qualys VM** tab in the top menu, you will see a summary dashboard provided by the app. It renders the following reports:

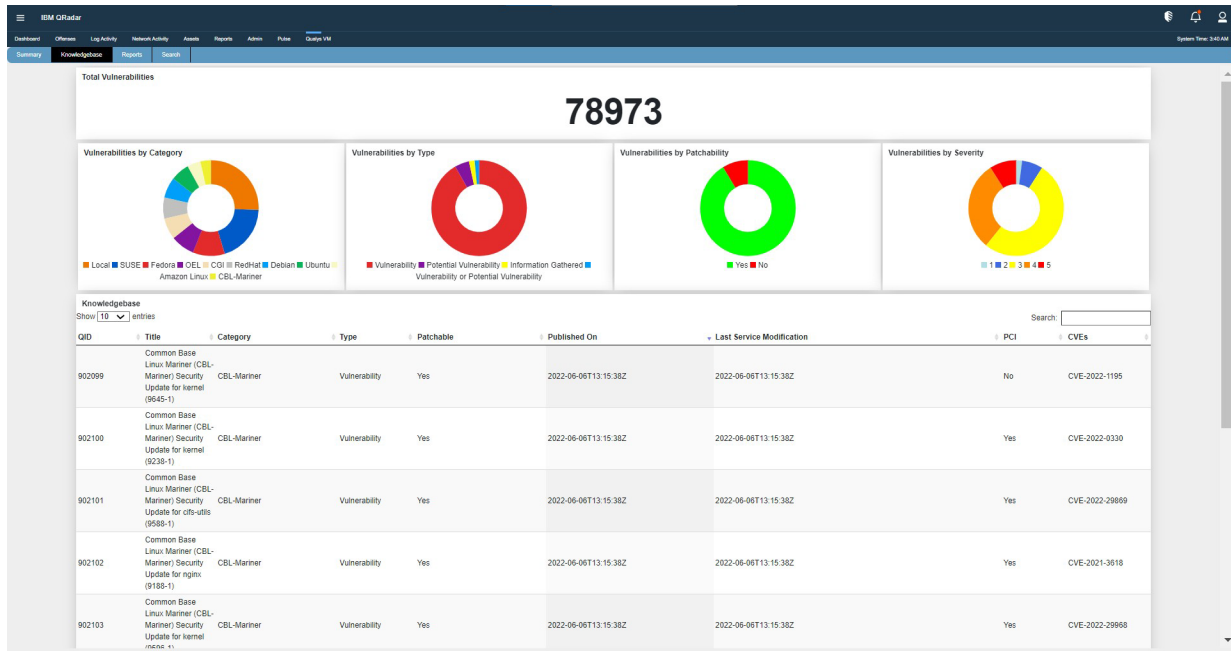
- Count of Active Hosts
- Detections by Severity
- Detections by Status
- Detections by Type
- Top 10 Affected Hosts
- Top 10 Vulnerabilities



By default, these reports are based on detection data in the last 20 days. To change this date-time range, use “Start Date-Time” and “End Date-Time” and click the **Search** button. When you click Search, all the reports are updated according to the new date-time range that you have defined.

Knowledgebase

The application has a default copy of knowledgebase bundled with it. This menu shows you some visualizations about current knowledgebase copy. If you enabled knowledgebase input, this copy will be kept up to date. It also shows knowledgebase in tabular format.



Reports

You can view reports for vulnerabilities by hosts and hosts by vulnerabilities within specific date range.

Note: Not all the data is pulled at once. Only 20 records of all the data are displayed. To get remaining data you can click the paginations option to view the remaining data.

Vulns by Hosts

IBM QRadar

Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Risks | Vulnerabilities | Admin | Pulse | Use Case Manager | Qualys VM

System Time: 5:18 AM

Report for Vulns by

Start Date-Time: 2021-04-15 17:17 | End Date-Time: 2021-04-22 17:17 | Search

Showing 0 to 0 of 0 entries

First | Previous | Next | Last

| Host ID | IP Address | Operating System | Total Vulnerabilities |
|---------|------------|------------------|-----------------------|
|---------|------------|------------------|-----------------------|

Click on count of Total Vulnerabilities to view vulnerabilities on the host.

Report for Vulns by Hosts

Start Date-Time: 2000-04-20 12:17 End Date-Time: 2021-04-27 12:17 Search

Showing 1 to 20 of 1,301 entries

| Host ID | IP Address | Operating System | Total Vulnerabilities |
|-----------|------------|---|-----------------------|
| 101166659 | | Windows 7 Ultimate 64 bit Edition Service Pack 1 | 810 |
| 109806509 | | Windows Server 2008 R2 Enterprise 64 bit Edition Service Pack 1 | 769 |
| 113870509 | | Ubuntu Linux 16.04 | 619 |
| 811299 | | Windows XP 64 bit Edition Service Pack 2 | 579 |
| 1080301 | | Windows XP 64 bit Edition Service Pack 2 | 560 |
| 968847 | | Windows 2003 R2 Service Pack 2 | 556 |
| 9532546 | | Windows XP 64 bit Edition Service Pack 2 | 553 |
| 15286517 | | Windows 2003 Service Pack 2 | 550 |

Vulns appear in table format.

Showing Vulnerabilities on 71226535

Showing 1 to 20 of 535 entries

| QID | QID Title | Severity | Category | Detection Type | Patchable | Status |
|-----------------------------|---|----------|------------|----------------|-----------|--------|
| 87120 | Apache HTTP Server HttpOnly Cookie Information Disclosure Vulnerability | 3 | Web server | Confirmed | Yes | New |
| 86477 | Apache Web Server ETag Header Information Disclosure Weakness | 1 | Web server | Confirmed | No | New |
| Web Server HTTP Trace/Track | | | | | | |

Showing 1 to 20 of 535 entries

Hosts by Vulns

Report for Hosts by Vulns by Hosts

Start Date-Time: 2021-04-15 17:20 End Date-Time: 2021-04-22 17:20 Search

Showing 0 to 0 of 0 entries

| QID | QID Title | Severity | Category | Detection Type | Patchable | Total Hosts |
|-----|-----------|----------|----------|----------------|-----------|-------------|
|-----|-----------|----------|----------|----------------|-----------|-------------|

Click on count of Total Hosts to view affected hosts on QID.

IBM QRadar

Dashboard

Offenses

Log Activity

Network Activity

Assets

Reports

Risks

Vulnerabilities

Admin

Putie

Use Case Manager

Qualys VM

Summary

Knowledgebase

Reports

Search

System Time: 11:55 AM

Report for Hosts by Vulns

Start Date-Time

2016-04-01 12:19

End Date-Time

2021-04-27 12:19

Search

Showing 1 to 20 of 7,927 entries

First

Previous

1

2

3

4

5

...

397

Next

Last

| QID | QID Title | Severity | Category | Detection Type | Patchable | Total Hosts |
|-------|--|----------|-------------------------|----------------|-----------|-------------|
| 38739 | Deprecated SSH Cryptographic Settings | 2 | General remote services | Confirmed | No | 372 |
| 38623 | OpenSSH Xauth Command Injection Vulnerability | 3 | General remote services | Potential | Yes | 297 |
| 42413 | OpenSSH LoginGraceTime Denial of Service Vulnerability | 3 | General remote services | Potential | Yes | 279 |

Hosts appears in table format.

Showing Affected Host for 27000

Showing 1 to 20 of 7,344 entries

FirstPrevious12345...368NextLast

| Host ID | IP Address | Operating System | Status |
|----------|------------|--|--------|
| 93751696 | | Debian Linux 7.1 | New |
| 93744170 | | Windows NT4 | Active |
| 75895479 | | HP BladeSystem | Active |
| 60188030 | | Windows 2000 Service Pack 3-4 | Active |
| 60188019 | | Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP | New |
| 55690307 | | Windows NT4 | New |

Showing 1 to 20 of 7,344 entries

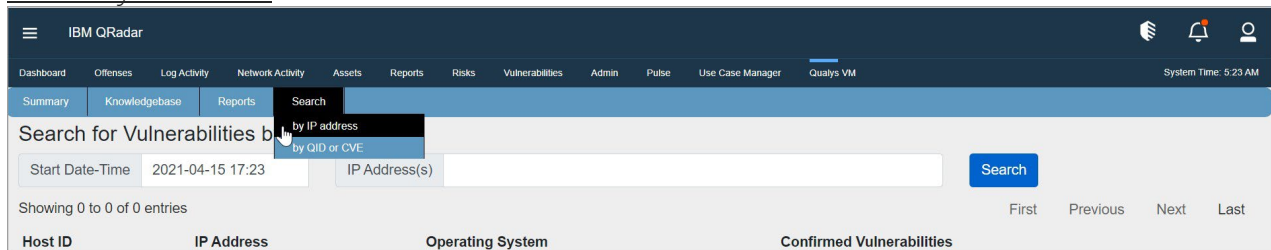
FirstPrevious12345...368NextLast

Search

You can search for vulnerabilities in **Search** tab by QID or CVE or by IP address.

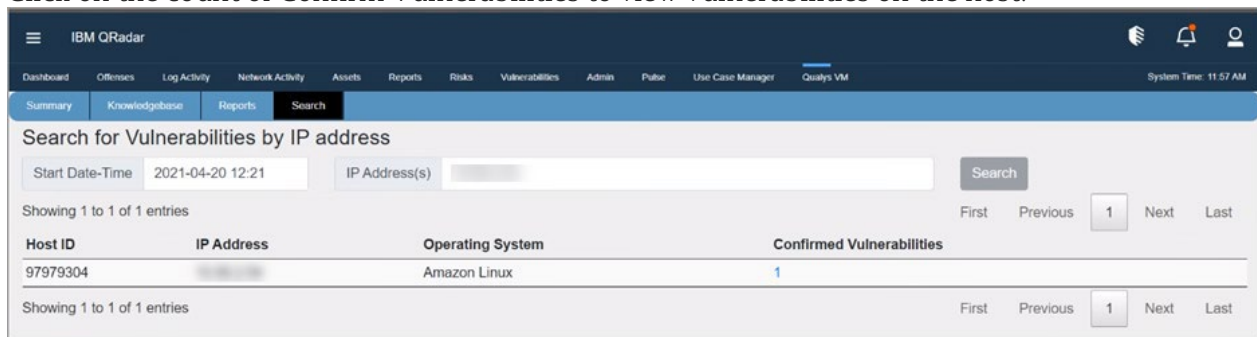
Note: Not all the data is pulled at once. Only 20 records of all the data are displayed. To get remaining data you can click the paginations option to view the remaining data.

Search by IP Address:



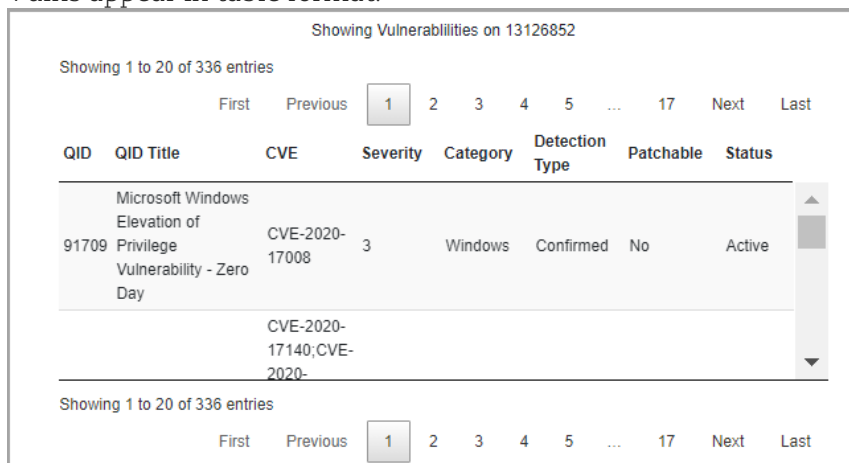
The screenshot shows the IBM QRadar Search interface. The top navigation bar includes tabs for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin, Pulse, Use Case Manager, and Qualys VM. The Search tab is active. Below the navigation bar, there is a search bar with the text "Search for Vulnerabilities by". A dropdown menu is open, showing options "by IP address" and "by QID or CVE". The search bar also includes a "Start Date-Time" field with the value "2021-04-15 17:23" and an "IP Address(s)" field. A "Search" button is located to the right of the search bar. Below the search bar, there is a table with columns: Host ID, IP Address, Operating System, and Confirmed Vulnerabilities. The table shows 0 to 0 of 0 entries.

Click on the count of Confirm Vulnerabilities to view vulnerabilities on the host.



The screenshot shows the IBM QRadar Search interface with search results for a specific IP address. The search bar has the text "Search for Vulnerabilities by IP address". The "Start Date-Time" field has the value "2021-04-20 12:21". The "IP Address(s)" field is empty. The "Search" button is located to the right of the search bar. Below the search bar, there is a table with columns: Host ID, IP Address, Operating System, and Confirmed Vulnerabilities. The table shows 1 to 1 of 1 entries. The first entry has Host ID "97979304", IP Address "131.268.52", Operating System "Amazon Linux", and Confirmed Vulnerabilities "1".

Vulns appear in table format.



The screenshot shows the IBM QRadar Search interface with search results for a specific IP address in table format. The table has columns: QID, QID Title, CVE, Severity, Category, Detection Type, Patchable, and Status. The table shows 1 to 20 of 336 entries. The first entry has QID "91709", QID Title "Microsoft Windows Elevation of Privilege Vulnerability - Zero Day", CVE "CVE-2020-17008", Severity "3", Category "Windows", Detection Type "Confirmed", Patchable "No", and Status "Active".

| QID | QID Title | CVE | Severity | Category | Detection Type | Patchable | Status |
|-------|---|----------------|----------|----------|----------------|-----------|--------|
| 91709 | Microsoft Windows Elevation of Privilege Vulnerability - Zero Day | CVE-2020-17008 | 3 | Windows | Confirmed | No | Active |

Search by QID or CVE:

The screenshot shows the IBM QRadar Search interface. The top navigation bar includes Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin, Pulse, Use Case Manager, and Qualys VM. The main search area is titled "Search for Vulnerabilities by" and includes a dropdown menu with options "by IP address", "by QID or CVE", and "by CVE". The "by QID or CVE" option is selected. Below the dropdown, there is a "Start Date-Time" field set to "2021-04-15 17:25" and a "Search" button. The results section shows "Showing 0 to 0 of 0 entries" and a table with columns: QID, QID Title, CVE, Severity, Category, Detection Type, Patchable, and Total Hosts.

Click on the count of Total Hosts to view affected hosts for the QID or CVE.

The screenshot shows the IBM QRadar Search interface with search results for QID 38739. The search bar is set to "Search for Vulnerabilities by QID or CVE" with "QID" selected. The "Start Date-Time" is "2021-04-20 12:20" and the search term is "38739". The results section shows "Showing 1 to 1 of 1 entries" and a table with columns: QID, QID Title, CVE, Severity, Category, Detection Type, Patchable, and Total Hosts. The table contains one entry for QID 38739, titled "Deprecated SSH Cryptographic Settings", with a severity of 2, category "General remote services", detection type "Confirmed", and patchable status "No". The "Total Hosts" column shows a count of 363, which is highlighted in blue.

Vulns appear in table format.

The screenshot shows the IBM QRadar Search interface with search results for QID 91709. The search bar is set to "Search for Vulnerabilities by QID or CVE" with "QID" selected. The "Start Date-Time" is "2021-04-20 12:20" and the search term is "91709". The results section shows "Showing 1 to 1 of 1 entries" and a table with columns: QID, QID Title, CVE, Severity, Category, Detection Type, Patchable, and Total Hosts. The table contains one entry for QID 91709, titled "Deprecated SSH Cryptographic Settings", with a severity of 2, category "General remote services", detection type "Confirmed", and patchable status "No". The "Total Hosts" column shows a count of 363, which is highlighted in blue.

Raw Data

There may be times when you want to see the raw data. Follow these steps:

- 1) Go to **Log Activity** tab and go to **Advance Search** field.
- 2) In the **Advance Search** field, post the sample AQL below. (Tip - For more AQLs please check the Troubleshooting section in this guide.)

```
SELECT "Qualys Host Id", "Operating System", "Last Scan Datetime", "Tracking Method", "Qualys QID", "Qualys Severity", "Detection Type", "Status" from events where devicetype = '4001'
```
- 3) Select the date range for which you want to see the data.
- 4) Click **Search**.

Depending on the results, you may want to change the date-time range to widen/shorten your search span. You can also execute your own AQL queries to find more appropriate data. Please refer to fields in "Qualys LEEF" log source to know the Qualys fields.

Input Logs

While running, host detection input sends its log to QRadar over syslog. To see them, you can use the following AQL in **Log Activity > Advance Search**. Follow the same steps mentioned above with below AQL.

Host Detection

```
SELECT UTF8(payload) as utf8_payload from events where utf8_payload ILIKE '%Qualys:HostDetection%' ORDER BY utf8_payload ASC
```

Knowledgebase

```
SELECT UTF8(payload) as utf8_payload from events where utf8_payload ILIKE '%Qualys:Knowledgebase%' ORDER BY utf8_payload ASC
```

Uninstalling the app

- 1) Uninstall the app from **Admin > Extensions Management**.
- 2) Delete custom events for this app:
 - a. Go to **Admin > Custom Event Properties**.
 - b. Search and delete all entries associated with Qualys LEEF log source type. (How to do? Just search “qualys” and delete all the entries that displayed in search results).
- 3) Delete Log Source extension:
 - a. Go to **Admin > Log Source Extensions**.
 - b. Delete entries with extension “QualysLEEFCustom_ext”.
- 4) Delete Log Source:
 - a. Go to **Admin > Log Sources**.
 - b. Delete log source named “Qualys” or “QualysMultiline”.
- 5) Delete custom event mapping from Qualys LEEF:
 - a. Go to **Admin > DSM Editor**.
 - b. Search and open **Qualys LEEF** and go to **Event Mappings** tab.
 - c. Delete the entry with Event ID / Category “Qualys” or “QualysMultiline”.
 - d. Click **Save** button and close the tab.

While uninstalling the app in unfortunate cases, it should be done cleanly. Any leftover artifacts can potentially interfere with next installation attempt creating unstable state.

When app gets installed following components will get installed in QRadar, so to uninstall completely following components also need to be removed.

Troubleshooting

If you see no data

If the application is not bringing in your VM detection data, please go through the list below:

- 1) Check the data whether data indexing is happening properly with the [help of AOI](#).
- 2) Check the app configuration.
 - Check host detection ETL is enabled in Qualys VM App Settings.
 - Check cron jobs scheduled properly. For more information about cron jobs scheduling, refer <https://crontab.guru/>.
 - Make sure you have the correct API and access permissions.
 - Make sure your credentials are correct.
 - If you set start date-time, make sure it complies with Qualys required format.
 - If you added extra API parameters, make sure the JSON is valid and that all the extra parameters listed are valid.
- 3) Make sure you have done Deploy Full Configurations and your [TCP port in listening](#).
- 4) Make sure QRadar has Internet access and can reach your Qualys API server.
- 5) Check your host detection ETL is running:

Login to Qualys App container and run below commands:

```
ps aux | grep python
```

```
sh-4.4$ python /opt/app-root/app/etl_host_detection.py -d
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection etl_host_detection DEBUG: Debugging Enabled!!
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection etl_host_detection INFO: Will be sending LEEF data to [REDACTED] over socket.
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection etl_host_detection INFO: Qualys app version : [REDACTED]
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection etl_host_detection INFO: Console IP: [REDACTED]
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection utils INFO: /opt/app-root/app/host_detection.pid had pid 7155, but there is no process running with th
at pid. Creating new pid file.
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection utils INFO: START: vm_detections xml clean-up.
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection utils INFO: vm_detections does not have any old xml files to clean.
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection etl_host_detection INFO: Using Log Source Identifier and Listen PORT for the Log Source Id: 162
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection etl_host_detection INFO: Log Source Identifier: QualysMultiline
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection etl_host_detection INFO: Opened socket connection to DSM Port:12468
```

If your host detection job is not running

To run the host detection ETL, run the following command:

```
python /opt/app-root/app/etl_host_detection -d
```

Once you run above command, make sure you can see screen like –

```
sh-4.4$ python /opt/app-root/app/etl_host_detection.py -d
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection etl_host_detection DEBUG: Debugging Enabled!!
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection etl_host_detection INFO: Will be sending LEEF data to [REDACTED] over socket.
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection etl_host_detection INFO: Qualys app version : 1.0.0
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection etl_host_detection INFO: Console IP: [REDACTED]
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection utils INFO: /opt/app-root/app/host_detection.pid had pid 7155, but there is no process running with th
at pid. Creating new pid file.
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection utils INFO: START: vm_detections xml clean-up.
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection utils INFO: vm_detections does not have any old xml files to clean.
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection etl_host_detection INFO: Using Log Source Identifier and Listen PORT for the Log Source Id: 162
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection etl_host_detection INFO: Log Source Identifier: QualysMultiline
2021-04-28T16:04:45Z PID=7159 Qualys:HostDetection etl_host_detection INFO: Opened socket connection to DSM Port:12468
```

If you get “[Errno 111] Connection refused” error

Following error messages will be displayed for different cases:

Case 1

```
ERROR: Socket connection on port 12468 configured for 'QualysMultiline' log
source is refused, 'Deploy Full Configuration'. Error while connecting to
socket: [Errno 111] Connection refused
```

This error occurs when the Listen port is not LISTENING. You need to do the Deploy Full Configuration on QRadar box to resolve this issue.

Case 2

Making Request - `https://qualysapi.qualys.com/msp/about.php` with PARAM: {}
2020-01-16T10:19:58Z PID=421 Qualys:HostDetection client ERROR: Error during request to `https://qualysapi.qualys.com/msp/about.php`:<urlopen error [Errno 111] Connection refused>

This error occurs if the proxy settings are not configured on Qualys VM App Settings page. You need to configure proxy setup in Qualys VM App Settings.

If you see “HTTP Error 401: Unauthorized” error

This error occurs if you provide invalid credentials. To resolve this issue, check the API server URL and credentials.

If you see the ‘Number of host detections logged = 0’ in host detection

This can be due to following reasons:

- No scan was performed on the POD in the given period.
- No vulnerabilities are detected for the scan.
- If the API parameters are incorrect.

For Example, the 'vm_processed_after': '1999-01-01 00:00' is wrong in following API Request.

<https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/> with
PARAM: {'truncation_limit': 10, 'show_results': 0, 'show_igs': 1,
'output_format': 'XML', 'show_tags': 0, 'action': 'list',
'vm_processed_after': '1999-01-01 00:00'}

If you see “corresponding record not found in KB” message

The following message may appear in Host Detection logs:

A record for QID QID-Number found on Host %s, but its corresponding record not found in KB. May be KB is not updated.

This means you have some detections of given QID, but since your knowledgebase is not up to date, the app could not enrich the event data with QID details (like title, category, CVEs, patchable etc.). You have not enabled the Knowledgebase input in Qualys VM App Settings. Enable it and schedule it to run at least once a week.

If you see “Internal Server Error” while saving settings

1) This error occurs if Log Source ‘QualysMultiline’ is not configured. You need to complete [Log Source configurations](#).

2) This error occurs if ‘Deploy Full Configuration’ is not done before configuring Qualys App for QRadar.

3) Log source TCP port is not listening. To check, run the following command on QRadar box.

```
netstat -tulpn | grep LISTEN
```

To enable TCP listen port, you need to Deploy Full Configurations. Even after the Deploy Full Configuration, please contact IBM Support.

4) There might be some issue with cron service. Please follow the steps given below to identify the issue.

- Go to QRadar terminal and connect to Qualys app's container. Check if cron service is up and running, if it is not running, start it.

- If you do not find cron service, which means QRadar did not install cron while installing Qualys app. You will have to manually install the cron service and start it. You can confirm the issue from /opt/app-root/store/log/startup.log file as well. It should indicate that cron installation failed.

If dashboard widgets are not showing data for multi-tenant environment

When the dashboard widgets are not loading or showing no data even if the data fetch is completed –

- Check whether the "Event ID", "Event Category", and "Event Mapping" is created for the desired log source as suggested.
- If more multiple log sources are created and the "Event ID", "Event Category" and "Event Mapping" are created, make sure all of them are created in same specific order. Suppose if the user has 3 log sources - "QualysMultiline"(default), "QualysTokyo" and "QualysBerlin", then while creating the event id and event category, order should be similar in both.

If the order of creating "Event ID" and "Event Category" with respect to the desired log sources mismatches, then the order in "QualysLEEFCustom_ext" may get affected and hence events parsing may get failed. Also, the events may get addressed as "Unknown" and not sent to the selected log source.

DSM editor does not show Tags or DNS properties and you cannot add them

After installation of Qualys App, if DSM editor does not show TAGS and DNS properties, you can try adding them manually. If you are unable to add them manually, please follow these steps:

- 1) Check if "QualysMultiline" Log Source has correct Log Source Type. If it is not correct, delete the log source.
- 2) From DSM editor, delete the "Qualys LEEF" entry and create a new one. Add appropriate event mappings as mentioned in the Check Log Source Event Mapping section of this document.
- 3) Create a new Log Source using newly created "Qualys LEEF" as Log Source Type.
- 4) Complete Deploy Full Configurations step.
- 5) Go through the Check Custom Event Properties section of this document to make sure event mappings are all correct.

If you need to delete and recreate Log Source Type "Qualys LEEF"

Add the following custom event properties to newly created Log Source Type. For each property in the table below, Type should be "Regex".

| Property Name | Log Source Type | Log Source | Event Name | Expression |
|----------------|-----------------|------------|-----------------------------|-------------------------|
| App Version | Qualys LEEF | All | QualysMultiline Information | app_version=([^\t]+) |
| CVE | Qualys LEEF | All | QualysMultiline Information | cves=([^\t]+) |
| DNS | Qualys LEEF | All | QualysMultiline Information | dns=([^\t]+) |
| Detection Type | Qualys LEEF | All | QualysMultiline Information | detection_type=([^\t]+) |

| Property Name | Log Source Type | Log Source | Event Name | Expression |
|----------------------|-----------------|------------|-----------------------------|-------------------------------|
| First Found Datetime | Qualys LEEF | All | QualysMultiline Information | first_found_datetime=([^\t]+) |
| Host IP | Qualys LEEF | All | QualysMultiline Information | ip=([^\t]+) |
| Last Fixed Datetime | Qualys LEEF | All | QualysMultiline Information | last_fixed_datetime=([^\t]+) |
| Last Found Datetime | Qualys LEEF | All | QualysMultiline Information | last_found_datetime=([^\t]+) |
| Last Scan Datetime | Qualys LEEF | All | QualysMultiline Information | last_scan_datetime=([^\t]+) |
| App ID | Qualys LEEF | All | QualysMultiline Information | app_id=([^\t]+) |
| Last Test Datetime | Qualys LEEF | All | QualysMultiline Information | last_test_datetime=([^\t]+) |
| Last Update Datetime | Qualys LEEF | All | QualysMultiline Information | last_update_datetime=([^\t]+) |
| Network ID | Qualys LEEF | All | QualysMultiline Information | network_id=([^\t]+) |
| Operating System | Qualys LEEF | All | QualysMultiline Information | os=([^\t]+) |
| PCI Flag | Qualys LEEF | All | QualysMultiline Information | pci_flag=([^\t]+) |
| Patchable | Qualys LEEF | All | QualysMultiline Information | patchable=([^\t]+) |
| QID Category | Qualys LEEF | All | QualysMultiline Information | category=([^\t]+) |
| QID Title | Qualys LEEF | All | QualysMultiline Information | title=([^\t]+) |
| Qualys Host Id | Qualys LEEF | All | QualysMultiline Information | host_id=([^\t]+) |
| Qualys QID | Qualys LEEF | All | QualysMultiline Information | qid=([^\t]+) |
| Qualys Severity | Qualys LEEF | All | QualysMultiline Information | severity=([^\t]+) |
| Severity Level | Qualys LEEF | All | QualysMultiline Information | severity_level=([^\t]+) |
| Status | Qualys LEEF | All | QualysMultiline Information | status=([^\t]+) |
| Tags | Qualys LEEF | All | QualysMultiline Information | tags=([^\t]+) |
| Tracking Method | Qualys LEEF | All | QualysMultiline Information | tracking_method=([^\t]+) |

Helpful AQLs to check VM Detection Logs and Events

Use the following AQLs to check VM detection data and perform troubleshooting.

To check the logs

You can download app logs from Qualys App container. Go to **Advanced** tab and click **Download** button next to Download Application Logs. You can also see ETL logs in ETL folder from the downloaded zip file.

Get the PID (process id) of either etl_host_detection or etl_knowledgebase using the below command inside the container:

```
cat /opt/app-root/app/host_detection.pid  
cat /opt/app-root/app/etl_knowledgebase.pid
```

On the Log Activity search following queries under Advance Search. It will show you the log for the particular PID (*replace the <PID> with the appropriate process id*):

```
SELECT UTF8(payload) as utf8_payload from events where utf8_payload ILIKE  
'%PID=<PID>%' ORDER BY utf8_payload ASC
```

```
SELECT UTF8(payload) as utf8_payload from events where utf8_payload ILIKE  
'%Qualys:HostDetection%' ORDER BY utf8_payload ASC
```

```
SELECT UTF8(payload) as utf8_payload from events where utf8_payload ILIKE  
'%Qualys:Knowledgebase%' ORDER BY utf8_payload ASC
```

```
SELECT UTF8(payload) as utf8_payload from events where utf8_payload ILIKE  
'%detections =%' ORDER BY utf8_payload ASC
```

```
SELECT UTF8(payload) as utf8_payload from events where  
LOGSOURCENAME(logsourceid) = 'Qualys' OR LOGSOURCENAME(logsourceid) =  
'QualysMultiline'
```

To check the event data payload

```
SELECT LOGSOURCENAME(logsourceid) as logsourceids, UTF8(payload) as  
utf8_payload from events where LOGSOURCENAME(logsourceid) = 'Qualys' OR  
LOGSOURCENAME(logsourceid) = 'QualysMultiline'
```

```
SELECT "Qualys Host Id", "Operating System", "Last Scan Datetime", "Tracking  
Method", "Qualys QID", "Qualys Severity", "Detection Type", "Status" from  
events where LOGSOURCENAME(logsourceid) = 'Qualys' OR  
LOGSOURCENAME(logsourceid) = 'QualysMultiline'
```

Note: User must enter the custom log source name in the where clause, that they have configured for data ingestion.

Compatibility for Qualys VM app for QRadar v3.1.0+

When a user upgrades QRadar Version 7.3.3 FixPack 6 (Build 20201205215722) to 7.3.3 FixPack 10 (Build 20211125190208) followed by 7.5.0 GA with the Qualys App Version 2.0.1 installed (No Application State Change)

Considering the upgrade information from <https://www.ibm.com/support/pages/release-qradar-750-sfs-750-qradar-qrsiem-20211220195207>

In QRadar Version 7.3.3 FixPack 6 (Build 20201205215722) installed Qualys VM App Version 2.0.1 Configured the Qualys VM App Version 2.0.1 - Pulled the HD and KB data and verified the checkpoints, and saved the Logs.

Upgraded the QRadar Version to 7.3.3 FP10 without the application state changed and with both the HD and KB data inputs enabled.

Verified the Qualys VM Application Version 2.0.1 in QRadar Version 7.3.3 FixPack 10 (Build 20211125190208) - Verified the API calls making requests for HD and KB and also verified the application configurations.

Upgraded the QRadar Version to 7.5.0 UpdatePackage 1 (Build 20220215133427) without the application state changed and with both the HD and KB data inputs enabled.

Verified the Qualys VM Application Version 2.0.1 in QRadar Version 7.5.0 UpdatePackage 1 (Build 20220215133427) - Verified the API calls making requests for HD and KB and also verified the application configurations, GUI of Qualys App.

Note : Here in this scenario user would not be able to configure multitenant environment in the upgraded QRadar Versions (** applicable if the user has upgraded to or amongst the multitenancy supported QRadar versions) as with the upgrade of QRadar environment, base image version will also be upgraded which would not let the older version of Qualys VM App for QRadar create a new instance in the environment due libraries conflict.

Based on the <https://www.ibm.com/docs/en/qradar-common?topic=2-qradar-app-base-image-changelog> we have verified the Qualys VM App Version 2.0.1 (published) compatible with the below QRadar Versions i.e 7.4.3 FP1, 7.4.2 FP3, 7.3.3 FP

Qualys Support

If you tried the troubleshooting steps but still need help, please contact Qualys Support at <https://www.qualys.com/support/>

Provide the following information to Qualys Support:

- Qualys App version number
- QRadar version number, including the patch number
- Steps to reproduce the issue
- Note any manual changes done to Qualys app's code
- Note any manual changes done to Qualys app's container
- Please download the logs from Admin > Qualys VM App Settings page and attach them to your support case.