Qualys App for IBM QRadar

User Guide

Version 1.1.2

August 28, 2020

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

Table of Contents

Introduction to Qualys App for QRadar

Use the Qualys App for QRadar 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 App 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 App and see useful reports.

What's New in this release

- If the KB file is not updated then NA will be provided for the QIDs in the host information.
- Updated the configuration missing warning on Qualys App dashboard. If any data pull is not enabled then it will show data pull specific warning.
- Updated the reports and search data tables to show the row details. The outer row will show important information and the inner rows will show associated rows.
- Jquery updated to 3.5.1 version.
- Using ([^\t]+) in all the custom event properties regex.
- If the data feed is running for HD or KB it will update the setting page tabs accordingly with the process ID.
- Non-Admin users can access the Qualys app for Qradar.
- How to manage user roles?

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

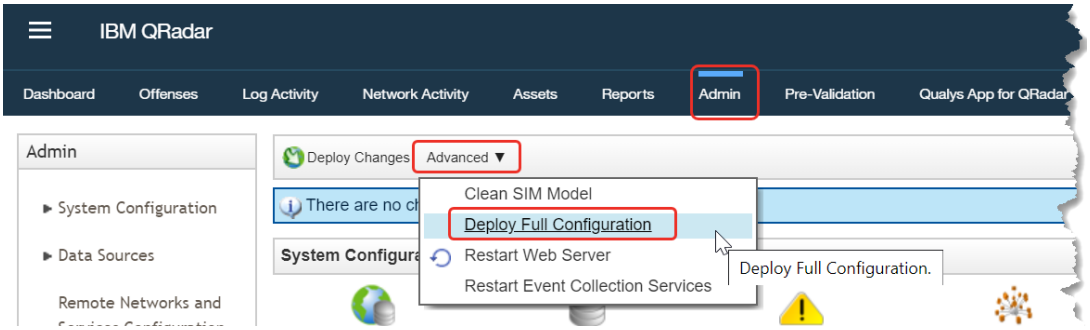
Install the App

Note

- Changes made for AQL are not compatible with QRadar 7.2.8 if your Qualys App version is 1.1.0 or later.
- Uninstall older version of Qualys App for QRadar before installing latest version(1.1.x.)

1) Log in to QRadar and go to the Admin tab.
2) Click on Extensions Management.
3) Click the Add button and upload the extensions .zip file. Don't have it? Click here to download Qualys App for QRadar

4) Confirm whether you want to replace/skip any existing contents with those coming from the extension, and click the Install button.
5) Once installation is completed, refresh your QRadar user interface.
6) You should see the tab "Qualys App for QRadar" in the top menu.
7) You can enable the Listen Port (default 12468) or any configuration in the Log source, full deployment is recommended. After installation of the Qualys App, choose "Deploy Full Configuration" to get all the required configurations properly enabled.



Application Dependencies

This application has the following dependencies. These are installed by QRadar's application management while spinning up the application container.

- vixie-cron
- python-crontab-2.1.1.tar.gz
- pycrypto-2.6.1.tar.gz

The vixie-cron is installed by installing the rpm of cronie-anacron-1.4.4-16.el6_8.2.x86_64 & cronie-1.4.4-16.el6_8.2.x86_64, whereas python-crontab-2.1.1 is installed locally using pip command.

Starting from version 1.1.0, all application dependencies are bundled with the application itself.

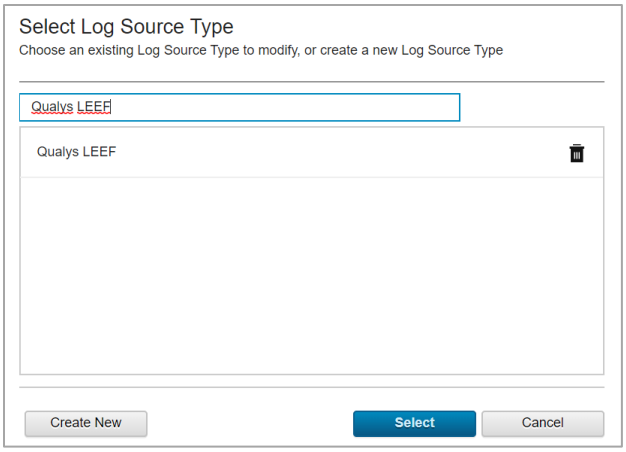
Configure the App

Complete Verification Steps

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.

Check Log Source Event Mapping

1) Go to Admin > DSM Editor.
2) In "Select Log Source Type", search for "Qualys LEEF" and click Select button.



3) From the Qualys LEEF screen, go to “Event Mappings” tab. The requirement is that there should be mapping for QualysMultiline and not for Qualys. If you see mapping for Qualys, delete it and if you don’t see mapping for QualysMuliline, create new (refer below steps).
4) Click on + 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.

Check Log Source

When you install app, it will create a new Log Source named “QualysMultiline”. Please check if it is created. If you see it is created, you should skip this section. Otherwise, please follow the steps below to create a new Log Source with the same name.

1) On your console UI, go to Admin > Data Sources > Log Sources and click the Add button.
2) Add the details shown below to the form to Create QualysMultiline Log Source. All fields marked with an asterisk (*) must match exactly.
3) 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".

Log Source Name	QualysMultiline	*
Log Source Description	QualysMultiline	
Log Source Type	Qualys LEEF	*
Protocol Configuration	TCP Multiline Syslog	*
Log Source Identifier	QualysMultiline	*
Listen Port	12468	
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	*

Check 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 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

- 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, please 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, please 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, please 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.

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 "Plug-ins" section and click on "Qualys App Settings". A pop-up window opens.

Qualys API

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

Proxy Configuration

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

You must enable this input in order 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’s advised that you keep the cron schedule in sync 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 “2007-07-01” or “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.

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 it runs (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 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 App for QRadar” tab in the top menu, you’ll 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
- Hosts Not Scanned in Last 30 Days
- Top 10 Vulnerabilities

By default, these reports are based on detection data in the last 20 days. To change this date-time range, please 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’ve 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.

Search

The Search by CVE or QID or IP will be searched on Host Detection data only.

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 LOGSOURCENAME(logsourceid) = 'Qualys' OR
LOGSOURCENAME(logsourceid) = 'QualysMultiline'
```

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 saved searches for this app (in case of Qualys App version 1.0.1 or lower):
   a. Go to Log Activity > Search > New Search.
   b. In Available Saved Searches, find saved searches starting with “Qualys” and delete it.

3) 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).

4) Delete Log Source extension:
   a. Go to Admin > Log Source Extensions.
   b. Delete entries with extension “QualysLEEFCustom_ext”.

5) Delete Log Source:
   a. Go to Admin > Log Sources.
   b. Delete log source named “Qualys” or “QualysMultiline”.

6) 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.

Troubleshooting

If you see no data

If the application isn't 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 AQL.
2) Check the app configuration.
   - Check host detection ETL is enabled in Qualys 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 application dependencies were installed correctly.
4) Make sure you have done Deploy Full Configurations and your TCP port in listening.
5) Make sure QRadar has Internet access and is able to reach your Qualys API server.
6) Check your host detection ETL is running:
   Login to Qualys App container and run below commands :
   `ps aux | grep python`

```
sh-4.1# ps aux | grep python
root       174  0.0  0.0 111408  1984 ?        S    May13   1:42 /usr/bin/python /usr/bin/supervisord -c /etc/supervisord.conf
root       176  0.0  0.2 841516 97044 ?        S    May13   4:24 python /run.py
root     27451  2.4  0.0 157956 30336 pts/13   S+   10:29   0:00 python /app/etl_host_detection.py -d
root     27467  0.0  0.0   6492   608 pts/14   S+   10:29   0:00 grep python
```

If your host detection ETL is not running

To run the host detection ETL, run the following command:
`python /app/etl_host_detection.py -d`
Once you run above command, make sure you can see screen like –

```
sh-4.1# python /app/etl_host_detection.py -d
2020-05-19T10:29:30Z PID=27451 Qualys:HostDetection etl_host_detection INFO: Will be sending LEEF data to 10.115.109.41 over so
cket.
2020-05-19T10:29:30Z PID=27451 Qualys:HostDetection utils INFO: START: vm_detections xml clean-up.
2020-05-19T10:29:30Z PID=27451 Qualys:HostDetection utils INFO: vm_detections does not have any old xml files to clean.
2020-05-19T10:29:30Z PID=27451 Qualys:HostDetection etl_host_detection INFO: Console IP: 10.115.109.41
2020-05-19T10:29:30Z PID=27451 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 App Settings page. You need to configure proxy setup in Qualys 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 of time.
- 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.). Maybe you have not enabled the Knowledgebase input in Qualys 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, that 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 /store/log/startup.log file as well. It should indicate that cron installation failed.

DSM editor doesn't show Tags or DNS properties and you can't 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	QualysMultiline	QualysMultiline Information	app_version=([^\t]+)
CVE	Qualys LEEF	QualysMultiline	QualysMultiline Information	cves=([^\t]+)
DNS	Qualys LEEF	QualysMultiline	QualysMultiline Information	dns=([^\t]+)
Detection Type	Qualys LEEF	QualysMultiline	QualysMultiline Information	detection_type=([^\t]+)
First Found Datetime	Qualys LEEF	QualysMultiline	QualysMultiline Information	first_found_datetime=([^\t]+)
Host IP	Qualys LEEF	QualysMultiline	QualysMultiline Information	ip=([^\t]+)
Last Fixed Datetime	Qualys LEEF	QualysMultiline	QualysMultiline Information	last_fixed_datetime=([^\t]+)
Last Found Datetime	Qualys LEEF	QualysMultiline	QualysMultiline Information	last_found_datetime=([^\t]+)
Last Scan Datetime	Qualys LEEF	QualysMultiline	QualysMultiline Information	last_scan_datetime=([^\t]+)
Last Test Datetime	Qualys LEEF	QualysMultiline	QualysMultiline Information	last_test_datetime=([^\t]+)
Last Update Datetime	Qualys LEEF	QualysMultiline	QualysMultiline Information	last_update_datetime=([^\t]+)
Network ID	Qualys LEEF	QualysMultiline	QualysMultiline Information	network_id=([^\t]+)
Operating System	Qualys LEEF	QualysMultiline	QualysMultiline Information	os=([^\t]+)
PCI Flag	Qualys LEEF	QualysMultiline	QualysMultiline Information	pci_flag=([^\t]+)
Patchable	Qualys LEEF	QualysMultiline	QualysMultiline Information	patchable=([^\t]+)

QID Category	Qualys LEEF	QualysMultiline	QualysMultiline Information	category=([^\t]+)
QID Title	Qualys LEEF	QualysMultiline	QualysMultiline Information	title=([^\t]+)
Qualys Host Id	Qualys LEEF	QualysMultiline	QualysMultiline Information	host_id=([^\t]+)
Qualys QID	Qualys LEEF	QualysMultiline	QualysMultiline Information	qid=([^\t]+)
Qualys Severity	Qualys LEEF	QualysMultiline	QualysMultiline Information	severity=([^\t]+)
Severity Level	Qualys LEEF	QualysMultiline	QualysMultiline Information	severity_level=([^\t]+)
Status	Qualys LEEF	QualysMultiline	QualysMultiline Information	status=([^\t]+)
Tags	Qualys LEEF	QualysMultiline	QualysMultiline Information	tags=([^\t]+)
Tracking Method	Qualys LEEF	QualysMultiline	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

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

```
cat app/host_detection.pid
```

```
cat 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'
```

Previous Releases

Following were the updates from previous releases:

1.1.1

- We have fixed an issue where 'Internal Server Error - 500' message was displayed on Settings page. This was occurring due to the App was not able to fetch DSM Port which is need for TCP Multiline Socket Connection.
- We have fixed and issue where '[Errno 111] Connection refused' message occurs if the DSM port is not listening and when the user tries to fetch Host Detection or Knowledgebase Data. For more details, refer Troubleshooting section.
- From Qualys App for QRadar version 1.1.1, API Password and Proxy Server Password is encrypted.
- From Qualys App for QRadar version 1.1.1, the proxy server password is masked while configuring proxy.
- While using the HTTPS in proxy URL, app uses ca-bundle.crt file. By default, IBM QRadar provides this file. If the user wants to use their CA certificate file, they should follow the steps given in the link: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/t_qradar_adm_updates_proxy.html

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