

# NetWitness<sup>®</sup> Platform

## Qualys Vulnerability Management Event Source Log Configuration Guide

# Qualys Vulnerability Management

Last Modified: Tuesday, October 8, 2024

## Event Source Product Information:

**Vendor:** [Qualys](#)

**Event Source:** Vulnerability Management Host Detections

**Versions:** API v2.0

## RSA Product Information:

**Supported On:** NetWitness Platform 12.2 and later

**Event Source Log Parser:** cef

**Note:** The CEF parser parses this event source as `device.type=qualysvmhosts`.

**Collection Method:** Plugin Framework

**Event Source Class.Subclass:** Host.Cloud

## Contact Information

NetWitness Community at <https://community.netwitness.com> contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

## Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

## License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates and are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

## Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

## Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

## Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at <https://www.netwitness.com/standard-form-agreements/>.

© 2024 RSA Security LLC or its affiliates. All Rights Reserved.

September 2024

# Contents

---

- Set Up Qualys Vulnerability Management ..... 6**
  - About Qualys VM ..... 6
  - Determine Your Qualys Platform ..... 6
- Set Up the Qualys VM Event Source in NetWitness Platform ..... 8**
  - Deploy Qualys Files from Live ..... 8
  - Configure the Qualys VM Event Source in NetWitness Platform ..... 8
- Qualys VM Collection Configuration Parameters ..... 11**
  - Basic Parameters ..... 11
  - Advanced Parameters ..... 12
- Getting Help with NetWitness Platform ..... 14**
  - Self-Help Resources ..... 14
  - Contact NetWitness Support ..... 14
  - Feedback on Product Documentation ..... 15

To configure Qualys Vulnerability Management Host Detections, you must complete these tasks:

- I. Set Up the Qualys Vulnerability Management event source
- II. Set Up Qualys Vulnerability Management Event Source in RSA NetWitness

## Set Up Qualys Vulnerability Management

---

### About Qualys VM

Qualys VM is a cloud-based service that gives you global visibility into where your IT systems might be vulnerable to the latest Internet threats and how to protect them. It helps you to continuously identify threats and monitor unexpected changes in your network before they turn into breaches.

The plugin provided by NetWitness helps download a list of hosts and their latest vulnerability data, based on the host-based scan data available in the user's account. This data provides the latest complete vulnerability status for the downloaded hosts (NEW, ACTIVE, FIXED, REOPENED), as well as history information.

Based on permissions, the following groups are defined:

- **Managers** can view all VM scanned hosts in a subscription
- **Unit Managers** can view VM scanned hosts in their own business unit
- **Scanners** and **Readers** can view VM scanned hosts in their own user account
- **Auditors** have no permission to view VM scanned hosts

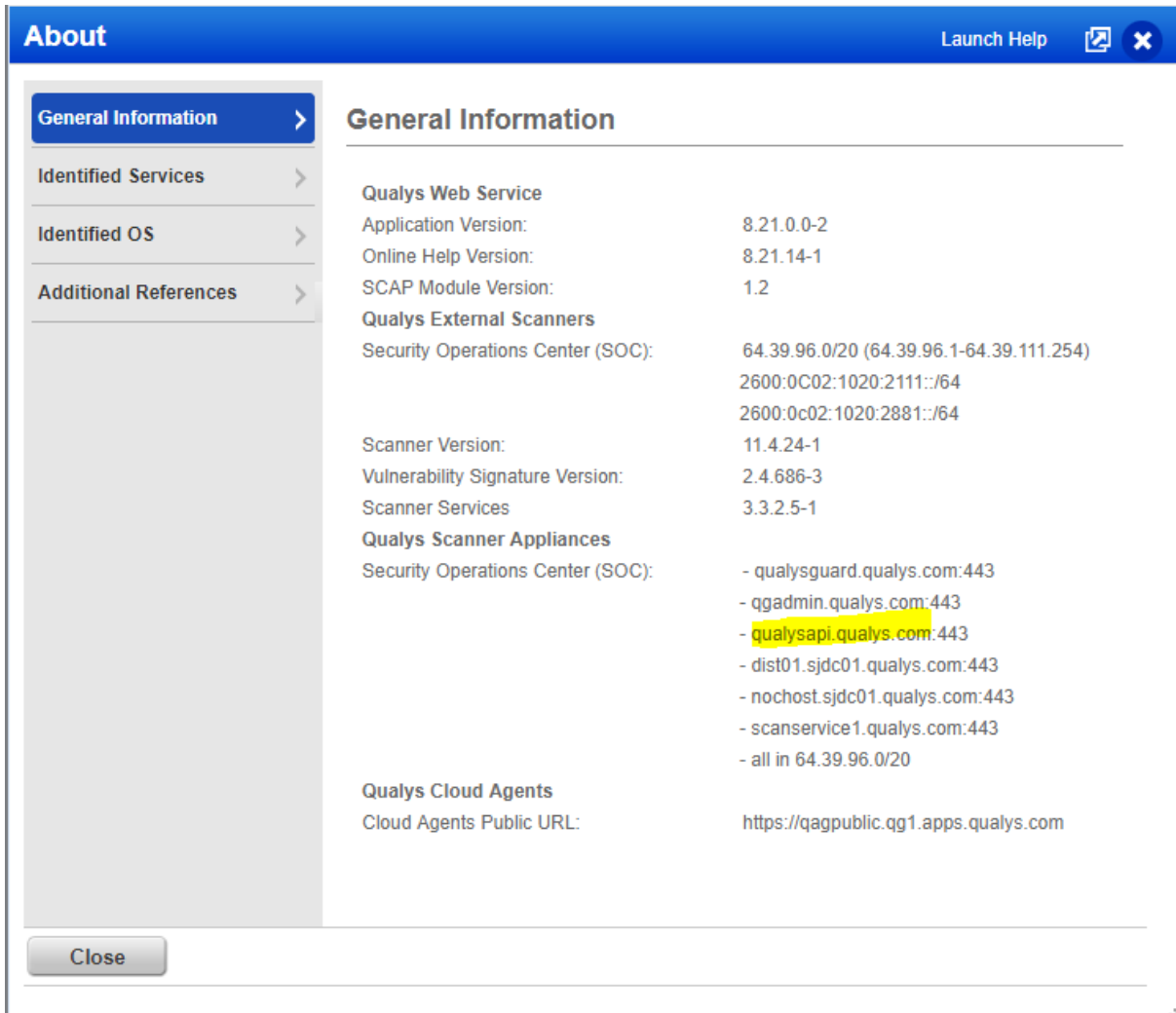
For details about scheduling and managing Host Scans please refer to the Qualys Documentation Page here: <https://www.qualys.com/documentation/>

### Determine Your Qualys Platform

To initialize an instance of the Qualys VM Host Detections plugin, you need to provide Username, Password and API Server Path. Qualys maintains multiple Qualys platforms: the API Server Path you need to use depends on the type of platform on which your account is located.

**To determine this information, do the following:**

1. Log on to your Qualys account and go to **Help > About**.
2. Look under the **Security Operations Center (SOC)** section of the screen:



In the above example, **qualysapi.qualys.com:443** is the API Server Path URL. You will need this information when you configure the event source in NetWitness Platform.

## Set Up the Qualys VM Event Source in NetWitness Platform

In `[[[Undefined variable SAVariables.ProductSuiteName]]]`, perform the following tasks:

- I. Deploy the CEF parser and supporting files from Live
- II. Configure the Qualys Vulnerability Management Event Source in NetWitness Platform.

### Deploy Qualys Files from Live

The Qualys VM Host Detections plugin requires resources available in Live in order to collect logs.

**To deploy the required content from Live:**

1. In the NetWitness Platform menu, select **CONFIGURE**.  
The **Live Content** tab is displayed.
2. Browse Live Content for the **Common Event Format (cef)** parser, using **Log Device** as the **Resource Type**.
3. Select the **cef** parser from the list and click **Deploy** to deploy it to the appropriate Log Decoders, using the Deployment Wizard.
4. You also need to deploy the **qualys\_vm\_hosts** package. Browse Live for Qualys content, typing "qualys" into the Keywords text box, then click **Search**.
5. Select the **qualys\_vm\_hosts** package and click **Deploy** to deploy it to the appropriate Log Collectors.

**Note:** If a remote VLC is being used for collection, then you need to deploy the plugin to the remote VLC as well as the Decoder.

6. Restart the **nwlogcollector** service.

For more details, see the [Add or Update Supported Event Source Log Parsers](#) topic, or the *Live Services Management Guide*.

## Configure the Qualys VM Event Source in NetWitness Platform

**To configure the Qualys VM Host Detections Event Source:**

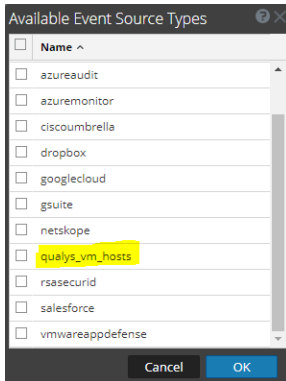
1. In the NetWitness Platform menu, select **ADMIN > Services**.
2. In the Services grid, select a Log Collector service, and from the Actions menu, choose **View > Config**.

3. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.

The Event Categories panel displays the plugin event sources that are configured, if any.

4. In the Event Categories panel toolbar, click **+**.

The Available Event Source Types dialog is displayed.

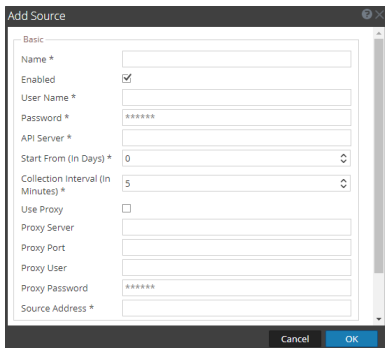


5. Select **qualys\_vm\_hosts** from the list, and click **OK**.

The newly added event source type is displayed in the Event Categories panel.

6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.

The Add Source dialog is displayed.



7. Define parameter values, as described in [Qualys VM Collection Configuration Parameters](#).
8. Click **Test Connection**.

The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

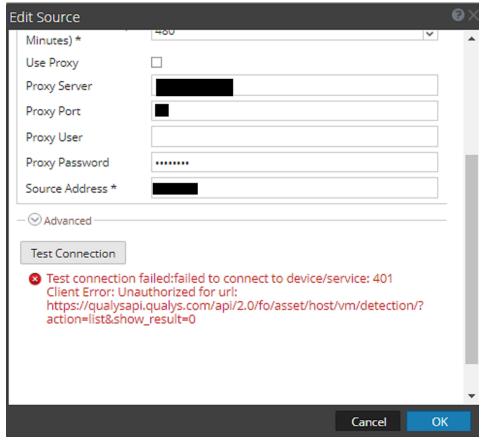
**Note:** The Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and NetWitness Platform displays an error message.

9. Depending on the result:

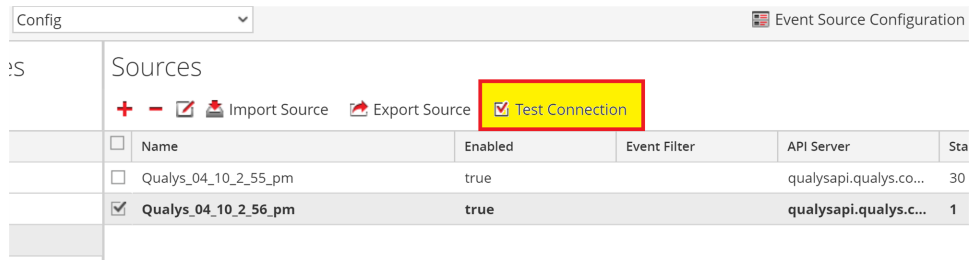
- If the test is successful, click **OK**.

The new event source is displayed in the Sources panel.

- There is a known issue that could cause the test to fail. The test connection might show an error in the edit source window:



If you see this error, click **Cancel** to close the dialog box, then click **Test Connection** at the top of the Sources pane:



If you entered the correct values in step 6, the test should now pass.

## Qualys VM Collection Configuration Parameters

The following table describes the configuration parameters for the Qualys VM integration with [[Undefined variable SAVariables.ProductSuiteName]]. Fields marked with an asterisk (\*) are required.

**Note:** Items that are followed by an asterisk (\*) required.

### Basic Parameters

| Name                              | Description  |
|-----------------------------------|--|
| Name*                             | Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen.   |
| Enabled                           | Select the box to enable the event source configuration to start collection. The box is selected by default.   |
| User Name*                        | Enter the credentials for your Qualys user account.  |
| Password*                         |  |
| API Server*                       | Enter the Qualys API Server URL: this information was displayed earlier, in the <b>Help &gt; About</b> screen for your Qualys account.   |
| Start From (In Days)*             | Enter the number of previous days from which to start collecting logs. This parameter defaults to the current date (0).  |
| Collection Interval (In Minutes)* | This is the interval, in minutes, between two consecutive polls for data from the Qualys event source.<br><br>For example, if you are generating a report every 24 hours, then RSA recommends that you set this value to <b>1440</b> (24 hours * 60 minutes per hour) to keep duplication to a minimum.  |
| Use Proxy                         | Check to enable proxy.   |
| Proxy Server                      | If you are using a proxy, enter the proxy server address.  |
| Proxy Port                        | Enter the proxy port.  |
| Proxy User                        | Username for the proxy (leave empty if using anonymous proxy).   |
| Proxy Password                    | Password for the proxy (leave empty if using anonymous proxy).   |
| Source Address *                  | IP address that is to be provided to the Qualys VM plugin instance: logs from this event source will be collected with this device IP.<br><br><b>Note:</b> This is an arbitrary IP address chosen by the user. This value has no bearing on the collection of logs: its value is captured by the device.ip meta key, and can help you to query or group events collected by a particular instance of the plugin. |

| Name            | Description   |
|-----------------|---|
| Test Connection | Checks the configuration parameters specified in this dialog to make sure they are correct. |

**Note:** Please avoid using special characters in the **Proxy User** and **Proxy Password** sections.

## Advanced Parameters

| Parameter          | Description  |
|--------------------|--|
| Polling Interval   | Interval (amount of time in seconds) between each poll. The default value is <b>180</b> .<br>For example, if you specify <b>180</b> , the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.   |
| Max Duration Poll  | Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit. The default is set to 600.  |
| Max Events Poll    | The maximum number of events per polling cycle (how many events collected per polling cycle).  |
| Max Idle Time Poll | Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.   |
| Command Args       | Optional arguments to be added to the script invocation.   |
| Debug              | <p><b>Caution:</b> Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector.</p> <p>Enables or disables debug logging for the event source. Valid values are:</p> <ul style="list-style-type: none"><li>• <b>Off</b> = (default) disabled</li><li>• <b>On</b> = enabled</li><li>• <b>Verbose</b> = enabled in verbose mode - adds thread information and source context information to the messages.</li></ul> <p>This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.</p> |
| SSL Enabled        | The check box is selected by default.<br>Uncheck this box to disable SSL certificate verification.   |

| Parameter   | Description  |
|-------------|--|
| HTTPS Proxy | If Proxy server is configured, enable or disable based on the proxy traffic allowed. By default HTTPS Protocol is enabled for the Proxy connection. If the only HTTP traffic allowed via proxy, then uncheck this parameter. |

## Getting Help with NetWitness Platform

---

### Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here:  
<https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation>.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: <https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions>.
- See the NetWitness Knowledge Base: <https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base>.
- See the documentation for Logstash JDBC input plugin here:  
<https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html>.
- See Troubleshooting section in the guides.
- See also [NetWitness® Platform Blog Posts](#).
- If you need further assistance, [Contact NetWitness Support](#).

### Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

|  |   |
|--|---|
| NetWitness Community Portal                                | <a href="https://community.netwitness.com">https://community.netwitness.com</a><br>In the main menu, click <b>Support</b> > <b>Case Portal</b> > <b>View My Cases</b> .                     |
| International Contacts (How to Contact NetWitness Support) | <a href="https://community.netwitness.com/t5/support/ct-p/support">https://community.netwitness.com/t5/support/ct-p/support</a>   |
| Community  | <a href="https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions">https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions</a> |

## Feedback on Product Documentation

You can send an email to [feedbacknwdocs@netwitness.com](mailto:feedbacknwdocs@netwitness.com) to provide feedback on NetWitness Platform documentation.