NetWitness® Platform

Radware DDoS Event Source Log Configuration Guide

NETWITNESS
Platform

Radware DDoS

Event Source Product Information:

Vendor: radware

Event Source: Radware ddos

Versions: API v1.0

NetWitness Product Information:

Supported On: NetWitness Platform 12.2 or later

Note: Radware DDoS is supported from NetWitness Platform 12.2 or later. However, NetWitness recommends you to update NetWitness Platform to the latest version.

Event Source Log Parser: radware_ddos

Note: The radware_ddos parser parses this event source as **device.type=radware_ddos**.

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 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/.

August 2024

Contents

Introduction to Radware DDoS

Radware DDoS is a hybrid DDoS protection solution integrating always-on DDoS prevention services such as detection and mitigation (on-premise or in the cloud) with cloud-based volumetric DDoS attack prevention, scrubbing and 24x7 cyber attack and DDoS security. Netwitness integrates the security and operational alerts provided by the radware API and allows you to analyze the data.

The following sections describe the configuration of the Radware DDoS as an event source in Netwitness Platform using the Radware API.

- Configure the Radware Protect Event Source
- Set Up the Radware DDoS Protect Event Source in NetWitness Platform
- Radware DDoS Collection Configuration Parameters.

Configure the Radware Protect Event Source

Netwitness supports the security and operational alerts collection from Radware DDoS API. In order to collect alerts from the DDoS API, we will need to authenticate to the API using a API key. For more information on Radware DDoS, see SSOLogin.

Set Up the Radware DDoS Protect Event Source in NetWitness Platform

In NetWitness Platform, perform the following tasks:

i. Deploy the Radware DDoS Files from NetWitness Live

ii. Configure the Event Source

Deploy the Radware DDoS Files from NetWitness Live

Radware DDoS event source require resources available in NetWitness Live to collect logs. Radware DDoS uses the radware_ddos json parser to parse the logs.

To deploy the Radware DDoS Protect content from Live:

1. In the NetWitness Platform menu, select  **(Configure)** .
2. Browse Live for the **radware_ddos** parser using NetWitness Log Device as the Resource Type. Select **radware_ddos** parser from the list.
3. Click **Deploy** to deploy the Radware DDoS parser to the appropriate Log Decoders using the Deployment Wizard.
4. You should also deploy the Radware DDoS log collection package. Browse Live for Radware DDoS log collector content by typing

   radware_ddos_alerts in the search text box and click **Search**.
5. Select the item returned from the search and click **Deploy** to deploy to the appropriate Log Collectors.

   Note: On a hybrid installation, you should deploy the package on both the Virtual Log Collector (VLC) and the Log Collector (LC). If you deploy the package on the LC, you should restart the log decoder and log collector services, otherwise logs will not be collected.
6. Restart the `nwlogcollector` service.

For more details, see the Add or Update Supported Event Source Log Parsers topic on NetWitness Community site.

Configure the Event Source

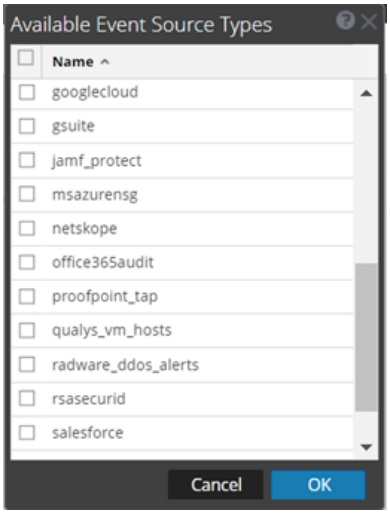
This section contains details on setting up the event source in NetWitness Platform. In addition to the procedure, the Radware DDoS Collection Configuration Parameters are described.

To configure the Radware DDoS 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** > **Event Sources**.
3. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.

   The **Event Categories** panel displays the File event sources that are configured, if any.
4. In the **Event Categories** panel toolbar, click +.

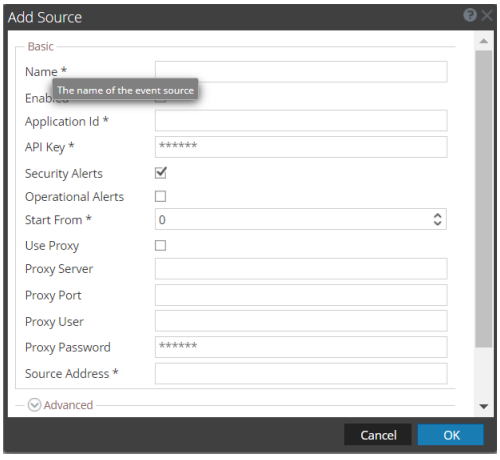
   The **Available Event Source Types** dialog is displayed.



5. Select **radware_ddos_alerts** 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 Radware DDoS 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. If the test is successful, click **OK**.

   The new event source is displayed in the Sources panel.

Radware DDoS Collection Configuration Parameters

The following table describes the configuration parameter for the Radware DDoS integration with NetWitness Platform. Fields marked with an asterisk (*) are required.

Note: When run from behind an SSL proxy, if certificate verification needs to be disabled, uncheck the **SSL Enable** checkbox in the **Advanced** section.

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.
Application ID *	The Cloud DDoS Portal account ID, which can be found on the Account Settings page.
API key	API key to authenticate with radware api.
Tick any one of the checkboxes to proceed with collection*	• Security: Select the checkbox if you want to collect security alert only. • Operational: Select the checkbox if you want to collect operational alert only.
Start From*	Choose the day from which you want to start collecting logs. This parameter defaults to the current day, i.e, 0 and the log collection will be real-time. The Maximum value is 7, when set, the last 7 days logs will be collected. **IMPORTANT:** Specify the number of days prior to the current date, from which log collection should start. Default value is 0 (current day), and the range is 0–7. For example, current date is 21 Apr 2023 and you want to collect logs from 19 Apr 2023, set the value to 2.
Use Proxy	Uncheck to disable proxy configuration. This is enabled by default.
Proxy Server	If you are using a proxy in your environment, 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).

Name	Description
Source Address	A custom value chosen to represent the hostname for the Radware DDoS Event Source in the customer environment and the value should be in IPV4 format. The value of this parameter is captured by the **device.ip** meta key.

Advanced Parameters

Click **Advanced** to view and edit the advanced parameters.

Name	Description
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is 180. For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, the collector waits for that cycle to finish. 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 Caution	**Caution:** 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. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages.

	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.
SSL Enable	Uncheck to disable certificate verification. This is enabled by default.

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

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.