NetWitness® Platform

NetSkope Event Source Log Configuration Guide

NETWITNESS
Platform

Netskope Cloud Security Platform

Last Modified: Tuesday, October 15, 2024

Event Source Product Information:

Vendor: Netskope Security Cloud

Event Source: Netskope Cloud Security Platform

Versions: API v2

NetWitness Product Information:

Supported On:

- NetWitness Platform 12.2 and later

Event Source Log Parser: netskope

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/.

September 2024

Contents

To configure Netskope Cloud Security Platform, you must complete these tasks:

I. Configure the Netskope Cloud Security Platform event source

II. Set Up the Netskope Event Source in NetWitness

About Netskope Cloud Security Platform

The Netskope Security Cloud helps organizations take advantage of the cloud and web without sacrificing security. Their Cloud XD technology targets and controls activities across thousands of cloud services and millions of websites. Netskope provides 360-degree data protection that guards data everywhere and advanced threat protection that stops elusive attacks.

Netskope provides different kinds of alerts and different kinds of events like page events, application events, audit events and infrastructure events. Additionally, Netskope provides the API support to fetch all these kinds of alerts and events.

Configure the Netskope Cloud Security Platform event source

To configure the Netskope Cloud Security Platform, you must generate a v2 API Key. We are using the /dataexport endpoint to collect all types of logs. Therefore, please select the /dataexport endpoints for all the required permissions. To create a new token for v2 api :

https://docs.netskope.com/en/rest-api-v2-overview-312207/

Note: We support Alerts, incidents, application, audit, infrastructure, page, connection, endpoint, network logs, therefore while generating the v2 api token please select the READ permission for all the above log types.

Set Up the Netskope Event Source in NetWitness Platform

In NetWitness Platform , perform the following tasks:

I. Deploy the plugin and parser from Live

II. Configure the event source.

Deploy the Plugin And Parser from Live

Netskope Cloud Security Platform requires resources available in Live in order to collect logs.

To deploy the plugin and parser from Live:

1. In the NetWitness Platform menu, select **CONFIGURE**.

   The **Live Content** tab is displayed.

2. Browse Live Content for the **netskope** json parser, using **Log Device** as the **Resource Type**.

3. Select the **netskope** json 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 netskopev2 package. Browse Live for Netskope content, typing "netskopev2" into the Keywords text box, then click **Search**.

5. Select the item returned from the search.

6. Click **Deploy** to deploy the netskopev2 Log Collection package to the appropriate Log Collectors, using the Deployment Wizard.

7. 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 Event Source

This section contains details on setting up the event source in NetWitness Platform .

To configure the netskopev2 Event Source:

1. In the NetWitness Platform menu, select **ADMIN > Services**.

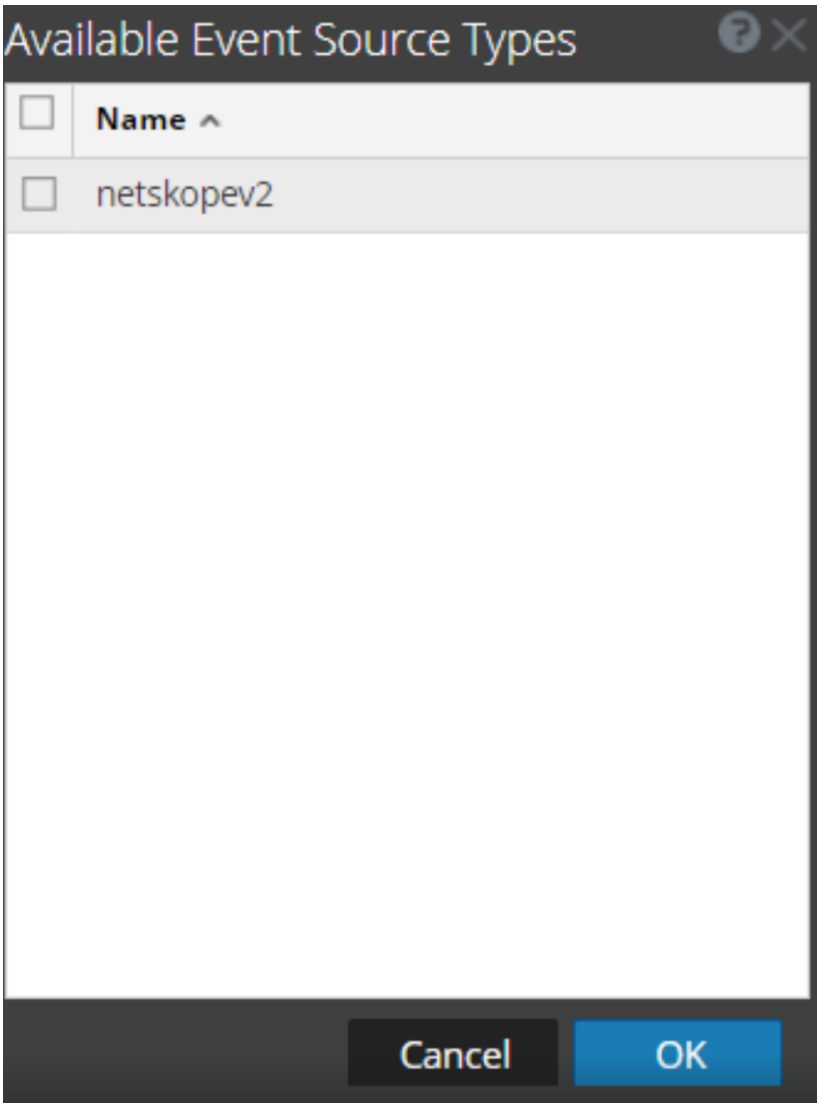
2. In the Services grid, select a Log Collector service, and from the Actions menu, choose **View** > **Config**.

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

   The Event Categories panel displays the 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 **netskopev2** 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. You need to create three instances: One for alerts, one for incidents and one for events

   a. To get alerts , you need to tick the checkbox for alerts.

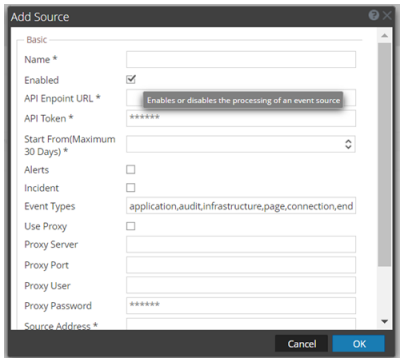
   b. To get incidents , you need to tick the check box for events

c. To collect events , you need to enter the events you want to collect in a comma separated list . Supported events =

[application,audit,infrastructure,page,connection,endpoint,network]

Note: For every instance of the plugin only one of the logs(alerts, incidents,events) can be selected.

d. For example to collect infrastructure and audit logs, the customer should choose infrastructure,audit as the input. It should be a comma separated list without spaces.



Netskope Collection Configuration Parameters

The following tables describe the configuration parameters for the Netskope Cloud Security Platform integration with NetWitness Platform . Fields marked with an asterisk (*) are 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.
API Endpoint URL *	The Endpoint URL for Netskope Cloud Security Platform Admin Logging REST API. For example: `https://XXX.goskope.com/`
Access Token *	Access token obtained from admin interface.
Start From (In Days) *	Specifies the number of days prior to the current time, from which log collection should start. Maximum 30 days.
Alerts	Select to collect the alerts.
Incidents	Select to collect incidents.
Event Types	Comma separated list of events(no spaces). [application,audit,infrastructure,page,connection,endpoint,network]
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	A custom value chosen to represent the IP address for the Netskope Cloud Security Platform Event Source in the customer environment. The value of this parameter is captured by the **device.ip** meta key.
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 **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, 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	**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 Enabled	The check box is selected by default. Uncheck this box to disable SSL certificate verification.

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.