NetWitness® Platform XDR

IPFIX Event Source Log Configuration Guide

NETWITNESS
Platform XDR

IPFIX

Event Source Product Information:

Vendor: IANA

Event Source: IPFIX

Versions: NetFlow v10

NetWitness Product Information:

Supported On: NetWitness Platform XDR 12.2 and later

Event Source Log Parser: ipfix

Collection Method: Logstash

Event Source Class.Subclass: Switch

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

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

November, 2022

Contents

Configure the IPFIX Event Sources (Exporters) **6**

Deploy Logstash IPFIX Pipeline Files from Live **7**

Deploy IPFIX Parser from NetWitness Live **8**

Setup the IPFIX Event Source in the NetWitness Platform XDR **9**

IPFIX Collection Configuration Parameters 11

Basic Parameters 11

Advanced Parameters 12

Getting Help with NetWitness Platform XDR **14**

Self-Help Resources 14

Contact NetWitness Support 14

Feedback on Product Documentation 15

To configure the IPFIX event source, you must complete these tasks:

I. Configure the IPFIX Event Sources (Exporters)

II. Deploy Logstash IPFIX Pipeline Files from Live

III. Deploy Logstash IPFIX Pipeline Files from Live

IV. Setup the IPFIX Event Source in the NetWitness Platform XDR.

Configure the IPFIX Event Sources (Exporters)

Managed Logstash acts as a Collector and uses Netflow codec to decode the IPFIX messages it receives in the designated port. Netflow codec supports a list of Exporters. Please refer to the Netflow Codec Plugin documentation for the list of IPFIX-supported exporters. Basic configuration steps include:

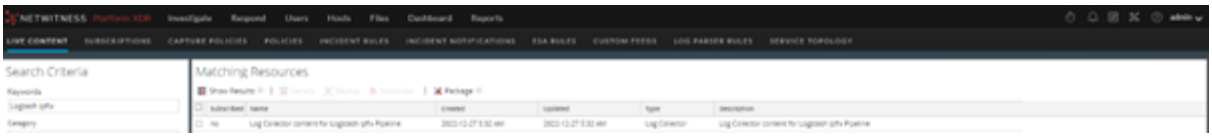
- Enabling IPFIX.
- Choose IPFIX Template.
- Host address and port of IPFIX Collector / Collectors.

Deploy Logstash IPFIX Pipeline Files from Live

Logstash IPFIX Pipeline files require resources available in Live in order to collect logs.

To deploy logstash ipfix pipeline files from Live:

1. In the NetWitness Platform XDR menu, select **Configure** > **Live Content**. Browse Live for IPFIX parser by typing **Logtash ipfix** into the Keywords text box and click **Search**.
2. Select the item returned from the Search.
3. Click **Deploy** to deploy the Logstash IPFIX Pipeline files to the appropriate Log Collector using the Deployment Wizard.



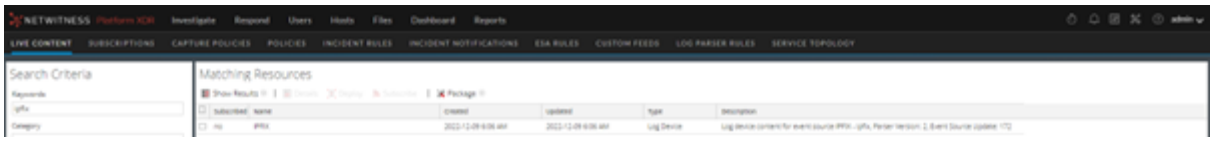
Note: If the number of messages in the queue is very high, create multiple instances of the Logstash IPFIX Pipeline to ingest the messages at a higher rate.

Deploy IPFIX Parser from NetWitness Live

IPFIX parser requires resources available in Live in order to collect logs.

To deploy ipfix pipeline files from Live:

1. In the NetWitness Platform XDR menu, select **Configure** > **Live Content**. Browse Live for IPFIX parser by typing **ipfix** into the Keywords text box and click **Search**.
2. Select the item returned from the Search.
3. Click **Deploy** to deploy the IPFIX parser to the appropriate Log Decoder using the Deployment Wizard.

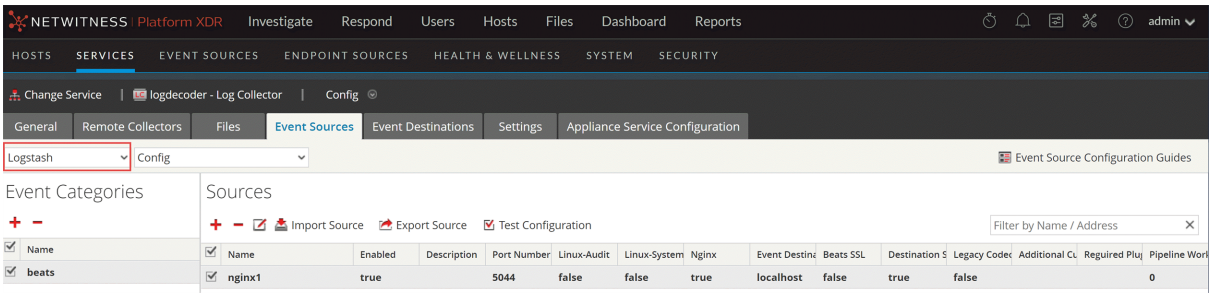


For more details, see the Add or Update Supported Event Source Log Parsers topic, or the Live Resource Guide on NetWitness Link.

Setup the IPFIX Event Source in the NetWitness Platform XDR

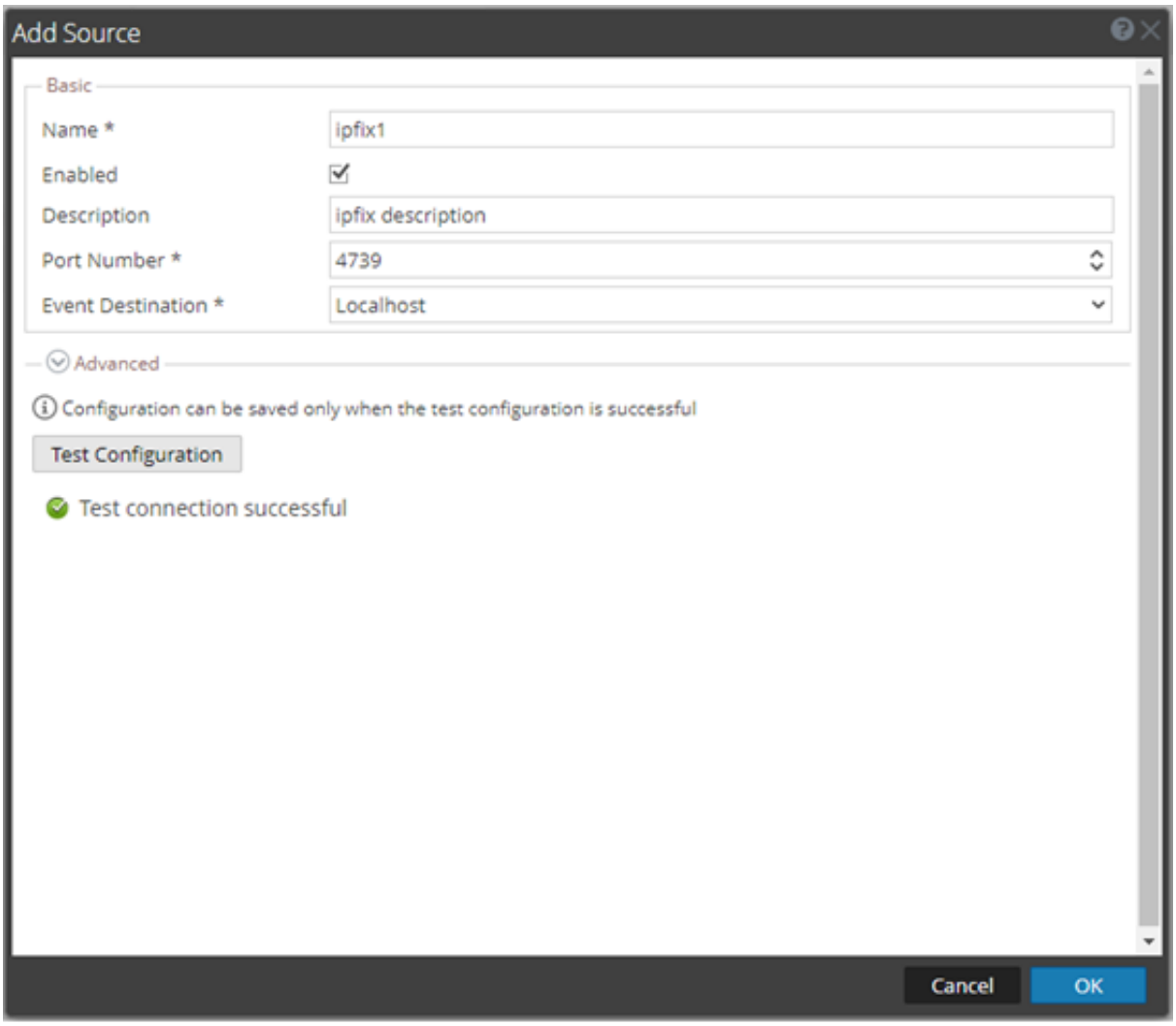
To configure the IPFIX Event Source:

1. In the NetWitness Platform XDR 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** view, select **Logstash** / **Config** from the drop-down menu.



4. In the **Event Categories** panel toolbar, click  .
5. Select **ipfix** from the list and in the **Sources** panel, click  .

   The **Add Source** dialog is displayed.

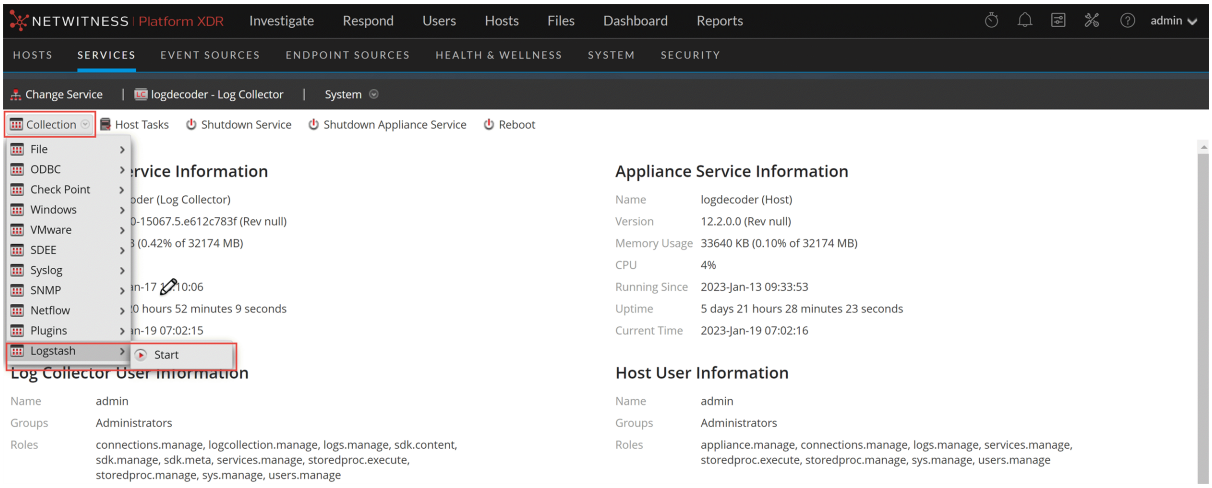


6. Define parameter values, as described in IPFIX Collection Configuration Parameters.
7. Click **Test Configuration**.

   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.
8. If the test is successful, click **OK**. The new event source is displayed in the **Sources** panel.
9. Save the configuration. From the **Actions** menu choose **System**.

10. In the **Collection** drop-down menu, select **Logstash** > **Start**, to start the log collection.



IPFIX Collection Configuration Parameters

The tables below list the configuration parameters required for integrating IPFIX with NetWitness Platform XDR.

Note: Fields that are followed by an asterisk (*) are mandatory.

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 checkbox to enable the event source configuration to start collection. The checkbox is selected by default.
Description	Enter the description for the Logstash pipeline.
Port Number *	Enter the port number (for example, 4739) that you configured for your event sources
IPFIX	Select the checkbox to enable processing for IPFIX.
Event Destination *	The NetWitness Log Decoder to which the event logs have to be sent.
Test Configuration	Checks the configuration parameters specified in this dialog to make sure they are correct.

Advanced Parameters

Click ‘V’ next to Advanced, to view and edit the advanced parameters, if necessary.

Name	Description
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. **Caution:** 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 for debugging and monitoring 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.
Destination SSL	Select the check box to communicate using SSL. The security of data transmission is managed by encrypting information and providing authentication with SSL certificates. This check box is selected by default.
Additional Custom	Use this text box for any additional configuration, in case you have multiple inputs or another set of outputs to send somewhere in addition to a NetWitness Log Collector or Log Decoder. For example, you can configure the data to be sent to Elasticsearch. In this case, each event that is sent to Netwitness Platform XDR will also be send to Elasticsearch.
Required Plugins	Specify the required plugins in a comma separated list. **Note:** - Backup and restore is not supported for custom plugins. - If the test connection failed due to required plugin is not installed, you must install the required plugin. For more information, see Install or Manage Logstash Plugin.

Name	Description
Required Ports	Enter a port number (for example, 5000 or UDP:5000, TCP:5000) and ensure the Enabled box is checked. This allows the plugins to collect logs over the network (For example, UDP, TCP). **IMPORTANT:** If you are configuring beats event source, make sure you provide beats event source port (For example, 4739) in the advance configuration even if you have updated the port in the basic parameters.
Pipeline Workers	Number of pipeline worker threads allocated for logstash pipeline.

Getting Help with NetWitness Platform XDR

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 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 XDR 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 nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform documentation.