# NetWitness® Platform XDR

## Kubernetes Event Source Log Configuration Guide

# Kubernetes

### Event Source Product Information:

**Vendor**: CNCF

**Event Source**: Kubernetes

**Versions**: 1.18

### NetWitness Product Information:

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

**Event Source Log Parser**: kubernetes (JSON)

**Collection Method**: Logstash

**Event Source Class.Subclass**: Configuration Management

## 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.

February, 2023

# Contents

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

I. Configure Kubernetes to Send Audit Logs to Logstash

II. Configure Filebeat DaemonSet

III. Deploy Logstash Kubernetes Pipeline Files from LIVE

IV. Deploy Kubernetes Parser from LIVE

V. Set Up Kubernetes Event Source in NetWitness Platform XDR

VI. Configure NetWitness Platform to Collect Events

# Configure Kubernetes to Send Audit Logs to Logstash

Kube-apiserver is a component of Kubernetes which performs auditing. Each request on each stage of its execution generates an event, which is then pre-processed according to a certain policy and written to a backend log files. The policy determines what's recorded and the log files persist the records.

### To configure Kubernetes to send audit logs to Logstash:

1. On the Kubernetes appliance, create the directory `/var/lib/k8s_audit` on the master node.
2. Copy the provided `audit-policy.yaml` file into the directory `/var/lib/k8s_audit`. (This directory will have access to te audit log files since it is mounted to the API server.)
3. Edit the `kube-apiserver.yaml` manifest file which has configurations accessed by **kube-apiserver**. The relevant section of the `kube-apiserver.yaml` will be as follows:

   ```
   ...
   spec:
   containers:
   - command:
   - kube-apiserver
   --audit-log-path=/var/lib/k8s_audit/audit.log
   --audit-policy-file=/var/lib/k8s_audit/audit-policy.yaml
   --audit-log-maxbackup=10
   --audit-log-maxsize=10
   --audit-dynamic-configuration
   --feature-gates=DynamicAuditing=true
   …
   ```

   **Note:** Following table provides the explanation for each of the arguments. The customer can set the values to the arguments based on their requirement.

   | Argument | Description |
   |---|---|
   | audit-log-path | If set, all requests coming to the `apiserver` will be logged to this file. |
   | audit-policy-file | Path to the file that defines the audit policy configuration |
   | audit-log-maxbackup | The maximum number of old audit log files to retain. |
   | audit-log-maxsize | The maximum size of the audit log file (in Megabytes) before it gets rotated. |
   | audit-dynamic-configuration | Enables dynamic audit configuration. This feature also requires the `DynamicAuditing` feature flag. |
   | feature-gates=DynamicAuditing | Set of "key=value" pairs that describe feature gates for alpha or experimental features. |

4. Mount the directory containing policy file and log files onto the Kubernetes container.

The relevant section for mounting the directory `/var/lib/k8s_audit` where our policy file and logs are located onto the kube-apiserver container will be as follows:

```
volumeMounts:
- mountPath: /var/lib/k8s_audit/
name: k8s-audit
...
...
volumes:
- hostPath:
path: /var/lib/k8s_audit
type: DirectoryOrCreate
name: k8s-audit
...
```

5. We have provided a sample `audit-policy.yml` file. The customer can create own policy file. For information on creating own policy file, click here.

**Note:** The `kube-apiserver` should be in running state after the above configuration changes are made.

# Configure Filebeat DaemonSet

**Note:** Deploy Filebeat as a DaemonSet to ensure there is a running instance on each node of the cluster.

### To configure the Filebeat DaemonSet:

1. Download the `daemonset file filebeat-kubernetes.yaml`.
2. The kubernetes audit logs host folder `(/var/lib/k8s_audit/)` is mounted on the Filebeat container. The sample is as follows:

   ```
   …
   volumeMounts:
   - name: k8s-audit
   mountPath: /var/lib/k8s_audit/
   readOnly: true
   volumes:
   - name: k8s-audit
   hostPath:
   path: /var/lib/k8s_audit
   type: DirectoryOrCreate
   …
   ```

3. Filebeat starts an input for the files `(/var/lib/k8s_audit/*audit*.log)` and begins harvesting them as soon as they appear in the folder. The format of the log is provided as **json**.Following is the filebeat input section:

   ```
   filebeat.inputs:
   - type: log
   paths:
   - /var/lib/k8s_audit/*audit*.log
   ```

4. The kubernetes server logs host folder `(/var/log/containers/)` is mounted on the Filebeat container. The sample is as follows:

   ```
   volumeMounts:
   - name: server
   mountPath: /var/log/containers/
   readOnly: true
   volume:
   - name: server
   hostPath:
   path: /var/log/containers/
   ```

```
type: DirectoryOrCreate
```

5. Filebeat starts an input for the files `(/var/log/containers/kube-apiserver-*.log)` and begins harvesting them as soon as they appear in the folder. The format of the log is provided as **json**.Following is the filebeat input section:

   filebeat.inputs:

   ```
   - type: log
   paths:
   - /var/log/containers/kube-apiserver-*.log
   ```

6. Everything is deployed under the **kube-system** namespace by default. To change the namespace, modify the `filebeat-kubernetes.yaml` file. The sample is as follows:

   …

   ```
   metadata:
   name: <name>
   namespace: kube-system
   ```

   …

7. Provide the output destination as **logstash**. This will route Kubernetes audit events to the **Logstash** service. Edit the `filebeat-kubernetes.yaml` and enter the logstash ip address as follows:

   …

   ```
   output.logstash:
   # The Logstash hosts
   hosts: ["<logstash-ip-address>:5044"]
   ```

   …

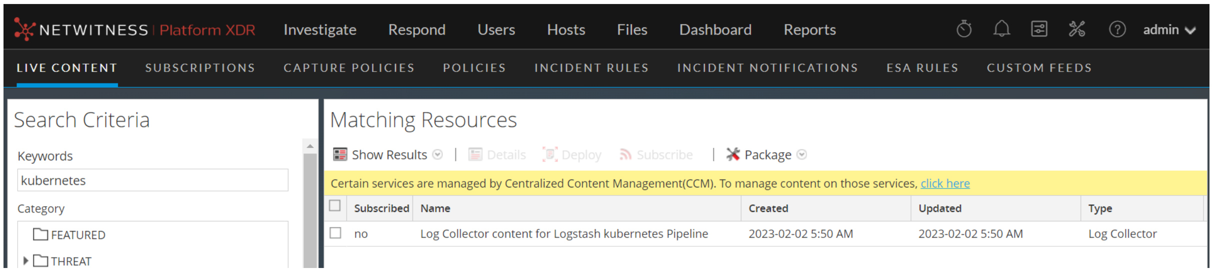
8. Deploy the `filebeat-kubernetes.yaml` to create the configMap, daemonset and service account. and The role is created to provide the required permissions for Filebeat pods. Use the **Kubectl** for deployment which allows you to run commands against Kubernetes clusters. The sample file structure is `Kubectl apply -f filebeat-kubernetes.yaml`.

# Deploy Logstash Kubernetes Pipeline Files from LIVE

Logstash Kubernetes Pipeline files requires resources available in Live to collect logs.

### To deploy Logstash Kubernetes Pipeline files from Live:

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



Keywords: kubernetes

Certain services are managed by Centralized Content Management(CCM). To manage content on those services, click here

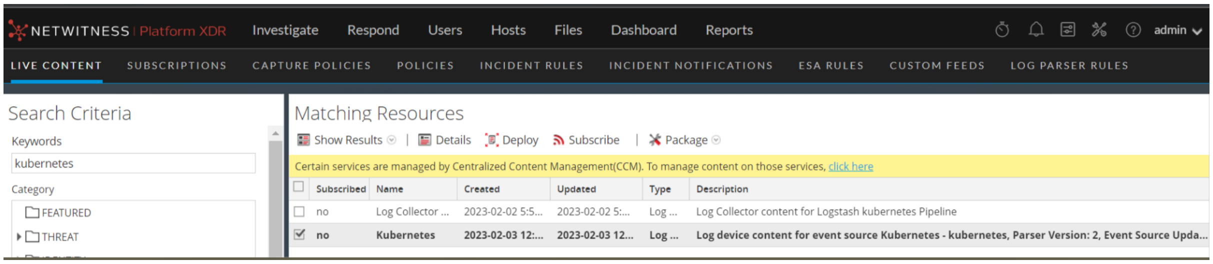
| □ | Subscribed | Name | Created | Updated | Type |
|---|---|---|---|---|---|
| □ | no | Log Collector content for Logstash kubernetes Pipeline | 2023-02-02 5:50 AM | 2023-02-02 5:50 AM | Log Collector |

# Deploy Kubernetes Parser from LIVE

Kubernetes parser requires resources available in Live to parse logs.

### To deploy Kubernetes content from Live:

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



Keywords: kubernetes

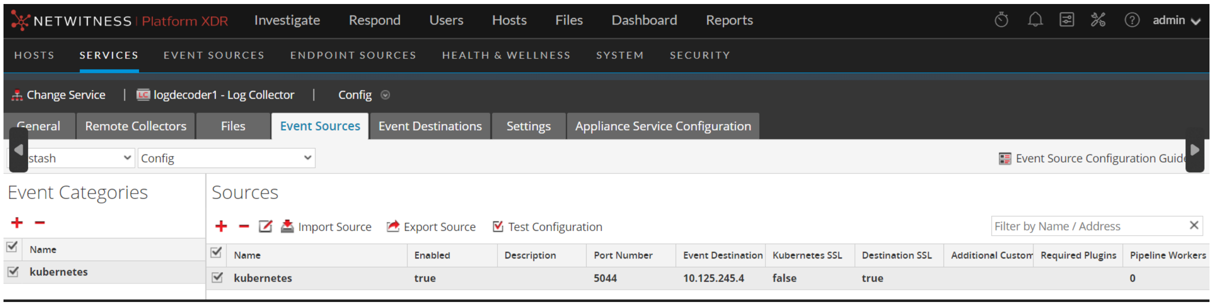
Certain services are managed by Centralized Content Management(CCM). To manage content on those services, click here

| □ | Subscribed | Name | Created | Updated | Type | Description |
|---|---|---|---|---|---|---|
| □ | no | Log Collector ... | 2023-02-02 5:5... | 2023-02-02 5:... | Log ... | Log Collector content for Logstash kubernetes Pipeline |
| ☑ | no | Kubernetes | 2023-02-03 12:... | 2023-02-03 12... | Log ... | Log device content for event source Kubernetes - kubernetes, Parser Version: 2, Event Source Upda... |

# Set Up Kubernetes Event Source in NetWitness Platform XDR

### To configure the Kubernetes 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.

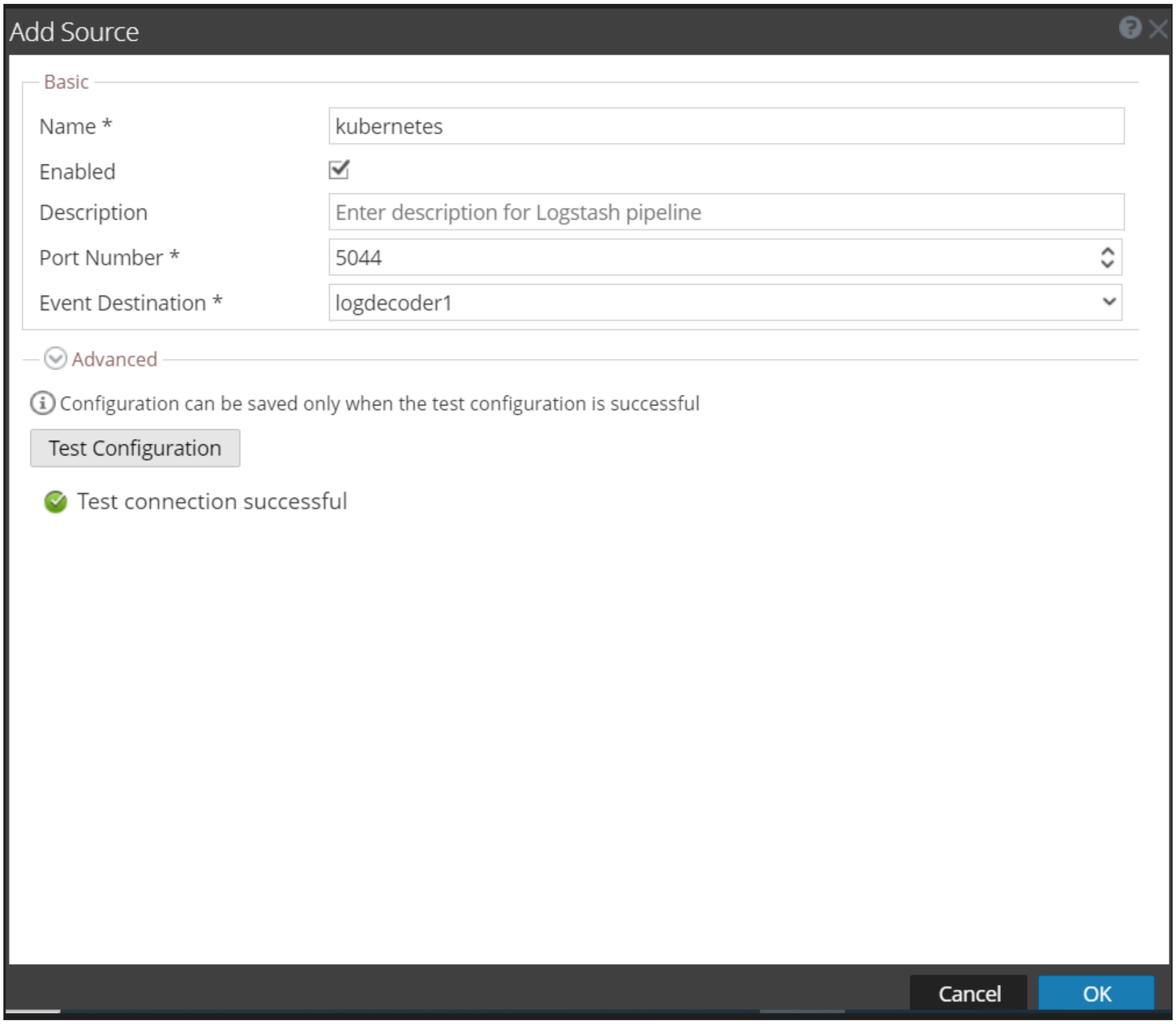


| ☑ | Name |
|---|---|
| ☑ | kubernetes |

| ☑ | Name | Enabled | Description | Port Number | Event Destination | Kubernetes SSL | Destination SSL | Additional Custom | Required Plugins | Pipeline Workers |
|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | kubernetes | true | | 5044 | 10.125.245.4 | false | true | | | 0 |

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

   The **Add Source** dialog is displayed.



Add Source

Basic

Name * kubernetes

Enabled ☑

Description Enter description for Logstash pipeline

Port Number * 5044

Event Destination * logdecoder1

Advanced

Configuration can be saved only when the test configuration is successful

Test connection successful

6. Define parameter values, as described in Kubernetes Collection Configuration Parameters.

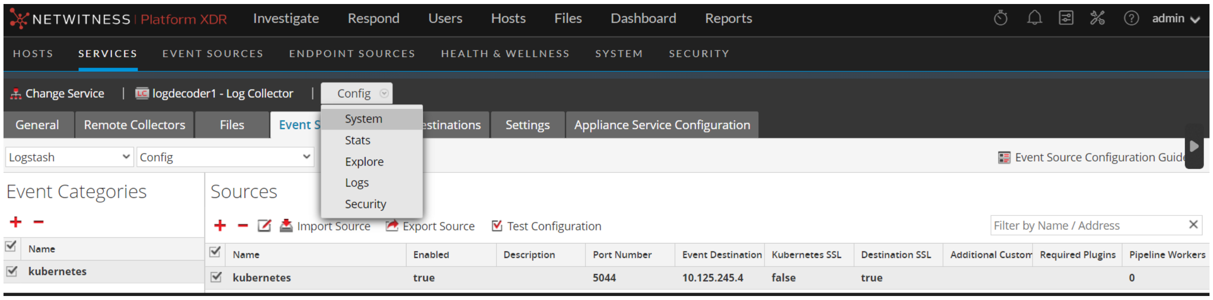
7. Click **Test Configuration**.

   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.

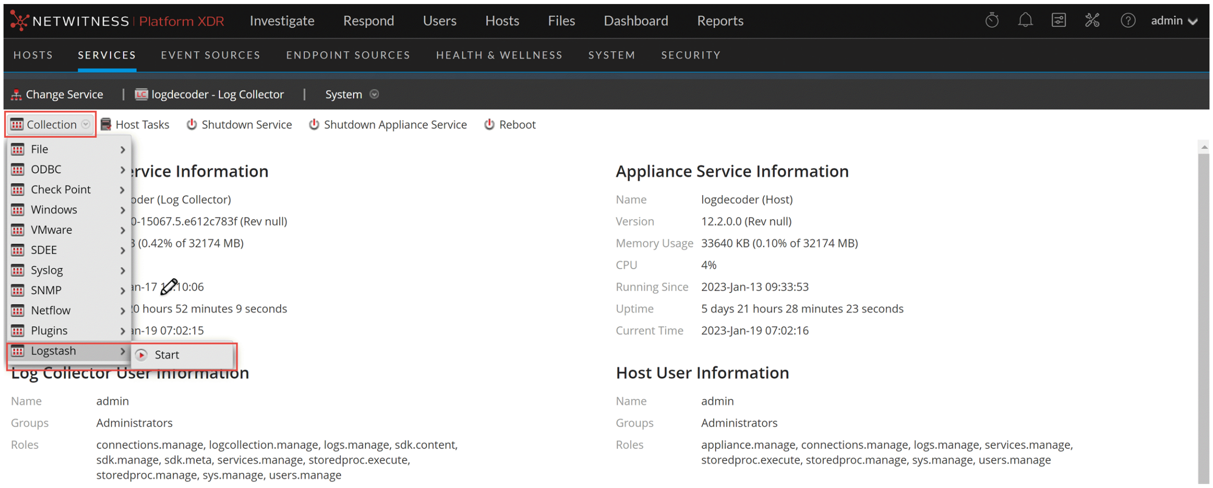
9. Save the configuration. From the **Actions** menu choose **System**.



| Name |
|---|
| kubernetes |

| Name | Enabled | Description | Port Number | Event Destination | Kubernetes SSL | Destination SSL | Additional Custom | Required Plugins | Pipeline Workers |
|---|---|---|---|---|---|---|---|---|---|
| kubernetes | true | | 5044 | 10.125.245.4 | false | true | | | 0 |

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



ervice Information

oder (Log Collector)
0-15067.5.e612c783f (Rev null)
3 (0.42% of 32174 MB)

n-17 10:06
0 hours 52 minutes 9 seconds
n-19 07:02:15

Appliance Service Information

| | |
|---|---|
| Name | logdecoder (Host) |
| Version | 12.2.0.0 (Rev null) |
| Memory Usage | 33640 KB (0.10% of 32174 MB) |
| CPU | 4% |
| Running Since | 2023-Jan-13 09:33:53 |
| Uptime | 5 days 21 hours 28 minutes 23 seconds |
| Current Time | 2023-Jan-19 07:02:16 |

Log Collector User Information

| | |
|---|---|
| Name | admin |
| Groups | Administrators |
| Roles | connections.manage, logcollection.manage, logs.manage, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage |

Host User Information

| | |
|---|---|
| Name | admin |
| Groups | Administrators |
| Roles | appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage |

# Kubernetes Collection Configuration Parameters

The tables below list the configuration parameters required for integrating Kubernetes 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 check box to enable the event source configuration to start collection. The check box is selected by default. |
| Description | Enter a text description for the event source. |
| Port Number* | Enter the port number that you configured for your event sources. The default value of port number is 5044. |

| Name | Description |
|---|---|
| Event Destination* | Select the NetWitness Log Collector or Log Decoder to which event needs to be send from the drop-down list. |
| Test Configuration | Checks the configuration parameters specified in this dialog to make sure they are correct. |

## Advanced Parameters

| 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.<br>**Caution:** Enabling debugging will adversely affect the performance of the Log Collector.<br>Enables or disables debug logging for the event source. Valid values are:<br>• **Off** = (default) disabled<br>• **On** = enabled<br>• **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages.<br>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. |
| Kubernetes SSL | Select this checkbox to communicate using Kubernetes SSL. The security of data transmission is managed by encrypting information and providing authentication with SSL certificates. This check box is not selected by default.<br>**Note:** Ensure that you copy the server SSL certificate and the key (generated in your system) to `/etc/logstash/pki` on Log Collector, which is used during SSL connection. `/etc/logstash/pki` is a path in the Log Collector node. |
| Certificate * | Select the name of a server SSL certificate located at `/etc/logstash/pki`. |
| Key * | Select the name of a server SSL key located at `/etc/logstash/pki`. |

| Name | Description |
|---|---|
| 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 Configuration | 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.<br>**Note:**<br>- Backup and restore is not supported for custom plugins.<br>- 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. |
| Required Ports | Enter the list of ports required for external access. |
| Pipeline Workers | Number of pipeline worker threads allocated for logstash pipeline. |

# Configure NetWitness Platform to Collect Events

### To configure NetWitness platform to collect events:

1. You must start capture on the Log Decoder to which you are sending the Logstash data. To start or restart network capture on a Log Decoder:

   i. In the NetWitness Platform XDR menu, select **Admin** > **Services**. The Services view is displayed.

   ii. Select a **Log Decoder** service.

   iii. Under **Actions**, select **View** > **System**.

   iv. In the toolbar, click **Start Capture**.

   > **Note:** If the toolbar is displaying the **Stop Capture ()** icon, then capture has already started.

   By default, Log Decoders support events that are up to 32 KB in size. If the events are getting truncated on the Log Decoder, use the following procedure to change the event size:

   1. Change `LogDecoder REST config at http://LogDecoder_IP:50102/decoder/config`, where LogDecoder_IP is the IP address of your Log Decoder.
   2. Set `pool.packet.page.size` to 64 KB.
   3. Restart the Log Decoder. This is required after you change the `pool.packet.page` value.

   > **Note:** If you are collecting events larger than 64 KB in size, follow instructions above in the Filter out unwanted logs section. You can drop unwanted logs or fields for a specific event source to reduce the size of the incoming data.

# 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<br>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.