

NetWitness[®] Platform

VMware vSphere Event Source Log Configuration Guide

VMware vSphere

Event Source Product Information:

Vendor: [VMware](#)

Event Source: ESXi, vCenter

Versions:

- ESXi : 7.0 U2 and later
- vCenter : 7.0 U2 and later

NetWitness Product Information:

Supported On: NetWitness Platform 12.0 and later

Event Source Type: vmware_esx_esxi or vmware_vc

Collection Method: Plugin

Event Source Class.Subclass: Host.Virtualization

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/>.

© 2023 RSA Security LLC or its affiliates. All Rights Reserved.

November, 2023

Contents

- Introduction to VMware vSphere 5**
- Configure the VMware Event Source 6**
- Set Up the VMware vSphere Event Source in NetWitness Platform 7**
 - Deploy VMware vSphere Files from Live 7
 - Configure the Event Source 7
- VMware vSphere Collection Configuration Parameters 10**
 - Basic Parameters 10
 - Advanced Parameters 11
- Getting Help with NetWitness Platform 12**
 - Self-Help Resources 12
 - Contact NetWitness Support 12
 - Feedback on Product Documentation 13

Introduction to VMware vSphere

VMware vSphere is the enterprise workload platform that brings the benefits of cloud to on-premises workloads. It combines industry-leading cloud infrastructure technology with DPU- and GPU-based acceleration to boost workload performance. vSphere centralizes management through the VMware Cloud Console to enhance operational efficiency and integrates with a growing catalog of add-on hybrid cloud services to expedite disaster recovery, ransomware protection, capacity optimization and planning, and more.

To configure VMware vCenter Server/VirtualCenter Server, perform the following tasks:

- I. [Configure the VMware Event Source](#)
- II. [Set Up the VMware vSphere Event Source in NetWitness Platform](#) .

Configure the VMware Event Source

Users can configure either [VMware ESX/ESXi](#) or [VMware vCenter Server](#) as an event source. This section describes creating a least privileged User to extract logs from an ESX/ESXi or vCenter Server host. You first create a role, then create the user, and finally, assign the role to the user. To create a necessary user and role, please refer to the instructions provided in the respective VMware documentation mentioned below:

IMPORTANT: While creating an user, ensure that role should have Diagnostics (**All Privileges > Global > Diagnostics**) as the only privilege for this role.

- Create a user in ESXi, see [Manage Permissions in the VMware Host Client](#).
- Create a user in vCenter, see [Create and Configure a vCenter Server User](#).

This completes the process of adding a least privilege user. When you configure the Log Collector for VMware vSphere plugin configuration in NetWitness Platform, make sure to enter the credentials for this user in the **Add Source** dialog box.


Set Up the VMware vSphere Event Source in NetWitness Platform

In NetWitness Platform, perform the following tasks:

- I. [Deploy VMware vSphere Files from Live](#)
- II. [Configure the Event Source](#).

Deploy VMware vSphere Files from Live

To deploy `Vmware_Vsphere` content from Live:



1. In the NetWitness Platform menu, select  (Configure) > **Live Content**.
The **Live Content** tab is displayed.
2. Browse Live for `Vmware_Vsphere` plugin by typing `Vmware_Vsphere` into the Keywords text box and click **Search**.
Select the `Vmware_Vsphere` plugin from the search results.
3. Click **Deploy** to deploy the `Vmware_Vsphere` to the appropriate Log Collectors using the Deployment Wizard.
4. Deploy the appropriate parsers used by this plugin:
 - For VMware ESXi, deploy `vmware_esx_esxi`.
 - For VMware vCenter, deploy `vmware_vc`.

Note: If the number of messages in the queue are very high, create multiple instances of the S3universal plugin to ingest the messages at a higher rate.

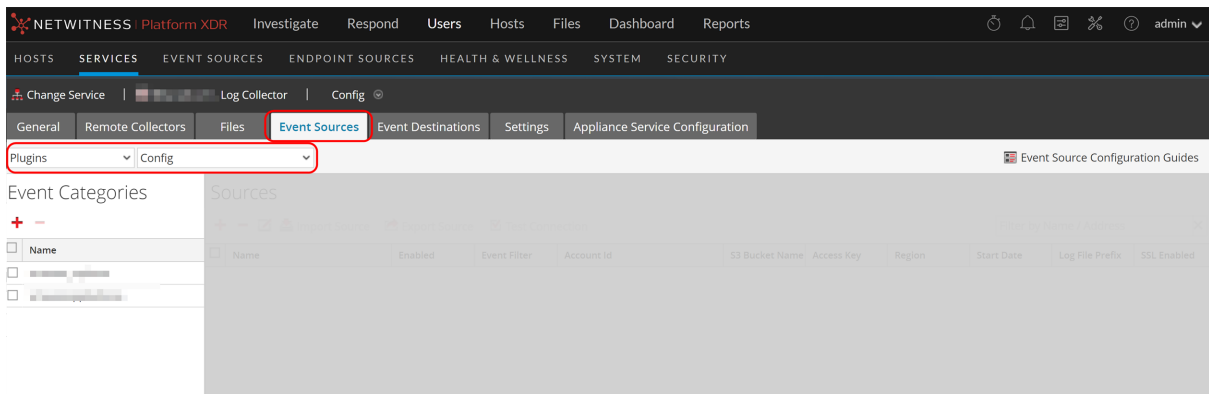
For more details, see the [Add or Update Supported Event Source Log Parsers](#) topic on NetWitness Community.

Configure the Event Source

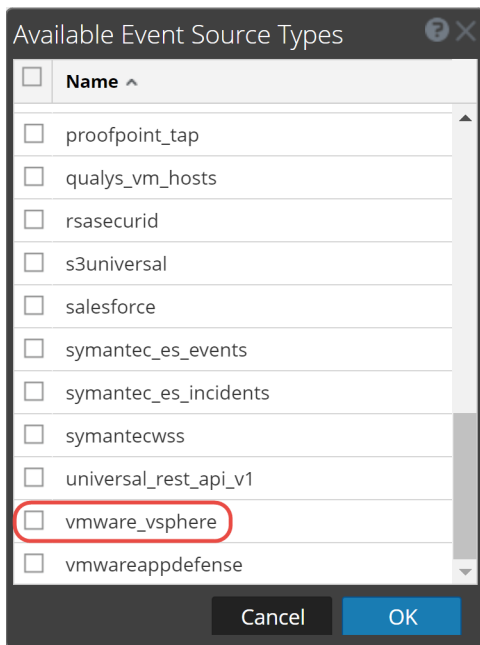
To configure the VMware vSphere Platform Event Source:

1. In the NetWitness Platform menu, select  (Admin) > **Services**.
2. In the Services grid, select a Log Collector, 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.



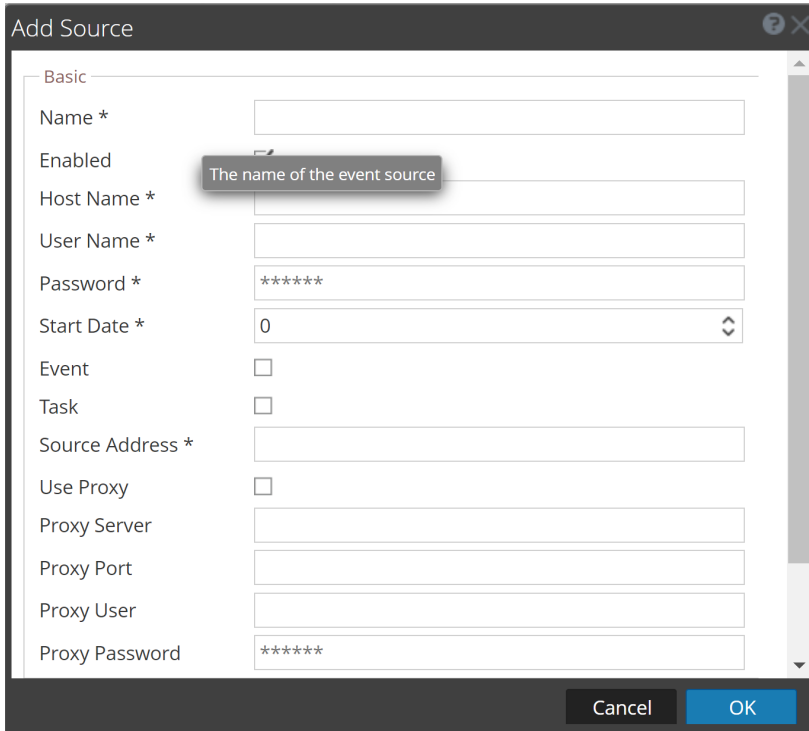
4. In the Event Categories panel toolbar, click **+**.
The Available Event Source Types dialog is displayed.



5. Select **vmware_vsphere** 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 [VMware vSphere Collection Configuration Parameters](#).
8. Click **Test Connection**.

The test result 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.
10. Repeat steps 4–9 to add another VMware vSphere plugin type.

VMware vSphere Collection Configuration Parameters

The following table describes the configuration parameters for the VMware vSphere Platform integration with NetWitness Platform.

Note the following:

- Fields marked with an asterisk (*) are required to successfully complete the configuration.
- If a proxy is being used, the proxy shall allow traffic through port 5671 (used for AMQPS).

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.
Host Name*	Host Name of VMware ESXi or VMware vCenter
User Name*	Username to be used for VMware ESXi or VMware vCenter authentication (created as part of Configure the VMware Event Source).
Password*	User Password (created as part of Configure the VMware Event Source).
Start Date*	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 89, when set, the last 89 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 0–89. For example, current date is 21 Apr 2023 and you want to collect logs from 19 Apr 2023, set the value to 2.
Event or Task	Select the respective box to enable Event or Task. The ESX/ESXi contains only Events, while vCenter contains both Events and Tasks. IMPORTANT: NetWitness recommends that you should enable either Event or Task exclusively. It is not recommended to enable both simultaneously. If you want to capture Tasks for the same vCenter, you should create another instance.
Use Proxy	Select the box to enable proxy.
Proxy Server	If you are using a proxy, enter the proxy server address.
Proxy Port	If proxy is being used, then the proxy shall allow traffic through port 5671, used for AMQPS.

Name	Description
Proxy User	Username for the proxy (leave empty if using anonymous proxy).
Proxy Password	Password for the proxy (leave empty if using anonymous proxy).

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	The maximum duration of polling cycle (how long the cycle lasts) in seconds.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	Maximum idle time, in seconds, of a polling cycle. 0 indicates no limit.> 300 is the default value.
Command Args	Optional arguments to be added to the script invocation.
Debug	<div style="border: 1px solid yellow; padding: 5px; margin-bottom: 10px;"> <p>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.</p> </div> <p>Enables and disables debug logging for the event source.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> • Off = (default) disabled • On = enabled • Verbose = enabled in verbose mode - adds thread information and source context information to the messages. <p>This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact.</p> <p>If you change this value, the change takes effect immediately (no restart required).</p>
SSL Enable	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.