

NetWitness[®] Platform

VMware ESX/ESXi Event Source Log Configuration Guide

VMware ESX/ESXi

Last Modified: Thursday, March 26, 2026

Event Source Product Information:

Vendor: [VMware](#)

Event Source: ESX, ESXi, Embedded ESXi

Versions:

- ESX: 3.0.3, 3.5, 4.0, 4.1
- Embedded ESXi: 3.5, 4.0
- ESXi: 3.5, 4.0, 4.1, 5.0, 5.1, 5.5, 6.x, 7.0 U2

Note: NetWitness supports the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case in the NetWitness Community Portal for support.

NetWitness Product Information:

Supported On: NetWitness Platform 12.3 and later

Event Source Type: vmware_esx_esxi

Collection Method: VMware collection, Plugin Framework (7.0 U2 or later)

Note: Use [VMWare_vsphere](#) plugin for event source version 7.0 U2 or later

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

NetWitness, the NetWitness logo, and other trademarks are trademarks of NetWitness Security LLC or its affiliates. Other names may be trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to NetWitness 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 NetWitness.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

Third-Party Licenses

This product may include software developed by parties other than NetWitness. 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 NetWitness Security LLC or its affiliates ("NetWitness") software described in this publication requires an applicable software license.

NetWitness 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." NetWitness 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/>.

© 2026 NetWitness Security LLC or its affiliates. All Rights Reserved.

January, 2026

Contents

- Configure the VMware ESX/ESXi Event Source 6**
- Configure the NetWitness Platform Log Collector for VMware Collection 9**
- Getting Help with NetWitness Platform 11**
 - Self-Help Resources 11
 - Contact NetWitness Support 11
 - Feedback on Product Documentation 12

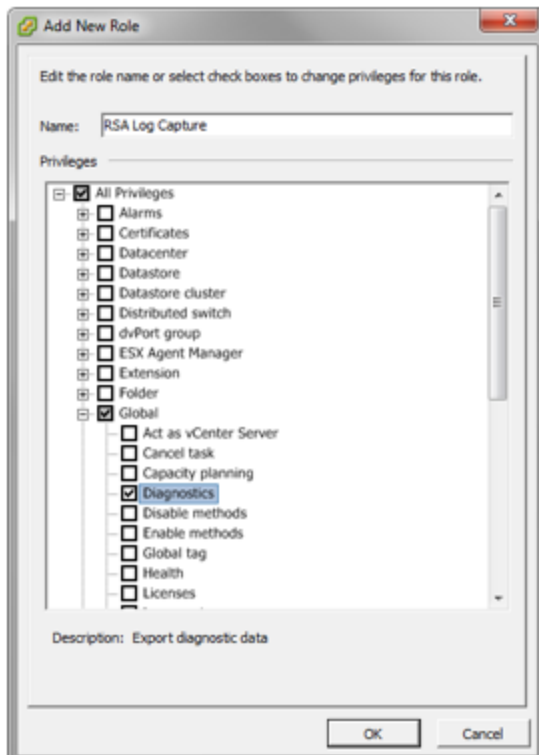
To configure VMware ESX/ESXi, perform the following tasks:

- I. [Configure the VMware event source](#)
- II. [Configure the NetWitness Platform Log Collector for VMware Collection](#)

Configure the VMware ESX/ESXi Event Source

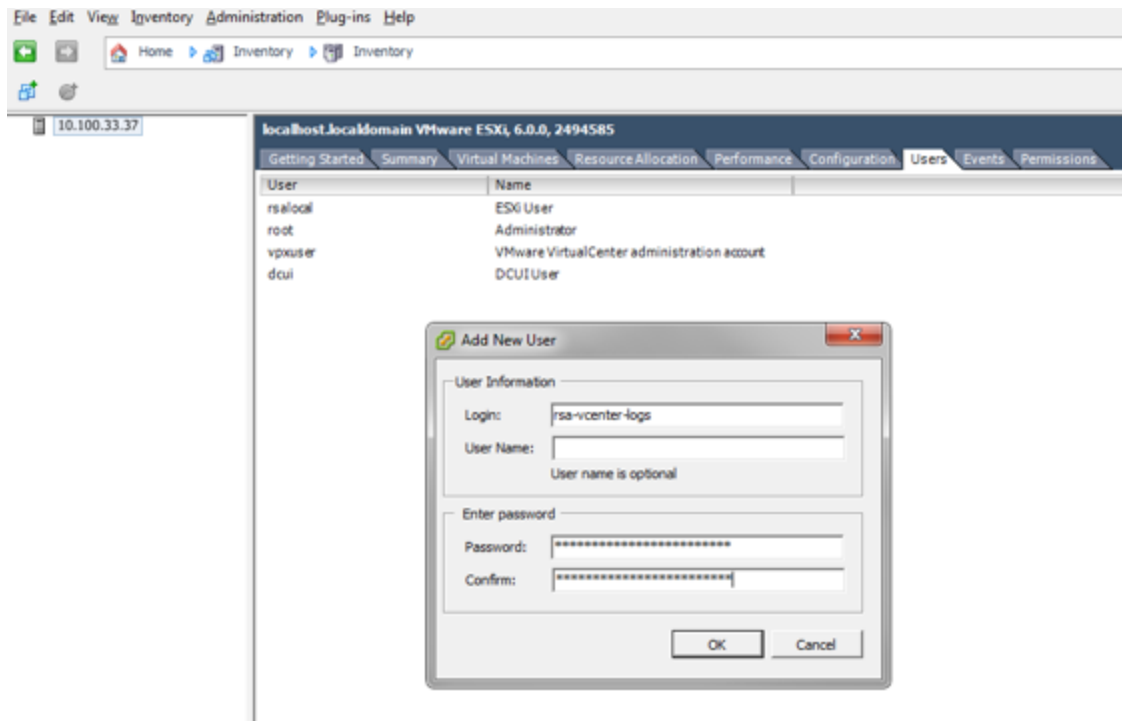
This section describes how to create a least privilege User to extract logs from an ESX/ESXi host. You first create a role, then you create the user, and finally, you assign the role to the user.

1. Create a role as follows:
 - a. Log onto the ESXi host using the vSphere Client, with administrative privileges.
 - b. Click on **Administration > Roles**.
 - c. Click on **Add Role**.
 - d. Enter **RSA Log Capture** as the name of the Role.
 - e. Choose **All Privileges > Global > Diagnostics** as the only privilege for this role:



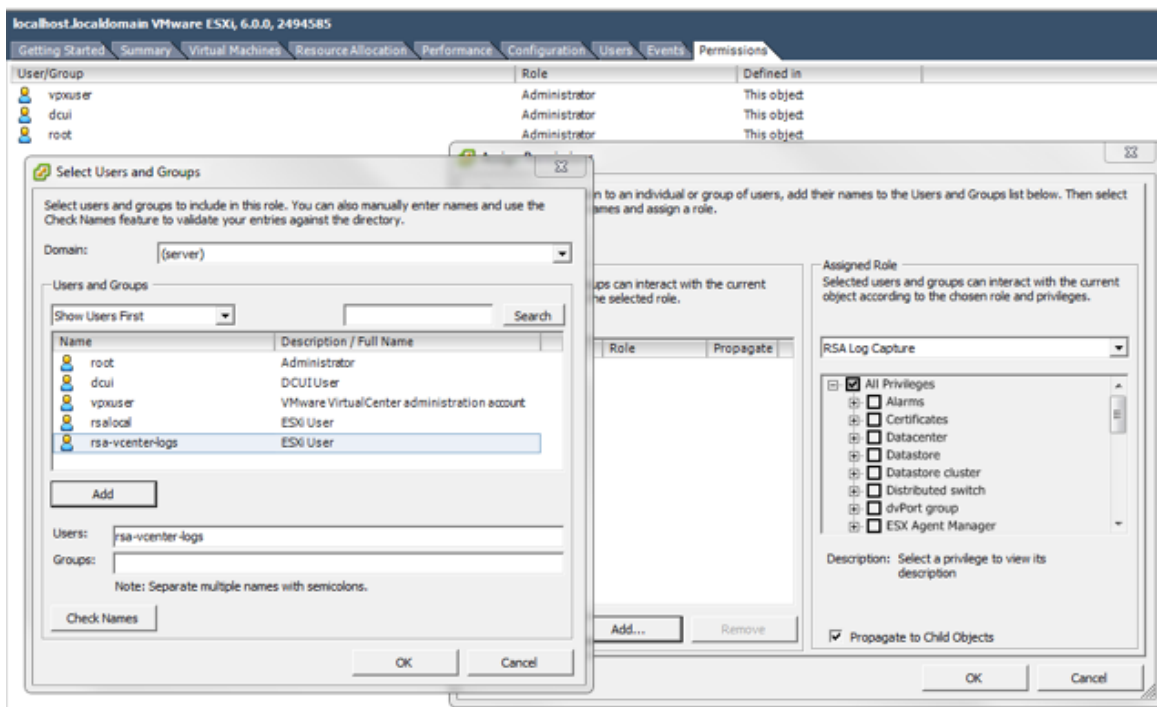
2. Create a local ESXi user as follows:
 - a. From the Left navigation pane, click on the ESXi host, then click the **Users or Local Users & Groups** tab. The name of the tab depends on the credentials you used to log onto the ESXi host.
 - b. Right click on the **Users** tab, then click **Add**.

- c. Enter **rsa-vcenter-logs** in the **Login** field, and choose a strong password:



3. Assign a role to the local user as follows:
 1. From the Left navigation pane, click on the ESXi host, then click the **Permissions** tab.
 2. Right click in the **Permissions** table, then click **Add Permission**.
 3. In the dialog box, under the **Assigned Role** drop-down menu, choose **RSA Log Capture**.
 4. Under **Users and Groups**, click **Add...**

The **Select Users and Groups** dialog box is displayed.
 5. In the dialog box, leave the Domain value as (server), and select the **rsa-vcenter-logs** user.




6. Click **Add**, then click **OK**.

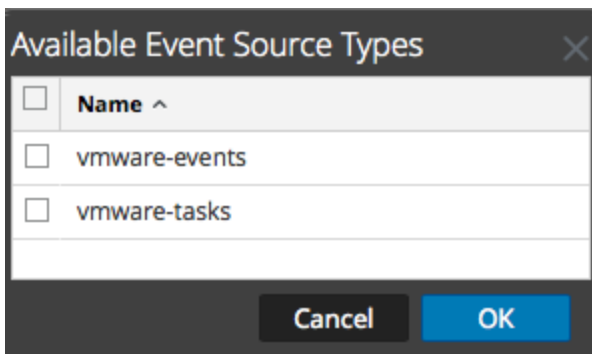
This completes the process of adding a least privilege user. When you configure the Log Collector for VMware collection in NetWitness Platform, make sure to enter the credentials for this user in the **Add Source** dialog box.

Configure the NetWitness Platform Log Collector for VMware Collection

Perform the following steps to configure the Log Collector for VMware collection.

Add the VMware Event Source Type:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the Services grid, select a Log Collector service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **VMware/Config** from the drop-down menu.
The Event Categories panel displays the VMware event sources that are configured, if any.
5. Click **+** to open the **Available Event Source Types** dialog.



6. Select **vmware-events** or **vmware-tasks** from the Available Event Source Types dialog and click **OK**.

The VMware available event source types are as follows:

- **vmware-events:** Setup vmware-events to collect events from vCenter Servers and ESX/ESXi servers.
 - **vmware-tasks:** (Optional) Setup vmware-tasks to collect tasks from vCenter Servers.
7. Select the new type in the Event Categories panel, and click **+** in the Sources toolbar.
 8. Add a Name, Username and Password, and modify any other parameters that require changes.

The screenshot shows the 'Add Source' dialog box with the following configuration:

Section	Field	Value
Basic	Name *	
	Address *	127.0.0.1
	Username *	
	Password *	*****
	Enabled	<input checked="" type="checkbox"/>
Advanced	Polling Interval	180
	Max Duration Poll	120
	Max Events Poll	1000
	Max Idle Time Poll	0
	Debug	Off

Caution: If you need to enter the domain name as part of the Username, you must use a double-backslash as a separator. For example, if the domain\username is corp\smithj, you must specify **corp\\smithj**.

9. Click **OK** to save your changes.

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.