

# NetWitness<sup>®</sup> Platform

## Vmware\_vCenter Event Source Log Configuration Guide

# VMware vCenter Server

Last Modified: Friday, March 27, 2026

## Event Source Product Information:

**Vendor:** [VMware](#)

**Event Source:** VirtualCenter Server, vCenter Server

## Versions:

- vCenter Server: 4.1, 5.0, 5.1, 5.5, 6.x

**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.

- VirtualCenter Server: 2.0.2, 2.5

## RSA Product Information:

**Supported On:** NetWitness Platform 12.3 and later

**Event Source Type:** vmware\_vc

**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

---

<b>Configure the VMware vCenter Server or VirtualCenter Server .....</b>	<b>6</b>
<b>Configure the NetWitness Platform Log Collector for VMware Collection .....</b>	<b>10</b>

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

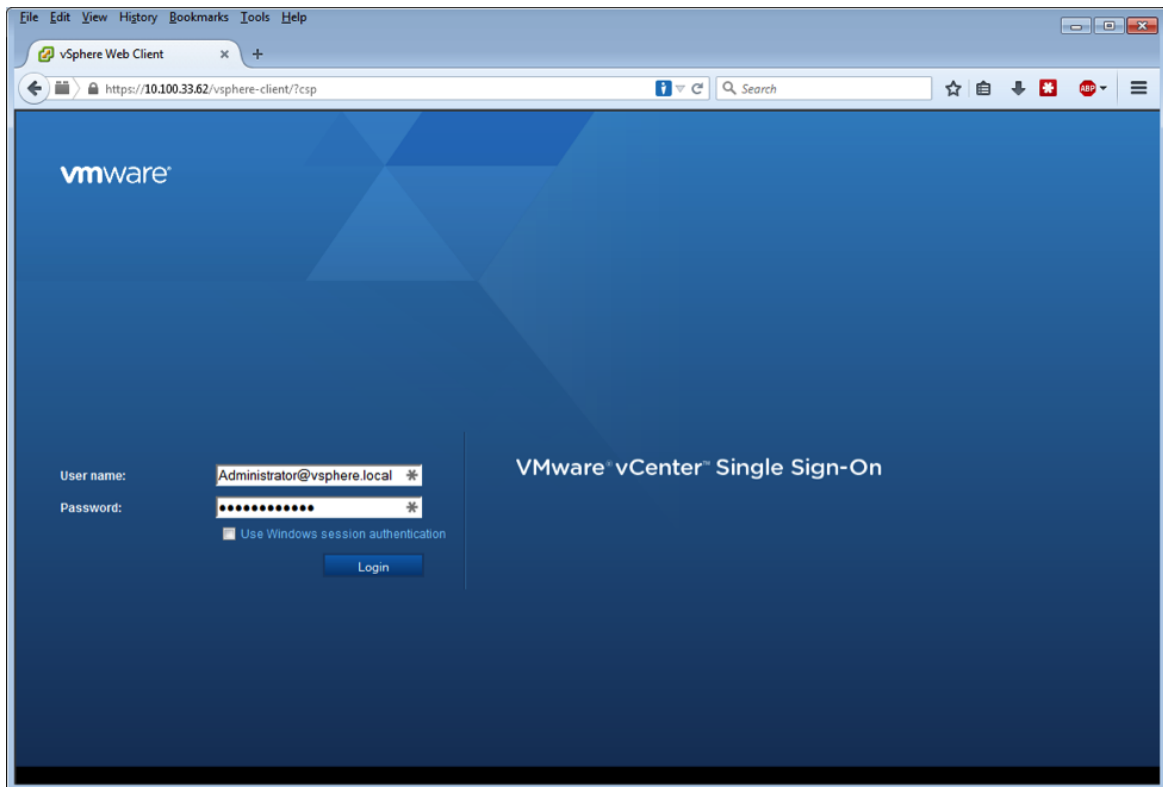
- I. [Configure the VMware event source](#)
- II. [Configure the RSA NetWitness Platform Log Collector for VMware Collection](#)

## Configure the VMware vCenter Server or VirtualCenter Server

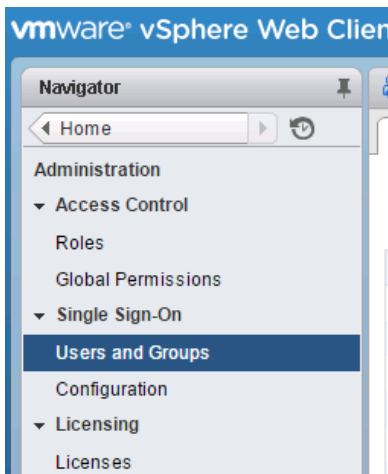
---

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

1. Create a user as follows:
  - a. Log onto the Single Sign-On Server. A popular credential is **administrator@vsphere.local**.



- b. Click on **Home > Administration > Users and Groups**.



- c. On the **Users** tab, click **+** and add a user.

The New User dialog box is displayed.

- d. Enter **rsa-vcenter-logs** as the user, and choose a strong password:

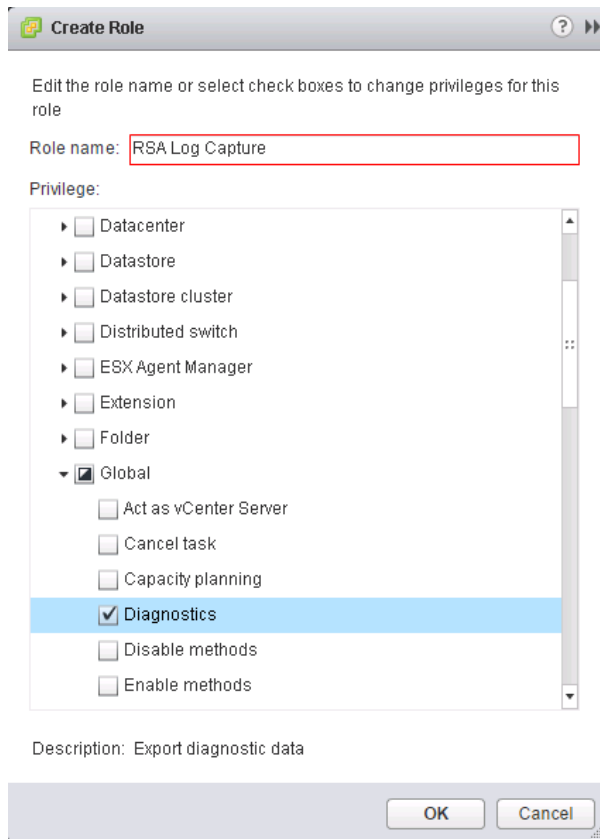
- e. Click **OK** to add the user and close the dialog box.

2. Create a role as follows:

- a. From the Left navigation pane, under **Access Control**, select **Roles** and click **+** to create a new Role.

The Create Role dialog box is displayed.

- b. Enter **RSA Log Capture** as the name of the Role.
- c. Select **Global > Diagnostics** to assign the correct privileges.




- d. Click **OK**.
3. Assign a role to the user as follows:
    1. From the Left navigation pane, select **Home > Hosts and Clusters**.
    2. To add the user account to the VirtualCenter, right click the VirtualCenter Server in the VirtualCenter client, and select **Add Permission**.  
The Add Permission dialog box is displayed.
    3. From the **Assigned Role** section, select the **RSA Log Capture** role, and click **Add**.

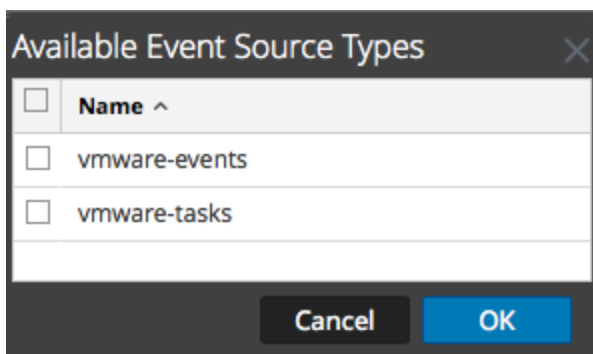


## Configure the NetWitness Platform Log Collector for VMware Collection

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.