

NetWitness[®] Platform

Vertiv Avocent IP KVM Event Source Log Configuration Guide

Vertiv Avocent IP KVM

Last Modified: Wednesday, December 4, 2024

Event Source Product Information:

Vendor: [Vertiv](#)

Event Source: Avocent IP KVM

Supported Version: Dell PowerEdge 2161DS-2

NetWitness Product Information:

Supported On: NetWitness Platform 12.3 and later

Event Source Log Parser: avocentkvm

Collection Method: SNMP

Event Source Class.Subclass: Network

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/>.

© 2024 RSA Security LLC or its affiliates. All Rights Reserved.

November 2024

Contents

- Configure Avocent IP KVM to send SNMP 6**
- Configure SNMP Event Sources on NetWitness Platform 7**
 - Ensure the Required Parser is Enabled 7
 - Add the SNMP Event Source Type 7
 - (Optional) Configure SNMP Users 8
 - SNMP User Parameters 9
- Getting Help with NetWitness Platform 11**
 - Self-Help Resources 11
 - Contact NetWitness Support 11
 - Feedback on Product Documentation 12

To configure Avocent IP KVM, you must complete these tasks:

- Configure Avocent IP KVM to send SNMP
- Configure SNMP Event Sources on the NetWitness Platform

Configure Avocent IP KVM to send SNMP

To configure the Avocent IP KVM event source to send SNMP:



1. Start the Dell Remote Console Switch Software.
2. Select the Remote Console Switches tab.
3. Select the Remote Console Switch and click **Manage Remote Console Switch**.
4. Log on with administrative credentials.
5. Select the Settings tab and select **SNMP** from the Categories pane.
6. Click **Add** and enter the IP address of the [[[Undefined variable SAVariables.ProductSuiteName]]] Log Collector.
7. Click **OK** and click **Apply**.
8. Expand **SNMP** in the Categories pane and select **Traps**.
9. Click **Enable All** and click **Apply**.

Configure SNMP Event Sources on NetWitness Platform

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Platform Live.

Ensure that the parser for your event source is available:

1. In the **NetWitness** menu, select  (Admin) > **Services**.
2. In the **Services** grid, select a Log Decoder, and from the **Actions** () menu, choose **View > Config**.
3. In the **Service Parsers Configuration** panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.


Note: The required parser is **avocentkvm**.

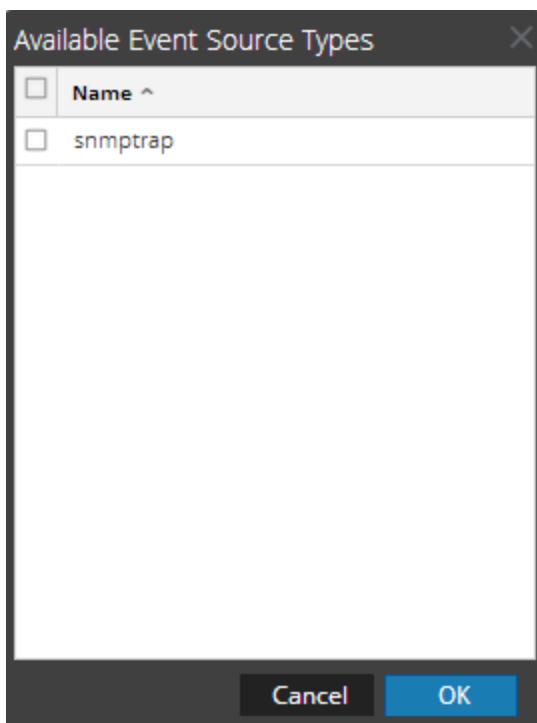
The first time that you configure an SNMP event source on [[[Undefined variable SAVariables.ProductSuiteName]]], you need to add the SNMP event source type and configure SNMP users.

Add the SNMP Event Source Type

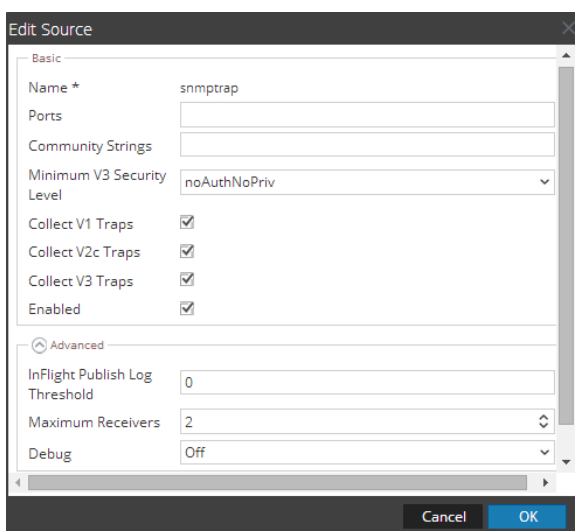
Note: If you have previously added the **snmptrap** type, you cannot add it again. You can edit it, or manage users.

Add the SNMP Event Source Type:

1. In the **NetWitness Platform** 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 **SNMP/Config** from the drop-down menu.
The Sources panel is displayed with the existing sources, if any.
5. Click **+** to open the **Available Event Source Types** dialog.



6. Select **snmptrap** from the Available Event Source Types dialog and click **OK**.
7. Select **snmptrap** in the Event Categories panel.
8. Select **snmptrap** in the Sources panel and then click the Edit icon to edit the parameters.




9. Update any of the parameters that you need to change.

(Optional) Configure SNMP Users

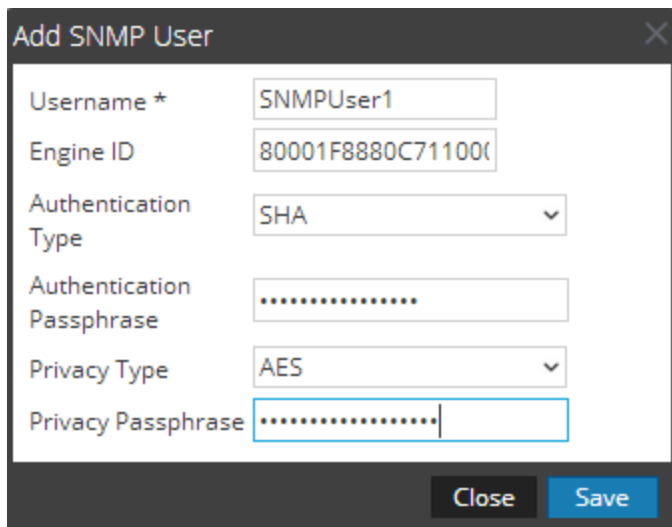
If you are using SNMPv3, follow this procedure to update and maintain the SNMP v3 users.

Configure SNMP v3 Users

1. In the **NetWitness Platform** 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 **SNMP/SNMP v3 User Manager** from the drop-down menu.

The SNMP v3 User panel is displayed with the existing users, if any.

5. Click **+** to open the **Add SNMP User** dialog.



6. Fill in the dialog with the necessary parameters. The available parameters are described below.

SNMP User Parameters

The following table describes the parameters that you need to enter when you create an SNMP v3 user.

Parameter	Description
Username *	User name (or more accurately in SNMP terminology, security name). NetWitness Platform uses this parameter and the Engine ID parameter to create a user entry in the SNMP engine of the collection service. The Username and Engine ID combination must be unique (for example, logcollector).
Engine ID	(Optional) Engine ID of the event source. For all event sources sending SNMP v3 traps to this collection service, you must add the username and engine id of the sending event source. For all event sources sending SNMPv3 informs, you must add just the username with a blank engine id.

Parameter	Description
Authentication Type	(Optional) Authentication protocol. Valid values are as follows: <ul style="list-style-type: none">• None (default) - only security level of noAuthNoPriv can be used for traps sent to this service• SHA - Secure Hash Algorithm• MD5 - Message Digest Algorithm
Authentication Passphrase	Optional if you do not have the Authentication Type set. Authentication passphrase.
Privacy Type	(Optional) Privacy protocol. You can only set this parameter if Authentication Type parameter is set. Valid values are as follows: <ul style="list-style-type: none">• None (default)• AES - Advanced Encryption Standard• DES - Data Encryption Standard
Privacy Passphrase	Optional if you do not have the Privacy Type set. Privacy passphrase.
Close	Closes the dialog without adding the SNMP v3 user or saving modifications to the parameters.
Save	Adds the SNMP v3 user parameters or saves modifications to the parameters.

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.