

RSA NetWitness Logs

Event Source Log Configuration Guide



EMC Fabric OS

Last Modified: Thursday, June 22, 2017

Event Source Product Information:

Vendor: [EMC](#)

Event Source: Fabric OS

Versions: Fabric OS 6.1 & 6.2

Platforms: EMC Connectrix, Brocade DCX Switch

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: fabricos

Collection Method: Syslog

Event Source Class.Subclass: Network.Switch

To configure the EMC Fabric OS event source, you must:

- I. Configure Syslog Output on EMC Fabric OS
- II. Configure RSA NetWitness Suite for Syslog Collection

Configure Syslog Output on EMC Fabric OS

You must complete these tasks to configure EMC Fabric OS:

- I. Configure EMC Fabric OS
- II. Configure Audit Logs for Event Classes

Configure EMC Fabric OS

To configure Fabric OS:

1. Connect to the switch as administrator.
2. To add the IP address, type:

```
syslogdIpAdd ip_address
```

where *ip_address* is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector
3. To verify the IP address, type:

```
syslogDIpShow
```
4. Ensure that the network is configured with a network connection between the switch and the remote host.

Configure Audit Logs for Event Classes

To configure an audit log for specific event classes:

1. To define the event classes to be filtered, type:

```
switch:admin> auditCfg --class variable
```

where *variable* is the audit filter you want.

Filter #	Audit Filter
1	ZONE
2	SECURITY

Filter #	Audit Filter
3	CONFIGURATION
4	FIRMWARE
5	FABRIC

Note: You can enter multiple variables separated by commas. For example,
switch:admin> auditcfg --class 2,4

2. To enable audit event logging based on the classes configured in step 1, type:

```
switch:admin> auditcfg --enable
```

Note: To disable the audit event configuration, use the **auditCfg --disable** command.

3. View the filter configuration to confirm that the correct event classes are being audited and that the filter is enabled. Type:

```
switch:admin> auditcfg --show
```

Configure RSA NetWitness Suite

Perform the following steps in RSA NetWitness Suite:

- Ensure the required parser is enabled
- Configure Syslog Collection

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 Suite Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Administration > 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 **fabricos**.



Configure Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > System**.
3. Depending on the icon you see, do one of the following:

- If you see  **Start Capture**, click the icon to start capturing Syslog.
- If you see  **Stop Capture**, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View > Config > Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.
The Event Categories panel displays the Syslog 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 either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.
The Add Source dialog is displayed.
7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.
Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Copyright © 2017 EMC Corporation. All Rights Reserved.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.