RSA NetWitness Platform

Event Source Log Configuration Guide

EMC Isilon

Last Modified: Tuesday, January 29, 2019

Event Source Product Information:

Vendor: EMC
Event Source: Isilon
Versions: 6.5.3.32, 6.5.5.7, 7.x, 8.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

Additional Download: nicsftpagent.conf.emcisilon

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: emcisilon
Collection Method: File, Syslog (7.1.1 and later)
Event Source Class.Subclass: Storage.Storage

To configure EMC Isilon, complete these tasks:

- Enable Protocol and Configuration Auditing on EMC Isilon
- Set up File Collection
- For versions 7.1.1 and later, you can collect access logs via Syslog
  - Configure EMC Isilon to send Syslog
  - Configure RSA NetWitness Platform for Syslog Collection

Enable Protocol and Configuration Auditing

To Enable Protocol and Configuration auditing on EMC Isilon:

1. Log onto the Administration interface for EMC Isilon with administrative privileges.
2. Go to **Cluster Management** > **Auditing**.
3. Under **Edit Settings**, select the following two boxes:
   - Enable Configuration Change Auditing
   - Enable Protocol Access Auditing
4. Under **Audited Zones**, ensure that at least one zone has been added.
5. Click **Save Changes**.

Set up File Collection

- Set Up the SFTP Agent
- Configure the Log Collector for File Collection

Set Up the SFTP Agent

To set up the SFTP Agent Collector, download the appropriate PDF from RSA Link:

- To set up the SFTP agent on Windows, see Install and Update SFTP Agent
- To set up the SFTP agent on Linux, see Configure SFTP Shell Script File Transfer

You can download the SFTP Agent sample file for EMC Isilon here: https://community.rsa.com/docs/DOC-45558. You need to edit the SFTP Agent sample file, updating the fields as follows:

```
#SILENT=false
PATH=/usr/xpg6/bin:/usr/xpg4/bin:/usr/css/bin:$PATH
RSA NetWitness Platform=<set this to the IP address of the RSA NetWitness Platform Log Decoder>
DATA_DIRECTORY=/var/log/
SA_DIRECTORY=/upload/emcisilon/<Directory name as specified in the SA UI>
PERSINFO_DIRECTORY=/usr/local/sa
TRANSFER_METHOD=SFTP
USERNAME=sftp
IDENTITY=~/.ssh/id_rsa
FILESPEC=audit_*.log
UPLOAD_SPEC=tmp
FLAG_REMOVE_FILE_AFTER_SEND=no
```

Note: For EMC Isilon version 6.5.3.32, and 6.5.5.7, set the Data Directory value as follows:

```
DATA_DIRECTORY=/var/log/:/var/log/audit
```

Configure the Log Collector for File Collection

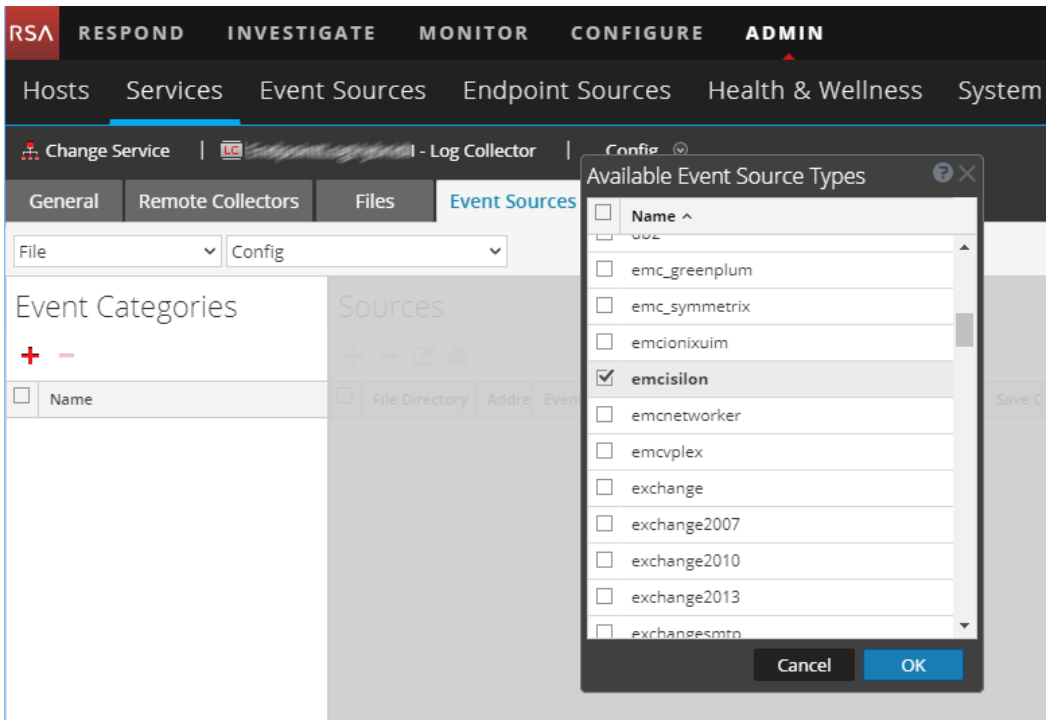
Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select **ADMIN > Services**.
2. In the Services grid, select a Log Collector, and from the Actions menu, choose **View > Config > Event Sources**.
3. Select **File/Config** from the drop-down menu.

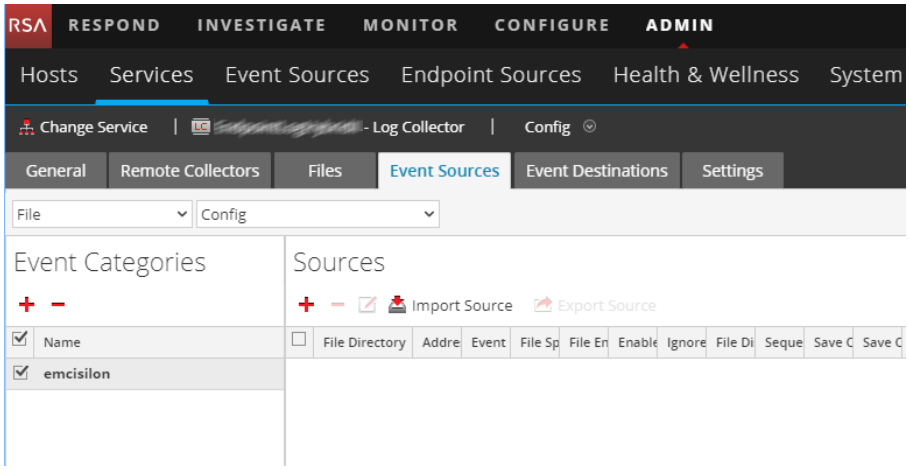
   The Event Categories panel displays the File event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.



5. Select **emcisilon** 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. Add a File Directory name, modify any other parameters that require changes, and click **OK**.

8. Stop and Restart File Collection. After you add a new event source that uses file collection, you must stop and restart the NetWitness File Collection service. This is necessary to add the key to the new event source.

Set up Syslog

Perform the following tasks to set up Syslog collection for EMC Isilon:

- Configure EMC Isilon to send Syslog
- Ensure the required parser is enabled
- Configure RSA NetWitness Platform for Syslog Collection

Configure EMC Isilon to send Syslog

Syslog collection is available only on EMC Isilon versions 7.1.1 and later.

To Enable EMC Isilon to send Syslog:

1. SSH to Isilon using administrative credentials.
2. Run the following command to enable protocol auditing, configuration auditing and syslog forwarding on the cluster:

   ```
   isi audit settings modify --config-auditing-enabled=yes
    --protocol-auditing-enabled=yes
   ```

3. Run the following command to enable Syslog forwarding for a Zone:

   ```
   isi zone zones modify zone_name --syslog-forwarding-enabled=yes
    --syslog-audit-events=all
   ```

   where ***zone_name*** is the name of the zone.

4. Update the Syslog Configuration to forward events:

   a. Find the `/etc/mcp/override/syslog.conf` file. If it does not exist, create it.

   b. Add or modify the following audit entries:

      ```
      !audit_protocol
      *.* @serverIP
      !audit_config
      *.* @serverIP
      ```

      where ***serverIP*** is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

   c. Save the file.

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 enabled:

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.

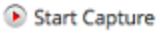
Note: The required parser is **emcisilon**.

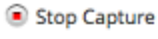
Configure RSA NetWitness Platform for Syslog Collection

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 

, click the icon to start capturing Syslog.
   - If you see 

, 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.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.