RSA NetWitness Logs

Event Source Log Configuration Guide

Oracle Solaris Basic Security Model (BSM)

Last Modified: Thursday, October 19, 2017

Event Source Product Information:

Vendor: Oracle
Event Source: Solaris Basic Security Model (BSM)
Versions: 8, 9, 10, 11
Additional Download: nicbsm.sh

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser:

- For File collection: solarisbsm
- For Syslog: solaris

Collection Method: File, Syslog
Event Source Class.Subclass: Host.UNIX

For Basic Security Model (BSM), RSA NetWitness Suite can use either File or Syslog collection. Perform the procedures that correspond to the collection method you prefer:

- Configure Solaris BSM for Syslog
- Configure Solaris BSM for File Collection

Configure Solaris BSM for Syslog

To configure the Solaris BSM event source for syslog collection, you must:

I. Configure Syslog Output on Solaris BSM

II. Configure RSA NetWitness Suite for Syslog Collection

Configure Solaris BSM to send Syslog messages to the RSA NetWitness Suite

Note: Syslog collection for Solaris BSM on RSA NetWitness Suite uses the **solaris** parser.

To configure Solaris BSM to send Syslog messages to RSA NetWitness Suite:

1. To determine what classes your Solaris BSM configuration uses, open the **audit_control** file located at `/etc/security/`. All classes are supported for archiving, but only the classes listed below are supported for reporting.

Name	Description
fw	file_write
fm	file_attr_mod
fc	file_creation
fd	file_deletion
ad	administrative actions: mount, exportfs, etc
lo	login_logout
ex	exec(2) system call
ua	user administration
ss	system state

Name	Description
na	Nonattributable events
aa	audit administration
as	system-wide administration

2. To edit the **audiit_control** file, follow these steps:
   a. Open the **audit_control** file located at `/etc/security/`.
   b. At the end of the file, type:

      `plugin: name=audit_syslog.so;p_flags=`*`classes`*

      where *classes* are the names of the classes of logs that you want to send to the RSA NetWitness Suite.

      Note: Separate the class names by commas.
3. To edit the **syslog.conf** file, follow these steps:
   a. Open the **syslog.conf** file located at `/etc/`.
   b. In the file, type:

      `audit.debug;*.err;kern.err;daemon.notice  @`*`remote_server`*

      where *remote_server* is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
4. To start the BSM module, go to `/etc/security/`, and run the following command:

   `./bsmconv`

   Note: You must restart the Solaris operating system.
5. To confirm that the auditing module is running, run the following command:

   `svcs auditd`
6. Click **Save Changes**.
7. To enable your settings, on the top right corner of the **Syslog Auditing** section, click **Enable**.

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 **solaris**.

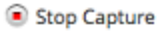
Configure Syslog Collection

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 

, 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.

Configure Solaris BSM for File Collection

To configure the Solaris BSM event source for File collection, you must:

I. Configure Solaris BSM to Generate Logs

II. If using SFTP, Configure the SFTP Agent

III. Configure RSA NetWitness Suite for File Collection

Configure Solaris BSM to Generate Logs

To configure Solaris BSM:

1. Open your BSM configuration in **/etc/security/audit_control** and **/etc/security/audit_users** to determine what classes your BSM configuration is using. All classes are supported for archiving, but only the classes listed below are supported for reporting purposes.

Name	Description
fw	file_write
fm	file_attr_mod
fc	file_creation
fd	file_deletion
ad	administrative actions: mount, exportfs, etc
lo	login_logout
ex	exec(2) system call
ua	user administration
ss	system state
na	Nonattributable events
aa	audit administration
as	system-wide administration

The server administrator must complete the following tasks to download and install the

nicbsm script on the Solaris server. The **nicbsm.sh** script extracts data from the BSM audit files, and transfers the data to RSA NetWitness Suite using SFTP or SCP.

a. Download the **nicbsm** script from RSA Link here: https://community.rsa.com/docs/DOC-58052.

b. Copy **nicbsm.sh** to the Solaris system. For example, **/usr/local/bin**.

c. Set execute permissions on **nicbsm.sh**. For example, **chmod 755 /usr/local/bin/nicbsm.sh**.\

d. Complete the following to modify the user configuration section of the **nicbsm.sh** script, and save the changes to the script:

Parameter	Value
ENVISION=	IP address of your RSA NetWitness Log Collector.
USERNAME= and **PASSWORD=**	Username and password for your NetWitness Suite FTP server. The default is **anonymous**. For SCP/SFTP, the username must be **nic_sshd** (the password setting will be ignored).
ROLL_LOGS=	**yes** (BSM must roll the log files in order for the script to convert the binary content into a readable format. This setting rolls the logs every time the script is run. No data is lost during this process.)
COMPRESS=	**no**
NIC_DIRECTORY=	Directory from which the script will run, for example `/usr/local/nic`. The script needs to track information about the log files it has processed, to avoid reprocessing data. The script maintains a list of processed files equal to the number of files in the source directory in a sub-folder of the directory defined by **NIC_DIRECTORY**.
ENVISION_DIRECTORY=	**SOLARIS_BSM_*1.2.3.4*** where ***1.2.3.4*** is the IP address of Solaris BSM.

Set up SFTP Agent

If you are using SCP or SFTP, set up the SFTP agent on Linux as described in the Configure SA SFTP Agent shell script PDF.

Configure the Log Collector for File Collection

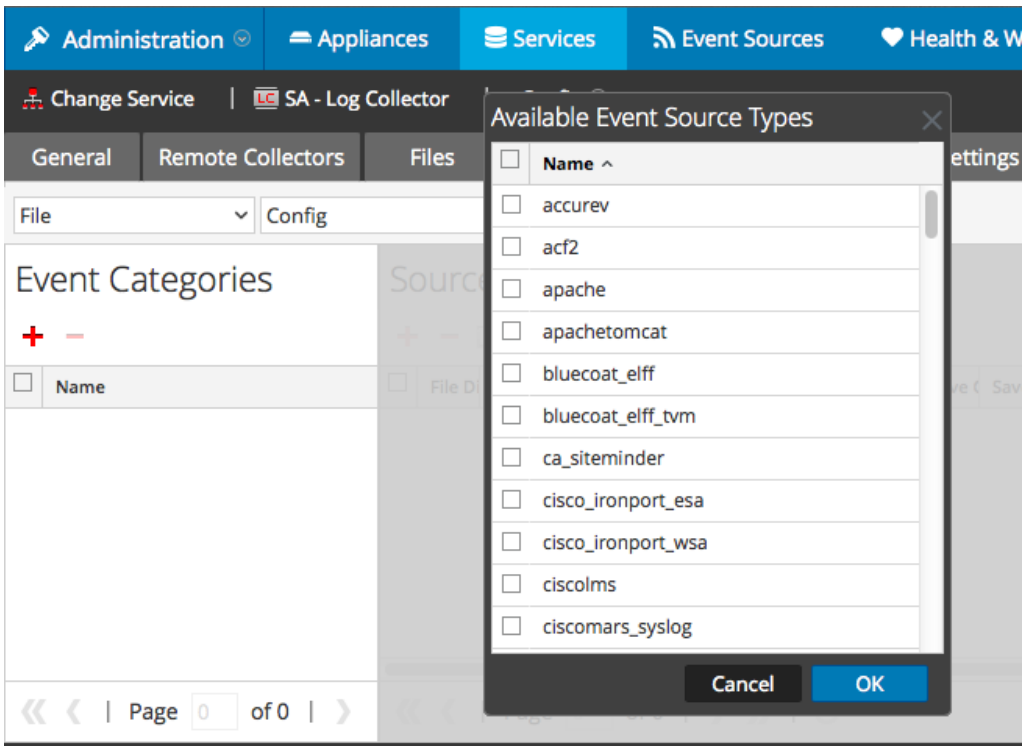
Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

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

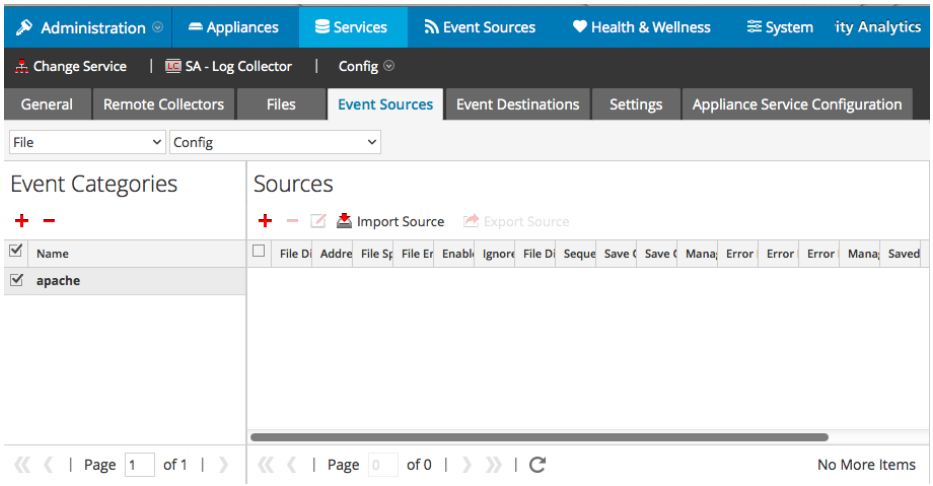


5. Select the correct type from the list, and click **OK**.

   Select **solaris_bsm** from the **Available Event Source Types** dialog.

   The newly added event source type is displayed in the Event Categories panel.

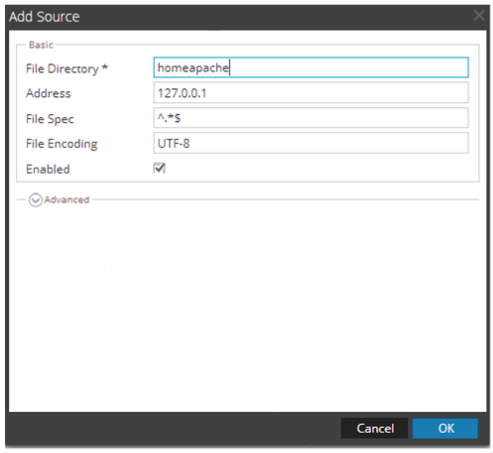
Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

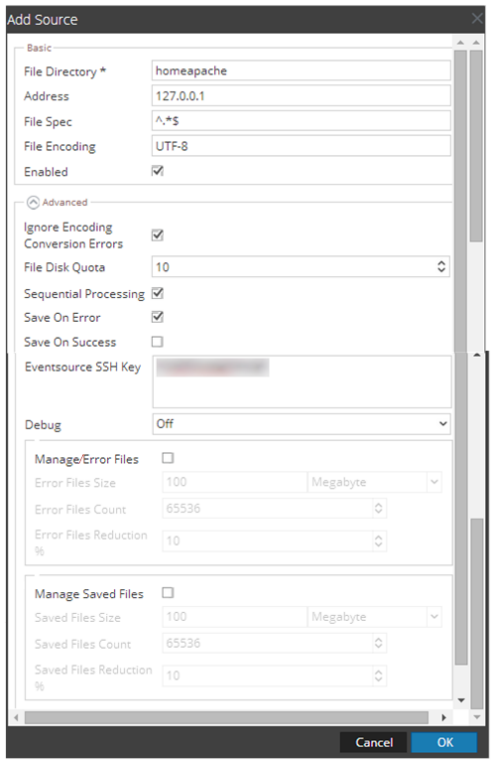


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.

   Note: Again, the image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.





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.

Trademarks