RSA NetWitness Logs

Event Source Log Configuration Guide

GlobalSCAPE Enhanced File Transfer (EFT) Server

Last Modified: Thursday, May 25, 2017

Event Source Product Information:

Vendor: GlobalSCAPE
Event Source: Enhanced File Transfer (EFT) Server
Versions: All versions up to 6.3.8
Platforms: Windows Server 2003, 2008 R2, XP Professional
Additional Download: sftpagent.conf.gseftserver

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: gseftserver
Collection Method: File
Event Source Class.Subclass: Host.Web Logs

GlobalSCAPE EFT Overview

The GlobalSCAPE Enhanced File Transfer Server is used to securely exchange files with remote locations. EFT Server is modular, and you can license individual components depending on your needs. The preferred deployment involves installing an optional DMZ Gateway on a separate server, which allows the EFT Server to remain behind the corporate firewall.

To configure GlobalSCAPE EFT Server to work with RSA NetWitness Suite, you must complete these tasks:

I. (Optional) Create a Web Site

II. Configure the Web Site for Transfers

III. Set Up the SFTP Agent

IV. Configure the Log Collector for File Collection

Create a Web Site

If you do not already have a web site for the EFT Server, you must create one. If you already have a web site, you can skip to the next section.

To create a web site:

1. On the GlobalSCAPE server, log on to the EFT Server administrator console.
2. In the navigation pane, right-click **LocalHost** and select **New Site**.
3. See the GlobalSCAPE documentation for details on how to create a new site.
4. Set up at least one user, so that you can configure the file transfer settings.

Configure the Web Site for Transfers

You can set the remote server files and folders, and view, start or stop the transfer queue. You can set the files and folders to monitor or queue for transfer. You first must log on to the web site that you created with the EFT Server console. For details on setting up remote files and queues, see your GlobalSCAPE EFT Server documentation.

Set Up the SFTP Agent

On the GlobalSCAPE event source, configure the SFTP Agent.

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 SA SFTP Agent shell script

The steps to set up the SFTP agent are described in the previous links. Note the following details:

- Save the SFTP configuration file as sftpagent.conf in the C:\NICsftpagent folder on the GlobalSCAPE EFT Server.
- Set the parameters of the files or directory to monitor. These parameters determine the path to where the logs are stored on the EFT Server. For example, if the IP address of your RSA NetWitness Log Collector is **172.16.0.51**, and your GlobalSCAPE EFT Server is at IP address **1.1.1.1**, and the logs are stored in `C:\ProgramData\GlobalSCAPE\EFT Server\logs`, then you should set the directory parameters as follows:

```
dir0=C:\ProgramData\GlobalSCAPE\EFT Server\Logs\
dir0.interval=5
dir0.compression=false
dir0.enabled=true
dir0.ftp=172.16.0.51,nic_sshd,publickey,GLOBALSCAPE_EFT_SERVER_
1.1.1.1
```

Configure the Log Collector for File Collection

This section describes steps you need to perform on RSA NetWitness Suite.

Configure the Log Collector for File Collection

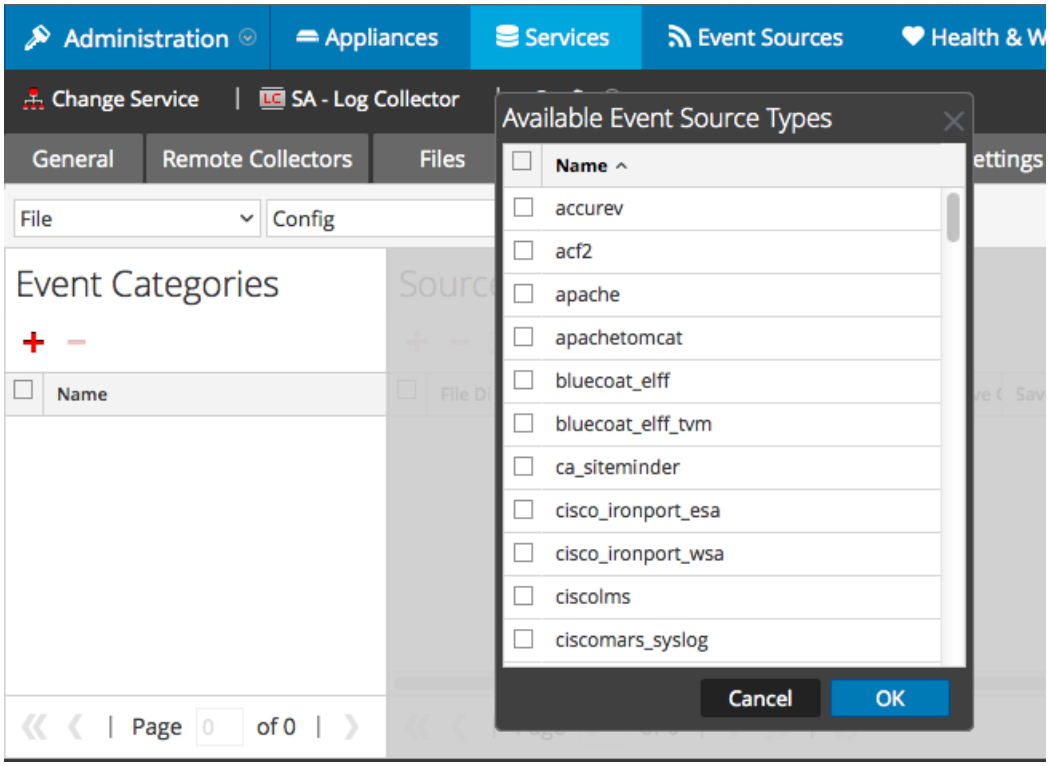
Perform the following steps to configure the Log Collector for File collection.

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 +.

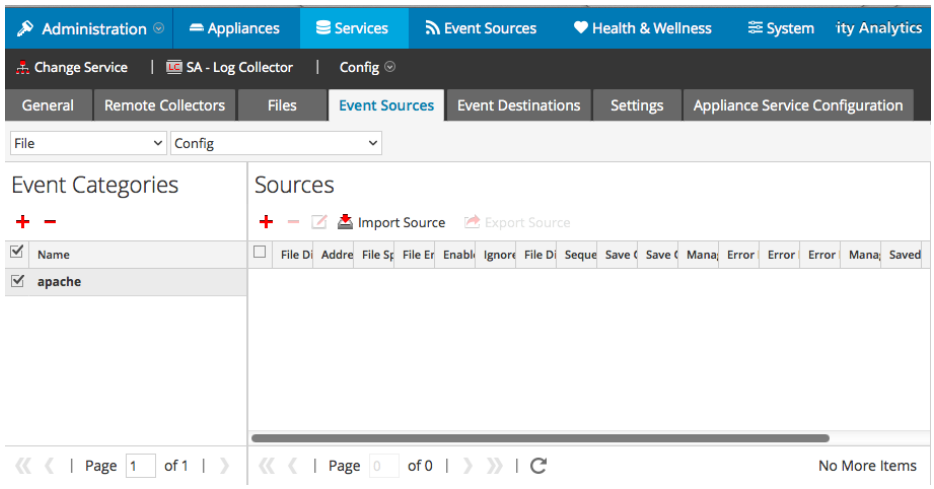
   The Available Event Source Types dialog is displayed.



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

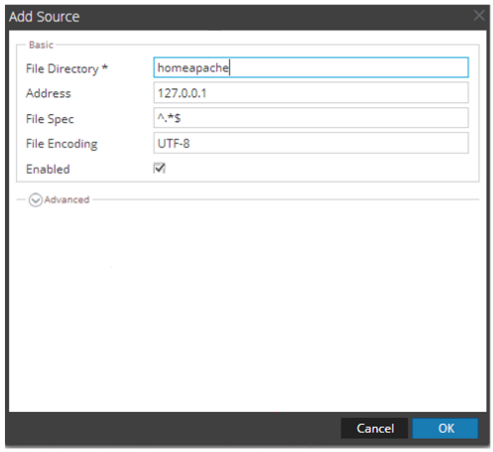
   Select **globalscape_eft_server** from the **Available Event Source Types** dialog.

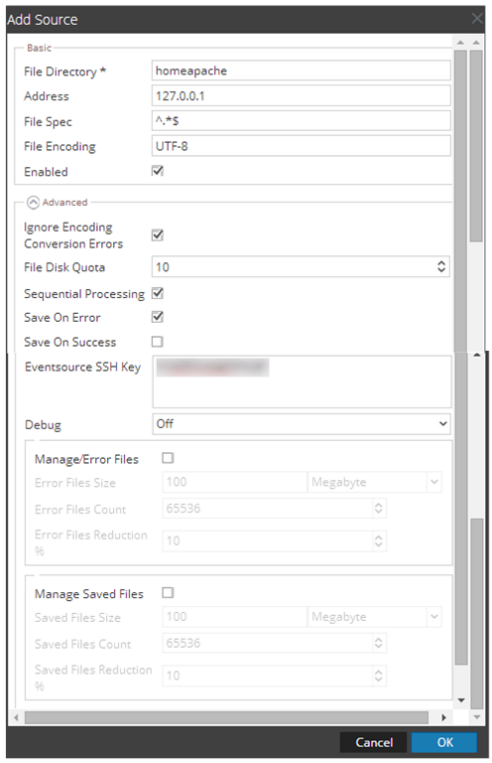
   The newly added event source type is displayed in the Event Categories panel.



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.

Trademarks