RSA NetWitness Platform

Event Source Log Configuration Guide

Blue Coat ProxySG SGOS

Last Modified: Tuesday, June 2, 2020

Event Source Product Information:

Vendor: Blue Coat Systems
Event Source: SGOS (Security Gateway Appliance)
Versions: 4.x, 5.x, 6.x, 7.x

Note: RSA supports the W3C Log format, and all minor versions of Blue Coat SGOS are expected to continue to support this format. Any deviation from this format, **or use of an older parser version**, may lead to unknown messages.

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parsers: cacheflowelff
Collection Method: File (using FTPS), Syslog
Event Source Class.Subclass: Host.Web Logs

The RSA NetWitness Platform supports two methods of log collection for the Blue Coat ProxySG SGOS event source:

- FTPS, for collecting access logs, and
- Syslog, for collecting access and event logs.

Note: To collect all messages from this event source, you must configure both File Reader and syslog collection.

Collect Access Logs using FTPS

FTPS is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols.

To collect the Blue Coat ProxySG SGOS access logs using FTPS, complete the following tasks:

I. Generate Certificates

II. Configure the FTP Server

III. Configure the Log Collector for File Collection

IV. Configure the Blue Coat ProxySG SGOS event source

Note: In addition to the steps below, there is a detailed document and video that walks through this process, as well as discussing possible issues with certificates. It is available in the RSA NetWitness Platform Community blog: Log Collector FTPS Configuration.

Generate Certificates

The certificates that you generate here are only used between the Blue Coat Proxy event source and the RSA NetWitness Platform.

On the Log Collector appliance, log on as the root user and create a directory to store the generated SSL certificates.

```
> cd
> rm -rf /root/vsftpd/*
> mkdir vsftpd && cd vsftpd
> chmod 0600 .
```

Note: When you generate the certificates, you can set any values you wish, or leave the defaults, for all fields except for the Common Name (CN) field. Ensure that the Common Name (CN) for the certificates is set to the IP address or hostname of the Log Collector service.

Generate your own Certificate Authority (CA) key and certificate, and enter the relevant details for the Certificate Authority:

```
> OWB_ALLOW_NON_FIPS=on openssl req -nodes -new -x509 -keyout ca.key.pem -
out ca.crt.pem -days 365
```

When prompted, enter values for the following parameters:

```
Country Name (2 letter code) [XX]:
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []: <IP address or hostname of the Log Collector>
Email Address []:
```

Generate vsftpd's key and a certificate signing request (CSR):

```
> OWB_ALLOW_NON_FIPS=on openssl req -nodes -new -sha256 -keyout vsftpd.key.pem -out vsftpd.csr.pem -days 365
```

When prompted, enter values for the following parameters:

```
Country Name (2 letter code) [XX]:
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:<IP address or hostname of the Log Collector>
Email Address []:
```

Choose a password for the CSR when prompted:

```
Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Next, sign vsftpd's CSR with your CA's private key:

```
> OWB_ALLOW_NON_FIPS=on openssl x509 -req -out vsftpd.crt.pem -in vsftpd.csr.pem -CA ca.crt.pem -CAkey ca.key.pem -CAcreateserial -days 365
```

Configure the FTP Server

Set the password for the upload user on the Log Collector by running the following command:

```
> passwd upload
```

Note: Make note of the password, as you need to enter it later in the configuration.

Edit the vsftpd service configuration file, located here: . Make the `/etc/vsftpd/vsftpd.conf`following changes:

1. The keys `rsa_cert_file` and `rsa_private_key_file` should point to the certificate and private key file generated and signed previously:

   ```
   rsa_cert_file=/root/vsftpd/vsftpd.crt.pem
   rsa_private_key_file=/root/vsftpd/vsftpd.key.pem
   ```

2. Set path of the `ca_certs_file` to the CA certificate generated previously:

   ```
   ca_certs_file=/root/vsftpd/ca.crt.pem
   ```

3. Ensure that both `require_cert` and `validate_cert` are set to **NO**. These two parameters are for client side certificates, which is disabled by default.

   ```
   require_cert=NO
   validate_cert=NO
   ```

   Note: Blue Coat ProxySG is unable to offer a client certificate when establishing the connection, so RSA must disable the client certificate checks.

4. Add the following line to the end of the file:

   ```
   require_ssl_reuse=NO
   ```

5. Save the file.

Restart the vsftpd service:

```
> service vsftpd restart
```

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:

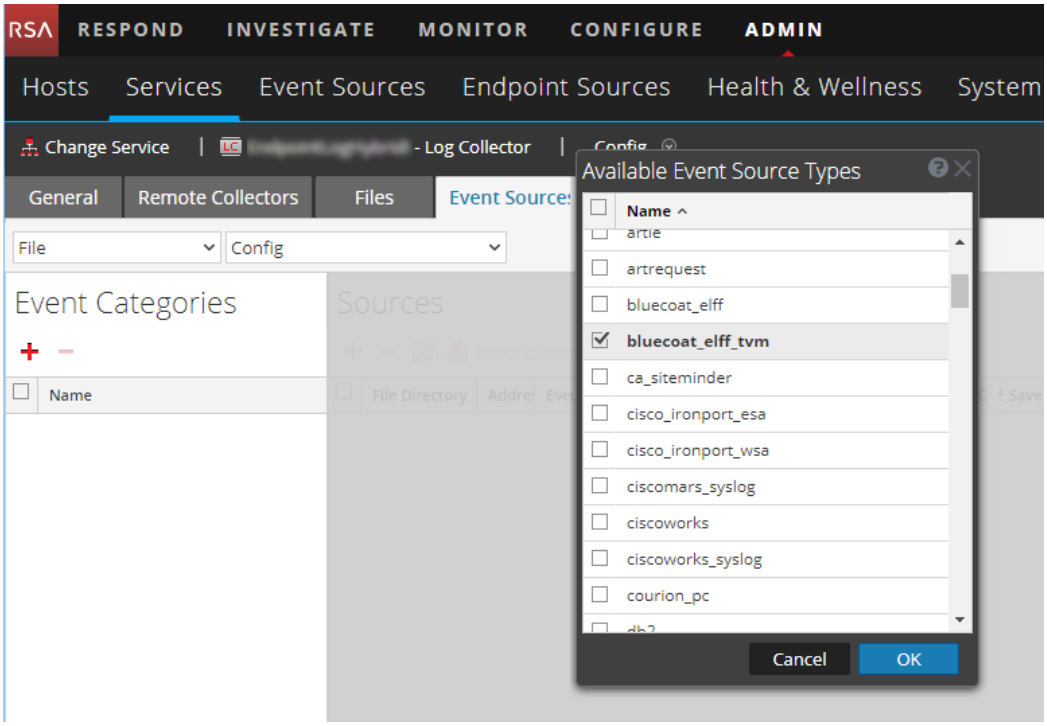
1. In the **NetWitness** menu, select **ADMIN** > **Services**.
2. In the Services grid, select a Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **File/Config** from the drop-down menu.

   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 **bluecoat_elff_tvm** from the list.



6. Click **OK**.

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

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

   The Add Source dialog is displayed.

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

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

Note: Choose a directory name, and make note of it, as the name is required later in the configuration. For example you can use **sgos**.

Configure the Blue Coat ProxySG SGOS event source

On the event source, you must configure SSL, logging, and upload. Optionally, you can also choose to export the ELFF logs to both RSA NetWitness Platform and Blue Coat Reporter simultaneously

To configure SSL:

1. Access the Blue Coat ProxySG web UI.
2. Navigate to **Configuration** > **SSL** > **CA Certificates**.
3. On the CA Certificates sub-tab, click **Import**.
4. Enter a name for the CA and paste the contents of **ca.crt.pem** (which you created earlier, when you generated certificates) into the text area.
5. Switch to the **SSL > CA Certificate List** sub-tab and select **browser-trusted**.
6. Click **Edit** and add the CA certificate to the list on the right.
7. Click **Apply**.

To configure logging:

1. Under the **Configuration** tab, select **Access Logging** > **Formats**.
2. Click **New** and enter **SA_FORMAT** as the **Format Name**.
3. Select **W3C Extended Log File Format (ELFF)**, and enter the following into the text box:

   ```
   date time time-taken c-ip s-action s-ip s-hierarchy s-supplier-name s-sitename cs-user cs-username cs-auth-group cs-categories cs-method cs-host cs-uri cs-uri-scheme cs-uri-port cs-uri-path cs-uri-query cs-uri-extension cs(Referer) cs(User-Agent) cs-bytes sc-status sc-bytes sc-filter-result sc-filter-category x-virus-id x-exception-id rs(Content-Type) duration s-supplier-ip cs(Cookie) s-computername s-port cs-uri-stem cs-version
   ```

   Note: If you cut and paste the above block of text, make sure to remove all line breaks.

4. Click **OK** and then **Apply**.

To configure upload:

1. Under **Access Logging** > **Logs**, select the **Logs** sub-tab.
2. Click **New** and complete the fields as follows:
   - Enter **SA_FORMAT** as the **Log Name**
   - Select **SA_FORMAT** as the **Log Format** from the drop-down list.
3. Select the **Upload Client** sub-tab and complete the fields as follows:
   - Select **SA_FORMAT** from the drop-down list at the top
   - Select **FTP Client** from the **Client Type** drop-down list
4. In the **Transmission Parameters** section, choose to **Save the log file as** a text file.
5. Click on **Settings** for the FTP Client above, and populate the fields in the new dialog as follows:
   - **Host:** enter the hostname or IP address of the Log Collector appliance
   - **Port:** enter `21`
   - **Path:** enter `/eventsources/bluecoat_elff_tvm/`**`directoryName`**

     where **directoryName** is the log file path created when you configured the Log Collector earlier.
   - **Username:** enter `upload`
   - Enter the password for the `upload` user; this is the password you entered earlier, when you configured the FTP server.
   - Enable **Use secure connections (SSL)**
   - Enable **Use PASV**
6. Click **OK** and then **Apply**.
7. To configure the upload interval, follow these steps:
   a. On the **Upload Schedule** tab, from the **LOG** drop-down list, select **SA_Format**.
   b. Under **Upload Type**, select **Periodically**.
   c. Under **Upload the Logfile**, select **Every**.
   d. In the **Hours** field, type **0**, and, in the **Minutes** field, type **1**.
   e. Click **Apply**.

Warning: : If you do not set the upload interval to one minute, RSA NetWitness Platform will improperly process the event source logs.

8. Repeat the steps 1 through 7 for **SA_Format**, **main**, and **im**.

(Optional) To export the ELFF logs to both RSA NetWitness Platform and Blue Coat Reporter simultaneously:

1. Open a browser and log on to the BlueCoat ProxySG appliance with administrative credentials.
2. Click the **Configuration** tab.
3. From the navigation pane, click **Policy** > **Visual Policy Manager**.
4. Click **Launch**.
5. Under the **Source** column, locate **Any**. In the **Any** row, right-click the corresponding value under the **Action** column, and select **Set**.
6. To create access logging objects, in the Set Action Object window, follow these steps:
   a. Click **New**, and from the list, select **Modify Access Logging**.
   b. Ensure that **Enable logging to** is selected, and from the drop-down list, select **SA_Format**.
   c. Click **OK**.
   d. Repeat steps **a**–**c** to create a second access logging object.
   e. Click **New**, and select **Combined Action Object**.
   f. In the Add Combined Action Object window, select **Allow**, and select both of the access logging objects that you created.
   g. Click **Add**, and click **OK**.

Collect Access and Event Logs Using Syslog

You can collect access and event logs using Syslog (either or both).

- Configure the Blue Coat ProxySG SGOS event source for event logging
- Configure the Blue Coat ProxySG SGOS event source for access logging
- Configure RSA NetWitness Platform for Syslog Collection

Configure Blue Coat ProxySG SGOS for Event Logging

Perform the following procedure to configure the Blue Coat event source to send event logs as Syslog formatted messages.

To enable event logging on the Blue Coat event source:

1. Open a browser and log on to the Blue Coat ProxySG appliance with administrative credentials.
2. Click the **Maintenance** tab.
3. From the navigation menu, click **Event Logging**.
4. Click the **Syslog** tab.
5. In the **Loghost** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
6. Ensure that **Enable syslog** is selected.
7. Click **Apply**.
8. Click the **Level** tab, and ensure that all of the event logging levels are selected.
9. Click **Apply**.

Configure Blue Coat ProxySG SGOS for Access Logging

Perform the following procedure to collect access logs using Syslog collection.

To enable access logging via Syslog on Blue Coat ProxySG:

1. Open a browser and log on to the Blue Coat Management console.
2. On the **Configuration** tab, in the navigation pane, click **Access Logging** > **Format** and click **New**.
3. Enter a Format Name, for example **syslog_custom**.
4. Select the **Custom format string (specify below)** option.
5. In the text box next to **Test Format**, enter the log format:
   - To get all of the available fields, enter the following:

```
<133>%%CACHEFLOWELFF_
syslog:date=\"$(date)\",time=\"$(time)\",time-taken=\"$(time-
taken)\",c-ip=\"$(c-ip)\",s-action=\"$(s-action)\",s-
ip=\"$(s-ip)\",s-supplier-name=\"$(s-supplier-name)\",s-
sitename=\"$(s-sitename)\",cs-user=\"$(cs-user)\",cs-
username=\"$(cs-username)\",cs-auth-group=\"$(cs-auth-
group)\",cs-categories=$(cs-categories),cs-method=\"$(cs-
method)\",cs-host=\"$(cs-host)\",cs-uri=\"$(cs-uri)\",cs-uri-
scheme=\"$(cs-uri-scheme)\",cs-uri-port=\"$(cs-uri-
port)\",cs-uri-path=\"$(cs-uri-path)\",cs-uri-query=\"$(cs-
uri-query)\",cs-uri-extension=\"$(cs-uri-extension)\",cs
(Referer)=\"$(cs(Referer))\",cs(User-Agent)=\"$(cs(User-
Agent))\",cs-bytes=\"$(cs-bytes)\",sc-status=\"$(sc-
status)\",sc-bytes=\"$(sc-bytes)\",sc-filter-result=\"$(sc-
filter-result)\",sc-filter-category=\"$(sc-filter-
category)\",x-virus-id=\"$(x-virus-id)\",x-exception-
id=\"$(x-exception-id)\",rs(Content-Type)=\"$(rs(Content-
Type))\",duration=\"$(duration)\",s-supplier-ip=\"$(s-
supplier-ip)\",cs(Cookie)=\"$(cs(Cookie))\",s-
computername=\"$(s-computername)\",s-port=\"$(s-port)\",cs-
uri-stem=\"$(cs-uri-stem)\",cs-version=\"$(cs-version)\"
```

     Warning: In the above text, the hyphen (-) at the end of line 6 **is necessary**. Be aware that when you cut and paste the text, it may disappear: if so, you must re-insert it.

   - Alternatively, the log format can be customized according to your requirements. The log format should begin with the following:

```
<133>%%CACHEFLOWELFF_syslog:
```

Note: You must select **cs-method**. All other selections are optional. Any combination of the available field formats can then be appended to the log format, with each being separated by a comma. For details about the available fields, see the Blue Coat Systems SGOS Administration Guide.

6. Click **Test Format** to ensure that the defined format is valid.
7. Under **Multiple-valued header policy**, select **Log last header**.
8. Click **OK** and then **Apply** to save the changes,
9. On the **Configuration** tab click **Access Logging** > **Logs** and click **New**.
10. Enter a Format Name, for example **syslog**.
11. Under **Log Format**, select the log format previously defined (e.g. **syslog_custom**) and click **OK** and **Apply**.
12. In the **Upload Client** tab, choose **syslog** from the drop-down menu and select **Custom Client** from the Client Type list.
13. Click **Settings** and enter the following:
    - Enter the IP address of the RSA NetWitness Platform Log Decoder in the **Host IP** field.
    - Enter 514 in the **Port** field.
14. Click **OK**.
15. Under the **Upload Schedule** tab, choose to upload the access log **continuously** and click **Apply** to save the changes.
16. Under the **Access Logging** > **General** tab, select the **HTTP** protocol and click **Edit**.
17. Select the logging policy previously defined (e.g. **syslog**) and **Apply** the changes.

Configure RSA NetWitness Platform for Syslog Collection

To collect the event logs, make sure RSA NetWitness Platform has been configured for 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 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.

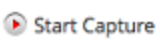
Note: The required parser is **cacheflowelff**.

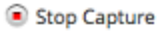
Configure Syslog Collection

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 **ADMIN** > **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 **ADMIN** > **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.

After 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.