Log Export

https://campus.barracuda.com/doc/79462622/

Barracuda WAF-as-a-Service generates various types of logs, as described in Log Retention and Location. The Log Export component enables you to export these logs in real time via the Syslog protocol or Azure event hubs. You can then stream the data from Azure event hubs to SIEM (Security Information and Event Management) tools, like Splunk, ArcSight, and others.

Before You Begin

Regardless of how you will export your logs, be sure to allow the source IPs for the export logs, as described in Restricting Direct Traffic.

- 34.227.174.172
- 40.71.30.40

Choose one of the following methods to export logs:

- Exporting to Syslog
- Exporting to Azure Event Hubs

Exporting to Syslog

Preparing to Export Logs

To export logs, you must have a Syslog server. You can set up your own server or use a server provided by a cloud service.

- If you are running syslog on a UNIX machine, be sure to start the syslog daemon process with the -r option so it can receive messages from external sources.
- Windows users require additional software when using syslog, because the Windows OS does not include the syslog capability. There are many syslog solutions available, both free and commercial, including Kiwi Syslog.
- If you are using a cloud service, they will provide you with the server hostname, port, and protocol. Barracuda WAF-as-a-Service can export logs via UDP, TCP, or SSL protocols.

Syslog Facility

Syslog receives different types of log messages. To differentiate and store them in distinct log files, log messages contain a logging priority and a logging facility, in addition to the actual message and IP address.

There are eight facility options. All log messages are marked with one of the facility options, labeled **local0** through **local7**. By default, each syslog server is marked with **local0**.

For each configured syslog server, you can associate a specific facility with each log type, so your syslog server can segregate the log of each type into a different file.

See the instructions below for setting a facility option.

> You can set the same facility for both Firewall Logs and Access Logs.

Severity Level

You can set the severity level to export firewall logs and system logs to the configured export log server(s). Barracuda WAF-as-a-Service severity levels, listed from greatest to least severity, are:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice – Default setting
- Information
- Debug

Notice is the default setting, indicating normal, but significant conditions.

Barracuda WAF-as-a-Service exports logs based on the selected severity level. For example, if you set the severity to **Critical**, then logs with a severity level of **Critical** and above (that is, **Emergency**, **Alert**, and **Critical**) are all sent to the external log server.

Configuring Export Log Information

1. Within Barracuda WAF-as-a-Service, open the application. In the left navigation panel, select **Log Export**.
2. Click **Add Export Log Server**.
3. In the **Add Export Log Server** page, specify the following information:

- **Name** – Enter a name for the new setting.
- **Log Server Type** – Select **Syslog NG**.
- **Server Address and Port** – Add the IP address or Hostname and Port for the external log server. The port is automatically entered based on your selection in **Connection Type** below.
- **Connection Type** – Select how you will connect with the external log server. Based on your selection, the appropriate port is automatically entered in the **Server Address and Port** field, located directly above.
- **Syslog Header** – Select a standard header or select Custom to specify your own header.
- **Firewall Logs** – Specify the export format for Firewall Logs. This typically matches the type of logging server to which you are exporting logs. If you do not see your log type listed, select **Custom** and enter your own format. See below for the format specifier. If you do not want to export Firewall Logs, select **Do Not Export**.
- **Severity** – Select the severity for log events you want to export. Events with that severity, and higher levels of severity, are exported. The default setting is **Notice**, described above.
- **Facility** – Specify where you want to store the log file, so logs are kept separate and are easy to retrieve. See more about facilities in the section above.
- **Event Logs** – Specify the export format for Event Logs. This typically matches the type of logging server to which you are exporting logs. If you do not see your log type listed, select **Custom** and enter your own format. See below for the format specifier. If you do not want to export Firewall Logs, select **Do Not Export**.
- **Facility** – Specify where you want to store the log file, so logs are kept separate and are easy to retrieve. See more about facilities in the section above.

4. Click **Add** to add the above settings.

Exporting to Azure Event Hubs

To use Azure Event Hubs, contact Barracuda Support.

Configuring Export Log Information for Azure Event Hubs

Exporting log data to Azure event hubs enables you to analyze that data with third party SIEM (Security Information and Event Management) tools. For more information, refer to this Microsoft document, Stream Azure monitoring data to an event hub or external partner.

1. Within Barracuda WAF-as-a-Service, open the application. In the left navigation panel, select **Log Export**.
2. Click **Add Export Log Server**.
3. In the **Add Export Log Server** page, specify the following information:
   - **Name** – Enter a name for the new setting.

- **Log Server Type** – Select **Azure Event Hubs**.
- **Event Hub Name** – Specify the name of your Azure event hub.
- **Service Bus Name** – Specify the name of the service bus for your Azure event hub.
- **Policy Name** – Specify the policy name for your event hub.
- **Policy SAS Key** – Specify the Microsoft Azure event hub SAS key value.
- **Send Traffic Logs** – Enable to export traffic logs.
- **Send WAF Firewall Logs** – Enable to export Barracuda Web Application Firewall logs.
- **Send WaaS Event Logs** – Enable to export Barracuda WAF-as-a-Service event logs.

4. Click **Add** to add the above settings.

Log information is automatically sent to your Azure event hub, and beyond if you choose.

Export Log Formats

When defining your own custom format, use the following strings to insert various fields of the log entry in the output:

Web Firewall Logs	Access Logs
%ai - Application IP	%ai - Application IP
%ap - Application Port	%ap - Application Port
%at - Action Taken	%au - Authenticated User
%ad - Attack Description	%br - Bytes Received
%adl - Attack Details	%bs - Bytes Sent
%ag - Attack Group	%ch - Cache Hit
%aid - Attack ID	%cu - Certificate User
%au - Authenticated User	%ci - Client IP
%ci - Client IP	%cp - Client Port
%cp - Client Port	%c - Cookie
%fa - Follow-up Action	%ct - Content Type
%seq - Log ID	%cs1 - Custom Header 1
%lt - Log Type	%cs2 - Custom Header 2
%m - Method	%cs3 - Custom Header 3
%p - Protocol	%h - Host
%px - Proxy IP	%s - HTTP Status
%pp - Proxy Port	%id - Login ID
%r - Referer	%seq - Log ID
%ri - Rule ID	%lt - Log Type

%rt - Rule Type	%m - Method
%sid - Session ID	%p - Protocol
%sl - Severity Level	%pf - Protected Field
%t - Time Stamp	%px - Proxy IP
%u - URL	%pmf - Profile Matched Field
%ua - User Agent	%pp - Proxy Port
%un - Unit Name	%q - Query
	%r - Referer
	%rtf - Response Type Field
	%sid - Session ID
	%si - Server IP
	%sp - Server Port
	%st - Server Time
	%t - Time
	%tt - Time Taken
	%u - URL
	%ua - User Agent
	%un - Unit Name
	%uid - Unique ID
	%v - Version
	%wmf - WF Matched
	%tarc - Epoch/Unix Time Stamp
	%ta - American Standard Format Timestamp
	%cfp - Client Fingerprint
	%rrs - Request Risk Score
	%crs -Client Risk Score