How to Configure Syslog and other Logs

https://campus.barracuda.com/doc/21364919/

You can add up to three syslog servers to receive logs from the Barracuda Load Balancer ADC. To differentiate the logs so they can be stored in distinct files on the syslog server, you can assign different log facilities to them. :

For each configured syslog server, you can associate a specific facility (default = local0) with each log type, so your syslog server can segregate the log of each type into a different file.

Prerequisites

If you are running syslog on a UNIX machine, start the syslog daemon process with the `-r` option so that it can receive messages from external sources. Windows users require additional software to use syslog because the Windows OS does not include the syslog capability. Kiwi Syslog is a popular solution, but there are many free and commercial options available.

Syslog messages are sent over UDP/TCP/SSL ports. If there are any firewalls between the Barracuda Load Balancer ADC and the syslog servers, ensure that the respective port is open on the firewalls.

Add a Syslog Server

To add a syslog server:

1. Go to the **ADVANCED > Export Logs** page.
2. In the **Syslog** section, click **Add Syslog Server**.
3. In the **Add Syslog Server** window, configure the settings for connecting to and sending logs to the syslog server.
   If you want the Barracuda Load Balancer ADC to present a certificate when it connects to a syslog server, ensure that you upload the certificate on the **BASIC > Certificates** page. For more information on how to upload a certificate, see How to Add an SSL Certificate.
4. Click **Add**. The server appears in the **Syslog** table.

Configure Syslog Facilities

The local0 to local7 facilities are available for each log type. You can select a different facility for each

log or select the same facility for all logs.

To select a syslog facility for each log type:

1. Go to the **ADVANCED > Export Logs** page.
2. In the **Syslog** section, click **Syslog Settings**.
3. In the **Syslog Settings** window, select a facility (Local0 to Local7) for each log type and click **Save Changes**.

Configure Log Levels

You can specify the minimum priority of the logs that you want to send for a module to the syslog server. By default, the log level for modules is set to *0-Emergency*. Note that the lower the level, the higher the priority and the more attention that the log entry demands. For example, log levels 0-Emergency and 1-Alert have the highest priority and demand more immediate response than 5-Notice or 6-Information.

1. Ensure that **Advanced Settings** are enabled. Go to the **ADVANCED > System Configuration** page, and ensure that **Advanced Settings** is set to **Yes**.
2. Go to the **ADVANCED > Export Logs** page.
3. In the **Module Log Levels** section, enter a name for the log level, select the module, and select the log level for the module. You can also enter comment about the new setting.
4. Click **Add**.

Configure Log Formats

You can configure the format of the logs that are sent to the syslog server. You can use the default log format, select a predefined format, or edit custom format.

> Depending upon the configuration, the IP address of a service, client IP address, or server IP address can be either IPv4 or IPv6.

1. Go to the **ADVANCED > Export Logs** page.
2. In the **Logs Format** section, select a format for the log. For more information on how you can edit customized formats, see the online help.
3. Click **Save**.

Table of Log Formats

The following table describes the names and values for each logs:

System Logs	Web Firewall Logs	Access Logs	Audit Logs
%ei - Event ID	%ai - Application IP	%ai - Application IP	%add - Additional Data
%ll - Log Level	%ap - Application Port	%ap - Application Port	%an - Admin Name
%ms - Message	%at - Action Taken	%au - Authenticated User	%cht - Change Type
%md - Module Name	%ad - Attack Description	%br - Bytes Received	%ct - Client Type
%t - Time Stamp	%adl - Attack Details	%bs - Bytes Sent	%cn - Command Name
	%ag - Attack Group	%ch - Cache Hit	%seq - Log ID
	%aid - Attack ID	%cu - Certificate User	%li - Login IP
	%au - Authenticated User	%ci - Client IP	%lp - Login Port
	%ci - Client IP	%cp - Client Port	%lt - Login Type
	%cp - Client Port	%c - Cookie	%nv - New Value
	%fa - Follow-up Action	%ct - Content Type	%on - Object Name
	%seq - Log ID	%cs1 - Custom Header 1	%ot - Object Type
	%lt - Log Type	%cs2 - Custom Header 2	%ov - Old Value
	%m - Method	%cs3 - Custom Header 3	%t - Time Stamp
	%p - Protocol	%h - Host	%tri - Transaction ID
	%px - Proxy IP	%s - HTTP Status	%trt - Transaction Type
	%pp - Proxy Port	%id - Login ID	%un - Unit Name
	%r - Referer	%seq - Log ID	%var - Variable
	%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	
		%rr - Request Referer	

		%rtf - Response Type Field	
		%sid - Session ID	
		%si - Server IP	
		%sp - Server Port	
		%st - Server Time	
		%t - Time Stamp	
		%tt - Time Taken	
		%u - URL	
		%ua - User Agent	
		%un - Unit Name	
		%v - Version	
		%wmf - WF Matched Field	