

Enabling Syslog from Linux Device

<https://campus.barracuda.com/doc/98217233/>

Please follow the steps below to enable logging of syslog error messages on a Unix or Linux based device.

To log from a Unix system, edit the system's syslog daemon config file, as described below for most common loggers.

First, determine which System Logger is your system using by running the following command:

```
Is -d/etc/*syslog*
```

Depending on which file is displayed, please follow these instructions below.

rsyslog.conf

rsyslog is often seen on Debian, Fedora, SuSE, Ubuntu and most other Linux distributions.

1. As root, edit /etc/rsyslog.conf or /etc/syslog.conf. Add this line at the end of the file:
*. * @ (IP OR DNS NAME OF ONSITE MANAGER)
2. Tell rsyslog to activate the change (on most OS's):
sudo killall -HUP rsyslog rsyslogd
On Ubuntu:
sudo service rsyslog restart

Log messages should begin to be sent to the Onsite Manager.

syslog-ng.conf

syslog-ng is often seen on Gentoo 2005.0+ and SuSE 9.3+.

1. Configure syslog-ng
As root, edit /etc/syslog-ng.conf . Find a line starting with source. For example: source s_sys { .. }.
At the end of the file, paste this configuration. Replace s_sys with the source name above, typically s_sys, src, s_all, or s_local:
destination d_onsitemanager {
 udp ("IP OR DNS NAME OF ONSITE MANAGER" port (514));
};
replace "s_sys" with the name you found:
Log { source (s_sys); destination (d_onsitemanager); };- 2. Tell syslog-ng to activate the change:
sudo killall -HUP syslog-ng

Log messages should begin transmitting to the Onsite Manager.

syslog.conf

syslogd and syslogd are often seen on BSDs, CentOS, Gentoo 2004.3 and older, Mac OS X, RHEL Slackware, Solaris and most other Unices.

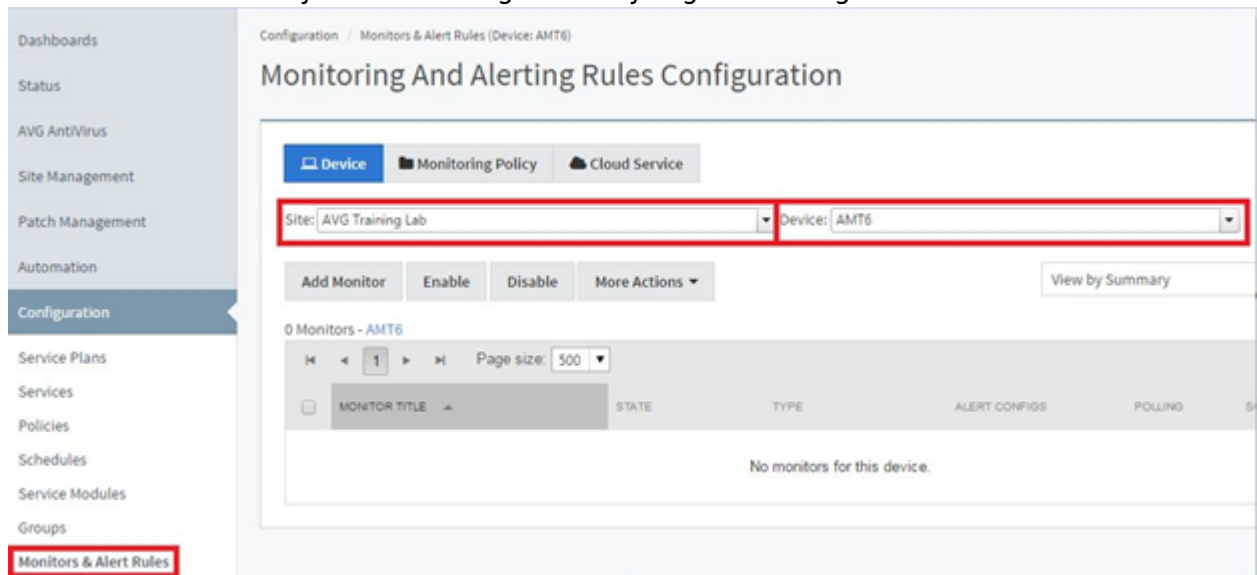
remote_syslog can also be used in lieu of syslogd.

1. As root, edit /etc/syslog.conf with a text editor (like pico or vi). Paste this line at the end of the file:
*. * @(IP OR DNS OF ONSITE MANAGER)
2. Tell syslog to activate the change (on most OS's):
`sudo killall -HUP syslog syslogd`

Log messages should begin transmitting to the Onsite Manager.

Configure Monitoring in Barracuda RMM.

1. Open **Configuration > Monitors and Alert Rules**.
2. Search for the device you are wanting to add syslog monitoring for.



3. Click **Add Monitor**, Select **Syslog Messages**, then click **Add Monitor**.

Choose monitor type

Bandwidth ▼

Add Monitor Cancel

Page size: 50 ▼

gabytes - C:

gabytes - E:

Space - C:

Space - E:

Bandwidth

Custom Logs

Device Availability

Device Warranty

MBSA Reports

Network Services

Patch Status

Performance Counters

SCE

SNMP Traps

Syslog Messages

Windows Events

Windows Services

4. Fill in a **Title**, and optionally a **Description**.
5. Choose the appropriate **Facility** and **Severity**. Optionally a **Syslog Message** if required.

Monitoring Rule

Title:

Description:

☒ Enabled

Syslog Rule

Facility: (All) ▼

Severity: (All) ▼

Syslog Message:

0 of 255 characters

6. Click **Alert**, give it a title. Optionally, add a description. Click **Add** under alert rules. Enter in the **Facility**, **Severity**, and optionally **Text** to contain or not contain within the alert.

Syslog Rule Parameters

Facility:	Equal To ▼	0 - kernel messages ▼
Severity:	Equal To ▼	Error ▼
Text:	All ▼	<div></div> <div>0 of 255 characters</div>

7. Fill out the actions to perform when the alert is triggered
8. Click **Save**.

Figures

1. linux1.png
2. linux2.png
3. linux3.png
4. linux4.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.