Adding a Monitor for Syslog Messages

https://campus.barracuda.com/doc/90443502/

A **Syslog Messages** monitor checks information in log messages across IP networks. **Syslogs** are sent by many operating systems and infrastructure devices, most notably **Unix**-based systems and security devices.

As with **SNMP traps**, **syslog messages** are the logical equivalent to an alert from the vendor's perspective and are sent from the device to Onsite Manager.

> You must understand how the device is sending the exact message you want to capture. It's a good idea to capture all **syslogs** for a period of time if documentation about the **syslogs** is not available. For more information, contact the device vendor or search their knowledgebase.

Syslog Facilities:

- **All**
- **kernel messages**
- **user-level messages**
- **system daemons**
- **security/authorization messages**
- **messages generated internally by syslogd**
- **line printer subsystem**
- **network news subsystem**
- **UUCP subsystem**
- **CRON facility**
- **clock daemon**
- **security/authorization messages**
- **FTP daemon**
- **NTP subsystem**
- **log audit**
- **log alert**
- **local use 0 - local use 7**

> Syslog facilities are case-sensitive, as per the original RFC based on Berkeley Style Distributions of Unix.

Syslog Severity:

- **All**

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Informational**
- **Debug**

What You Can Do

You can

- collect information about **Unix** systems and applications they host
- receive critical security information from firewalls

The **Syslog Messages** monitors only function correctly if Onsite Manager has been defined as a **Syslog Message** receiver on the devices being monitored.

To add a monitor for Syslog Messages

1. In Service Center, click **Configuration** > **Monitor & Alert Rules**.
2. From the **Site** list, select the site where the device is located.
3. From the **Device** list, select the device to which you want to add a monitor.
4. Click **Add Monitor**.
5. Select **Syslog Messages** from the list.
6. Click **Add Monitor**.
7. In the **Monitor** tab, type a title for the monitor.
8. Optionally, type a description for the monitor.
9. Ensure the **Enabled** check box is selected.
10. Select a **Facility** from the drop-down list.
11. Select a **Severity** from the drop-down list.
12. Type part of a syslog message in the **Syslog Message** box.
13. To configure an alert, see Setting Alert Actions.
14. Click **Save**.

    If you selected **All** from the **Facility** or **Severity** lists, a warning message may appear informing you of the possible impact on storage costs, due to the large amount of data storage required. You must click **Yes** to continue adding the **Syslog Messages** monitor.