Adding a Monitor for Custom Log Files

https://campus.barracuda.com/doc/90443564/

A **Custom Log File** monitor parses text files for content that you specify, and raises an alert if the character string is found inside the file. You can specify whether the case or whole word must be found, and you can use regular expressions to add power and flexibility to the search.

> **Custom Log File** monitors cannot be added to monitoring policies.

When to Use

Custom Log File monitors are useful when you encounter applications that do not expose their status by any other means. When this occurs, typically applications continue appending to text logs to record status events for use during troubleshooting.

Additionally, custom logs present a significant opportunity for you to design your own solutions when combined with Barracuda Managed Workplace's scripting. Partners without development resources available will still have technicians capable of creating batch files that pipe results to a text file.

To add a monitor for Custom Logs

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. From the **Choose Monitor Type** list, select **Custom Logs**.
6. Click **Add Monitor**.
7. In the **Monitor** tab, type a **title** for the monitor.
8. Optionally, type a **description** for the monitor.
9. In the **Custom Log Monitor** section, type the full **UNC** path to the log file in the **File Path** box. For example, **`\\ComputerName\SharedFolder\Resource.`**
   > The log file must be accessible via **UNC** path from Onsite Manager. Network-mapped drives are user specific and are not accessible to Windows Services.
10. If authentication is required to access the log file, in the **Authentication** section, do the following:
    1. Type a logon name in the **User Name** box.
       The user can be a local or a **Domain** user (defined with **Domain\User**) providing the user has read access to the log file.
    2. Type the associated password in the **Password** box.
11. In the **Search String** box, type the search values (either as a text string or using regular expressions).
12. If desired, do one of the following:

- To return only similarly cased entries in the log, select the **Match Case** check box.
- To prevent finding the search string contained in another word, select the **Match Whole Word** check box.
- To use regular expressions in the **Search String** box, select the **Use Regular Expressions** check box.

13. To configure an alert, see Setting Alert Actions.
14. Click **Save**.