Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring NGINX Web Server to Forward Logs to EventTracker

Publication Date:

November 11, 2021

Abstract

This guide provides the instructions to retrieve the NGINX **Web Server** events via remote syslog on the Linux operating system, and Log Filter Monitor on the Microsoft Windows operating system. After the logs start coming into EventTracker, the reports, alerts, and saved searches can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or above and NGINX **Web Server.**

Audience

Administrators who are assigned the task to monitor the NGINX **Web Server** events using EventTracker.

Table of Contents

1. Overview

The NGINX is a web server that can also be used as a reverse proxy, load balancer HTTP cache, and a generic TCP/UDP proxy server.

EventTracker helps to monitor events from the NGINX Web Server. Its dashboard and reports will help you track the user requests which are suspicious with reference to SQL injection, access logs with a bad request, and user requests which are suspicious with reference to Cross-Site Scripting.

2. Prerequisites

- **EventTracker v9.3** or **above** should be installed.
- A user with administrator access to make configuration changes on the NGINX Web Server.
- Port should be allowed in the firewall (Port 14505).
- Administrative access on EventTracker.

3. Configuring NGINX Web Server to Forward Logs to EventTracker

The NGINX Web Server can be integrated with EventTracker by forwarding via remote syslog on the Linux operating system, and Log Filter Monitor on the Microsoft Windows operating system to the EventTracker Manager.

3.1 Forwarding syslog data to EventTracker for Linux Operating System

Configuring nginx.conf

1. Edit the nginx.conf file using the following command:
   vi /etc/nginx/nginx.conf

2. In the nginx.conf file scroll to the **logging settings** and add the following lines.
   access_log syslog:server=Eventracker_server_IP:514,facility=local7,tag=nginx;
   error_log syslog:server=Eventracker_server_IP:514,facility=local7,tag=nginx;

3. Save and exit.

```
##
# Logging Settings
##

access_log syslog:server=192.168.1.230:514,facility=local7,tag=nginx;
error_log syslog:server=192.168.1.230:514,facility=local7,tag=nginx;
```

Configuring rsyslog.conf

1. Edit the rsyslog.conf file using the following command:
   vi /etc/rsyslog.conf

2. In the rsyslog.conf file scroll to the bottom and add the following line.
   local7.debug /var/log/nginx/access.log; RemoteFormat
   local7.debug /var/log/nginx/error.log; RemoteFormat

3. Save and exit.

4. Restart the rsyslog services by running the following command:
   Sudo /etc/init.d/rsyslog restart

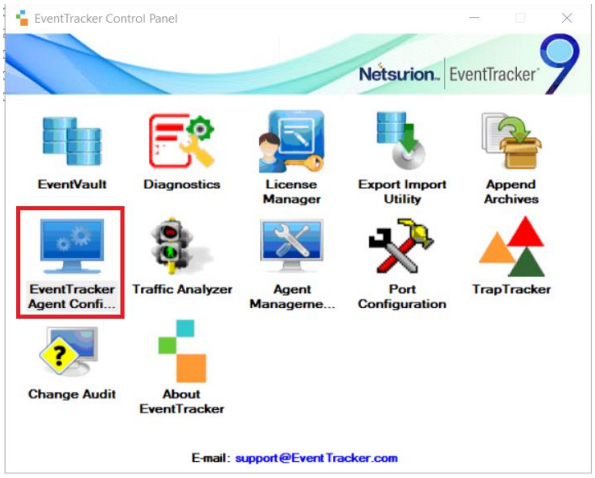
```
#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf

local7.debug    /var/log/nginx/access.log; RemoteFormat
local7.debug    /var/log/nginx/error.log; RemoteFormat
```

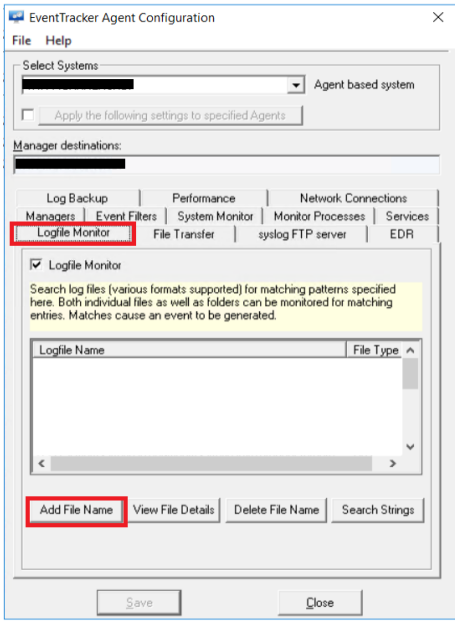
- This will ensure the logs are forwarded to EventTracker.

3.2 Forwarding via Log File Monitor to EventTracker for Windows Operating System

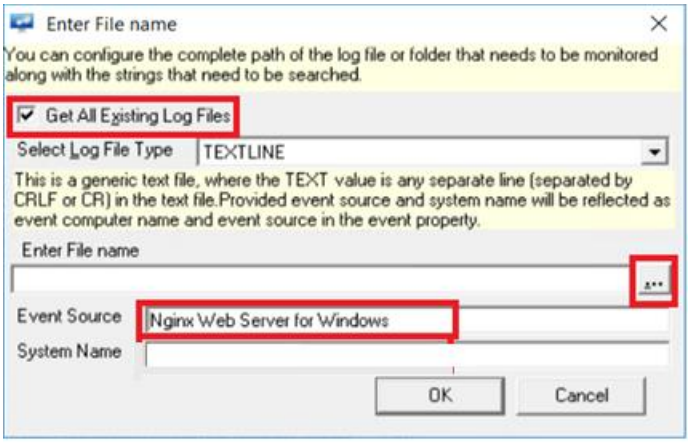
1. Open the EventTracker **Control Panel**.
2. Click the **EventTracker Agent Configuration**.



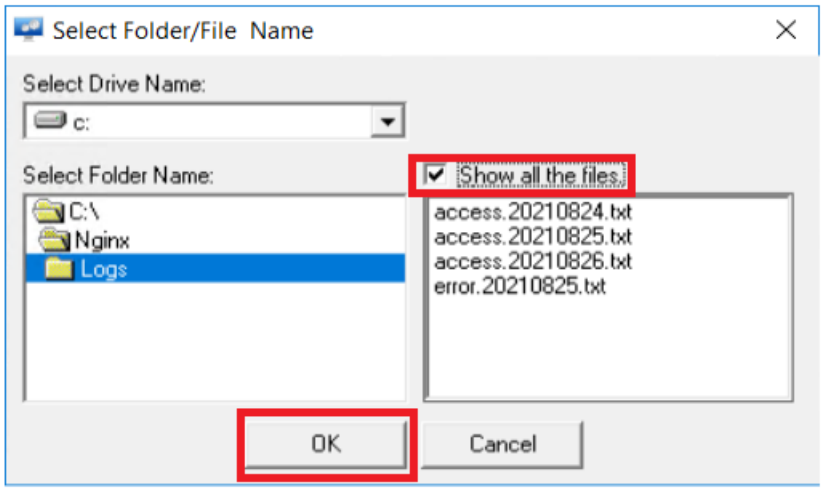
3. Click the **Log File Monitor** tab.
4. Click the **Add File Name** button.



5. Do following steps
    a. Enable the check box **Get All Existing Log Files**.
    b. Enter the Event Source as **Nginx Web Server for Windows**.
    c. Click the **Browse** file.

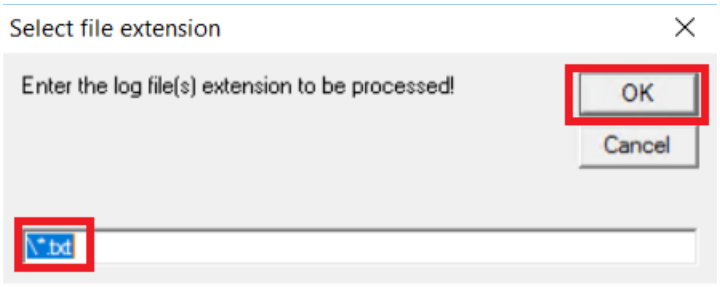


    d. Browse to the location where **NGINX** Web **Server logs** are available.
    e. Enable the check box **Show all the files.**
    f. Click **OK**.

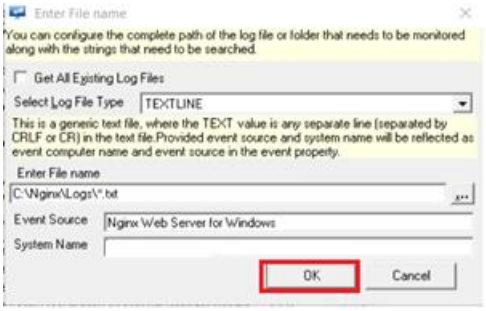


g. Enter **"*.text"** in the Text Box.

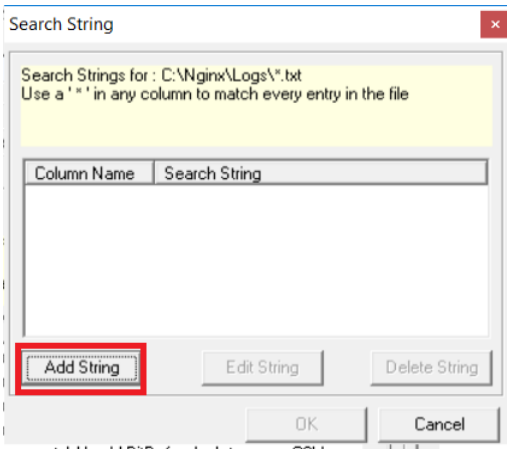
h. Click **OK**.



i. Click **OK** and click **OK** again on the Information Message Box.



j. Click **Add String**.

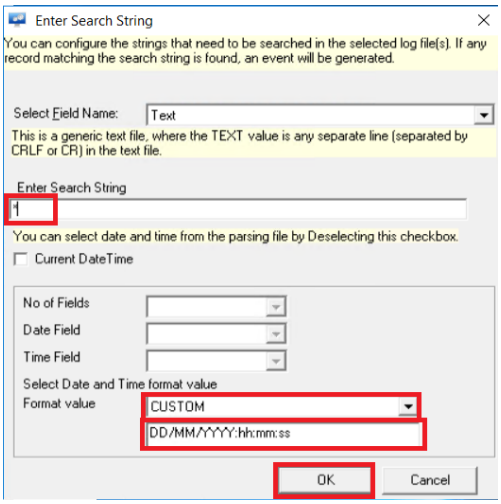


k. Enter "*" in "**Enter Search String**".

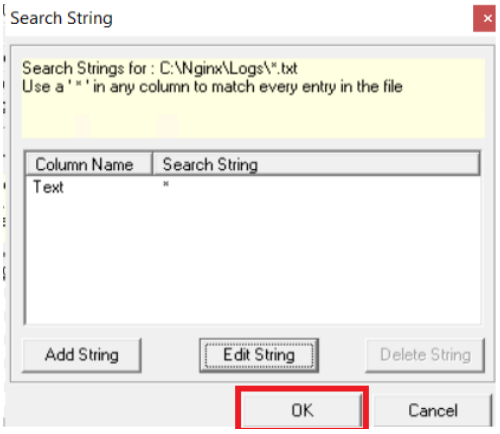
l. On the **Format Value,** click the dropdown button and select **Custom**.

m. In the **Text Box** enter **DD/MM/YYYY:hh:mm:ss.**

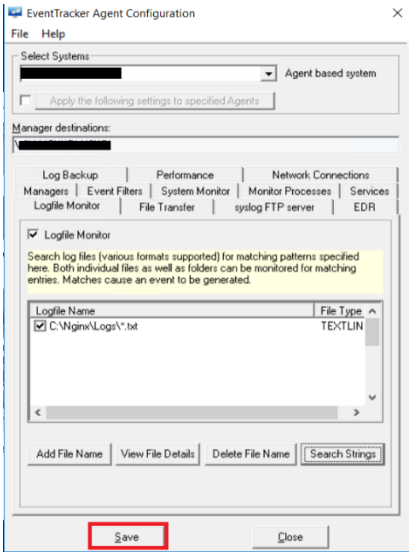
n. Click OK.



o. Click **OK** in the Search String window.



p. Click **Save**.



6. Check EventTracker to verify the logs are forwarding.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #23 among MSSP Alert's 2021 Top 250 MSSPs.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support