Netsurion. | EventTracker®

How to – Configure Linux with EventTracker

EventTracker v9.2 and later

Publication Date: August 10, 2020

Abstract

This guide provides instructions to retrieve the **Linux** events via syslog. Once the logs start coming-in into EventTracker, reports, dashboards, alerts and saved searches can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and **Linux (Red Hat/Cent OS version 7.0 and later).**

Audience

Administrators who are assigned the task to monitor **Linux** events using EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Table of Contents

1. Overview 3

2. Prerequisites 3

3. Integrating Linux with EventTracker 3

3.1 Configuring Linux system to forward logs to EventTracker 3

3.2 Verifying the audit configurations and services 4

1. Overview

Linux is a family of open source Unix-like operating systems based on the Linux kernel, an operating system kernel. An operating system is software that manages all the hardware resources associated with your desktop or laptop.

EventTracker, when integrated with Linux, collects logs from it and creates a detailed reports, alerts, dashboards, and saved searches. These attributes of EventTracker helps user to view/receive the critical and relevant information with respect to security, operations and compliance.

Reports contains a detailed summary of events such as success/failed user authentications, passed authentications, sudo command executions, device mount/unmount activities, software/package management activities, and many more in column-value pair.

Alerts are triggered as soon as a critical event are received by EventTracker for Linux, such as failed authentications, user password changes, changes made in sudoers file, user removed or deleted from Linux system.

Dashboards represents all the activities in Linux. These includes, user login success by source IP address, software/package management, user command execution, a dashlet displaying the types of events available at present for Linux etc.

These attributes or configurations of EventTracker allows administrators to quickly take appropriate actions against any threat/adversaries trying to jeopardize an organizations normal operation.

2. Prerequisites

- EventTracker v9.2 and above should be installed.
- Administrative/root access to Linux console.
- Syslog port (e.g. 514) should be allowed in firewall.
- EventTracker (Linux) bash script, ‘LinuxIntegrator.sh’. (contact EventTracker support).

3. Integrating Linux with EventTracker

3.1 Configuring Linux system to forward logs to EventTracker

Integration of Linux OS with EventTracker can be achieved by using ‘rsyslog’. Follow the following steps to integrate Linux logs with EventTracker.

1. Open your favorite Linux editor and edit the ‘**LinuxIntegrator.sh**’ file. e.g.:

```
[maya@centos7 ReceivedFiles]$ vi LinuxIntegrator.sh
```

2. Edit the below lines by providing the EventTracker manager IP address.

```
#!/bin/bash
 EventTrackerManagerIP='x.x.x.x'  # Enter EventTracker IP address
 EventTrackerManagerSyslogport='<syslog port>' # e.g. 514
```

(Note: Users can specify syslog port number other than 514 if they want to.**)**

3. Once done, save the file and run it using root privilege, e.g.:

```
[maya@centos7 ReceivedFiles]$ sudo sh LinuxIntegrator.sh
```

OR

```
[root@centos7 ~]# sh LinuxIntegrator.sh
```

3.2 Verifying the audit configurations and services

1. Verify the added audit rules using:

```
[maya@centos7 ReceivedFiles]$ auditctl -l
```

2. Verify the service status to auditd:

```
[maya@centos7 ReceivedFiles]$ service auditd status
```

3. Verify the service status of rsyslog:

```
[maya@centos7 ReceivedFiles]$ service rsyslog status
```