Netsurion | EventTracker®

How to – Configure Arista EOS to forward logs to EventTracker

EventTracker v9.x and later

Abstract

This guide provides instructions to retrieve the **Arista EOS** events by syslog configuration. Once **EventTracker** is configured to collect and parse these logs, dashboard and reports can be configured to monitor **Arista EOS**.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and **Arista EOS 4.23.x and above.**

Audience

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

Table of Contents

1. Introduction

Extensible Operating System (EOS) is Arista's network operating system. It comes as one image that runs across all Arista devices and in virtual machines (VM). EOS is a scalable network Operating System (OS) that offers high availability, streamlined maintenance processes, and enhanced network security.

Arista EOS when configured, sends events to EventTracker using syslog. Arista EOS sends events like switch configuration, interface status, user logon activities, etc. Generates reports on user login success, user logout, and configuration changes on Arista EOS. It contains username, client IP address, login status, interface status, and message. Graphically displays user login and logout by usernames, configuration changes by usernames, etc. It generates alerts, network interface card shutdown, user login fail, and switch restart, etc.

2. Prerequisites

- Arista EOS 4.23.x and above should be installed.
- Administrative access on Arista EOS Switch.
- Allow 514 port number if any firewall exists between the EventTracker and Arista switch.

3. Configuring Arista EOS Syslog

Configuring syslog for Arista EOS to forward logs to EventTracker.

Enable syslog (Command Mode - Global Configuration)

1. Login into your Arista switch.
2. Enter global config mode:
   ```
   Arista(config)#
   ```
3. Type "logging host x.x.x.x", where x.x.x.x is the ip address of EventTracker.
   ```
   Arista(config)#logging host 172.1.1.63
   Arista(config)#logging vrf Management host 172.1.1.63 514
   Arista(config)#logging vrf Management source-interface Management1
   Arista(config)#logging synchronous
   Arista(config)#logging buffered 100000000 informational
   ```
4. Save the configuration.