Netsurion®

Powering Secure and Agile Networks

How-To Guide

Configuring ntopng to Forward Logs to EventTracker

EventTracker v9.2 and later

Publication Date:

April 30, 2021

Abstract

This guide helps you in configuring ntopng with EventTracker to receive ntopng events. In this guide, you will find the detailed procedures required for monitoring ntopng.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 and later, ntopng v4.2.

Audience

Administrators who are assigned the task to monitor and manage ntopng events using EventTracker.

Table of Contents

1. Overview

ntopng is the next-generation version of the original ntop. It is a passive network monitoring tool focused on flows and statistics that can be obtained from the traffic captured by the server.

EventTracker integrates with ntopng using syslog. ntopng sends events information like alerts, web traffic activities, etc. EventTracker generates a detail reports for ,suspicious traffic activities, web traffic activities, etc. Its graphical representation shows web traffic activities source IP address, destination IP address, top accessed URL, etc.

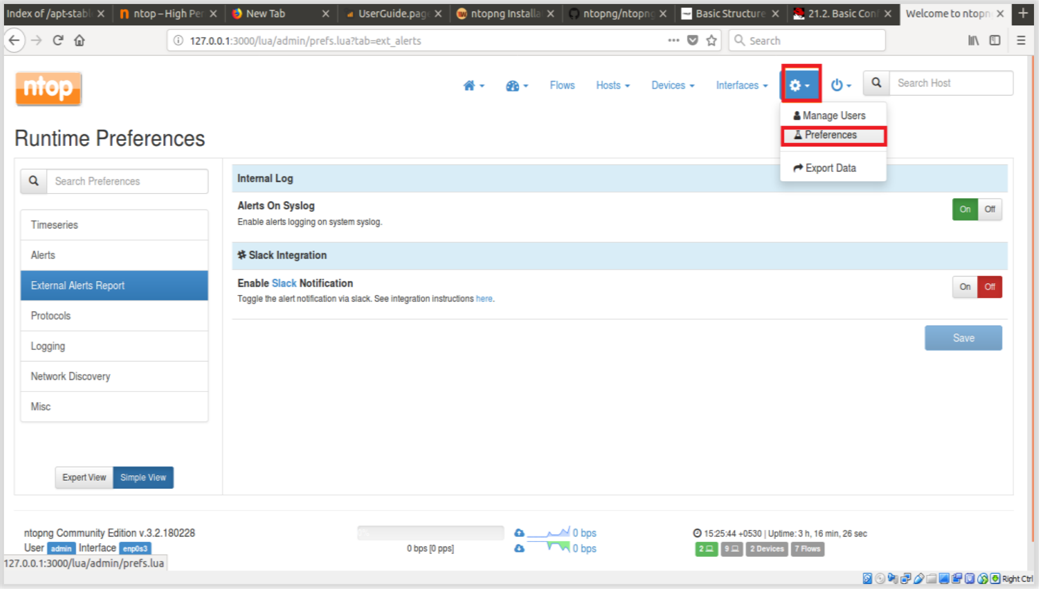
EventTracker triggers alerts in the event when suspicious traffic is detected by ntopng.

2. Prerequisites

- Admin access to ntopng web interface.
- Collect EventTracker IP address for log integration.
- Allow syslog server port 514 if any firewall exists between ntopng and EventTracker.

3. Integrating ntopng events to EventTracker server

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.
   If $programname == ‘ntopng’ then @eventtracker_ip:514
3. Launch ntopng Web Interface.
4. Hover over setting and select **Preferences**.



Runtime Preferences

Internal Log

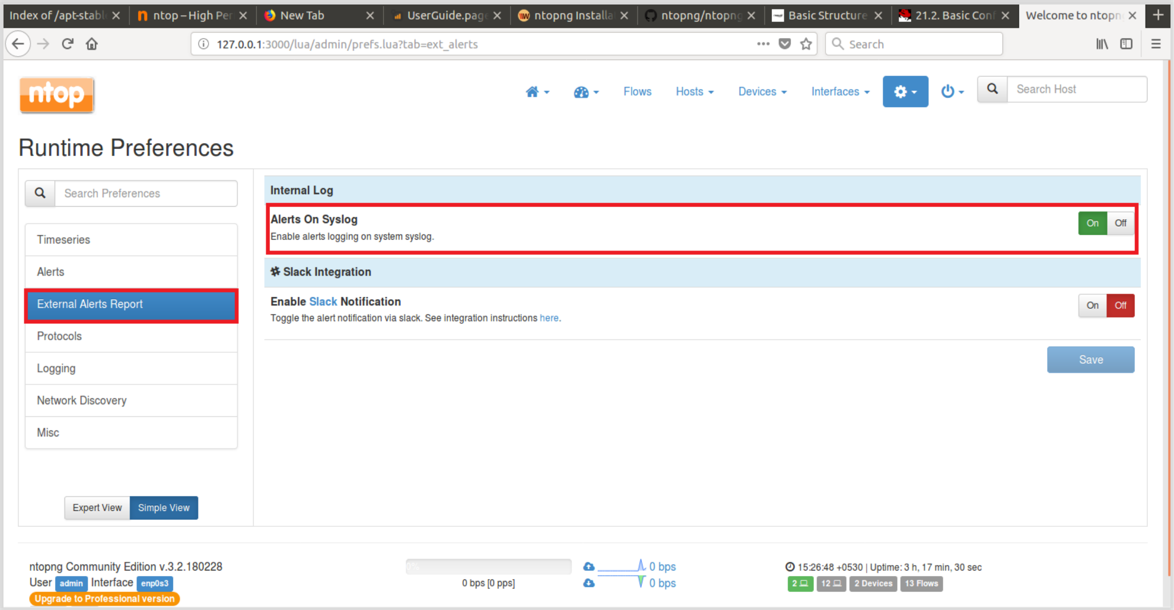
Alerts On Syslog — On
Enable alerts logging on system syslog.

Slack Integration

Enable Slack Notification — Off
Toggle the alert notification via slack. See integration instructions here.

ntopng Community Edition v.3.2.180228
User admin Interface enp0s3
0 bps [0 pps]
0 bps
0 bps
15:25:44 +0530 | Uptime: 3 h, 16 min, 26 sec
2 | 9 | 2 Devices | 7 Flows
127.0.0.1:3000/lua/admin/prefs.lua

5. On the left-hand pane, select **External Alerts Report**.
6. Enable **Alerts on Syslog** option.



Runtime Preferences

Internal Log

Alerts On Syslog — On
Enable alerts logging on system syslog.

Slack Integration

Enable Slack Notification — Off
Toggle the alert notification via slack. See integration instructions here.

ntopng Community Edition v.3.2.180228
User admin Interface enp0s3
Upgrade to Professional version

0 bps [0 pps]
0 bps
0 bps

15:26:48 +0530 | Uptime: 3 h, 17 min, 30 sec
2 | 12 | 2 Devices | 13 Flows

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 #19 among MSSP Alert's 2020 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