Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring Tanium to Forward Logs to EventTracker

EventTracker v9.x and above

Publication Date:

July 9, 2021

Abstract

This guide provides instructions to configure/ retrieve Tanium logs via syslog.

Scope

The configuration details in this guide are consistent with EventTracker version v 9.x or above and Tanium Endpoint Security or Endpoint Management.

Audience

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

Table of Contents

1. Overview

Tanium is a feature-packed endpoint management and endpoint security platform designed to strengthen and optimize an organization's cybersecurity efforts. The platform allows security and IT operations team to get access to visibility and accurate information on the state of endpoints at all times to protect against modern-day disruptions and realize new levels of business resilience.

EventTracker helps to monitor events from Tanium via syslog. EventTracker flex reports, alerts, and dashboards will help you to analyze the activity logs such as, vulnerability management, login failed by any user, administrative activities, etc.

2. Prerequisites

- Admin access to Tanium platform.
- Enable subscription for Tanium Connect.
- EventTracker server IP address. (If Tanium is cloud, the public IP is required.)
- EventTracker server port. E.g. 514 or 6514.
- Enable TLS on EventTracker Manager in case of syslog "TCP" connection.

3. Configuring Tanium

Syslog configuration for both On-Prem solution and cloud (TaaS) solution is very much the same.

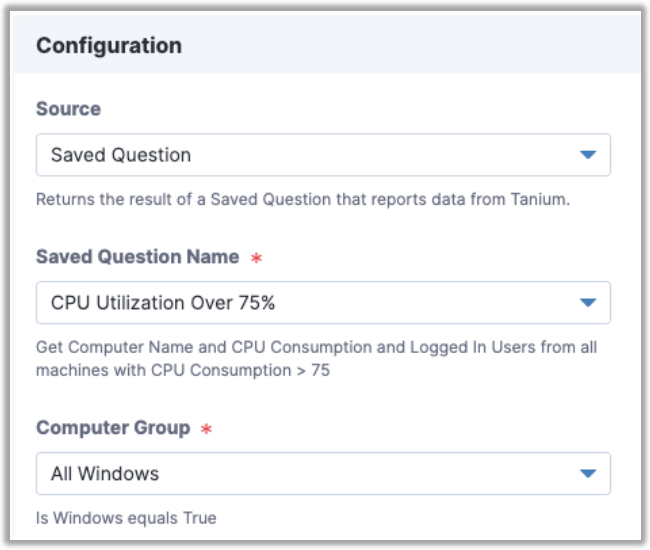
The steps provided below will help to configure Tanium via syslog to help forward logs to EventTracker servers.

1. Login to your Tanium platform.
2. On the **Connect Overview** page, scroll to the **Connections** section and click **Create Connection**.
3. Enter a name and description for the connection.

3.1 Configuring the connection source.

The connection source determines what data you are sending to the destination. This data is usually information from Tanium, such as a saved question, question log, client status, or event. The settings vary depending on which source you choose.

There are multiple connection sources that can be considered for e.g., Action History, Client Status, Event, Tanium Audit Source, Tanium™ Threat Response, etc.



3.2 Configuring the SIEM Destination.

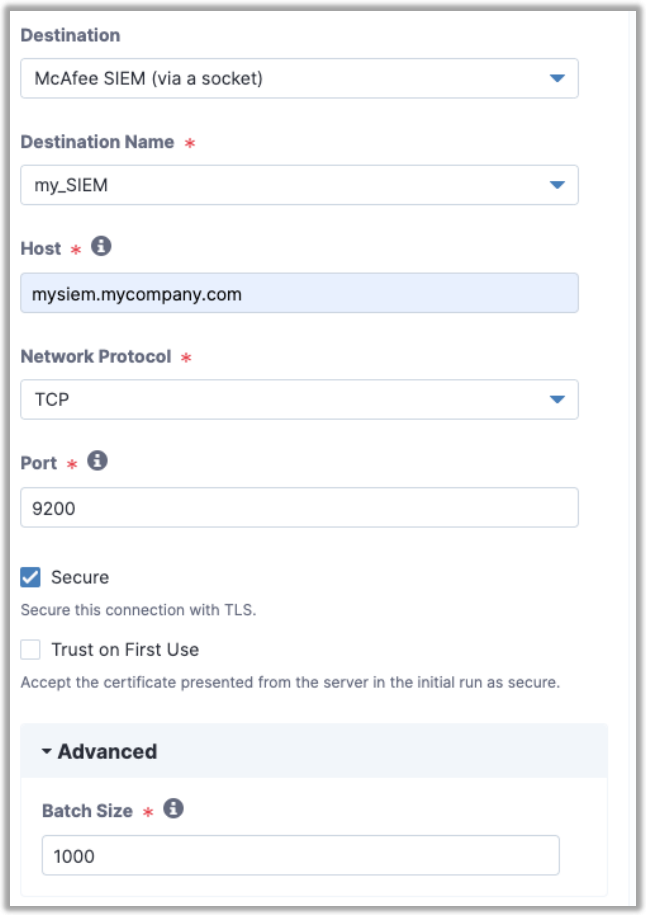
Specify details about the server to which you want to send the SIEM data.

1. For the **Destination**, select the type of SIEM that you are configuring.
2. Specify a name for the destination:
    - You can specify a unique name to save the configuration information as a new destination or select an existing SIEM destination from the list.
    - If you edit the settings for an existing destination, all connections that use that destination are affected.
    - To clone an existing destination, select the existing destination and change the name.
3. Specify how to connect with the server (TCP/UDP), and where you want the data to go, such as the SIEM host and port.
   Fill-in the below required fields:
    - **Host** – EventTracker server IP address/ hostname
    - **Network Protocol** – UDP/TCP. (Select UDP in case of On-prem)
    - **Port** – e.g., 514 or 6514. (Select 514 in case of UDP)

(**Note** – Optionally, a self-signed certificate can be created to use in case of TCP as network protocol. You can also select Trust on First Use to accept the certificate presented from the server and trust only that certificate for future connection runs.)

3.3 Saving and verifying connection

After you enter the details for the connection, click **Save**. (To save the connection and immediately run the connection, click **Run and Save**.)



4. System Licensing

For On-Prem solution, a single system will get created by the format of <HostName~syslog> or <ComputerName~syslog>.

For Cloud-based solution, multiple system with format <IPAddress~syslog> may get created. If logs are coming in from multiple IP addresses for the same customer, the system name extraction can be done from the logs.

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