Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configure Citrix Cloud Analytics to forward logs to EventTracker

Publication Date:

June 06, 2022

Abstract

This guide provides instructions to retrieve the Citrix Cloud Analytics events via the Logstash data collection engine and then forward the logs to EventTracker from the syslog extension.

Scope

The configuration details in this guide are consistent with Citrix Cloud Analytics and EventTracker 9.3 or later.

Audience

This guide is for the Administrators responsible for configuring the Citrix Cloud Analytics events to forward logs to EventTracker.

Table of Contents

1 Overview

Citrix Cloud Analytics solutions facilitate organizations to detect and deflect potential threats and instantly address performance issues long before security incidents occur, or employees begin to submit help desk tickets. Citrix Analytics for Security continuously assesses the behavior of Citrix Virtual Apps and Desktops users, Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) users, and Citrix Workspace users. It applies actions to protect sensitive corporate information.

EventTracker dashboard and reports will supply information about possible attacks, suspicious activities, or any other threat noticed in user activities based on the user's risk score.

2 Prerequisites

- Administrator privilege to configure Citrix Analytics account to forward log data to Logstash.
- Logstash to receive logs from Citrix Analytics.

3 Configure Citrix Cloud Analytics

The Citrix Cloud Analytics is integrated with EventTracker by streaming the logs to Logstash and then to EventTracker from the syslog extension.

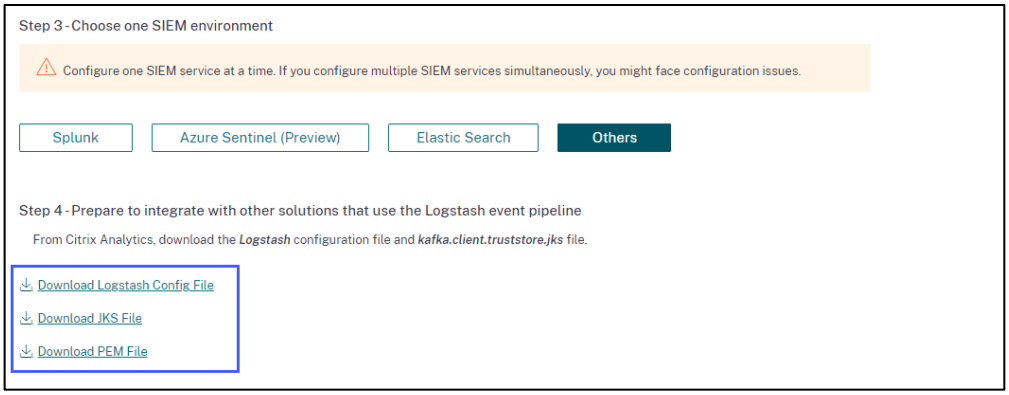
3.1 Configuring Citrix Cloud Analytics to forward Logs to Logstash

To send the log data to a syslog server, use the Logstash data collection engine to send the processed data from Citrix Cloud Analytics for Security to the Logstash supported Syslog plug-ins.

Refer to Syslog to configure the Syslog plugin.

Refer to logstash-output-syslog for the GitHub repository.

1. In the **Citrix Cloud** console, go to **Settings** > **Data Sources** > **Security** > **DATA EXPORTS**.
2. On the SIEM site card, select **Get Started**.
3. On the **Configure SIEM integration** page, create an account by setting the username and password. This account is for creating the configuration file required for integration.
4. Click **Configure** to generate the Logstash configuration file.
5. Go to the **Others** tab to download the configuration files.
    - **Logstash config file**: This file contains the configuration data (input, filter, and output sections) for sending events from Citrix Analytics for Security using the Logstash data collection engine. For information regarding the Logstash config file structure, see the Logstash documentation.
    - **JKS file**: This file contains the certificates required for SSL connection. This file is required when you integrate your SIEM using Logstash.



6. Configure Logstash.

   - On your Linux or Windows host machine, install Logstash. You can also use your existing Logstash instance.
   - On the host machine where you have installed Logstash, place the following files in the specified directory:

Host machine type	File name	Directory path
Linux	CAS_Others_LogStash_Config.config	For Debian and RPM packages: `/etc/logstash/conf.d/`
		For .zip and .tar.gz archives: `{extract.path}/config`
	kafka.client.truststore.jks	For Debian and RPM packages: `/etc/logstash/ssl/`
		For .zip and .tar.gz archives: `{extract.path}/ssl`
Windows	CAS_Others_LogStash_Config.config	`C:\logstash-7.xx.x\config`
	kafka.client.truststore.jks	

   - Open the Logstash config file and do the following: In the input section of the file enter the following information.

     Password: The password of the account that you created in Citrix Analytics for Security to prepare the configuration file.
     SSL truststore location: The location of your SSL client certificate. This is the location of the kafka.client.truststore.jks file in your host machine.

3.2 Forwarding Logs from Logstash to EventTracker

Open the Logstash config file and do the following:

- In the output section of the file, enter the following information:

```
output {
  syslog {
        host=> "10.1.2.1"
        port=> 514
  }
}
```

- In the host section update the IP address of the EventTracker manager.
- In the port section type 514 and make sure the port is up and running.

About Netsurion

Flexibility and security within the IT environment are two of the most crucial factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion Managed Threat Protection combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion Secure Edge Networking delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all 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.

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 MSPs 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