

How to - Configure Heroku to forward logs to EventTracker

EventTracker v9.3 and above

Abstract

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

Scope

The configuration details in this guide are consistent with EventTracker version v9.3 or above and **Heroku**.

Audience

Administrators, who are assigned the task to monitor and manage **Heroku** 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.

© 2021 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

1. Overview.....	3
2. Prerequisites.....	3
3. Integrating Heroku with EventTracker	3
3.1 EventTracker uses syslog drain to receive logs from Heroku.....	3
3.2 System Licensing.....	4

1. Overview

Heroku is a container-based cloud Platform as a Service (PaaS) that is used to build, deploy, manage, and scale modern applications. Heroku Enterprise provides services to large companies which help them to improve collaboration among different teams. It provides a set of features like fine-grained access controls, identity federation, and private spaces to manage their enterprise application development process, resources, and users.

This guide helps you in configuring **Heroku** with EventTracker to receive **Heroku** events. Once Heroku is configured to send logs to EventTracker, EventTracker's knowledge pack will help in monitoring events from **Heroku**.

EventTracker's knowledge pack consists of dashboard (graphical representation of events), alerts (near real-time notification of important events), saved searches (for searching specific category of logs with a single click) and reports (structured and details info of events) to help you correct problems long before a disastrous failure occurs.

EventTracker's built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

2. Prerequisites

- **EventTracker v9.3** or **above** should be installed.
- **Heroku** should be configured.
- Heroku Command Line Interface (CLI) must be installed.

3. Integrating Heroku with EventTracker

3.1 EventTracker uses syslog drain to receive logs from Heroku.

1. Create an app in Heroku.
2. Login to Heroku CLI.
3. Turn on debug and runtime logging.
 - **Turn on debug logging:**
 - `$ heroku config:add LOG_LEVEL=DEBUG --app <YOUR_APP_NAME>`
 - **Turn on runtime logging:**
 - `$ heroku labs:enable log-runtime-metrics --app <YOUR_APP_NAME>`
4. Restart your app to apply changes:

- **Restart your app:**
 - `$ heroku restart --app <YOUR_APP_NAME>`
5. Using command line, add syslog URL (which contains the host and port) as a syslog drain.

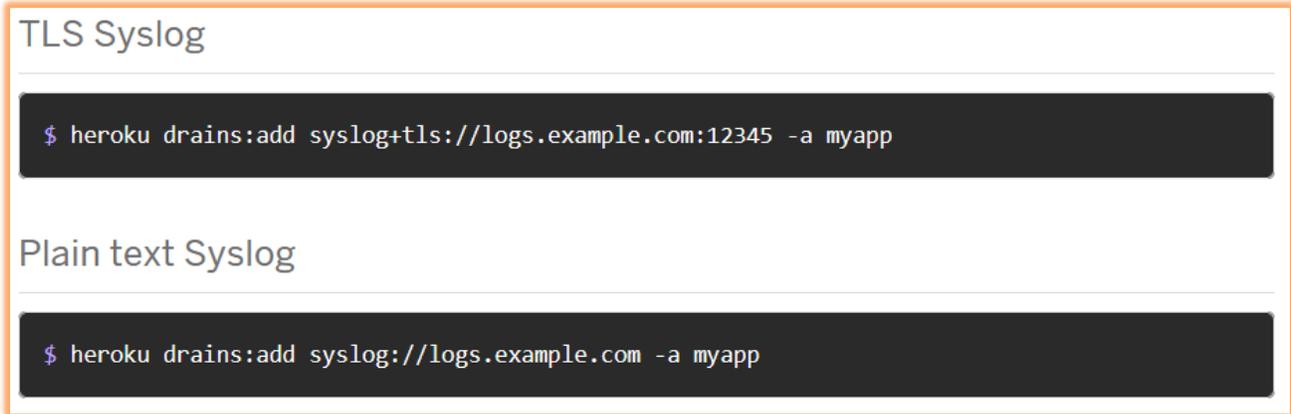


Figure 1

Here, **myapp** = the name of your Heroku application

e.g. `heroku drains:add syslog://<EventTracker Manager IP>:<port> --app <YOUR APP NAME>`

EventTracker will receive events/logs of applications for which syslog drain has been created.

3.2 System Licensing

1. Click on **Manager** under **Admin**.

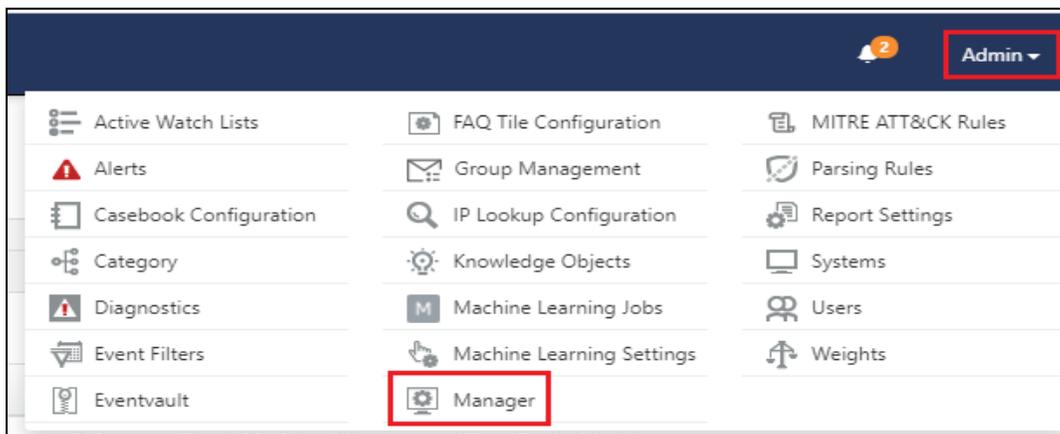


Figure 2

2. Go to **syslog/Virtual Collection Point** tab.

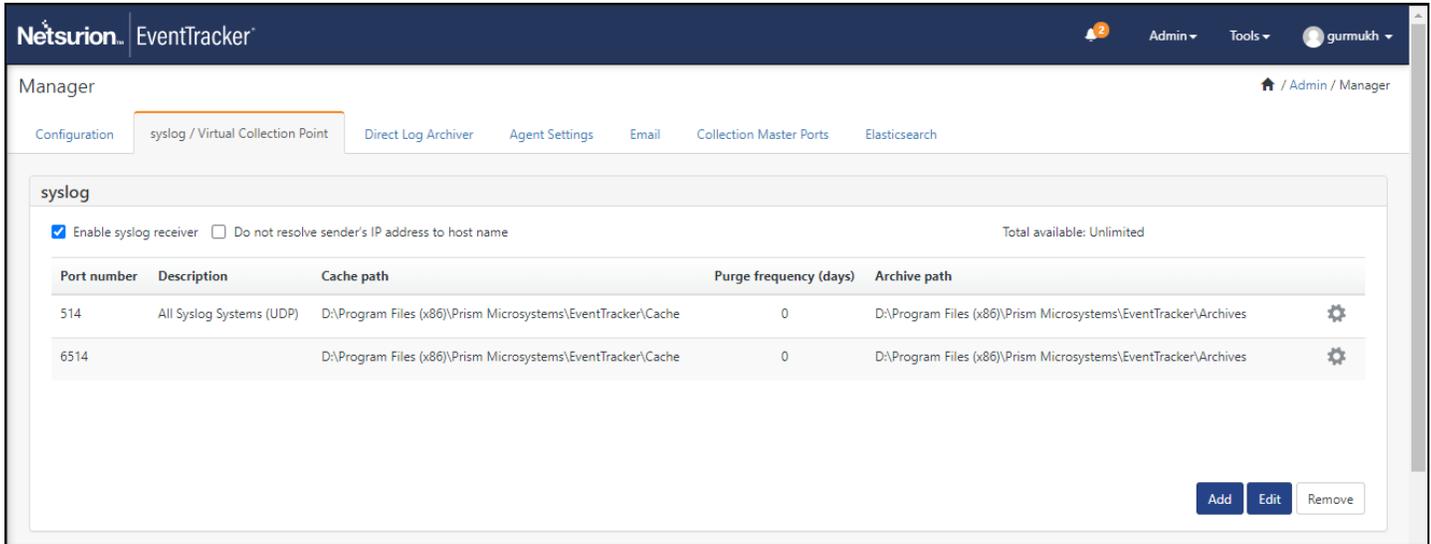


Figure 3

3. Click on the  symbol and then select **Extract device Id**.

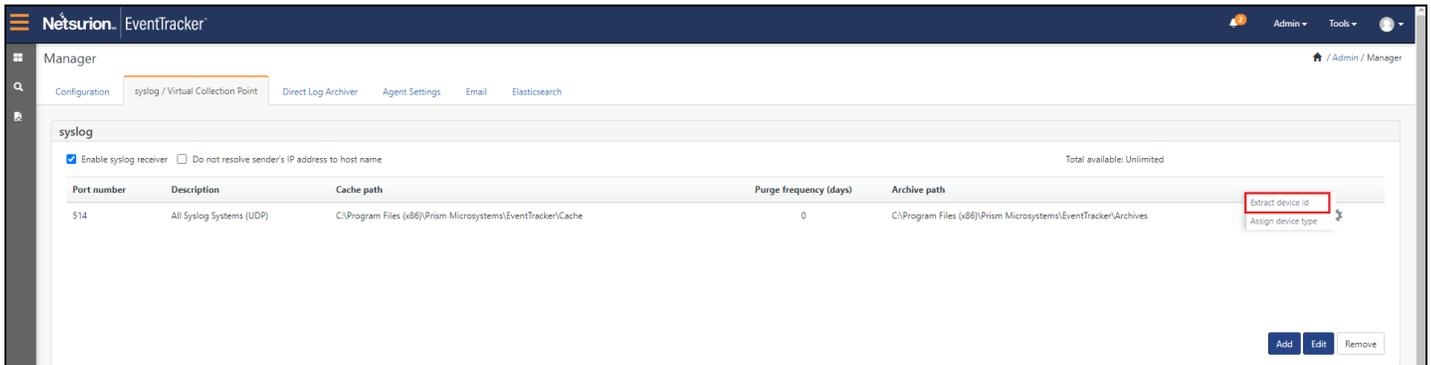


Figure 4

4. Provide below **Regex** in Regular Expression space.

`\+{d+}\:d+\s(?P<Computer>d\.[^\s]+)`

5. Provide below value in Token name.

Computer

6. Check **Active** box.

7. Click **Add** and then **close**.

Extract device id from syslog devices

Port number: 6514
 Note: Adding multiple regular expression for extracting device id or name may cause the EventTracker receiver performance degradation

Regular expression	Token name	Active
<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/> Active <input type="checkbox"/> Ignore syslog message if regular expression does not match

Regular expression

Token name

Note: The provided token must be same as Named Capture Group given in the regular expression

Figure 5

8. Click **Save**.

syslog

Enable syslog receiver Do not resolve sender's IP address to host name

Total available: Unlimited

Port number	Description	Cache path	Purge frequency (days)	Archive path
514	All Syslog Systems (UDP)	D:\Program Files (x86)\Prism Microsystems\EventTracker\Cache	0	D:\Program Files (x86)\Prism Microsystems\EventTracker\Archives
6514		D:\Program Files (x86)\Prism Microsystems\EventTracker\Cache	0	D:\Program Files (x86)\Prism Microsystems\EventTracker\Archives

Virtual Collection Points

Total available: Unlimited

Port number	Description	Cache path	Purge frequency (days)	Archive path
14505	All Systems	D:\Program Files (x86)\Prism Microsystems\EventTracker\Cache	0	D:\Program Files (x86)\Prism Microsystems\EventTracker\Archives
14525	APACHE	D:\Program Files (x86)\Prism Microsystems\EventTracker\Cache	0	D:\Program Files (x86)\Prism Microsystems\EventTracker\Archives

Figure 6