

## How-To Guide

# Configuring Azure Kubernetes Service to Forward Logs to EventTracker

**Publication Date:**

March 28, 2022

## Abstract

This guide provides instructions to retrieve the **Azure Kubernetes Service** events via the Azure Event Hub and then configure the **Azure function app** to forward the logs to EventTracker. After EventTracker receives the logs from the Event Hub, the reports, dashboard, alerts, and saved searches can be configured.

## Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or above and **Azure Kubernetes Service**.

## Audience

The Administrators who are assigned the task to monitor the **Azure Kubernetes Service** events using EventTracker.

## Table of Contents

Table of Contents .....	3
1. Overview .....	4
2. Prerequisites.....	4
3. Configuring Azure Kubernetes Service to Forward Logs to EventTracker .....	4
3.1 Forwarding Event Hub data to EventTracker.....	4
3.2 Configuring Azure Kubernetes Service to stream events to Event Hub.....	4
About Netsurion .....	7
Contact Us.....	7

## 1. Overview

Azure Kubernetes Service (AKS) deploys and manages the containerized applications easily with a fully-managed Kubernetes service. It offers serverless Kubernetes, an integrated continuous integration and continuous delivery (CI/CD) experience, and enterprise-grade security and governance. Unite your development and operations teams on a single platform to rapidly build, deliver, and scale the applications with confidence.

EventTracker helps to monitor events from the Azure Kubernetes Service. Its dashboard and reports will help you track, delete and update action for the Azure Kubernetes instances, unauthorized deletion could lead to data loss and/or potential denial of service or potentially compromised credentials, and create an action that helps you understand the cluster building with resources.

## 2. Prerequisites

- An Azure Subscription and a user who is a global administrator.
- Azure Resource group.
- EventTracker Manager public IP address.

## 3. Configuring Azure Kubernetes Service to Forward Logs to EventTracker

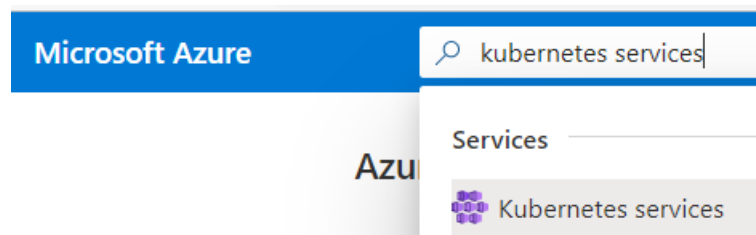
Azure Kubernetes Service can be integrated with EventTracker by streaming the logs to the Azure Event Hub, and from Azure Event Hub to EventTracker.

### 3.1 Forwarding Event Hub data to EventTracker

Refer to the [configuration of Azure function app](#) to forward logs to EventTracker.








### 3.2 Configuring Azure Kubernetes Service to stream events to Event Hub

1. Login to [portal.azure.com](https://portal.azure.com) using the Admin account and [create an event hub namespace](#), if not created.
2. Search and select **Azure Kubernetes Service** from **All services**.



3. From the left panel under **Monitoring**, select **Diagnostics settings**.

## Monitoring

-  Insights
-  Alerts
-  Metrics
-  **Diagnostic settings**
-  Advisor recommendations
-  Logs
-  Workbooks

### 4. Click **Add diagnostics settings**.

Diagnostic settings

Name	Storage account	Event hub	Log
No diagnostic settings defined			

[+ Add diagnostic setting](#)

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- kube-apiserver
- kube-audit
- kube-audit-admin
- kube-controller-manager
- kube-scheduler
- cluster-autoscaler
- cloud-controller-manager
- guard
- AllMetrics

### 5. Provide the inputs.

**Diagnostics settings name**, such as **EventTracker\_AKS**.

Select all **log** types, i.e., kube-audit-admin

In the **Destination details** section, select **stream to an Event Hub** and then choose the following options.

- **Subscription:** Select the desired Azure subscription.
- **Event Hub namespace:** Select the Event Hub namespace.
- **Event Hub name:** Select the Event Hub created under Event Hub namespace.
- **Event Hub policy name:** Select the Event Hub policy.

### 6. Click **OK/Save**.

[Home](#) / [Kubernetes Service](#) / [AKS](#) /

## Diagnostic setting

[Save](#) [Discard](#) [Delete](#) [Feedback](#)

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name \* 

### Logs

Category groups ⓘ

☐ allLogs ☐ audit

Categories

☐ kube-apiserver☐ kube-audit☒ kube-audit-admin☐ kube-controller-manager☐ kube-scheduler☐ cluster-autoscaler☐ cloud-controller-manager

### Destination details

☐ Send to Log Analytics workspace☐ Archive to a storage account☒ Stream to an event hubFor potential partner integrations, see documentation [here](#)

Subscription

Event hub namespace \*

Event hub name (optional) ⓘ

Event hub policy name

## About Netsurion

Flexibility and security within the IT environment are two of the most important 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](https://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>