Netsurion | EventTracker®

How to- Integrate Azure Monitor with EventTracker

EventTracker v9.x and later

Publication Date: May 27, 2020

Abstract

This guide provides instructions to retrieve the **Azure Monitor** events via Azure event hub. Once **Azure event hub** is configured to forward the logs to EventTracker, dashboard and reports can be configured to monitor **Azure Monitor**.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and **Azure Monitor.**

Audience

Administrators who are assigned the task to monitor **Azure Monitor** events using EventTracker.

Table of Contents

1. Overview

Azure Monitor is one of the Mizrosoft Azure cloud services. It provides a single source monitoring Azure resources/services. It allows the users to view, query, route, archieve and take actions on metrics, and logs collected from different Azure resources/services.

EventTracker, when integrated with Azure Monitor, collects log from Azure Monitor and creates a detailed reports, alerts, dashboards and saved searches. These attributes of EventTracker help users to view the critical and important information on a single platform.
Reports contain detailed overview of the activities that are associated with virtual machines, audit events such as authorization to services, and events that are performed by users with administrative privilege.
Alerts are provided as soon as any critical event are triggered by the Azure Monitor. With alerts, users will be able to get notifications about real time occurrences of events such as, failed authentication while accessing azure services, security events such as detection of trojan.
Visual/graphical representations, i.e. dashboard, consists of events such as administrative operation by source IP, security events by event name such as antimalware action taken, number/percentage of events available in each category, azure resources attacked by an adversary, etc.

2. Prerequisites

- An Azure Subscription and a user who is global administrator.
- Azure Resource group.
- EventTracker manager public IP address.
- Collect Azure Integration package from EventTracker Support.

3. Integrating Azure Monitor with EventTracker

Azure Monitor can be integrated with EventTracker by streaming the logs to Azure event hub, and from Azure event hub to EventTracker.

3.1 Forwarding Event hub data to EventTracker

Refer to configuration of Azure function app to forward logs to EventTracker.

3.2 Configuring Azure Monitor to stream events to event hub

1. Login to portal.azure.com using admin account. And create an event hub namespace, if not already created.
2. Next, search and select "**Monitor**" services from All services.

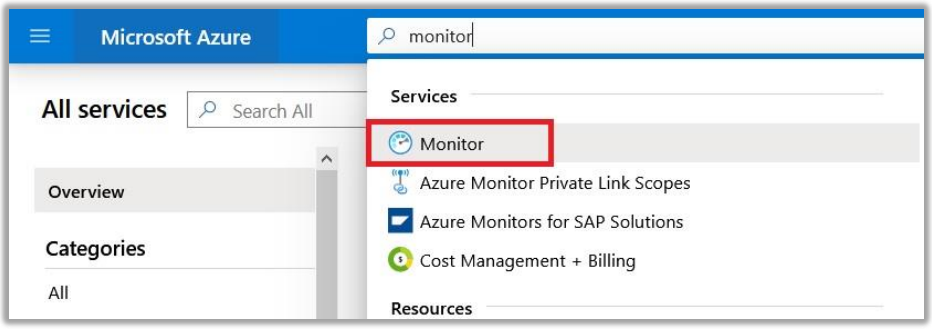

Figure 1

3. From the left panel select "**Activity log**".

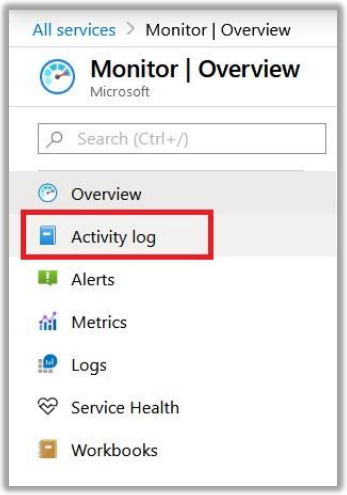

Figure 2

4. Select "**Diagnostics settings**".

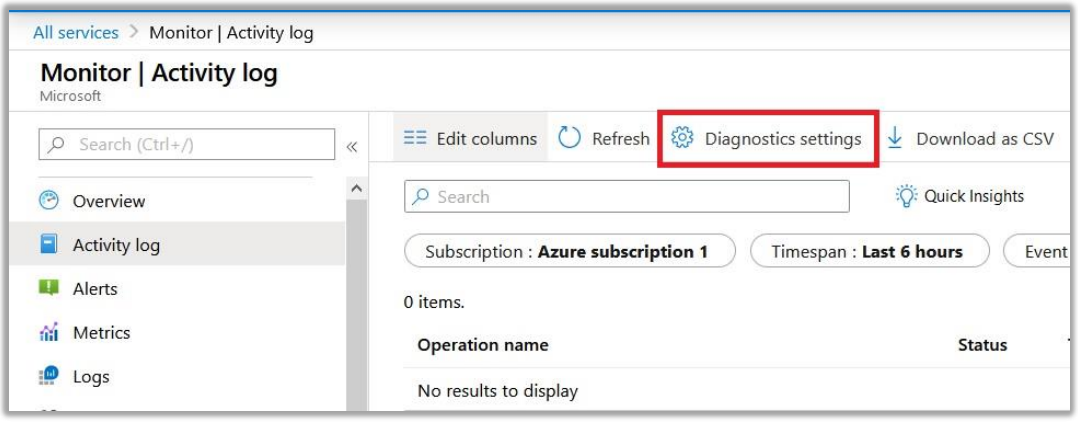

Figure 3

5. Click on "**Add diagnostics setting**".

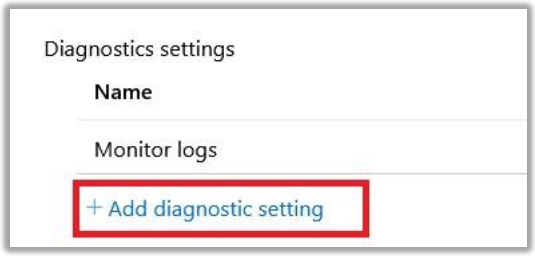

Figure 4

6. Provide the inputs.
   - **Diagnostics settings name**, such as 'EventTracker_logs'.
   - Select all **log** type, i.e. Administrative, Security, and so on.
   - In **Destination details** section select **"stream to an event hub"**. When you click this several options will be asked.
     - **Subscription**, select the desired Azure subscription.
     - **Event hub namespace**, select the event hub namespace.
     - **Event hub name**, select event hub created under event hub namespace.
     - **Event hub policy name**, select the event hub policy.
   - Click **OK/Save**

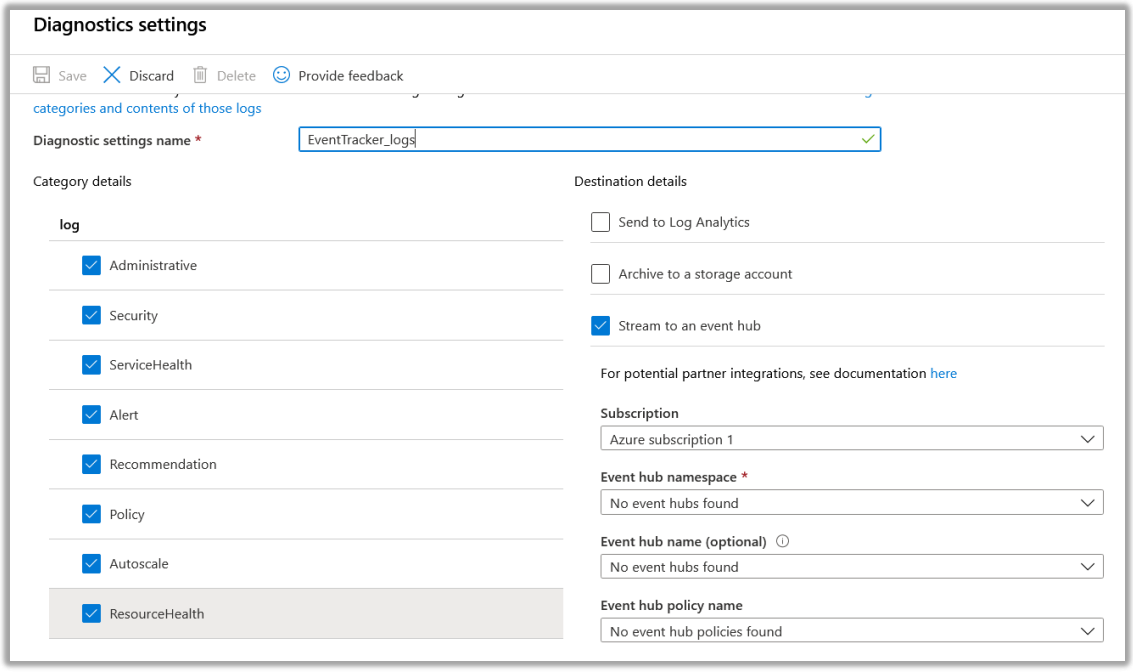

Figure 5