How-To Guide

Configuring Azure App Service to Forward Logs to EventTracker

Publication Date:

March 31, 2022

© Copyright Netsurion. All Rights Reserved.

Abstract

This guide provides instructions to retrieve the **Azure App 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, 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 App Service.**

Audience

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

Table of Contents

© Copyright Netsurion. All Rights Reserved.

1. Overview

Azure App Service helps to create apps faster with a one-of-a-kind cloud service to create enterprise-ready web and mobile apps quickly and easily for any platform or device and deploy them on a scalable and reliable cloud infrastructure.

EventTracker helps to monitor events from the Azure App Service. Its dashboard and reports will help you track, login activities of site content in the Azure App Service, IP access restriction with web traffic allowed or denied activities, and web traffic with user agent and status code which helps to detect potential directories brute force and invalid access.

2. Prerequisites

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

3. Configuring Azure App Service to Forward Logs to EventTracker

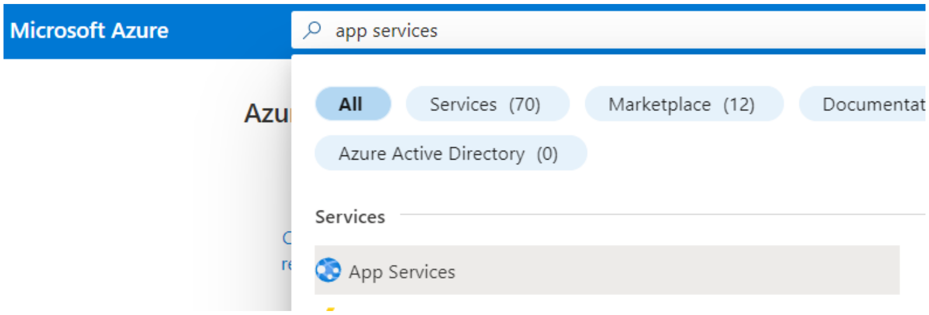
Azure App Service can be integrated with EventTracker by streaming the logs to the Azure Event Hub, and from Azure Event Hub to EventTracker.

3.1 Forwarding Event Hub data to EventTracker

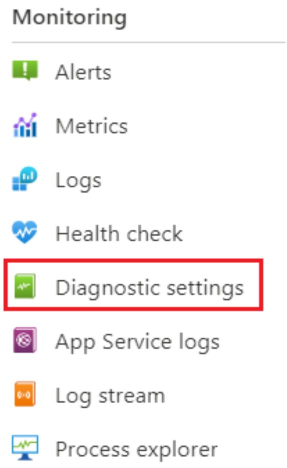
Refer to the Configuration of the Azure function app to forward logs to EventTracker.

3.2 Configuring Azure App Service to stream events to Event Hub

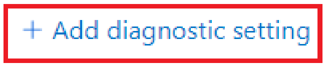
1. Login to portal.azure.com using the Admin account and create an event hub namespace, if not created.
2. Search and select **App Services** from **All services**.

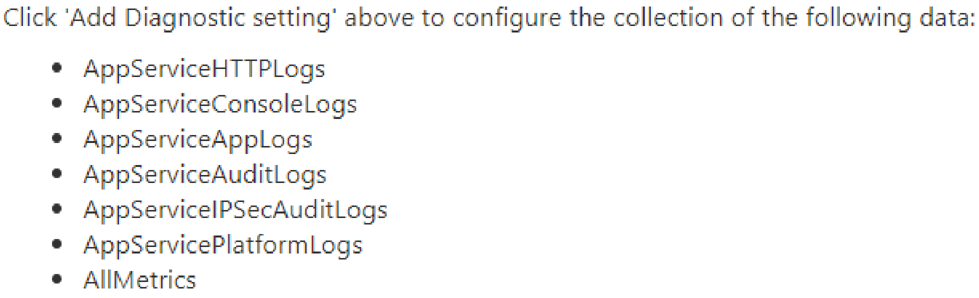


3. From the left panel under **Monitoring**, select **Diagnostics settings**.



4. Click on **Add diagnostics settings**.





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

- AppServiceHTTPLogs
- AppServiceConsoleLogs
- AppServiceAppLogs
- AppServiceAuditLogs
- AppServiceIPSecAuditLogs
- AppServicePlatformLogs
- AllMetrics

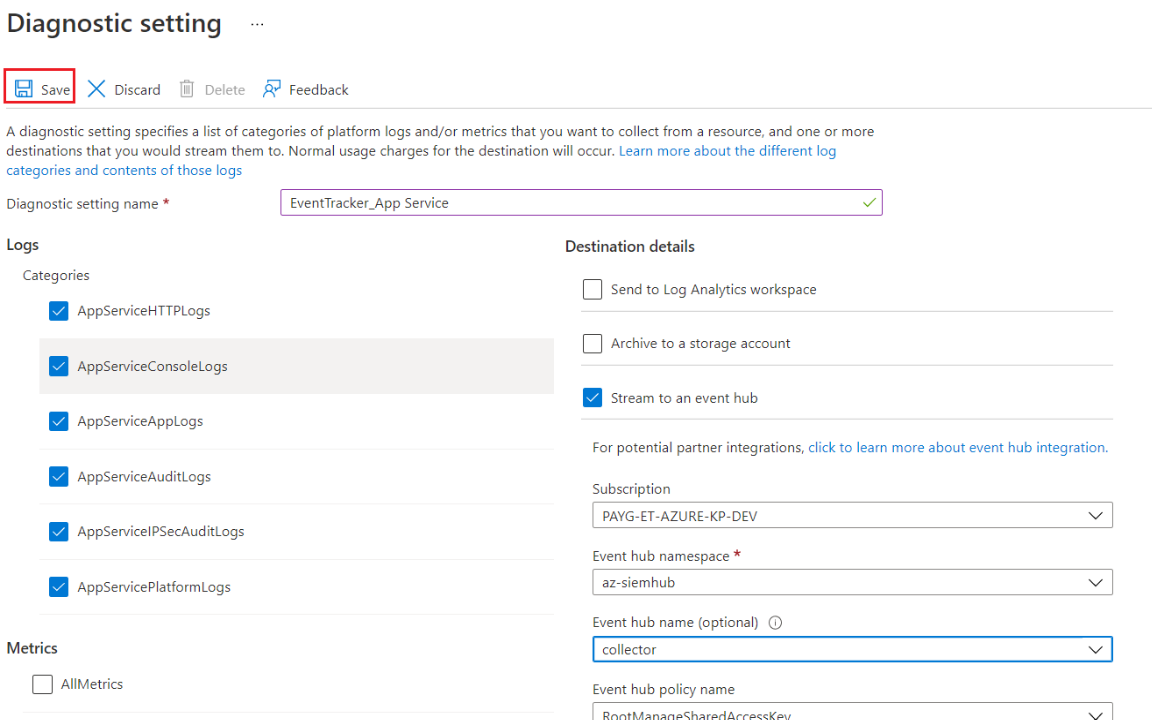
5. Provide the inputs.

   Diagnostics settings name, such as **EventTracker_App Service**.
   Select all **log** type, i.e., AppServiceHTTPLogs
   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 Event Hub created under the Event Hub namespace.
   - **Event Hub policy name:** Select the Event Hub policy.

6. Click **Save.**

© Copyright Netsurion. All Rights Reserved.



Diagnostic setting

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 * EventTracker_App Service

Logs

Categories

☑ AppServiceHTTPLogs

☑ AppServiceConsoleLogs

☑ AppServiceAppLogs

☑ AppServiceAuditLogs

☑ AppServiceIPSecAuditLogs

☑ AppServicePlatformLogs

Metrics

☐ AllMetrics

Destination details

☐ Send to Log Analytics workspace

☐ Archive to a storage account

☑ Stream to an event hub

For potential partner integrations, click to learn more about event hub integration.

Subscription: PAYG-ET-AZURE-KP-DEV

Event hub namespace *: az-siemhub

Event hub name (optional): collector

Event hub policy name: RootManageSharedAccessKey

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 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

© Copyright Netsurion. All Rights Reserved.