How-To Guide

Configure Azure Data Factory to forward logs to EventTracker

Publication Date:

September 26, 2022

© Copyright Netsurion. All Rights Reserved.

Abstract

This guide provides instructions to configure and retrieve the Azure Data Factory events via the Azure Event Hub and then forward the logs to EventTracker.

Scope

The configuration details in this guide are consistent with Azure Data Factory and EventTracker version 9.3 or later.

Audience

This guide is for the administrators responsible for configuring the Azure Data Factory events using EventTracker.

© Copyright Netsurion. All Rights Reserved.

Table of Contents

© Copyright Netsurion. All Rights Reserved.

1 Overview

Azure Data Factory is a cloud-based data integration service used to create data-driven workflows in the cloud for orchestrating and automating data movement and transformation. It also helps to monitor and manage workflows using both programmatic and UI mechanisms.

Netsurion facilitates monitoring events retrieved from the Azure Data Factory. The dashboard, category, alerts, and reports in Netsurion's threat protection platform, EventTracker, benefit in tracking possible attacks, suspicious activities, or any other threat noticed.

2 Prerequisites

- An Azure subscription and a user who is a global administrator.
- An Azure Resource group.
- EventTracker Manager details (Manager Hostname, Port, Manager public IP address, and Organization name).

3 Configuring Azure Data Factory to forward logs to EventTracker

Integrate Azure Data Factory with EventTracker by streaming the logs to the Azure Event Hub, and from Azure Event Hub to EventTracker using the function app.

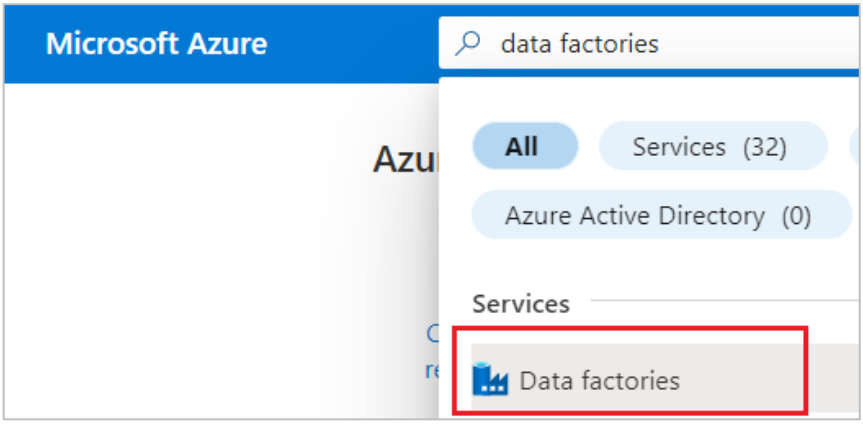
3.1 Create Event Hub and Function App

Refer to the configuration of Azure Data Factory to forward logs to EventTracker.

3.2 Configuring Azure Data Factory to stream events to Event Hub

To configure Microsoft Azure Data Factory to stream events to Event Hub, as an Administrator,

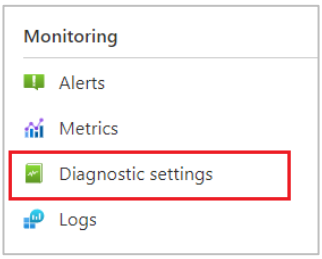
1. Log in to Microsoft Azure and create an event hub namespace.
2. In the **Microsoft Azure** console, click **All** services, then search and click **Data factories**.

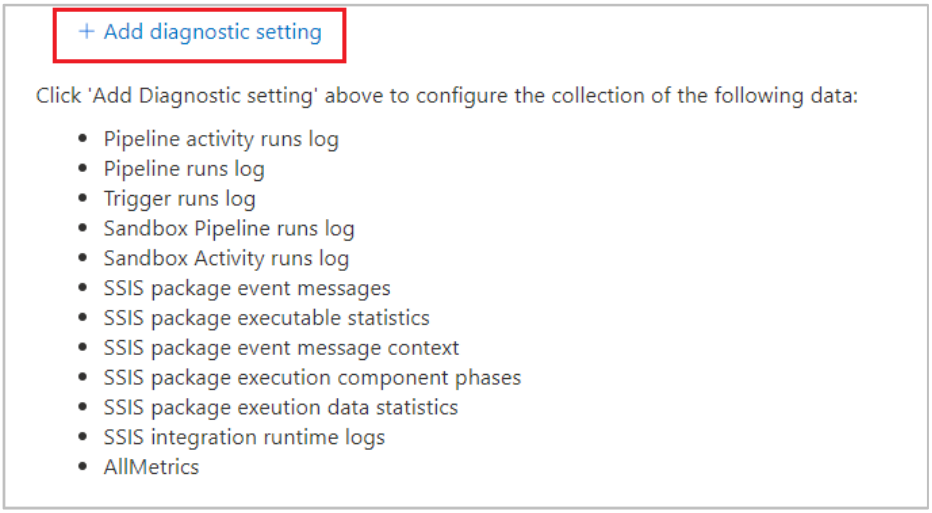


3. Then, select the appropriate Data factory which to monitor.

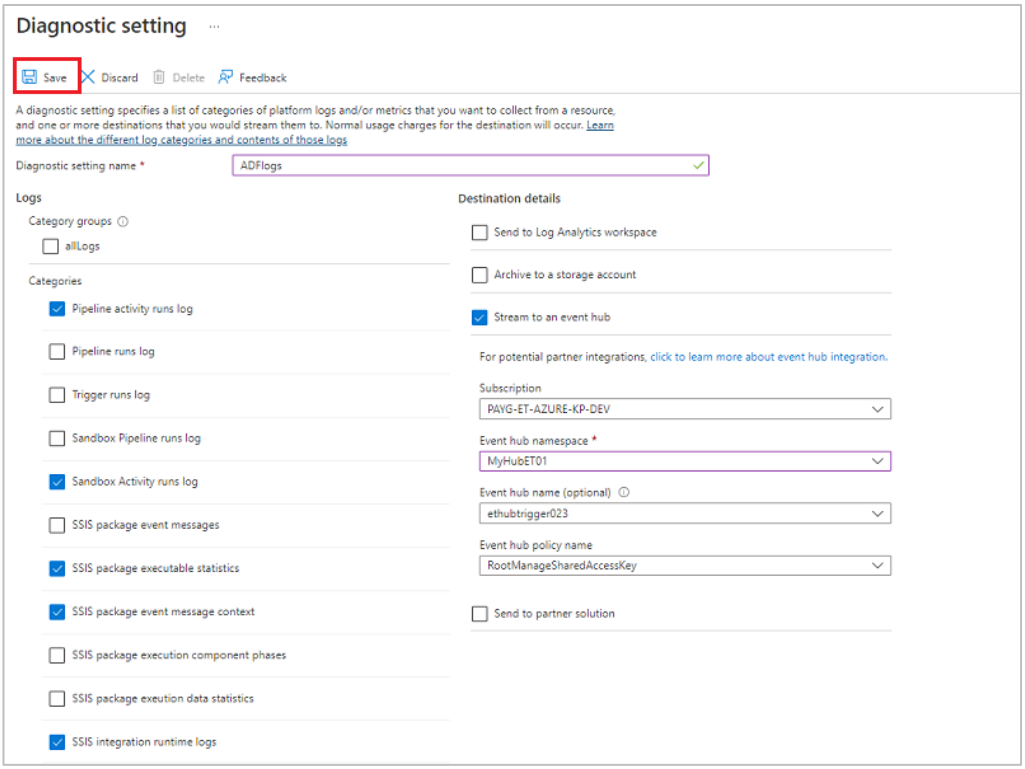
© Copyright Netsurion. All Rights Reserved.

4. From the left panel, go to **Monitoring** > **Diagnostics settings** and click **Add diagnostics setting.**





5. In the **Diagnostic setting** interface, specify the following details.



© Copyright Netsurion. All Rights Reserved.

- Provide the **Diagnostics settings name**, such as **EventTracker_Data factory**.
- From the left of the interface, in the **Logs** section select the following logs.
  - Pipeline activity runs log
  - Sandbox Activity runs log
  - SSIS package executable statistics
  - SSIS package event message context
  - SSIS integration runtime logs
  - SSIS execution data statistics
- From the right of the interface, in the **Destination details** section, select **stream to an Event Hub** and then choose the following.
  - **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.

6. After providing all the details, click **Save.**

© Copyright Netsurion. All Rights Reserved.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at www.netsurion.com.

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.