Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring SQL Server on Azure to Forward Logs to EventTracker

Publication Date:

March 29, 2022

Abstract

This guide provides instructions to retrieve the **SQL Server on Azure** 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, then 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 **the SQL Server on Azure.**

Audience

The Administrators who are assigned the task to monitor the **SQL Server on Azure** events using EventTracker.

Table of Contents

1. Overview

SQL Server on Azure gets a high-performing, unified SQL platform built on the industry-leading SQL Server engine with limitless scalability and intelligent performance and security. Migrate without the need to redesign your apps, improve the performance of the existing apps, and build highly scalable cloud services by switching to Azure—the best cloud destination for your mission-critical SQL Server workloads. EventTracker helps to monitor events from the SQL Server on Azure. Its dashboard and reports will help you track, SQL server activity with the performed statement, actions performed with session Id for a better understanding of database action flow which potentially leads to data loss and manipulation of organization decisions, functions.

2. Prerequisites

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

3. Configuring SQL Server on Azure to Forward Logs to EventTracker

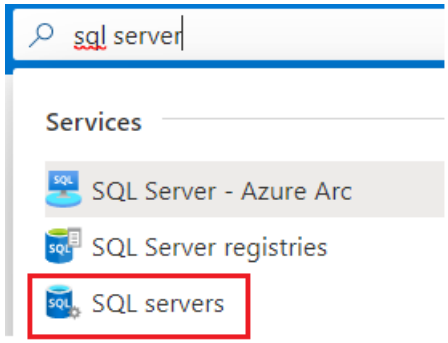
SQL Server on Azure can be integrated with EventTracker by streaming the logs to the Azure Event Hub, and from Azure Event Hub to EventTracker.

3.1 Forwarding Event Hub data to EventTracker

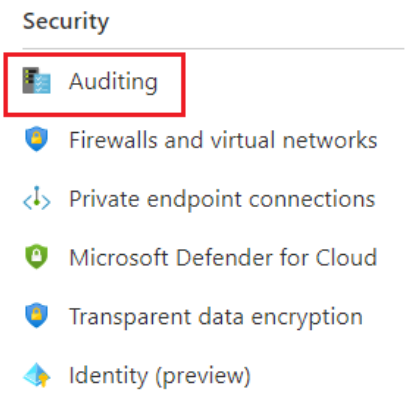
Refer to the configuration of the Azure function app to forward the logs to EventTracker.

3.2 Configuring SQL Server on Azure to stream events to Event Hubs

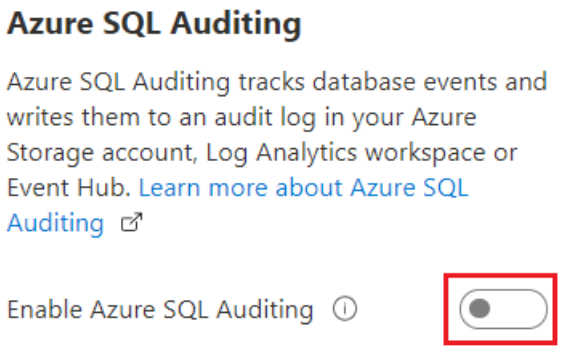
1. Login to portal.azure.com using the Admin account and create an event hub namespace, if not created.
2. Search and select **SQL Server** from **All services**.



3. From the left panel under **Security** select **Auditing**.



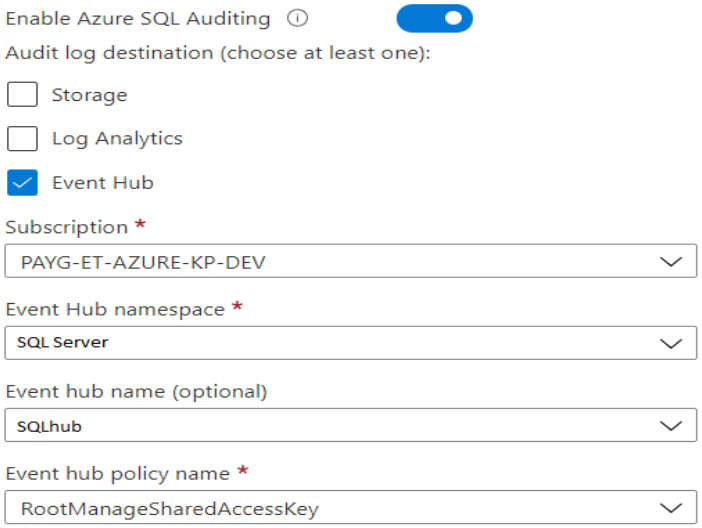
4. **Enable** Azure SQL Auditing.



5. Provide the inputs.

   In the **Audit log Destination** section, check **Event Hubs** and then choose the following options.

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



6. Click **OK/Save.**

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