Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configure Azure Cache for Redis to forward logs to EventTracker

Publication Date:

June 21, 2022

Abstract

This guide provides instructions to configure and retrieve the events from the Azure Cache for Redis via the Azure Event Hub and then forward the logs to EventTracker.

Scope

The configuration details in this guide are consistent with Azure Cache for Redis and EventTracker version 9.3 or above.

Audience

This guide is for the administrators responsible for configuring the Azure Cache for Redis events using EventTracker.

Table of Contents

1 Overview

Azure Cache for Redis is a fully managed, in-memory cache service on Microsoft Azure that implements the open-source Redis. Redis enables high-performance and scalable architectures that bring a critical low-latency and high-throughput data storage solution to modern applications. It can process large volumes of application requests by retaining frequently accessed data in the server memory, which can be written to and read quickly.

Netsurion facilitates monitoring events retrieved from the Azure Cache for Redis. The dashboard, category, alerts, and reports in Netsurion's threat protection platform, EventTracker, will benefit you in tracking users connected to cache and their connection count.

2 Prerequisites

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

3 Configuring Azure Cache for Redis to forward logs to EventTracker

Azure Cache for Redis can be integrated with EventTracker by streaming the logs to the Azure Event Hub, and from Azure Event Hub to EventTracker.

3.1 Create Event Hub and Function App

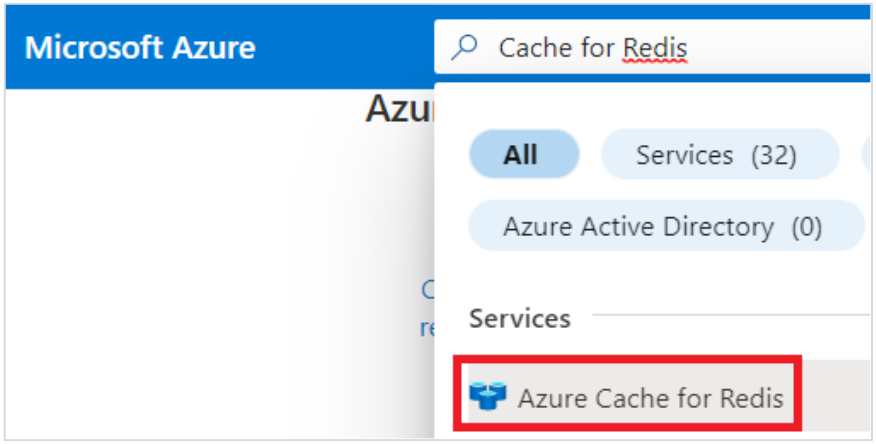
Refer to the configuration of Azure Cache for Redis to create the Event Hub and Function App.

3.2 Configuring Azure Cache for Redis to stream events to Event Hub

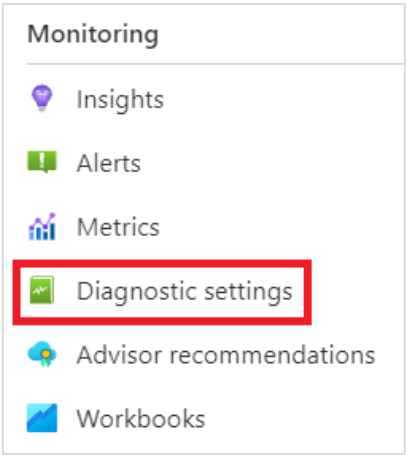
To configure Microsoft Azure Cache for Redis to stream events to Event Hub, as an Administrator,

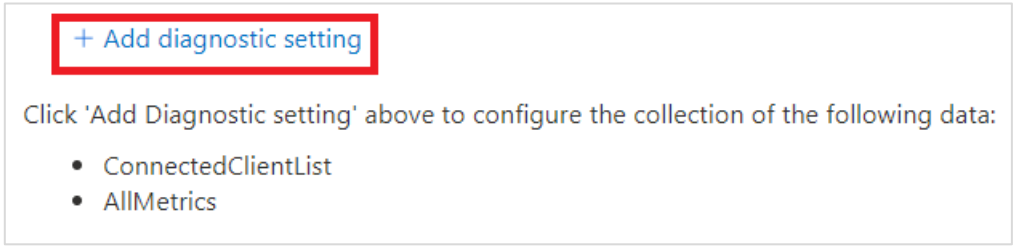
1. Log in to portal.azure.com and create an event hub namespace.

2. In the **Microsoft Azure** webpage, click **All** services, then search and select **Azure Cache for Redis** and choose the required Cache to monitor.



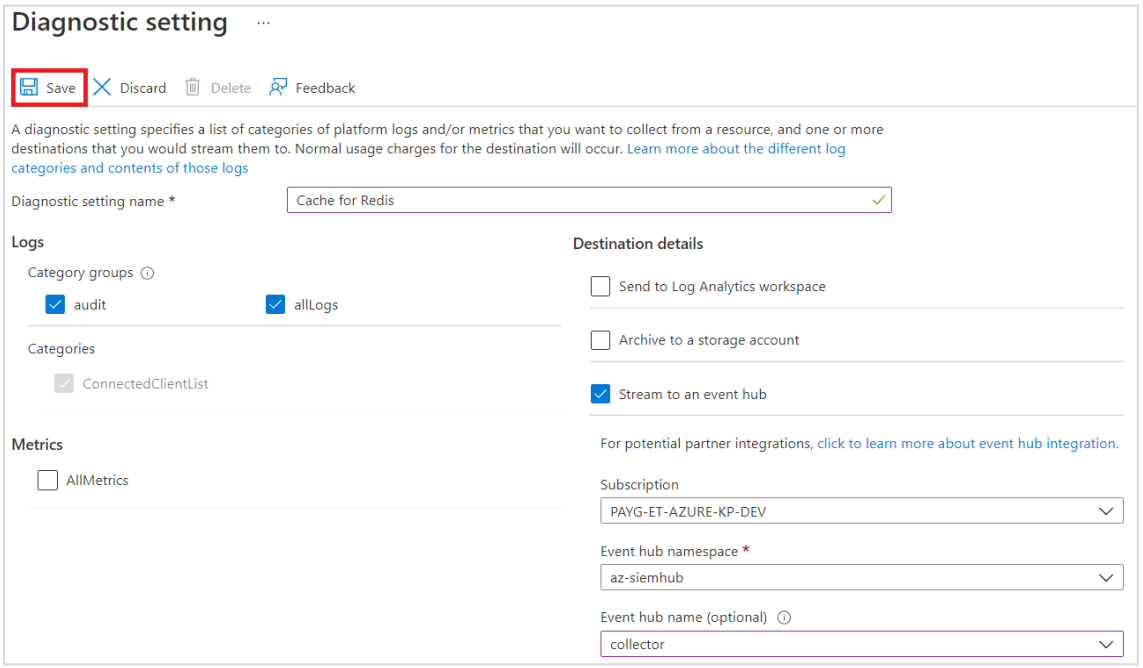
3. From the left panel, go to **Monitoring** > **Diagnostics settings** and click **Add diagnostics setting.**





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

   - Provide the **Diagnostics settings name**, such as **EventTracker_Cache for Redis**.
   - From the left of the interface, in the **Logs** > **Category groups** section, select **allLogs** to include all the logs from the **Categories** section.
   - From the right of the interface, in the **Destination details** section, select **Stream to an event hub** and then choose the following.
     - **Subscription:** Choose the appropriate Azure subscription from the drop-down list.
     - **Event Hub namespace:** Choose the Event Hub namespace from the drop-down list.
     - **Event Hub name:** Choose the Event Hub created under Event Hub namespace from the drop-down list.
     - **Event Hub policy name:** Choose the Event Hub policy from the drop-down list.



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

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