How-To Guide

Configure Azure Database for MySQL to forward logs to EventTracker

Publication Date:

July 11, 2022

Abstract

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

Scope

The configuration details in this guide are consistent with Azure Database for MySQL and EventTracker version 9.3 or later.

Audience

This guide is for the administrators responsible for configuring the Azure Database for MySQL events using EventTracker.

Table of Contents

1 Overview

Azure Database for MySQL is a relational database service in the Microsoft Azure cloud that uses the MySQL Community Edition database engine. It benefits you to stay focused on rapid app development and rev your time to market rather than managing virtual machines and infrastructure.

Netsurion facilitates monitoring events from the Azure Database for MySQL. The dashboard, categories, alerts, and reports interface in Netsurion's threat protection platform, EventTracker, benefits in tracking database activities and changes to detect any suspicious activities performed on the MySQL database.

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 Database for MySQL to forward logs to EventTracker

Integrate Azure Database for MySQL with EventTracker by streaming the logs to the Azure Event Hub and from Azure Event Hub to EventTracker.

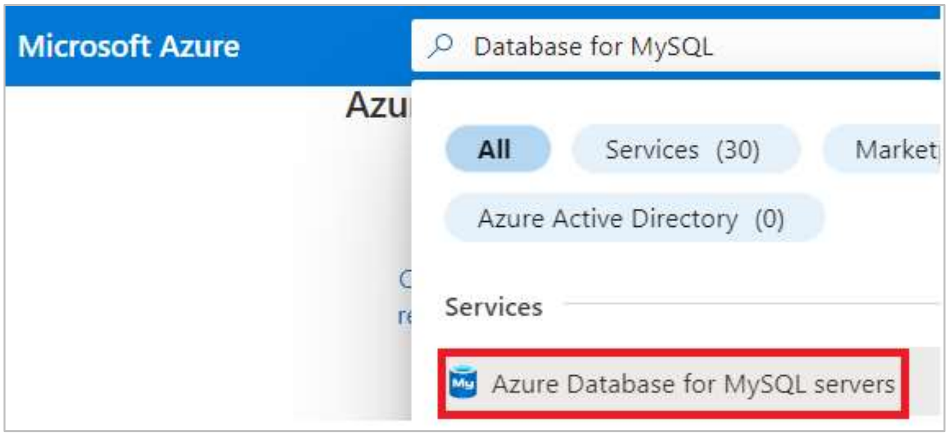
3.1 Create Event Hub and Function App

Refer to the configuration of Azure Database for MySQL to create the Event Hub and Function App.

3.2 Configuring Azure Database for MySQL to stream events to Event Hub

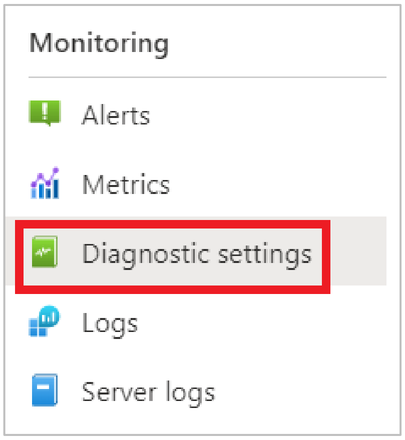
To configure Microsoft Azure Database for MySQL to stream events to Event Hub, as an Administrator,

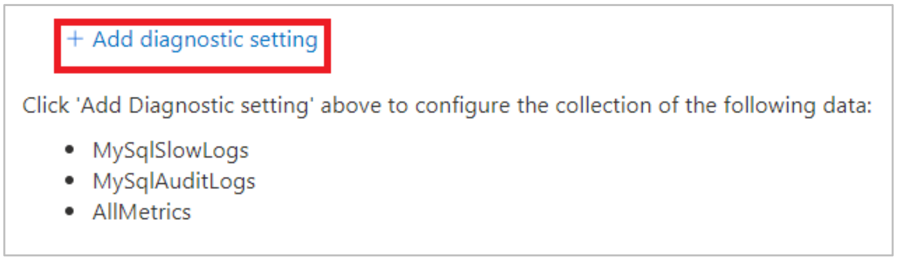
1. Log in to Microsoft Azure account and create an event hub namespace.
2. In the **Microsoft Azure** console, click **All** services, then search and select **Database for MySQL**.



3. Then select the appropriate Database for MySQL to monitor.

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



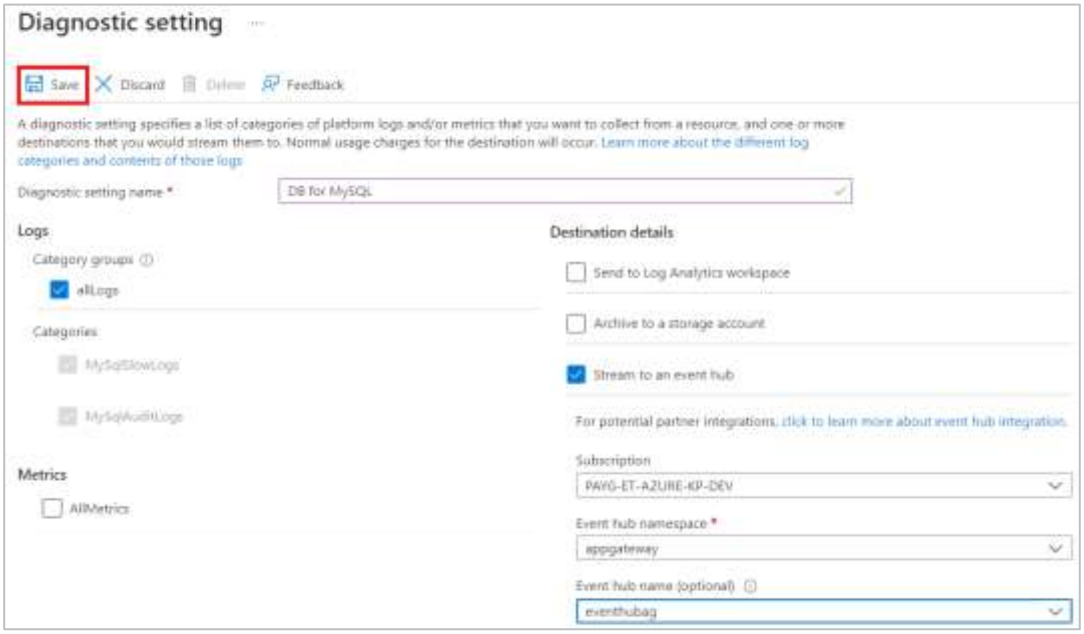


Click 'Add Diagnostic setting' above to configure the collection of the following data:

- MySqlSlowLogs
- MySqlAuditLogs
- AllMetrics

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

- Provide the **Diagnostics settings name**, such as **EventTracker_Database for MySQL**.
- From the left of the interface, in the **Logs** > **Category groups** section, select **allLogs** to include all the logs from the **Categories** section.



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 * DB for MySQL

Logs

Category groups

☑ allLogs

Categories

☑ MySqlSlowLogs

☑ MySqlAuditLogs

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 *: appgateway

Event hub name (optional): eventhubag

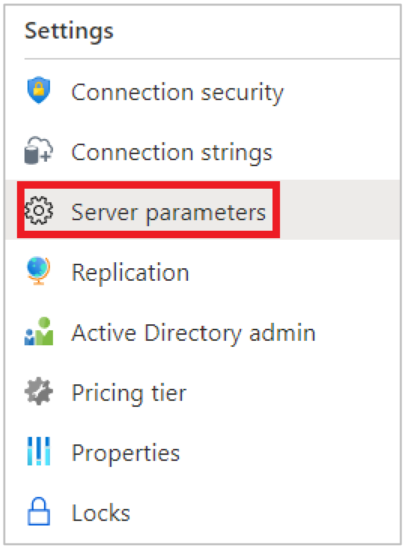
- From the right of the interface, in the **Destination details** section, select **Stream to an event hub** and then choose the following.
  - **Subscription:** Choose the appropriate Azure subscription from the drop-down list.
  - **Event Hub namespace:** Choose the Event Hub namespace from the drop-down 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.

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

Note

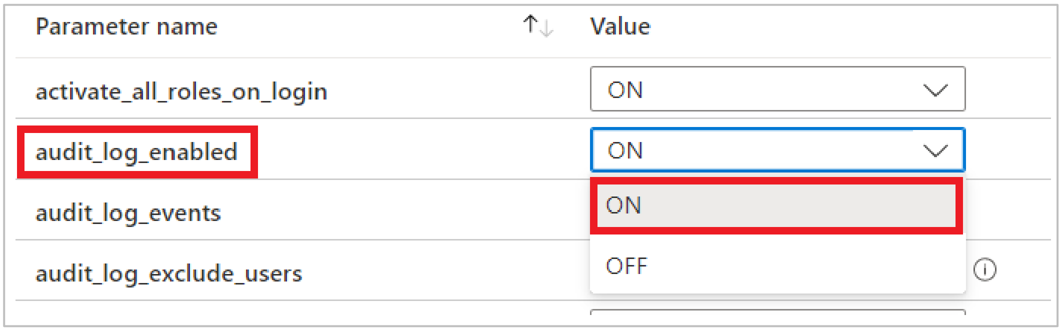
Verify if the audit and the slow logs are enabled, else perform the following process.

7. In the **Microsoft Azure** console, go to **Settings** and click **Server parameters** to enable the audit and slow logs.



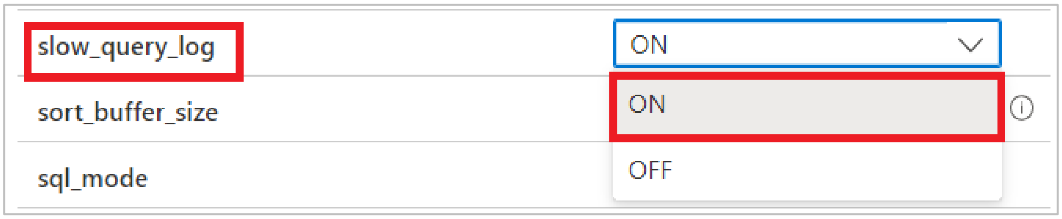
8. In the **Server parameters** interface, specify the following details:

- **Audit_log_enabled**: Click **ON** from the drop-down list to enable the audit log.



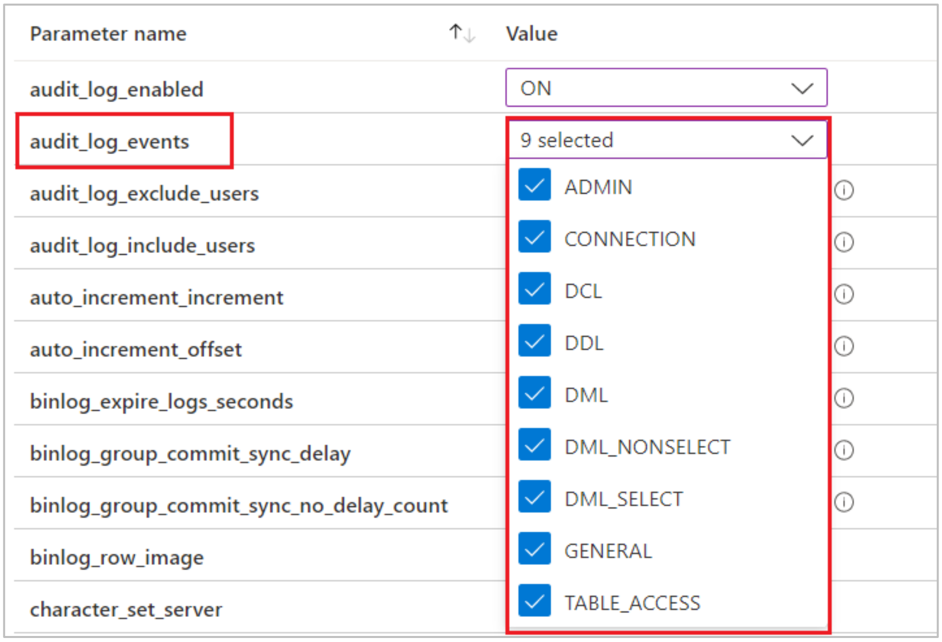
Parameter name	Value
activate_all_roles_on_login	ON
audit_log_enabled	ON
audit_log_events	
audit_log_exclude_users	

- **Slow_query_log:** Click **ON** from the drop-down list to enable the slow log.



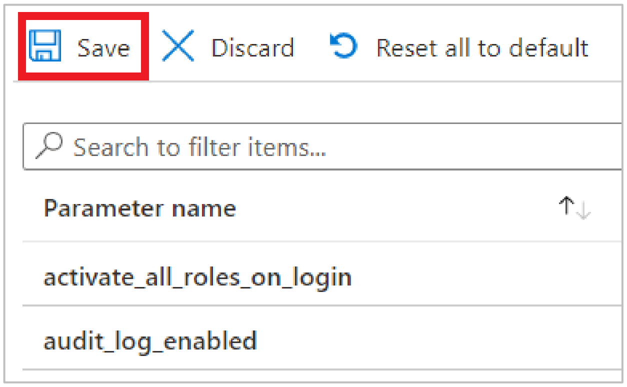
slow_query_log	ON
sort_buffer_size	ON
sql_mode	OFF

- **audit_log_events**: Select the required audit events to be included in log from the drop-down.



Parameter name ↑↓	Value
audit_log_enabled	ON
audit_log_events	9 selected
audit_log_exclude_users	☑ ADMIN
audit_log_include_users	☑ CONNECTION
auto_increment_increment	☑ DCL
auto_increment_offset	☑ DDL
binlog_expire_logs_seconds	☑ DML
binlog_group_commit_sync_delay	☑ DML_NONSELECT
binlog_group_commit_sync_no_delay_count	☑ DML_SELECT
binlog_row_image	☑ GENERAL
character_set_server	☑ TABLE_ACCESS

9. 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 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