

How-To Guide

Configure Azure Application Gateway to forward logs to EventTracker

Publication Date:

September 02, 2022

Abstract

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

Scope

The configuration details in this guide are consistent with ETS-Azure-LogForwarder version 1.0 and above and EventTracker version 9.3 or later.

Audience

This guide is for the administrators responsible for configuring the Azure Application Gateway events using EventTracker.

Table of Contents

1	Overview	4
2	Prerequisites	4
3	Configuring Azure Application Gateway to forward logs to EventTracker	4
3.1	Create Event Hub and Function App	4
3.2	Configuring Azure Application Gateway to stream events to Event Hub	4

1 Overview

Azure Application Gateway is a web traffic load balancer that enables managing traffic to web applications. The Azure Application Gateway supports features like SSL/TLS termination, Autoscaling, Zone redundancy, Static VIP, Web Application Firewall, Ingress Controller for AKS, URL-based routing, Multiple-site hosting, Redirection, Session affinity, and more.

Netsurion facilitates monitoring events retrieved from the Azure Application Gateway. The dashboard, category, alerts, and reports in Netsurion's threat protection platform, EventTracker, benefit in tracking application vulnerabilities, brute force attacks, scripting attacks, SQL injection attacks, and others.

2 Prerequisites

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

3 Configuring Azure Application Gateway to forward logs to EventTracker

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

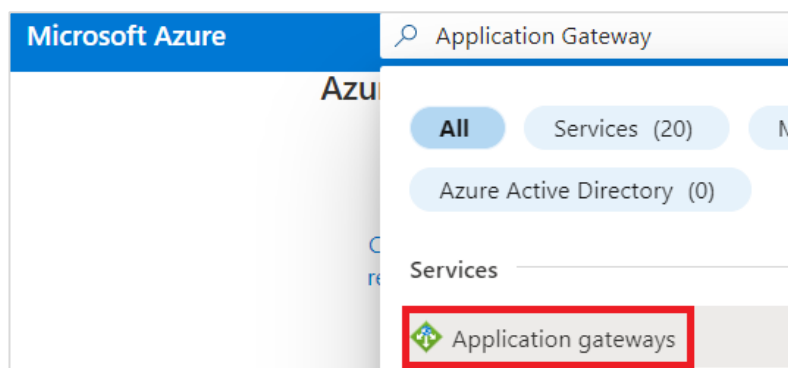
3.1 Create Event Hub and Function App

Refer to the configuration of [Azure Active Directory](#) to create the Event Hub and Function App.

3.2 Configuring Azure Application Gateway to stream events to Event Hub

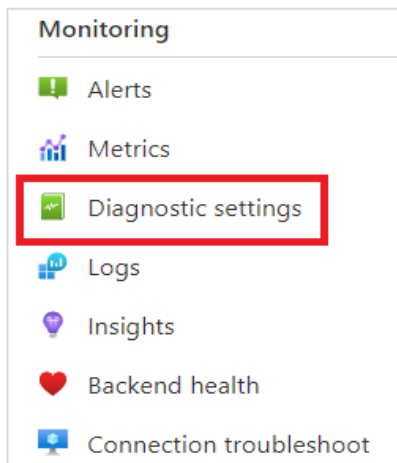
To configure Microsoft Azure Application Gateway to stream events to Event Hub, as an Administrator,

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 **Application Gateway**.



3. Then, select the appropriate Application Gateway to monitor.

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

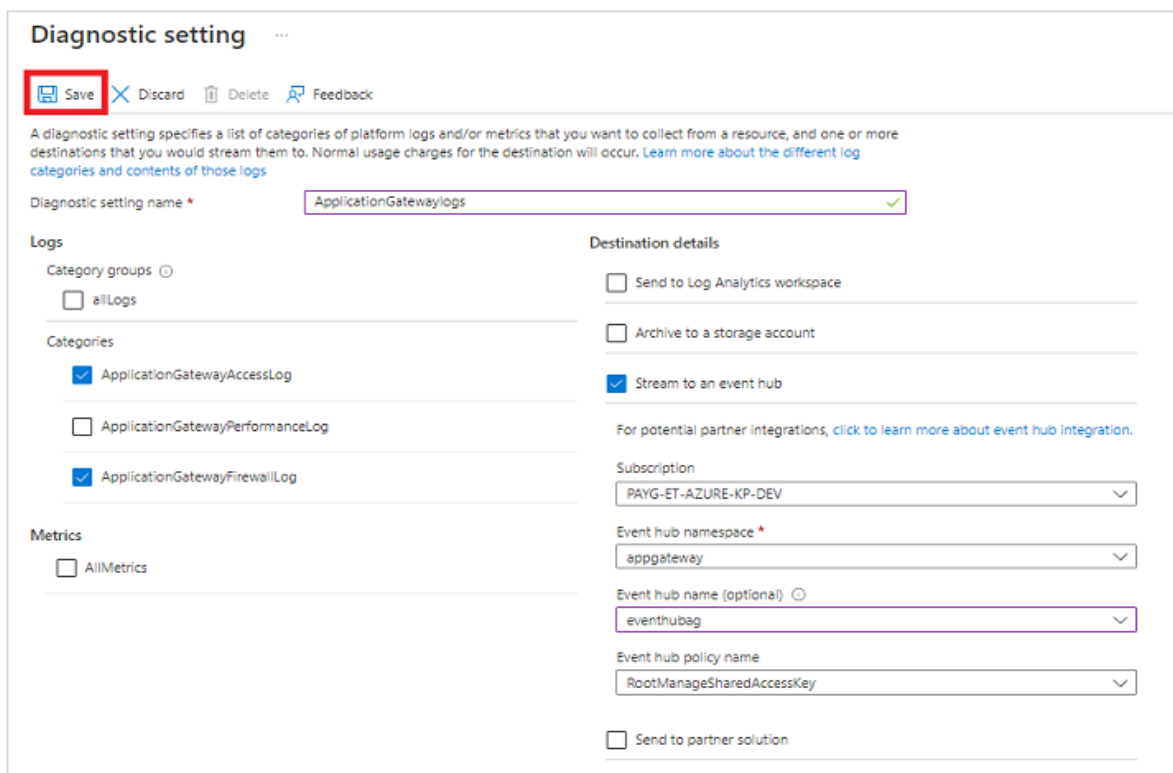


+ Add diagnostic setting

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

- ApplicationGatewayAccessLog
- ApplicationGatewayPerformanceLog
- ApplicationGatewayFirewallLog
- AllMetrics

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



The image shows the 'Diagnostic setting' configuration page. At the top, there are buttons for 'Save' (highlighted with a red box), 'Discard', 'Delete', and 'Feedback'. Below the buttons is a description: '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](#)'.

The 'Diagnostic setting name' field is set to 'ApplicationGatewaylogs'.

Under the 'Logs' section, there are two sub-sections: 'Category groups' and 'Categories'. In 'Category groups', the 'allLogs' checkbox is unchecked. In 'Categories', the checkboxes for 'ApplicationGatewayAccessLog', 'ApplicationGatewayPerformanceLog', and 'ApplicationGatewayFirewallLog' are checked.

Under the 'Metrics' section, the 'AllMetrics' checkbox is unchecked.

Under the 'Destination details' section, there are two checkboxes: 'Send to Log Analytics workspace' (unchecked) and 'Archive to a storage account' (unchecked). The 'Stream to an event hub' checkbox is checked. Below this, there is a link: 'For potential partner integrations, [click to learn more about event hub integration](#)'.

The 'Subscription' dropdown is set to 'PAYG-ET-AZURE-KP-DEV'. The 'Event hub namespace' dropdown is set to 'appgateway'. The 'Event hub name (optional)' dropdown is set to 'eventhubag'. The 'Event hub policy name' dropdown is set to 'RootManageSharedAccessKey'. The 'Send to partner solution' checkbox is unchecked.

- Provide the **Diagnostics settings name**, such as **EventTracker_Application Gateway**.
 - From the left of the interface, in the **Logs > Categories** section select **ApplicationGatewayaccessLog** and **ApplicationGatewayFirewallLog**.
 - 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**.

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>