Netsurion | EventTracker®

How to - Configure F5 Big IP DNS to forward logs to EventTracker

EventTracker v9.x and above

Publication Date: July 1, 2020

Abstract

This guide provides instructions to configure F5 Big IP DNS to send its logs to EventTracker.

Scope

The configuration details in this guide are consistent with EventTracker version v9.x or above and **F5 Big IP DNS**

Audience

Administrators who are assigned the task to monitor F5 Big IP DNS events using EventTracker.

Table of Contents

1. Overview

The **BIG IP** platform delivers F5's high-performance DNS Services with visibility, reporting, and analysis hyper scales and secures DNS responses geographically to survive DDoS attacks, delivers a real-time DNSSEC solution and ensures high availability of global applications in all cloud environments.

EventTracker helps to monitor events from F5 BIG IP DNS. EventTracker's reports provide detailed information of all events, alerts are helpful to determine and stop the attack and suspicious activities in real-time, and dashboards will help you to analyze all the security-related events in a single console. Also, we can create and save log search rules/queries under the saved search feature for real-time and historical log search.

2. Prerequisites

- Admin privileges for **F5 BIG IP DNS** to configure DNS logging.
- **EventTracker agent** should be installed in the system.

3. Integration of F5 Big IP DNS with EventTracker

F5 Big IP DNS logs we can get by using syslog.

3.1 Creating a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the EventTracker that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG IP system.

Create a pool of remote log servers to which the BIG IP system can send log messages.

1. On the **Main** tab, click **DNS** > **Delivery** > **Load Balancing** > **Pools** or **Local Traffic** > **Pools**. The **Pool List** screen opens.
2. Click **Create**. The new Pool screen opens.
3. In the **Name** field, type name as "**EventTracker-F5-DNS**" for the pool.
4. Using the **New Members** setting, add the EventTracker IP address that you want to include in the pool.
   Type an **EventTracker IP address** in the **Address** field or select the EventTracker address from the **Node** List.
   Type a service number **514** in the **Service Port** field or select a service name from the list.
   Note: Typical remote logging servers require UDP port 514.
   Click **Add**.
5. Click **Finished**.

3.2 Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG IP system.
Create a log destination of the Remote High-Speed Log type to specify that log messages are sent to a pool of remote log servers.

1. On the **Main** tab, click **System** > **Logs** > **Configuration** > **Log Destinations**. The **Log Destinations** screen opens.
2. Click **Create**
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log.**
   Important: If you use log servers such as **Remote Syslog**, EventTracker, which require data be sent to the servers in a specific format, you must create an additional log destination of the required type, and associate it with a log destination of the Remote High-Speed Log type. With this configuration, the BIG IP system can send data to the servers in the required format.
   The BIG IP system is configured to send an unformatted string of text to the log servers.
5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG IP system to send log messages.
6. From the **Protocol list**, select the protocol used by the high-speed logging pool members.
7. Click **Finished**.

3.3 Creating a formatted remote high-speed log destination

Ensure that at least one remote high-speed log destination exists on the BIG IP system.
Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog, EventTracker.

1. On the Main tab, click **System > Logs > Configuration > Log Destinations**. The Log Destinations screen opens.
2. Click **Create.**
3. In the **Name field**, type a unique, identifiable name “” for this destination.
4. From the **Type list**, select a formatted logging destination, such as **Remote Syslog**.
5. The BIG IP system is now configured to send a formatted string of text to the log servers.
6. If you select **Remote Syslog**, from the **Type list**, select a format for the logs, and then from the **Forward To** select **High-Speed Log Destination** list, select the destination that points to a pool of remote syslog servers to which you want the BIG IP system to send log messages.
7. Click **Finished**.

3.4 Creating a custom DNS logging profile for logging DNS queries and responses

Create a custom DNS logging profile to log both DNS queries and responses when troubleshooting a DDoS attack.

Note: Logging both DNS queries and responses has an impact on the BIG IP system performance.

1. On the **Main** tab, click **DNS > Delivery > Profiles > Other > DNS Logging** or **Local Traffic > Profiles > Other > DNS Logging**. The **DNS Logging** profile list screen opens.
2. Click **Create**. The **New DNS Logging Profile** screen opens.
3. In the **Name field**, type name as "EventTracker-DNS" for the profile.
4. From the **Log Publisher** list, select EventTracker a destination to which the BIG IP system sends DNS log entries.
5. For the **Log Queries setting**, ensure that the **Enabled** checkbox is selected, if you want the BIG IP system to log all DNS queries.
6. For the **Log Responses setting**, select the **Enabled** checkbox, if you want the BIG IP system to log all DNS responses.
7. For the Include **Query ID setting**, select the **Enabled** checkbox, if you want the BIG IP system to include the query ID sent by the client in the log messages.
8. Click **Finished**.

3.5 Creating a custom DNS profile to enable DNS logging

Ensure that at least one custom DNS logging profile exists on the BIG IP® system.

Create a custom DNS profile to log specific information about DNS traffic processed by the resources to which the DNS profile is assigned. Depending upon what information you want the BIG IP system to log, attach a custom DNS Logging profile configured to log DNS queries, to log DNS responses, or to log both.

1. On the **Main** tab, click **DNS > Delivery > Profiles > DNS or Local Traffic > Profiles > Services > DNS**.
2. The DNS profile list screen opens.
3. Click **Create**.
4. The New DNS Profile screen opens.
5. In the Name field, type a unique name for the profile.
6. Select the Custom check box.
7. In the Logging and Reporting area, from the Logging list, select **Enabled**.
8. In the Logging and Reporting area, from the Logging Profile list, select a custom DNS Logging profile.
9. Click Finished.

You must assign this custom DNS profile to a resource before the BIG IP system can log information about the DNS traffic handled by the resource.

3.6 Configuring a listener for DNS logging

Ensure that at least one custom DNS profile with logging configured exists on the BIG IP® system.
Assign a custom DNS profile to a listener when you want the BIG IP system to log the DNS traffic the listener handles.
Note: This task applies only to GTM™-provisioned systems.

1. On the **Main tab**, click **DNS > Delivery > Listeners**.
2. The Listeners List screen opens.
3. Click the name of the listener you want to modify.
4. In the Service area, from the DNS Profile list, select a custom DNS profile that is associated with a DNS Logging profile.
5. Click Update.

3.7 Configuring an LTM virtual server for DNS logging

Ensure that at least one custom DNS profile with logging enabled exists on the BIG IP® system.
Assign a custom DNS profile with logging enabled to a virtual server when you want the BIG IP system to log the DNS traffic the virtual server handles.
Note: This task applies only to LTM®-provisioned systems.

1. On the Main tab, click **Local Traffic > Virtual Servers**.
2. The Virtual Server List screen opens.
3. Click the name of the virtual server you want to modify.
4. From the **Configuration** list, select **Advanced**.
5. From the DNS Profile list, select a custom DNS profile that is associated with a DNS Logging profile.
6. Click **Update** to save the changes.