Netsurion. | EventTracker®

How to – Configure Microsoft DNS Server with EventTracker

EventTracker v9.2 and later

Publication Date: February 24, 2021

Abstract

The purpose of this document is to help the user in monitoring the Microsoft DNS server analytics log files by deploying Windows Agent.

Scope

The configuration details in this guide are consistent with **EventTracker v9.2** and later, and DNS server hosted on **Windows Server 2012 R2** and later.

Audience

Administrators, who are assigned the task to monitor and manage Microsoft DNS Server events using EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Table of Contents

1. Overview

A DNS server hosts the information that enables client computers to resolve memorable, alphanumeric DNS names to the IP addresses that the computers use to communicate.

EventTracker platform supports Microsoft DNS Server and it facilitates viewing DNS analytics logs to monitor configuration changes, policy changes, creation, deletion and modification in resource record and zones. It also generates alert for configuration changes, deletion of zone and resource record when DNS server is down.

EventTracker provides a deeper insight using advanced DNS KP (Knowledge Pack), with DNS debug logs to detect various suspicious activities. It can monitor malicious site from client machine by comparing DNS queries generated by DNS client with malicious site database (periodically updated) and generate alerts about the client and geological information of malicious site (IP, Country).

EventTracker advanced DNS KP detects the access of DGA (Domain Generated Algorithm) domains, which are used as command control centers for malwares and trojans. Its persistent statistics monitoring of query, client, record type and error helps in detecting various DDOS attacks such as NXDOMAIN attack, phantom domain attack, random sub-domain attack, etc. It can monitor server DNS latency and client DNS settings to detect DNS hijacking. It generates alerts for suspicious DNS setting on client and high server latency.

EventTracker's flex dashboard provides visualization and correlation of detected attack with client and domain details, thus preventing prevalent threats and abnormal behavior.

2. Prerequisites

Prior to configuring Windows Server 2012 R2 and later and EventTracker v8.x or later, ensure to meet the following pre-requisites :

- Administrative access to EventTracker.
- Microsoft DNS Server should be installed and configured.
- User should have administrative rights on Microsoft DNS Server.
- Firewall between Microsoft DNS Server and EventTracker should be off or exception for EventTracker ports.
- EventTracker agent should be installed on Microsoft DNS Server.

3. Enabling Microsoft DNS Server Analytical logging

Following are the steps for getting enhanced analytic logs for Microsoft DNS Server:

3.1 Install DNS diagnostic logging

DNS diagnostics logging is available by default in Windows Server 2016 but not present in Windows Server 2012 R2. However, this feature can be made available in Windows Server 2012 R2 Standard and below versions by installing **Hotfix.**
Note: Hotfix should be downloaded in Windows Server 2012 R2 Standard and below versions only.

Steps to install DNS diagnostic logging for Windows Server 2012 R2 Standard is given below.

1. Download **Hotfix for Windows (KB2956577)** from here.
2. Install Hotfix.
3. Verify installation of the hotfix by typing the below command in Command prompt.
   wmic qfe | find KB2956577.
4. It will display URL and date of installation for the hotfix.

3.2 Enable DNS diagnostic and analytical logging.

Note: DNS diagnostic and analytical logging capability are available by default in Windows Server 2016, Windows Server 2012 Datacenter and above.
Steps for enabling DNS diagnostic logging.

1. Go to **Event Viewer** on Windows DNS Server.
2. Navigate to **Applications and Services Logs\Microsoft\Windows\DNS-Server.**

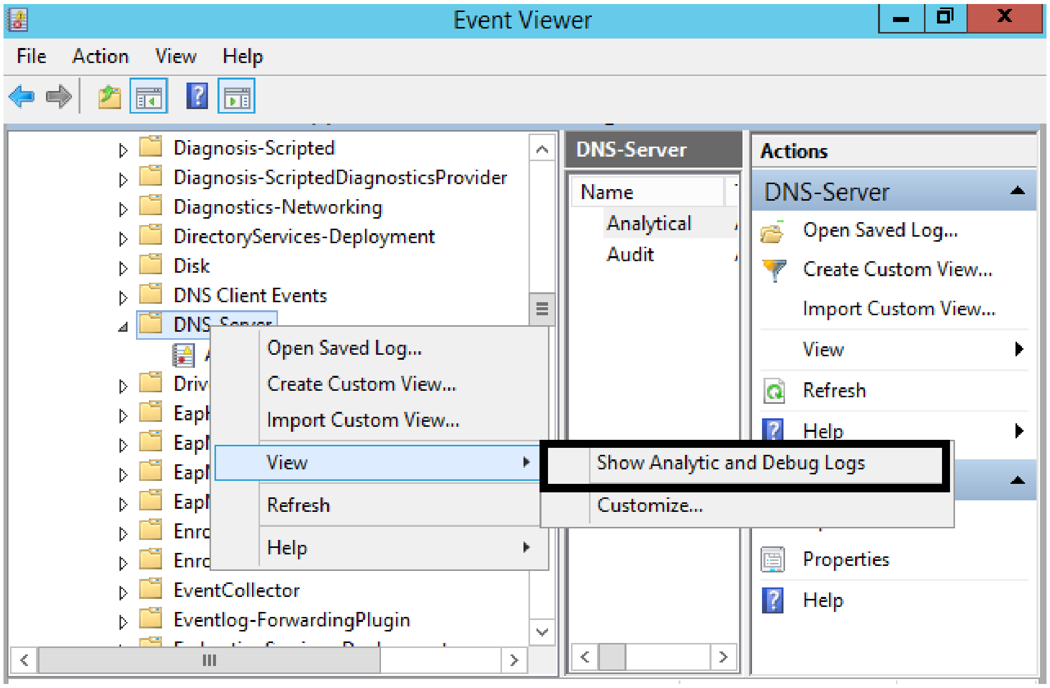


Figure 1

3. Right-click **DNS-Server**, point to **View**, and then click **Show Analytic and Debug Logs**.

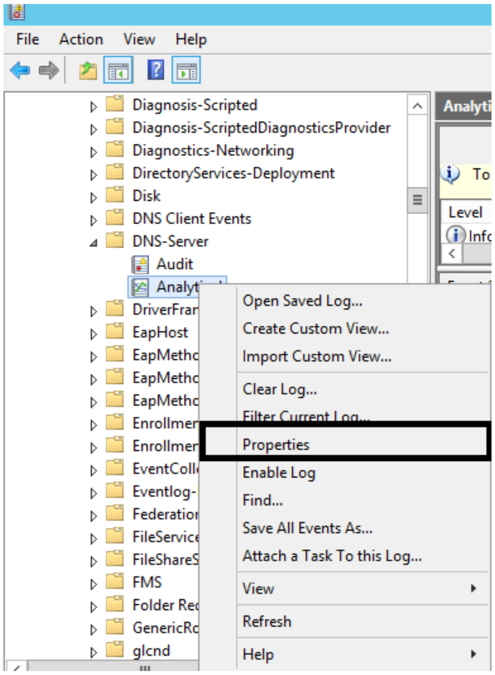
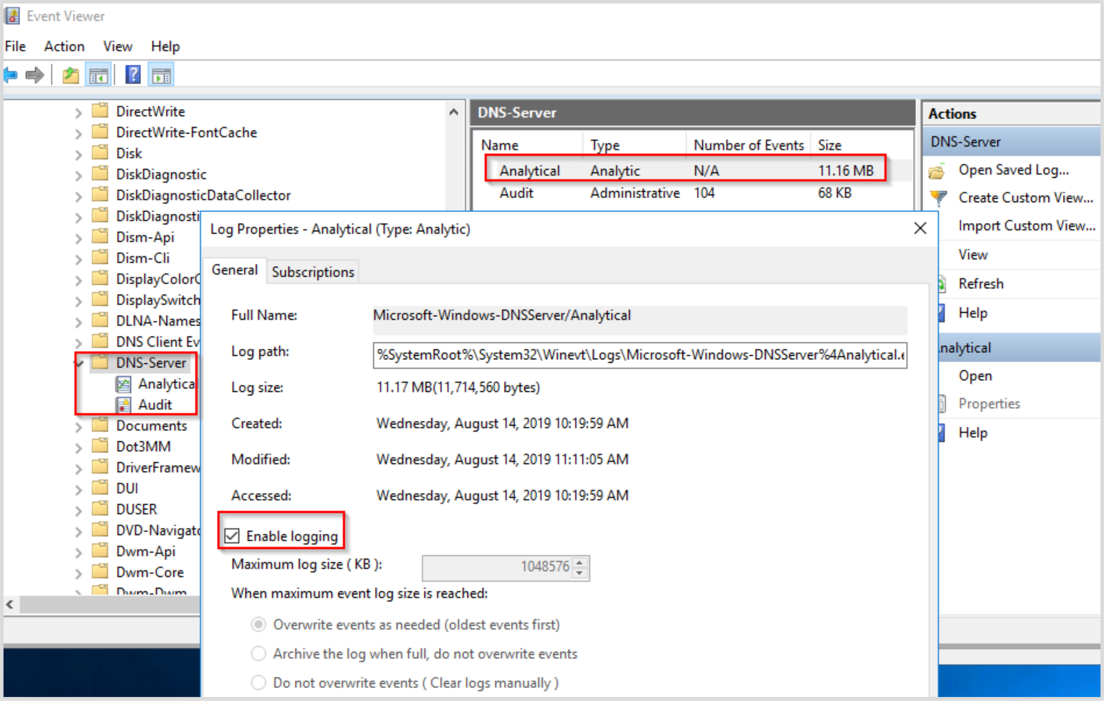


Figure 2

4. Right-click **Analytical** and then click **Properties**.



Name	Type	Number of Events	Size
Analytical	Analytic	N/A	11.16 MB
Audit	Administrative	104	68 KB

Log Properties - Analytical (Type: Analytic)

General | Subscriptions

Full Name: Microsoft-Windows-DNSServer/Analytical

Log path: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-DNSServer%4Analytical.e

Log size: 11.17 MB(11,714,560 bytes)

Created: Wednesday, August 14, 2019 10:19:59 AM

Modified: Wednesday, August 14, 2019 11:11:05 AM

Accessed: Wednesday, August 14, 2019 10:19:59 AM

☑ Enable logging

Maximum log size (KB): 1048576

When maximum event log size is reached:

● Overwrite events as needed (oldest events first)

○ Archive the log when full, do not overwrite events

○ Do not overwrite events (Clear logs manually)

Figure 3

5. Enter **maximum log size** 1048576 kb.
6. Click **Overwrite events as needed (oldest events first)**.
7. click **OK.**
8. Check **Enable logging** to enable the DNS Server Analytical log. Then click **OK**.

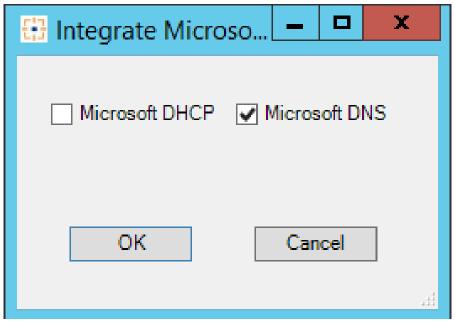
By default, analytic logs are written to the file:

%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-DNSServer%4Analytical.etl.

4. Configuration for sending logs to EventTracker

NOTE: To forward logs to EventTracker, LFM need to be configure using PowerShell script.

1. EventTracker uses Log File Monitor (LFM) in the Windows agent to access DNS analytical logs. To perform LFM configuration, deploy the EventTracker agent on DNS server.
2. Contact support team to get integrator for DNS.
3. Refer EventTracker Agent installation guide.
4. After installation ET agent and run “Integrate DNS and DHCP.exe”.



Integrate Microso...

☐ Microsoft DHCP ☑ Microsoft DNS

Figure 4

5. Check the option **Microsoft DNS** and click **ok.**
6. Integrator will configure LFM for **Microsoft DNS Server** and logs sent to EventTracker.