Integrate Microsoft DNS Server

EventTracker v8.x and above

Publication Date: March 29, 2019
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 configurations detailed in this guide are consistent with EventTracker Enterprise v8.x 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.
Table of Contents

Abstract .................................................................................................................................................. 1
Scope .................................................................................................................................................... 1
Audience ................................................................................................................................................ 1
Overview ............................................................................................................................................... 3
Prerequisites .......................................................................................................................................... 3
Enabling Microsoft DNS Server Analytical logging .............................................................................. 3
   Install DNS diagnostic logging ........................................................................................................ 3
   Enable DNS diagnostic and analytical logging .................................................................................. 4
Configuration for sending logs to EventTracker .................................................................................... 6
EventTracker Knowledge Pack .............................................................................................................. 7
   Reports ............................................................................................................................................... 7
   Alerts .................................................................................................................................................. 8
   Dashboards ........................................................................................................................................ 10
Import knowledge pack into EventTracker ............................................................................................ 11
   Alerts ................................................................................................................................................ 12
   Category ........................................................................................................................................... 15
   Tokens .............................................................................................................................................. 17
   Templates ......................................................................................................................................... 18
Verify knowledge pack in EventTracker .................................................................................................. 20
   Alerts ................................................................................................................................................ 20
   Categories ........................................................................................................................................ 21
   Tokens .............................................................................................................................................. 22
   Templates ......................................................................................................................................... 22
   Flex Reports ..................................................................................................................................... 23
   Sample Dashboard ............................................................................................................................. 26
Overview

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

The EventTracker Enterprise supports Microsoft DNS Server. This guide employs DNS analytics logs to aid monitoring of configuration changes, policy changes, creation, deletion and modification in resource record and zones. It also generates alert for changes in configuration, deletion of zone and resource record and when DNS server services are down.

EventTracker Enterprise can also provide a deeper insight using advanced DNS KP which employs DNS debug logs to detect an array of suspicious activities which include access monitoring of malicious site from client machine by comparing DNS queries generated by DNS client with malicious site database (periodically updated) and generates alert about the client and geological information about that malicious site (IP, Country).

EventTracker advanced DNS KP is capable to detect the access of DGA (Domain Generated Algorithm) domains which are used as command control centers for malwares and Trojans. It’s persistent statistics monitoring of query, client, record type and error will help you to detect many DDOS attacks like (NXDOMAIN attack, Phantom domain attack, Random sub-domain attack, etc.). It can keep a watch on sever DNS latency and client DNS settings and help in detection of DNS hijacking and generate alert for suspicious DNS setting on client and high server latency. EventTracker’s flex dashboard helps in visualization and correlation of detected attack with client and domain details, thus providing protection against prevalent threats and abnormal behavior.

Prerequisites

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

- Administrative access to EventTracker.
- Microsoft DNS Server should to 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.

Enabling Microsoft DNS Server Analytical logging

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

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 by installing Hotfix.
Steps for installing DNS diagnostic logging for Windows Server 2012 R2

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.

Enable DNS diagnostic and analytical logging.

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
3. Right-click DNS-Server, point to View, and then click Show Analytic and Debug Logs.
4. Right-click Analytical and then click Properties.
5. Click “Do not overwrite events (Clear logs manually)”. Then click OK again to enable the DNS Server Analytical log.

6. By default, analytic logs are written to the file:
   %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-DNSServer%4Analytical.etl.

**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”.

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

**EventTracker Knowledge Pack**

Once logs are received into EventTracker; Categories and Reports can be configured into EventTracker. The following Knowledge Packs are available in EventTracker Enterprise to support Microsoft DNS Server.

**Reports**

- **Microsoft DNS-Zone creation, deletion and updating**: This report provides information related to zone creation, deletion and updating in scope and by whom.
- **Microsoft DNS-Resource record creation and deletion**: This report provides information related to Resource record creation and deletion in zone and by whom.
- **Microsoft DNS-Configuration changes**: This report provides information related to configuration changes with the name of the configuration and by whom it was made.
- **Microsoft DNS-Query resolution successfully**: This report provides information related to FQDN or IP address, query type (forward lookup or reverse), status of query, when query successfully resolved from DNS Server.
- **Microsoft DNS-Query resolution failed**: This report provides information related to FQDN or IP address, query type (forward lookup or reverse), status of query, when query fails to resolve from DNS Server.
- **DNS- Error type count details**: This report provides information about error queries count for an error type. It gives details of error type and count of query for it.
- **DNS- Error client count details**: This report provides information about error queries count for a client. It gives details of client IP address and count of query for it.
• **DNS- Summary client count details:** This report provides information about successful query count for a client. It gives details of client IP address and count of query for it.

• **DNS- Summary query count details:** This report provides information about successful query for a FQDN resolution request. It gives details of FQDN query requested and its count.

• **DNS- Error query count details:** This report provides information about error query for a FQDN resolution request. It gives details of FQDN query requested and its count.

• **DNS- Traffic details:** This report provides information about the query request to DNS server. It gives details of query request (FQDN, record type) and client details (IP address).

• **DNS- Summary record type details:** This report provides information about successful query for a record type. It gives details of record type requested and count of queries.

• **DNS-Malicious domain detection details:** This report provides information related to detection of malicious domain from DNS logs. It gives information about malicious domain, client trying to access, its record type and when the client trying to access it.

• **DNS-Malformed domain detection details:** This report provides information related to detection of malformed domain from DNS logs. It gives information about malformed domain, method of creation (typo-squatted methods), client trying to access such domain and its geological details.

• **DNS-Suspicious DNS settings detection details:** This report provides information related to suspicious client DNS setting. It gives information for client having suspicious DNS setting and its DNS settings.

• **DNS-DGA domain detection details:** This report provides information related to detection of DGA domains from DNS logs. It gives information for DGA domain details (FQDN and its IP) and client details.

• **DNS-Least resolved domain details:** This report provides information about least resolved domain in a network. It gives information for least domains resolved from DNS server and client details.

• **DNS-Server latency details:** This report provides information about latency of provided DNS (private and public DNS). It gives information for DNS server and its latency.

**Alerts**

• **Microsoft DNS: Service down** - This alert is generated when DNS service is down in Microsoft DNS Server.
• **Microsoft DNS: Configuration changes** - This alert is generated when configuration changes happen in scope, zone or resource record in Microsoft DNS Server.

• **Microsoft DNS: Object deletion in zone** – This alert is generated when zone or resource record is deleted from any scope in Microsoft DNS Server.

• **Microsoft DNS: Name resolution failed** – This alert is generated when resolution of FQDN name is failed by Microsoft DNS Server.

• **DNS: Malformed domain detected** - This alert is generated when EventTracker detects malformed (typo-squatted) domains from queries in the DNS logs.

• **DNS: Snort high priority alert generated** - This alert is generated when Snort detects high priority alerts for DNS.

• **DNS: DGA domain detected** - This alert is generated when EventTracker detects DGA (Domain generated algorithm) domains from DNS logs.

• **DNS: Suspicious DNS settings detected** - This alert is generated when DNS setting of clients is other than recommended settings.

• **DNS: Malicious domain detected** - This alert is generated when malicious domain is detected from DNS logs.

• **DNS: High DNS server latency detected** - This alert is generated when latency of DNS server is greater than threshold value.

• **DNS: High error query count detected for domain** - This alert is generated when error query count is greater than threshold for a domain.

• **DNS: High error query count detected for type** - This alert is generated when error query count is greater than threshold for a record type.

• **DNS: High error query count detected from client** - This alert is generated when error query count is greater than threshold for a client.

• **DNS: High query count detected for record type** - This alert is generated when successful query count is greater than threshold for a record type.
Integrate Microsoft DNS Server

- **DNS: High query count detected from client** - This alert is generated when successful query count is greater than threshold for a client.

- **DNS: High query count detected from domain** - This alert is generated when successful query count is greater than threshold for a domain.

Dashboards

- **Microsoft DNS: Top URL usage** – This dashboard gives us the information about usage of URL inside the network.

- **Microsoft DNS: Resource record operations** – This dashboard gives us the information about the created and deleted resource record in a DNS zone.

- **Microsoft DNS: Zone operations** – This dashboard gives us the information about the creation, deletion and the updating of DNS zone.

- **DNS: Error pattern** – This dashboard gives us the information about the count of query for an error type.

- **DNS: Top queried domains** – This dashboard gives us the information about the count of query for a domain.

- **DNS: Top queried domains with errors** – This dashboard gives us the information about the count of error query for a domain.

- **DNS: Top querying clients** - This dashboard gives us the information about the count of query for a client.

- **DNS: Top querying clients with errors** – This dashboard gives us the information about the count of error query for a client.

- **DNS: Record type pattern** – This dashboard gives us the information about the count of query for a record type.

- **DNS: Suspicious domains detected** - This dashboard gives us the information of access of malware domain from a client.

- **DNS: Received traffic** – This dashboard gives us the information of received traffic in DNS server.
- **DNS: Send traffic** – This dashboard gives us the information of send traffic from DNS server.

- **DNS: Malformed domains detected** – This dashboard gives us the information of typo-squatted domains access from a client.

- **DNS: Server latency** – This dashboard gives us the information about latency of a public and internal DNS server.

- **DNS: DGA domain detected** – This dashboard gives us the information about the access of DGA domains access by a client.

- **DNS: Suspicious DNS settings detected** – This dashboard gives us the information about the client having suspicious DNS settings.

- **DNS: Least resolved domains** – This dashboard gives us the information about the least domain resolved over network.

### Import knowledge pack into EventTracker

**NOTE**: Import knowledge pack items in the following sequence:
- Alerts
- Categories
- Token templates
- Flex Reports

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.
3. Click the **Import** tab.

**Alerts**

1. Click **Alerts** option, and then click the browse button.

2. Locate **.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

   EventTracker displays success message.

   ![Import Success](image)

   **Figure 7**

4. Click **OK**, and then click the **Close** button.

5. After importing the alerts configuration, please select the Window DNS server system.

6. Logon to **EventTracker Enterprise**.
7. Click **Admin** dropdown, and then click **Alerts**.

8. In **Search** field, type ‘**Microsoft DNS**’, and then click the **Go** button.

9. Click any **Microsoft DNS alert** and then click **Systems** tab and then select the Window DNS server machine.
10. After selecting Microsoft DNS Server machine, click **FINISH** button to save the configuration.

**Category**

1. Click **Category** option, and then click the browse button.
2. Locate .iscat file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays success message.

4. Click **OK**, and then click the **Close** button.
Tokens

1. Click **Token value** option, and then click the browse button.

2. Locate the `.istoken` file, and then click the **Open** button.

3. To import tokens, click the **Import** button.

   EventTracker displays success message.
4. Click OK, and then click the Close button.

Templates

1. Logon to EventTracker Enterprise.
2. Click the Admin menu and then click the Parsing rule.
3. Click the Template tab.
4. Click the Import button, it will open new window. (Note: Make sure pop-up is enabled for EventTracker).

7. Locate and choose .ETTD file and then click the Open button.
8. Select the template you want to upload.
9. Then click **Import configuration** button.
EventTracker displays success message.

![Image of success message]

Figure 17

10. Click **OK** and it will automatically close the window.

**Verify knowledge pack in EventTracker**

**Alerts**

1. Logon to **EventTracker Enterprise**.
2. Click **Admin** dropdown, and then click **Alert**
3. In **Search** field, type ‘**Microsoft DNS**’, and then click the **Go** button.

Alert Management page will display all the imported Microsoft DNS alerts.

![Image of Alert Management page]

Figure 18

4. To activate the imported alerts, select the respective checkbox in the **Active** column.
EventTracker displays message box.

![Successfully saved configuration.

Figure 19](image)

5. Click **OK**, and then click the **Activate Now** button.

**NOTE:** You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

**Categories**

1. Logon to **EventTracker Enterprise**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand Microsoft DNS Server group folder to view the imported categories.
Tokens

1. Logon to EventTracker Enterprise.
2. Click the Admin dropdown, and then click Parsing rule.
3. Imported Microsoft DNS Server tokens added in Token-Value Groups list at the right side of Parsing rule tab of EventTracker Enterprise (as shown in below figure).

Templates

1. Logon to EventTracker Enterprise and navigate to Admin->Parsing rule.
2. Click Template tab.
3. Click Microsoft DNS Server group.
4. Check the template you have uploaded.
Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports.
3. Select the Configuration.
4. In the Reports Configuration, select Defined radio button. EventTracker displays Defined page.
5. In search box enter Microsoft DNS. EventTracker displays flex reports of Microsoft DNS.
Here you can find imported defined reports such as Microsoft DNS-Name resolution successfully.

1. Microsoft DNS-Resource record creation and deletion

<table>
<thead>
<tr>
<th>LogTime</th>
<th>EventUser</th>
<th>Computer</th>
<th>Name</th>
<th>Action</th>
<th>Zone</th>
<th>Scope</th>
<th>Type</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/25/2015 04:05:06 PM</td>
<td>John</td>
<td>ESXWIN2K12R2VM2</td>
<td><a href="http://www.contoso">www.contoso</a></td>
<td>deleted</td>
<td>contoso</td>
<td>Default</td>
<td>600</td>
<td></td>
</tr>
<tr>
<td>09/25/2016 04:05:06 PM</td>
<td>Sam</td>
<td>ESXWIN2K12R2VM2</td>
<td><a href="http://www.contoso">www.contoso</a></td>
<td>created</td>
<td>contoso</td>
<td>Default</td>
<td>3600</td>
<td></td>
</tr>
</tbody>
</table>
2. Microsoft DNS-Name resolution successfully.

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Source Addr</th>
<th>Source Port</th>
<th>Interface IP</th>
<th>Query Name</th>
<th>Query Type</th>
<th>Status</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-09-25T06:55:37.536881300000Z</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0</td>
<td>google.com.Teens.local</td>
<td>RECURSE_QUERY</td>
<td>RECURSE_QUERY_OUT</td>
<td></td>
</tr>
<tr>
<td>2015-09-25T06:55:32.340676200000Z</td>
<td>127.0.0.1</td>
<td>69723</td>
<td>127.0.0.1</td>
<td>1.0.127.in-addr.arpa.</td>
<td>LOCK_UP</td>
<td>RESPONSE_SUCCESS</td>
<td></td>
</tr>
<tr>
<td>2015-09-25T06:55:37.536881300000Z</td>
<td>192.5.5.241</td>
<td>0</td>
<td>0.0.0.0</td>
<td>google.com.Teens.local</td>
<td>RECURSE_QUERY</td>
<td>RECURSE_QUERY_OUT</td>
<td></td>
</tr>
<tr>
<td>2015-09-25T06:55:32.340676200000Z</td>
<td>192.5.5.241</td>
<td>0</td>
<td>0.0.0.0</td>
<td>google.com.Teens.local</td>
<td>RECURSE_QUERY</td>
<td>RECURSE_QUERY_OUT</td>
<td></td>
</tr>
<tr>
<td>2015-09-25T06:55:32.340676200000Z</td>
<td>192.5.5.241</td>
<td>0</td>
<td>0.0.0.0</td>
<td>google.com.Teens.local</td>
<td>RECURSE_QUERY</td>
<td>RECURSE_QUERY_OUT</td>
<td></td>
</tr>
<tr>
<td>2015-09-25T06:55:32.340676200000Z</td>
<td>192.5.5.241</td>
<td>0</td>
<td>0.0.0.0</td>
<td>google.com.Teens.local</td>
<td>RECURSE_QUERY</td>
<td>RECURSE_QUERY_OUT</td>
<td></td>
</tr>
<tr>
<td>2015-09-25T06:55:32.340676200000Z</td>
<td>192.5.5.241</td>
<td>0</td>
<td>0.0.0.0</td>
<td>google.com.Teens.local</td>
<td>RECURSE_QUERY</td>
<td>RECURSE_QUERY_OUT</td>
<td></td>
</tr>
<tr>
<td>2015-09-25T06:55:32.340676200000Z</td>
<td>192.5.5.241</td>
<td>0</td>
<td>0.0.0.0</td>
<td>google.com.Teens.local</td>
<td>RECURSE_QUERY</td>
<td>RECURSE_QUERY_OUT</td>
<td></td>
</tr>
<tr>
<td>2015-09-25T06:55:32.340676200000Z</td>
<td>192.5.5.241</td>
<td>0</td>
<td>0.0.0.0</td>
<td>google.com.Teens.local</td>
<td>RECURSE_QUERY</td>
<td>RECURSE_QUERY_OUT</td>
<td></td>
</tr>
<tr>
<td>2015-09-25T06:55:32.340676200000Z</td>
<td>192.5.5.241</td>
<td>0</td>
<td>0.0.0.0</td>
<td>google.com.Teens.local</td>
<td>RECURSE_QUERY</td>
<td>RECURSE_QUERY_OUT</td>
<td></td>
</tr>
<tr>
<td>2015-09-25T06:55:32.340676200000Z</td>
<td>192.5.5.241</td>
<td>0</td>
<td>0.0.0.0</td>
<td>google.com.Teens.local</td>
<td>RECURSE_QUERY</td>
<td>RECURSE_QUERY_OUT</td>
<td></td>
</tr>
<tr>
<td>2015-09-25T06:55:32.340676200000Z</td>
<td>192.5.5.241</td>
<td>0</td>
<td>0.0.0.0</td>
<td>google.com.Teens.local</td>
<td>RECURSE_QUERY</td>
<td>RECURSE_QUERY_OUT</td>
<td></td>
</tr>
<tr>
<td>2015-09-25T06:55:32.340676200000Z</td>
<td>192.5.5.241</td>
<td>0</td>
<td>0.0.0.0</td>
<td>google.com.Teens.local</td>
<td>RECURSE_QUERY</td>
<td>RECURSE_QUERY_OUT</td>
<td></td>
</tr>
<tr>
<td>2015-09-25T06:55:32.340676200000Z</td>
<td>192.5.5.241</td>
<td>0</td>
<td>0.0.0.0</td>
<td>google.com.Teens.local</td>
<td>RECURSE_QUERY</td>
<td>RECURSE_QUERY_OUT</td>
<td></td>
</tr>
<tr>
<td>2015-09-25T06:55:32.340676200000Z</td>
<td>192.5.5.241</td>
<td>0</td>
<td>0.0.0.0</td>
<td>google.com.Teens.local</td>
<td>RECURSE_QUERY</td>
<td>RECURSE_QUERY_OUT</td>
<td></td>
</tr>
<tr>
<td>2015-09-25T06:55:32.340676200000Z</td>
<td>192.5.5.241</td>
<td>0</td>
<td>0.0.0.0</td>
<td>google.com.Teens.local</td>
<td>RECURSE_QUERY</td>
<td>RECURSE_QUERY_OUT</td>
<td></td>
</tr>
</tbody>
</table>

Figure 25
Sample Dashboard

1. Microsoft DNS: Top URL usage

![Microsoft DNS: Top URL usage](image1)

Figure 26

2. Microsoft DNS: Resource record and operations today

![Microsoft DNS: Resource record and operations today](image2)

Figure 27
3. DNS-Error pattern

![Figure 28](image)

**Figure 28**

4. DNS-Top queried domains

![Figure 29](image)

**Figure 29**
5. DNS-Top queried domains with errors

Figure 30

6. DNS-Top querying clients

Figure 31
7. DNS-Top querying clients with errors

Figure 32

8. DNS-Record type pattern

Figure 33