Integrate Microsoft DNS Server (Advanced)

EventTracker Enterprise
Abstract
This guide provides instructions to configure Microsoft DNS server and forward debug events to EventTracker Enterprise, which performs threat and performance analytics on collected logs.

Scope
The configurations detailed in this guide are consistent with EventTracker Enterprise version 8.x and later, and DNS server hosted on Windows server 2008 r2 and later.

Audience
Administrators, who wish to monitor Microsoft DNS server using EventTracker Enterprise.
Table of Contents

Abstract.................................................................................................................................................. 1
  Scope................................................................................................................................................ 1
  Audience....................................................................................................................................... 1

Introduction ................................................................................................................................... 4

General Prerequisites ......................................................................................................................... 4

Configuration on DNS server workstation .......................................................................................... 4
  Prerequisites................................................................................................................................. 4
  DNS Server Configuration ............................................................................................................. 4
  EventTracker Agent Configuration .................................................................................................. 7

Configuration on EventTracker Manager workstation ........................................................................ 8
  Prerequisites................................................................................................................................. 8
  Configure Malware domain watch list ............................................................................................ 9
    Prerequisites............................................................................................................................ 9
    Malware script schedule .......................................................................................................... 9
    Watch List Verification ............................................................................................................. 14

Configure DGA detection script ......................................................................................................... 14
  Prerequisites............................................................................................................................... 14
  Python script configuration ......................................................................................................... 14
  Python script verification ............................................................................................................ 15

Configure DNS log parse script ........................................................................................................ 15
  DNS log script schedule .............................................................................................................. 15

Configure DNS settings script ........................................................................................................... 20
  Prerequisites............................................................................................................................... 20
  DNS settings script schedule ...................................................................................................... 20

Configure DNS latency script ........................................................................................................... 24
  DNS latency script schedule ........................................................................................................ 24

Configuration on EventTracker ............................................................................................................ 28
  Create Event Filters ..................................................................................................................... 28
Introduction

A **DNS server** is any computer registered to join the Domain Name System. It runs special-purpose networking software, features a public IP address, and contains a database of network names and addresses for other Internet hosts.

Microsoft Windows server operating systems can run the DNS Server service. This is a monolithic DNS server that provides many types of DNS service, including caching, Dynamic DNS update, zone transfer, and DNS notification.

General Prerequisites

1. DNS server must be installed on **Windows 2008 R2 and later**.
2. **EventTracker agent 7.6 or later** should be installed on the DNS server workstation.
3. **PowerShell 3.0 or later** must be installed on EventTracker Manager workstation.
4. **EventTracker 8.x or later** must be installed on EventTracker Manager workstation for creating flex dashlets.

Configuration on DNS server workstation

Prerequisites

1. To perform this procedure, you must be a member of the **Administrators group** on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, **members of the Domain Admins group** should be able to perform this procedure.

DNS Server Configuration

Below mentioned procedure helps to enable debug logging on DNS server.

1. Logon to Windows server hosting DNS with administrative credentials.
2. Navigate to **Start>Administrative Tools>DNS**.

DNS Manager window opens;
3. Right-click on your configured DNS server and click **Properties**.

DNS server properties window opens:
4. Click **Debug Logging** tab and select checkboxes as shown in the above example.
5. In the **Log file** section, select appropriate path for log file storage and set maximum file size as **100 KB**.
6. Click **Apply** to save.
7. Open PowerShell with administrative privileges, enter following command to enable DNS log file roll-over.

```
Set-DnsServerDiagnostics –EnableLogFileRollover $true
```

![Figure 2](image2.png)

![Figure 3](image3.png)
8. To verify log file rollover setting, open registry editor and navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters`. Check if registry name `EnableLogFileRollover` has value set as ‘1’.

**EventTracker Agent Configuration**

Below mentioned procedure helps to configure DNS log file transfer to EventTracker Manager.

![EventTracker Agent Configuration](image)

*Figure 4*
1. Logon to Windows server hosting DNS with administrative credentials.
2. Open **EventTracker Agent Configuration**, select **File Transfer** tab.
3. In the Manager section, click **Add**.

DLA Manager pane opens;

![DLA Manager Pane](image)

**Figure 5**

4. Enter the IP Address of **EventTracker Manager workstation** in System field and **14505** in port field.
5. Set encryption as per your network requirements.
6. Click **OK** and **Save** to apply changes.

**Configuration on EventTracker Manager workstation**

**Prerequisites**

1. Download DNS KP package provided by **EventTracker Support**.
2. Extract downloaded files to **C:\Program Files (x86)\Prism Microsystems\EventTracker\Configuration Files\**

EventTracker installation folder
Configure Malware domain watch list

This section provides instructions to download online malware domain list and store it as a watch list on EventTracker Manager. Domains in DNS logs are verified against this watch list for malware detection.

Prerequisites

1. Administrative privileges to EventTracker Manager workstation.
3. “SQLPS” module must be installed on PowerShell.
4. PowerShell modules can be downloaded online using following command.

```powershell
Import-Module 'sqlps'
```

Malware script schedule

1. Logon to EventTracker Manager workstation with administrative privileges.
3. In the **Actions** tab select **Create task**.
4. Configure Task properties as shown below.
5. Select **General** tab, provide appropriate task name and in **Security options** section, enable "Run whether user is logged on or not" and "Run with highest privileges" options.
6. Select **Triggers** tab, select **Weekly** with appropriate schedule settings.
7. Select **Actions** tab, enter `powershell.exe` as program name and compose argument as given below:

```
powershell.exe -executionpolicy bypass -file "C:\Program Files (x86)\Prism Microsystems\EventTracker\Configuration Files\DNS\Scripts\malware domain list download.ps1"
```

EventTracker installation folder

8. Click **OK** to save task.
Watch List Verification

1. After successful script execution, to verify new watch list on EventTracker, logon to EventTracker Manager and navigate to Admin>Active Watch Lists. New watch list named ‘Malware list’ can be found under ‘Domains’ group.

Configure DGA detection script

For DGA and detection python script is employed. Domains in DNS logs are verified against this script to identify suspicious domains.

Prerequisites

1. Python 3.x or later must be installed.
2. Python ‘Pip’ module must be installed.

Python script configuration

1. Move content from C:\Program Files (x86)\Prism Microsystems\EventTracker\Configuration Files\DNS\dga_detector-master to Python installation directory.
2. Extract download file to python installation directory.
3. Navigate to Python installation directory.
4. Install ‘tldextract’ from online python repository using following parameters.
Python script verification

1. After successful completion, check script execution as follows.

```
python .\dga_detector.py
```

Configure DNS log parse script

This script performs following activities:

1. Merges and parses raw DNS logs.
2. Detects malicious domains in DNS logs.
3. Detects DGA domains in DNS logs.
4. Summarizes DNS logs into various parameters.
5. Generates alert for suspicious domains and abnormal counts, detected in summary results.

DNS log script schedule

1. Logon to EventTracker Manager workstation with administrative privileges.
3. In the **Actions** tab select **Create task**.
4. Configure Task properties as shown below.
5. Select **General** tab, provide appropriate name and in **Security options** section, enable ’**Run whether user is logged on or not**’ and ’**Run with highest privileges**’ options.
6. Select **Triggers** tab, select **Daily** with appropriate schedule settings to ensure hourly execution.
7. Select Actions tab, enter ‘powershell.exe’ as program name and compose argument as given below:

```
powershell.exe -executionpolicy bypass -file "C:\Program Files (x86)\Prism Microsystems\EventTracker\Configuration Files\DNS\Scripts\Get-Dnslog.ps1" –computername ESXWIN2K12R2VM2 –errorthreshold 600 –summarythreshold 1000
```

- Green: EventTracker installation folder
- Red: EventTracker agent workstation name
- Blue: Threshold to trigger alerts for DNS error traffic parameters (i.e. domain, client, error types).
- Brown: Threshold to trigger alerts for DNS summary traffic parameters (i.e. domain, client, record types).
8. Click OK to save task.

Configure DNS settings script

This script performs following activities:

1. Detects DNS settings of configured IP address range.
2. Generates alerts for anomalies in DNS settings of workstations.

Prerequisites

1. Domain administrator privileges must be used for scheduling this script.

DNS settings script schedule

1. Logon to EventTracker Manager workstation with administrative privileges.

3. In the Actions tab select Create task.

Figure 18
4. Configure Task properties as shown below.

![Create Task dialog box](image)

Figure 19

5. Select **General** tab, provide appropriate name and in **Security options** section, enable "Run weather user is logged on or not" and "Run with highest privileges" options.
6. Select **Triggers** tab, select **Weekly** with appropriate schedule setting.
7. Select **Actions** tab, enter `powershell.exe` as program name and compose argument as given below:

```powershell
powershell.exe -executionpolicy bypass -file "C:\Program Files (x86)\Prism Microsystems\EventTracker\Configuration Files\DNS\Scripts\Get-Dnssetting.ps1" -start 192.168.1.118 -end 192.168.1.120 -recprim 192.168.1.11 -recsec 192.168.1.12
```

- **EventTracker installation folder**
- **DNS script location**
- **IP address range of workstations**
- **Prescribed primary and secondary DNS servers**

8. Click **OK** to save task.
Configure DNS latency script

This script measures DNS latency against locally configured and public DNS servers. E.g. OpenDNS, Google.

DNS latency script schedule

1. Logon to EventTracker Manager workstation with administrative privileges.

![Task Scheduler](image)

Figure 22

3. In the Actions tab select **Create task**.
4. Configure Task properties as shown below:
5. Select **General** tab, provide appropriate name and in **Security options** section, enable ‘**Run weather user is logged on or not**’ and ‘**Run with highest privileges**’ options.
6. Select Triggers tab, select Daily with appropriate schedule settings to ensure hourly execution.
EventTracker installation folder

Threshold to trigger alerts for local DNS server latency(ms)

8. Click OK to save task.
Configuration on EventTracker
Create Event Filters

- Logon to EventTracker manager workstation.

- Open EventTracker control panel, click **EventTracker Agent Configuration**.
Select Event Filters tab, click Filter Exception.

Filter exception window opens,
EventTracker: Microsoft DNS Server (Advanced)

Figure 28

- Click **New**, and configure event filter properties as shown below.

DNS log filter

This filter matches **DNS query logs**.

- Configure event filter details as shown below.
Figure 29

- Enter following as matching description.

```
Date&&Query&&Type&&Client&&SendReceive&&Protocol&&RecordType&&Query&&Result&&Response&&Flags
```

- Click OK to apply.

**DNS summary log filter**

This filter matches **DNS query summary logs**.

- Configure event filter details as shown below.
Enter following as matching description.

```
ParseTime && EventType
```

Click **OK** to apply.

**DNS latency filter**

This filter matches DNS latency logs.

- Configure event filter details as shown below.
• Enter following as matching description.

**DNSServerName&&LatencyInMS**

• Click **OK** to apply.

• Click **Save** to apply configured filters.
Configure Log Consumption

Prerequisites

1. Administrative privileges to EventTracker Manager workstation.

Configure LFM for DNS query log

Below mentioned procedure helps to configure LFM for DNS query logs.

1. Logon to EventTracker manager workstation.

2. Open EventTracker Control Panel, double-click EventTracker Agent Configuration.

Figure 32
3. Click **Logfile Monitor** tab, select respective checkbox
4. Click **Add File Name**.
5. Configure DNS log file as shown above. Compose log file path as given below.

```
C:\Program Files (x86)\Prism Microsystems\EventTracker\DLA\ESXWIN2K12R2VM2\LFM\Parsedlog.csv
```

- **EventTracker installation folder**
- **EventTracker agent workstation name**
- **Parsed log file name**

6. Click **Add String** in Search string window. Select “Date” from **Field Name** dropdown and ‘*’ as search string.
7. Click **OK** and **Save** to apply changes.

**Configure DLA for DNS miscellaneous logs**
Below mentioned procedure helps to configure DLA for DNS summary, latency and setting logs.

1. Logon to EventTracker.
2. Navigate to **Admin>Manager**.

![Manager Configuration](image)

**Figure 36**

4. Enter appropriate purge frequency and click **Add**.
5. Configure DLA options as shown below.
6. Configure DNS log file as shown above. Compose log file path as given below.

```
C:\Program Files (x86)\Prism Microsystems\EventTracker\DLA\ESXWIN2K12R2VM2\DLA\EventTracker installation folder EventTracker agent workstation name
```

7. Scroll down and click **Save** to proceed.
8. Select Log Source as ‘DNS Server’. Enter DNS server’s IP Address and Name in respective columns.
9. Scroll down and click Save and Close to apply.
10. Click Save on DLA pane to complete configuration.

Configure Microsoft DNS KP

1. Launch EventTracker Control Panel.
2. Double click Export Import Utility, and then click the Import tab.
Please import KP items in the following sequence:

- Token Templates
- Parsing Rules
- Behavior Rules
- Alerts
- Reports
- Knowledge Object

Import mentioned KP items as given below:

Import Token Templates

1. Click the Admin menu, and then click Parsing rule.

2. Select Template tab, and then click on ‘Import’ option.
3. Click the Browse button.

4. Locate All Microsoft DNS token template.etttd file, and then click the Open button.
5. Now select the corresponding check boxes and then click on 'Import' option.

EventTracker displays success message.

![Figure 43: Template(s) imported successfully]

6. Click on OK button.

**Import Parsing Rules**

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

![Figure 44: Export Import Utility window with Token Value option selected]
2. Locate **All Microsoft DNS parsing rules.istoken** file, and then click the **Open** button.

3. To import the token value, click the **Import** button.

   EventTracker displays success message.

   ![Figure 45](image)

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

**Import Behavior Rule**

5. Click **Behavior Rules** option, and then click the **browse** button.

   ![Figure 46](image)
6. Locate All Microsoft DNS behavior rules.isrule file, and then click the Open button.

7. To import behavior rule, click the Import button.

   EventTracker displays success message.

   ![Export Import Utility window](image)

   Figure 47

8. Click OK, and then click the Close button.

Import Alerts

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

2. Locate All Microsoft DNS alerts.isalt file, and then click the Open button.

   ![Export Import Utility window](image)

   Figure 48
3. To import alerts, click the **Import** button.

   EventTracker displays success message.

   ![Figure 18](image)

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

**Import Flex Reports**

1. Click **Reports** option, and then click the 'browse' button.
2. Locate **All Microsoft DNS reports.issch** file, and then click the **Open** button.

   ![Figure 49](image)
3. To import reports, click the **Import** button. EventTracker displays success message.

![Figure 50](image)

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

**Import Knowledge Object**

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on ‘**Import**’ icon.

![Figure 51](image)
3. In IMPORT pane click on Browse button.

![Figure 52](image)

4. Locate All Microsoft DNS KO.etko file, and then click the UPLOAD button.

![Figure 53](image)

5. Now select the check box and then click on 'OVERWRITE' option.

EventTracker displays success message.
6. Click on OK button.

Verify Microsoft DNS KP

Token Templates
1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Parsing rule.
3. Select Template tab.
4. In Token Templates Groups Tree, select Microsoft DNS group folder.

Imported token templates are shown on the right pane.
Behavior Rule
1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Behavior Rules.
3. Scroll and find Microsoft DNS query traffic rule name.
4. Select ACTIVE checkbox to enable behavior rule.
Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and select **Alerts**.
3. In **Search** field, type ‘**Microsoft DNS**’, and then click the ✕ button.

Alert Management page will display all the imported Microsoft DNS alerts.
4. To activate the imported alerts, select the respective checkbox in the Active column.

EventTracker displays message box.

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

NOTE: Please specify appropriate systems in alert configuration for better performance.

Flex Reports
1. Logon to EventTracker Enterprise.
2. Click the **Reports** menu and select **Configuration**.
3. Select **Defined** in report type.

Imported reports are displayed on the right pane.

![Figure 59](image)

**Knowledge Object**

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Knowledge Objects**.
3. In **Objects Tree**, select **Microsoft DNS group** folder.

Imported **Microsoft DNS** objects are shown on the right pane.
EventTracker Knowledge Pack (KP)

Once logs are received into EventTracker, Behavior Rules, Alerts, Reports and Dashboards can be configured into EventTracker. The following Knowledge Packs are available in EventTracker to support Microsoft DNS monitoring.

Reports

- **Microsoft DNS - Traffic details**

This report provides information related to DNS query traffic.
EventTracker: Microsoft DNS Server (Advanced)

**Date:** 06/01/2016 17:48:41.19  
**Query Type:** Forward  
**Client:** 10.30.6.17  
**Send/Receive:** Snd  
**Protocol:** TCP  
**Record Type:** A  
**Query:** google.com  
**Results:** NOERROR  
**Response:** Q  
**Flags:** D

- **Microsoft DNS- Error type count**

This report provides information related to error type counts in DNS logs.

```
<table>
<thead>
<tr>
<th>Event Time</th>
<th>Computer</th>
<th>Error Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/01/2016 17:48:25.92</td>
<td>CONTOSO-DNSSVR1</td>
<td>NXDOMAIN</td>
<td>77</td>
</tr>
<tr>
<td>06/01/2016 17:48:26.17</td>
<td>CONTOSO-DNSSVR1</td>
<td>REFUSED</td>
<td>63</td>
</tr>
<tr>
<td>06/01/2016 17:48:26.34</td>
<td>CONTOSO-DNSSVR1</td>
<td>SRVFAIL</td>
<td>28</td>
</tr>
</tbody>
</table>
```

**Figure 62**

- **Name:** NXDOMAIN  
  **Count:** 77  
  **Parse Time:** 06/01/2016 17:48:25.92  
  **Event Type:** DNS Error Type Summary

- **Microsoft DNS- Error client count**

This report provides information related to client counts for DNS logs with errors.

```
<table>
<thead>
<tr>
<th>Event Time</th>
<th>Computer</th>
<th>Client Address</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/01/2016 17:48:25.32</td>
<td>CONTOSO-DNSSVR1</td>
<td>10.30.6.17</td>
<td>37</td>
</tr>
<tr>
<td>06/01/2016 17:48:25.74</td>
<td>CONTOSO-DNSSVR1</td>
<td>10.30.6.201</td>
<td>70</td>
</tr>
<tr>
<td>06/01/2016 18:04:43.64</td>
<td>CONTOSO-DNSSVR1</td>
<td>10.30.6.17</td>
<td>12</td>
</tr>
<tr>
<td>06/01/2016 18:04:44.04</td>
<td>CONTOSO-DNSSVR1</td>
<td>10.30.6.201</td>
<td>51</td>
</tr>
</tbody>
</table>
```

**Figure 63**

- **Name:** 10.30.6.17  
  **Count:** 37  
  **Parse Time:** 06/01/2016 17:48:25.32  
  **Event Type:** DNS Error Client Summary
- **Microsoft DNS- Error domain count**

This report provides information related to domain counts for DNS logs with errors.

![Figure 64](image)

Name: download.com  
Count: 72  
ParseTime: 06/01/2016 18:04:42.67  
EventType: DNS Error Query Summary

- **Microsoft DNS- Summary record type count**

This report provides information related to record type counts for DNS logs.

![Figure 65](image)

Name: AAAA  
Count: 12  
ParseTime: 06/01/2016 18:04:40.92  
EventType: DNS Record Type Summary

- **Microsoft DNS- Summary client count**

This report provides information related to client counts for DNS logs.

![Figure 66](image)

Name: CONTOSO-DNSSVR1  
Client Address: 10.30.6.214  
Count: 63

Name: CONTOSO-DNSSVR1  
Client Address: 10.30.6.17  
Count: 28

Name: CONTOSO-DNSSVR1  
Client Address: 10.30.6.21  
Count: 28

Name: CONTOSO-DNSSVR1  
Client Address: 10.30.6.201  
Count: 70
EventTracker: Microsoft DNS Server (Advanced)

- **Microsoft DNS- Summary domain count**

This report provides information related to domain counts for DNS logs.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Computer</th>
<th>Domain Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/01/2016 17:48:22.82</td>
<td>CONTOSO-DNSSVR1</td>
<td>mmexe.com</td>
<td>63</td>
</tr>
<tr>
<td>06/01/2016 17:48:23.16</td>
<td>CONTOSO-DNSSVR1</td>
<td>ocsp.usertrust.com</td>
<td>37</td>
</tr>
<tr>
<td>06/01/2016 17:48:23.41</td>
<td>CONTOSO-DNSSVR1</td>
<td>cortoso.local</td>
<td>71</td>
</tr>
<tr>
<td>06/01/2016 17:48:23.61</td>
<td>CONTOSO-DNSSVR1</td>
<td>ocsp.comodo.ca.com</td>
<td>28</td>
</tr>
</tbody>
</table>

Figure 67

- **Microsoft DNS- Least resolved domain count**

This report provides information related to least resolved domain counts for DNS logs.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Computer</th>
<th>Domain Name</th>
<th>Count</th>
<th>Client Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/01/2016 17:48:18.39</td>
<td>CONTOSO-DNSSVR1</td>
<td>19ve.co</td>
<td>1</td>
<td>10.30.6.214</td>
</tr>
<tr>
<td>06/01/2016 17:48:21.91</td>
<td>CONTOSO-DNSSVR1</td>
<td>facebook.net</td>
<td>1</td>
<td>10.30.6.17</td>
</tr>
<tr>
<td>06/01/2016 17:48:22.09</td>
<td>CONTOSO-DNSSVR1</td>
<td>amazon.o.org</td>
<td>1</td>
<td>10.30.6.21</td>
</tr>
<tr>
<td>06/01/2016 17:48:41.35</td>
<td>CONTOSO-DNSSVR1</td>
<td>19ve.co</td>
<td>1</td>
<td>10.30.6.214</td>
</tr>
</tbody>
</table>

Figure 68

- **Microsoft DNS- Malicious domain detection**

This report provides information related to malicious domain detected in DNS logs.
This report provides information related to suspicious DNS settings, detected for network's workstations.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Device Name</th>
<th>Device IP</th>
<th>Device MAC</th>
<th>Device DNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/01/2016 05:48:18 PM</td>
<td>Contoso-WRK01</td>
<td>10.30.6.17</td>
<td>08:0C:29:16:7D:A3</td>
<td>77.88.8.9</td>
</tr>
<tr>
<td>06/01/2016 05:48:33 PM</td>
<td>Contoso-WRK01</td>
<td>10.30.6.17</td>
<td>08:0C:29:16:7D:A3</td>
<td>77.88.8.8</td>
</tr>
<tr>
<td>06/01/2016 05:48:33 PM</td>
<td>Contoso-WRK13</td>
<td>10.30.6.201</td>
<td>08:0C:29:36:7D:A6</td>
<td>8.8.4.4</td>
</tr>
<tr>
<td>06/01/2016 05:48:34 PM</td>
<td>Contoso-WRK13</td>
<td>10.30.6.201</td>
<td>08:0C:29:36:7D:A6</td>
<td>8.8.8.8</td>
</tr>
</tbody>
</table>

Suspicious DNS setting detected
SystemName:Contoso-WRK01
SystemIP:10.30.6.17
SystemMAC:08:0C:29:16:7D:A3
DNSIP:77.88.8.9
### Microsoft DNS Server latency details

This report provides information related to latency of local configured and public servers.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Computer Name</th>
<th>Computer IP</th>
<th>DNS Server Name</th>
<th>DNS Server IP</th>
<th>DNS Server Type</th>
<th>Latency in ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/01/2016</td>
<td>17:48:18.24</td>
<td>10.30.6.21</td>
<td>CONTOSO-DNSSVR2</td>
<td>10.30.6.12</td>
<td>Local DNS</td>
<td>100.19</td>
</tr>
<tr>
<td>06/01/2016</td>
<td>17:48:18.34</td>
<td>10.30.6.21</td>
<td>CONTOSO-DNSSVR2</td>
<td>10.30.6.12</td>
<td>Local DNS</td>
<td>8.9</td>
</tr>
<tr>
<td>06/01/2016</td>
<td>17:48:31.34</td>
<td>10.30.6.21</td>
<td>google-public-dns-b.google.com</td>
<td>8.8.4.4</td>
<td>Public DNS</td>
<td>5.16</td>
</tr>
</tbody>
</table>

### Behavior Rule

- **Microsoft DNS query traffic** - This behavior rule assists an administrator to track unique domains observed in DNS traffic.

### Alerts

- **Microsoft DNS: High error query count detected for domain** - This alert is generated when high error DNS traffic is detected from domains.
• **Microsoft DNS: High error query count detected for type** - This alert is generated when high error DNS traffic is detected for error types.

• **Microsoft DNS: High error query count detected from client** - This alert is generated when high error DNS traffic is detected from clients.

• **Microsoft DNS: High query count detected for record type** - This alert is generated when high DNS traffic is detected for record types.

• **Microsoft DNS: High query count detected from client** - This alert is generated when high DNS traffic is detected from clients.

• **Microsoft DNS: High query count detected from domain** - This alert is generated when high DNS traffic is detected from domains.

• **Microsoft DNS: DGA domain detected** - This alert is generated when DGA domain is detected in DNS traffic.

• **Microsoft DNS: Suspicious DNS settings detected** - This alert is generated when suspicious DNS settings are detected in network’s workstations.

• **Microsoft DNS: Malicious domain detected** - This alert is generated when malicious domain is detected in DNS traffic.

• **Microsoft DNS: High DNS server latency detected** - This alert is generated when high DNS server latency is detected for local DNS servers.

**Knowledge Object**

• **Microsoft DNS query traffic** - This KO aids an administrator to analyze and visualize all the query logs generated by DNS servers.

**Create Dashboards in EventTracker**

**Schedule Reports**

1. Open **EventTracker** in browser and logon.
2. Navigate to **Reports>Configuration**.

3. Select ‘**Microsoft DNS**’ in report groups. Check **Defined** dialog box.

4. Click on ‘**schedule**’ to plan a report for later execution.
5. Choose appropriate time for report execution and in Step 8 check **Persist data in Eventvault Explorer** box.

---

**Figure 75**

**Figure 76**
6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
7. Proceed to next step and click **Schedule** button.
8. Wait for scheduled time or generate report manually.

## Create Dashlets

1. **EventTracker 8 or later** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.

![Flex Dashboard pane](image)

**Figure 77**

3. Navigate to **Dashboard**>**Flex**.
   Flex Dashboard pane is shown.

![Flex Dashboard configuration pane](image)

**Figure 78**

4. Click **+** to add a new dashboard.
   Flex Dashboard configuration pane is shown.
5. Fill appropriate title and description and click **Save** button.
6. Click 🔄 to configure a new flex dashlet. Widget configuration pane is shown.

7. Locate earlier scheduled report in **Data Source** dropdown.
8. Select **Chart Type** from dropdown.
9. Select extent of data to be displayed in **Duration** dropdown.
10. Select computation type in **Value Field Setting** dropdown.
11. Select evaluation duration in **As Of** dropdown.
12. Select comparable values in **X Axis** with suitable label.
13. Select numeric values in **Y Axis** with suitable label.
14. Select comparable sequence in **Legend**.
15. Click **Configure** button to apply.

**Figure 81**

16. Click ‘customize’ to locate and choose created dashlet.
17. Click  to add dashlet to earlier created dashboard.

**Sample Dashboards**

- **Microsoft DNS-Error pattern in last 12 hrs**

**Figure 82**
• **Microsoft DNS-Top queried domains with errors in last 12 hrs**

![Image of domain query chart]

**Figure 83**

• **Microsoft DNS-Top querying clients with errors in last 12 hrs**

![Image of client query chart]

**Figure 84**
• Microsoft DNS-Record type pattern in last 12 hrs

Figure 85

• Microsoft DNS-Top queried domains in last 12 hrs

Figure 86
• **Microsoft DNS-Top querying clients in last 12 hrs**

![Graph showing top querying clients](image-url)

*Figure 87*

• **Microsoft DNS-Malicious domains detected in last 12 hrs**

![Graph showing malicious domains](image-url)

*Figure 88*
- Microsoft DNS-Server latency in last 12 hrs

![Graph showing DNS latency](image)

**Figure 89**

- Microsoft DNS-DGA domains detected in last 12 hrs

![Graph showing DGA domains](image)

**Figure 90**
Microsoft DNS—Suspicious DNS settings detected in last 12 hrs

Figure 91

<->X->