EventTracker
Secure. Comply. Succeed.

Integrate Microsoft DNS Server (Advanced)

EventTracker Enterprise

Publication Date: Jun 8, 2016

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

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

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;

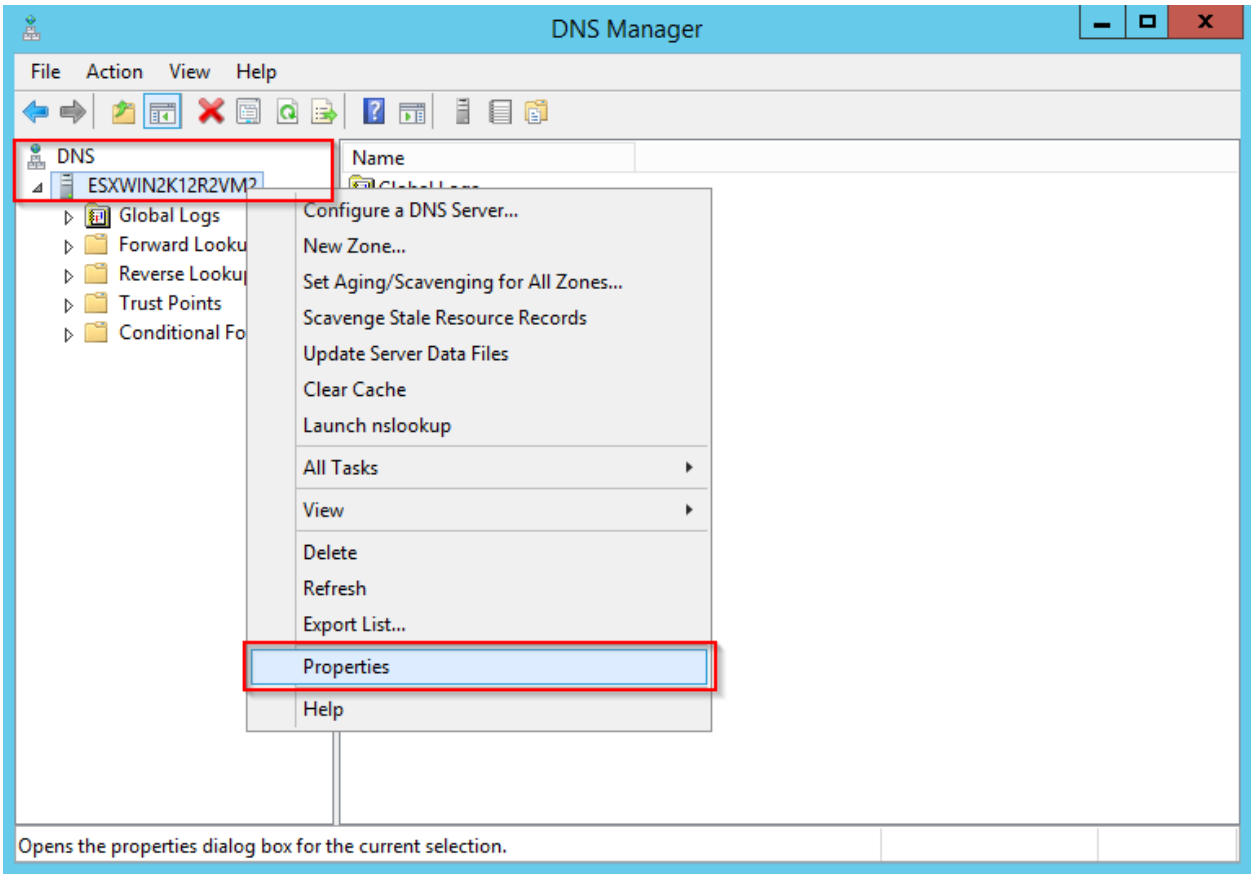

Figure 1

3. Right-click on your configured DNS server and click **Properties**.

DNS server properties window opens:

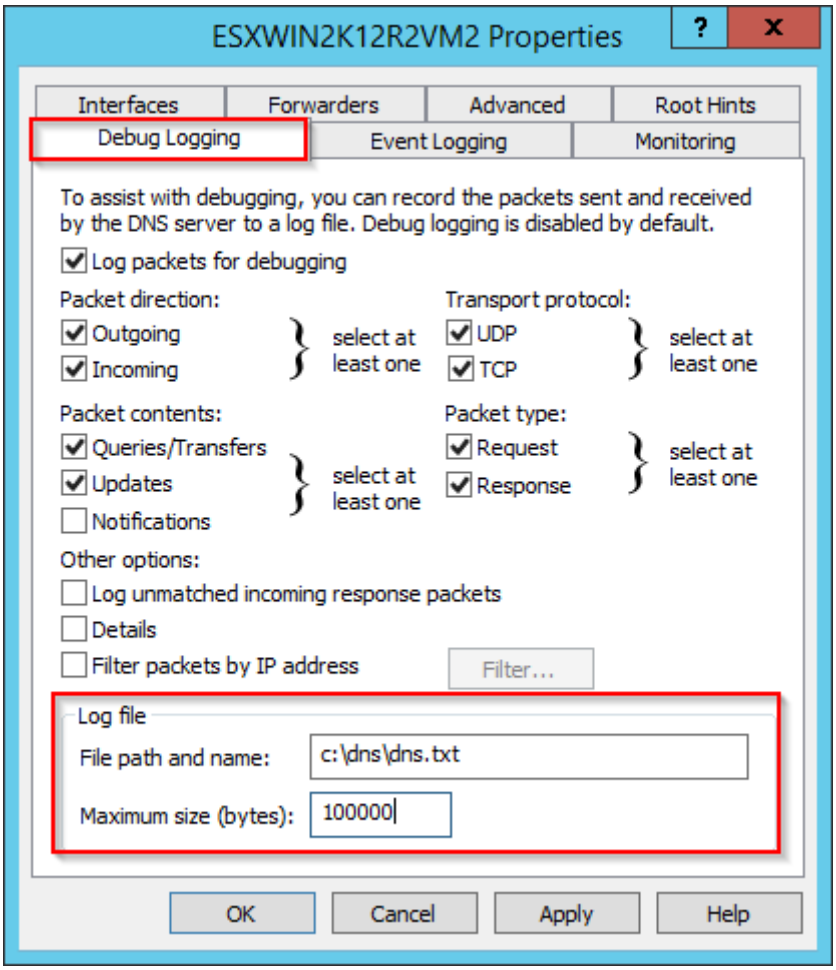

Figure 2

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
```

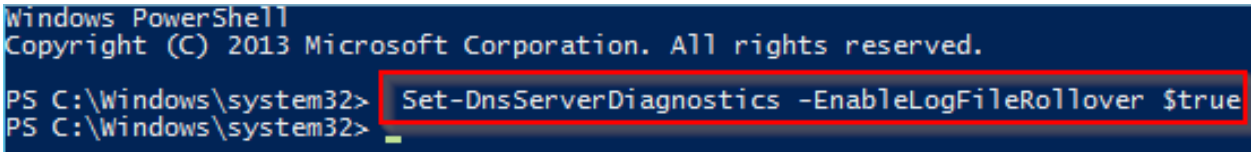

Figure 3

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.

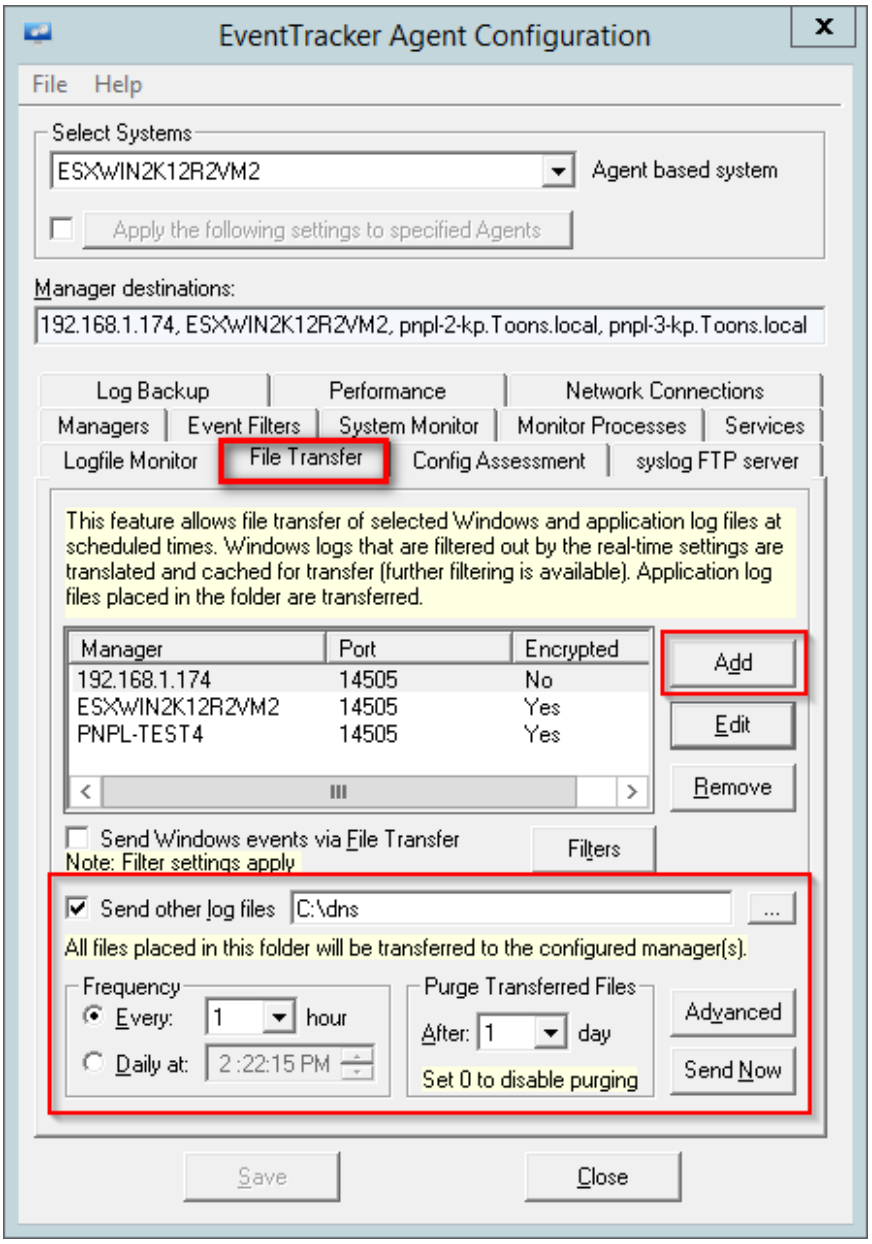

Figure 4

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;

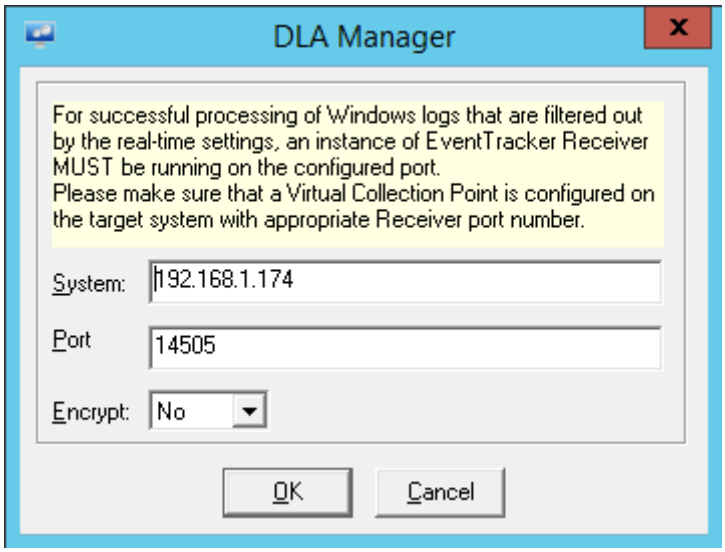

Figure 5

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.
2. Web access to **http://mirror1.malwaredomains.com/files/domains.txt.**
3. '**SQLPS**" module must be installed on PowerShell.
4. PowerShell modules can be downloaded online using following command.

```
Import-Module 'sqlps"
```

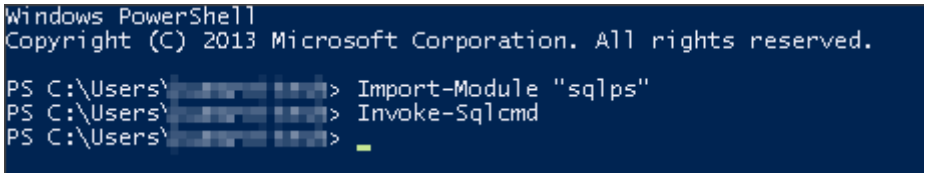

Figure 6

Malware script schedule

1. Logon to EventTracker Manager workstation with administrative privileges.
2. Navigate to **Start>Administrative Tools>Task Scheduler**.

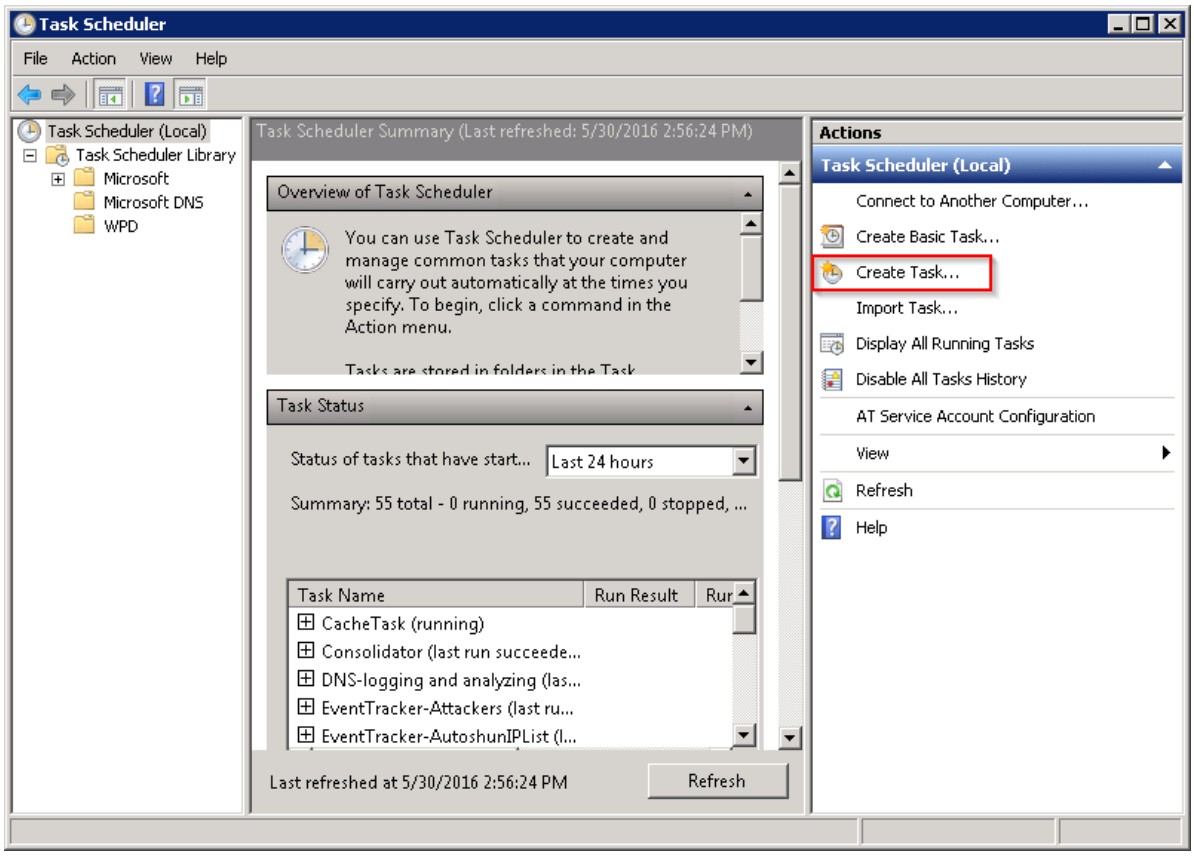

Figure 7

3. In the **Actions** tab select **Create task**.
4. Configure Task properties as shown below.

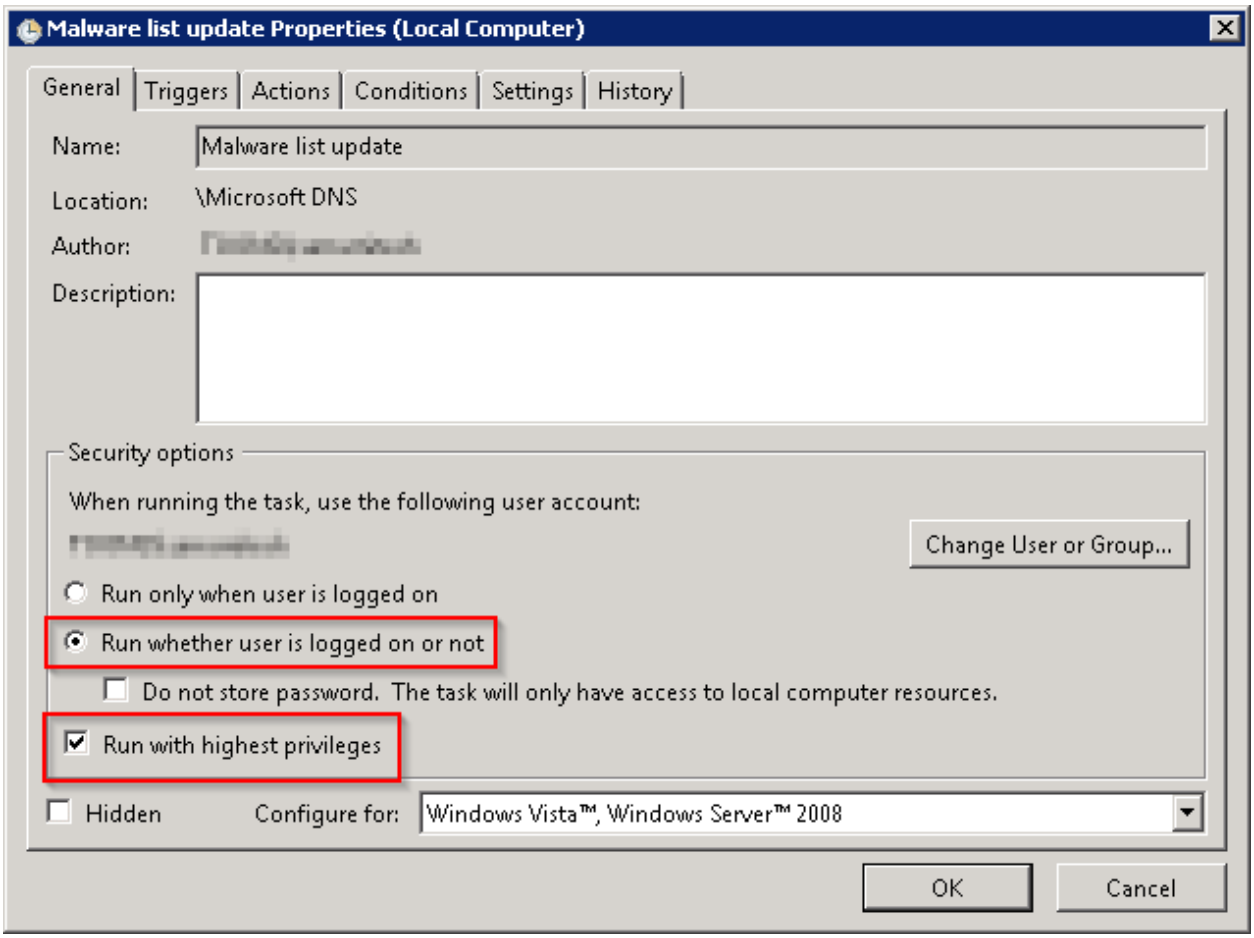

Figure 8

5. Select **General** tab, provide appropriate task name and in **Security options** section, enable '**Run weather user is logged on or not**" and '**Run with highest privileges**" options.

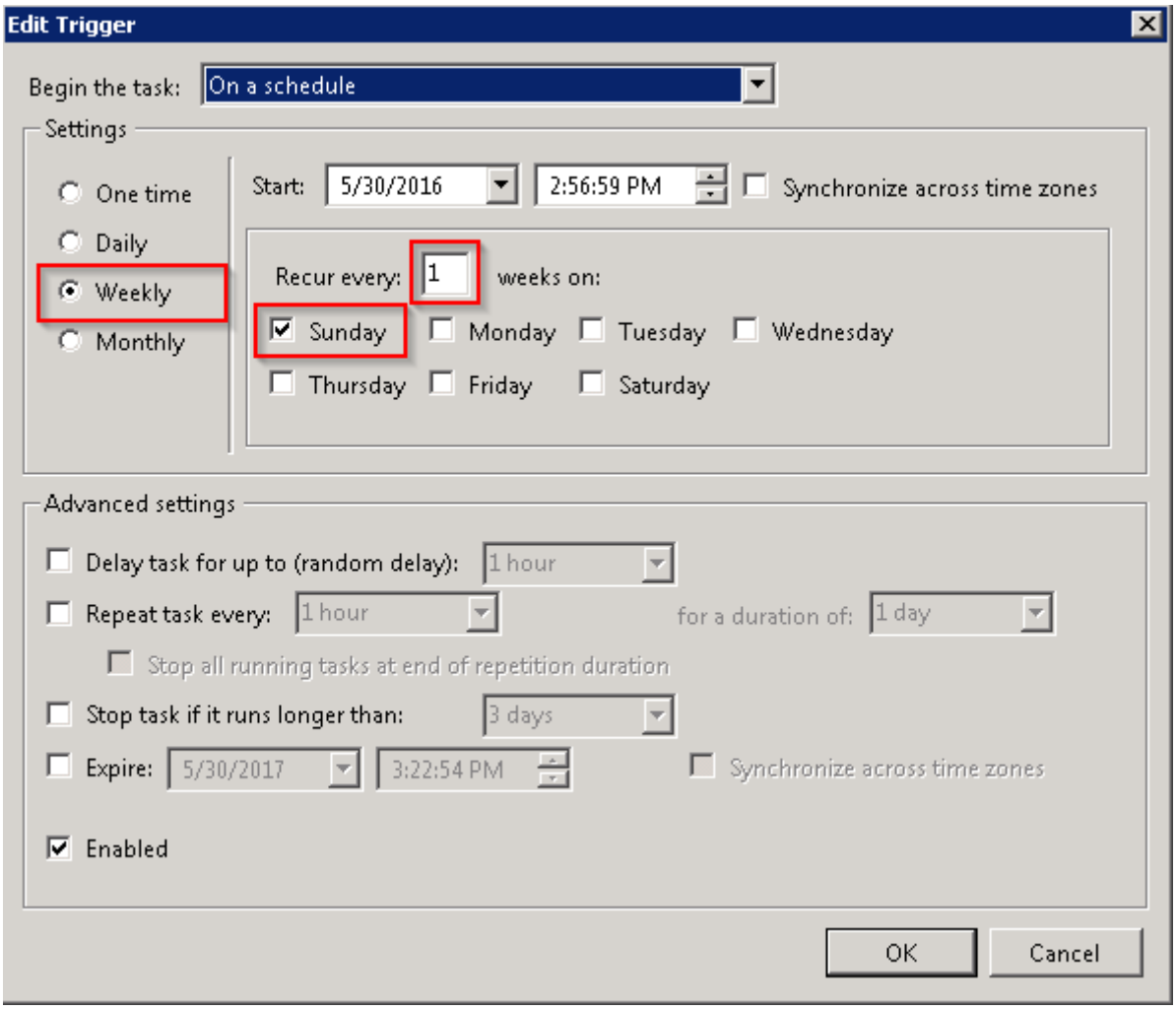

Figure 9

6. Select **Triggers** tab, select **Weekly** with appropriate schedule settings.

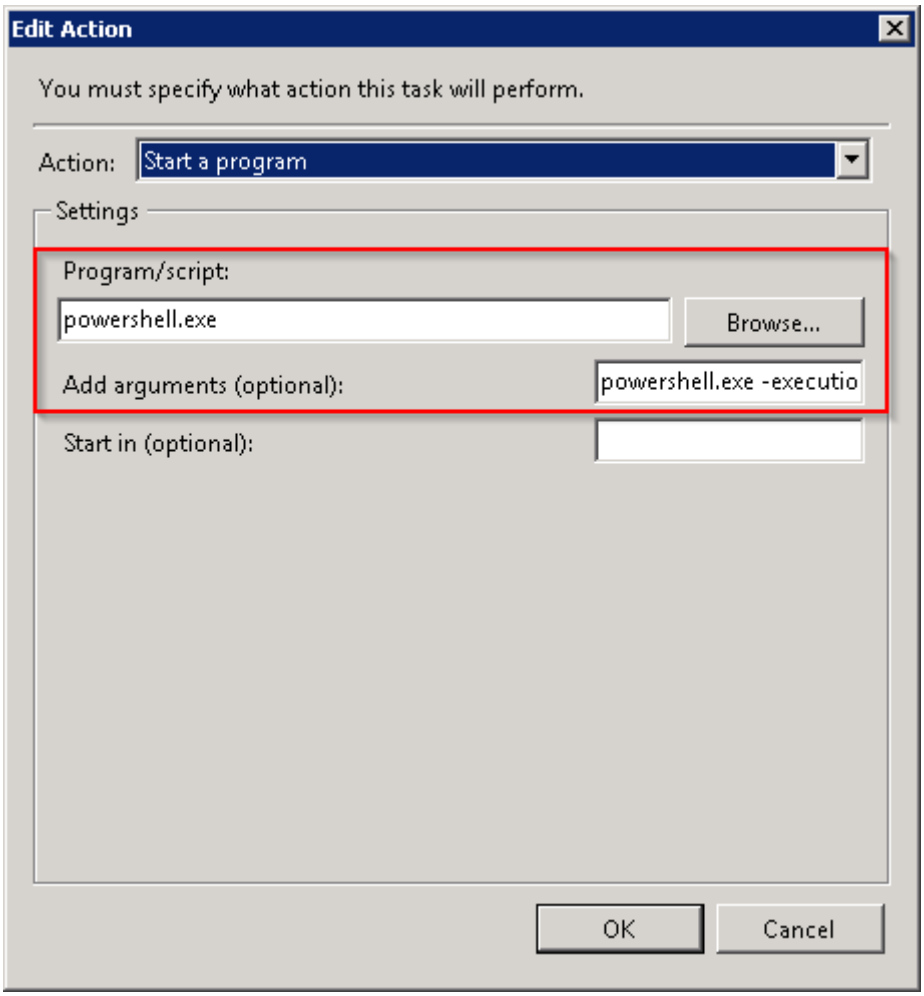

Figure 10

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

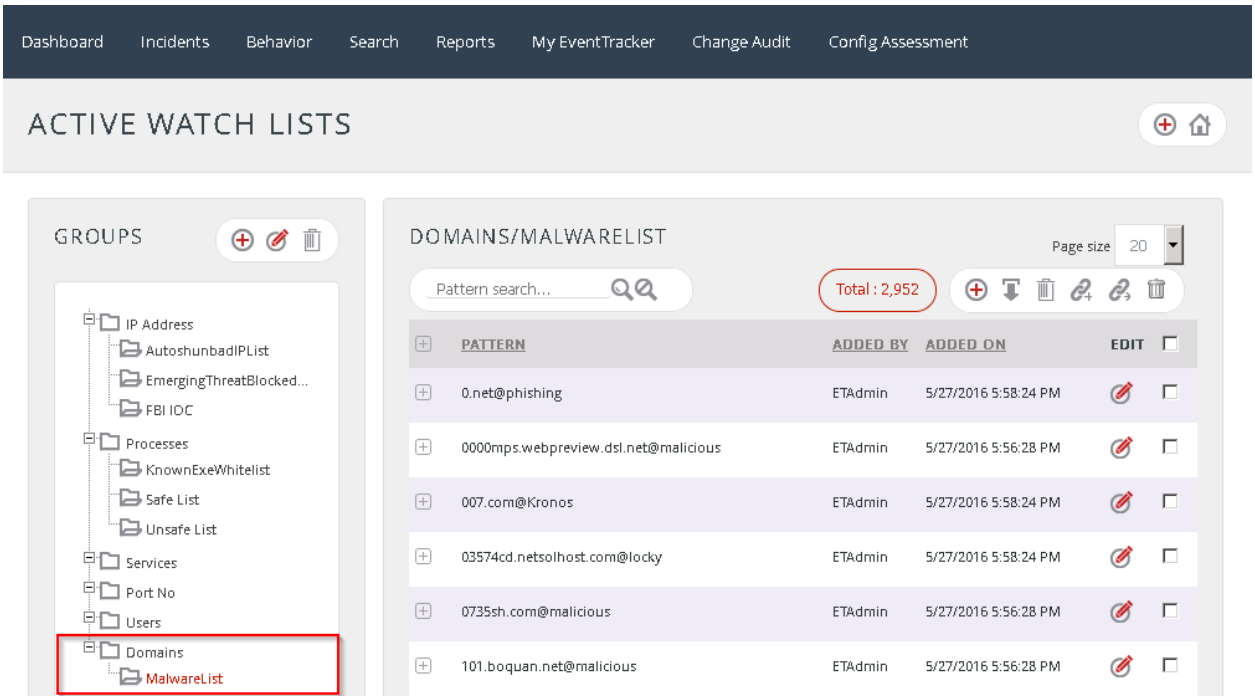

Figure 11

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 .\pip.exe install tldextract
```

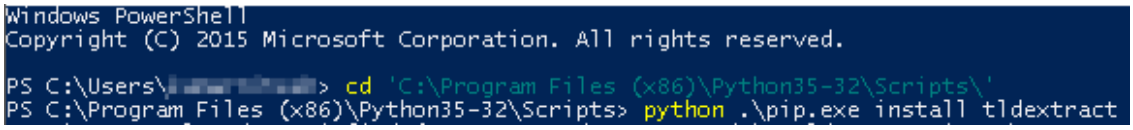

Figure 12

Python script verification

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

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

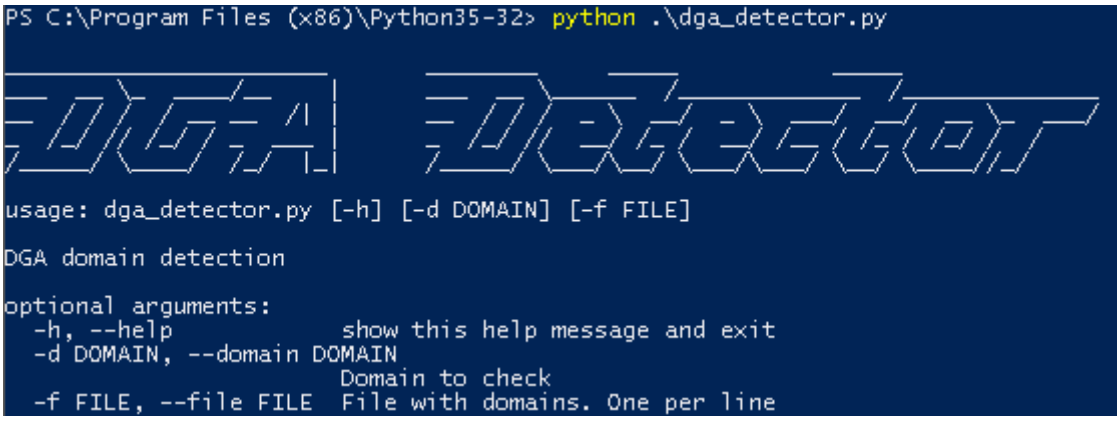

Figure 13

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.
2. Navigate to **Start>Administrative Tools>Task Scheduler**.

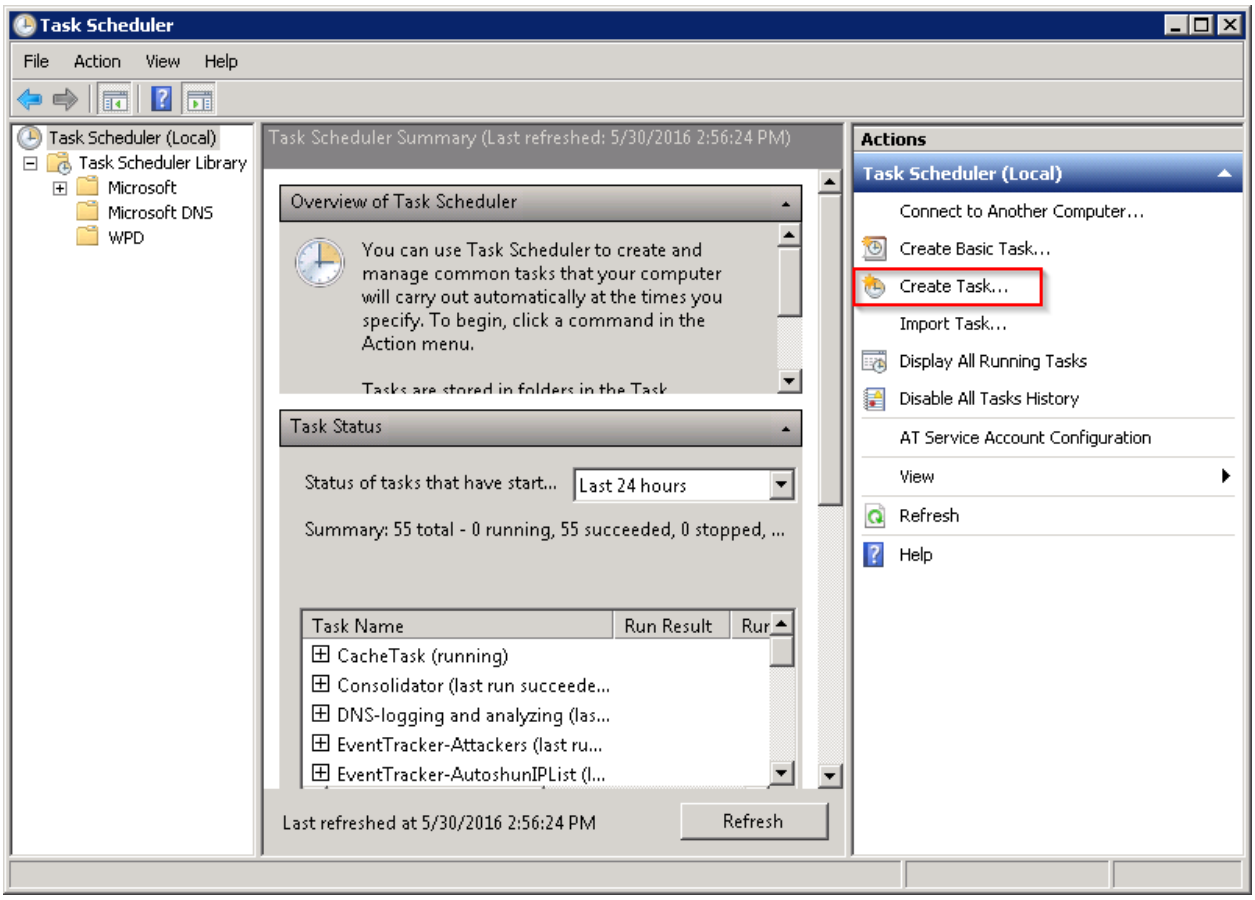

Figure 14

3. In the **Actions** tab select **Create task**.
4. Configure Task properties as shown below.

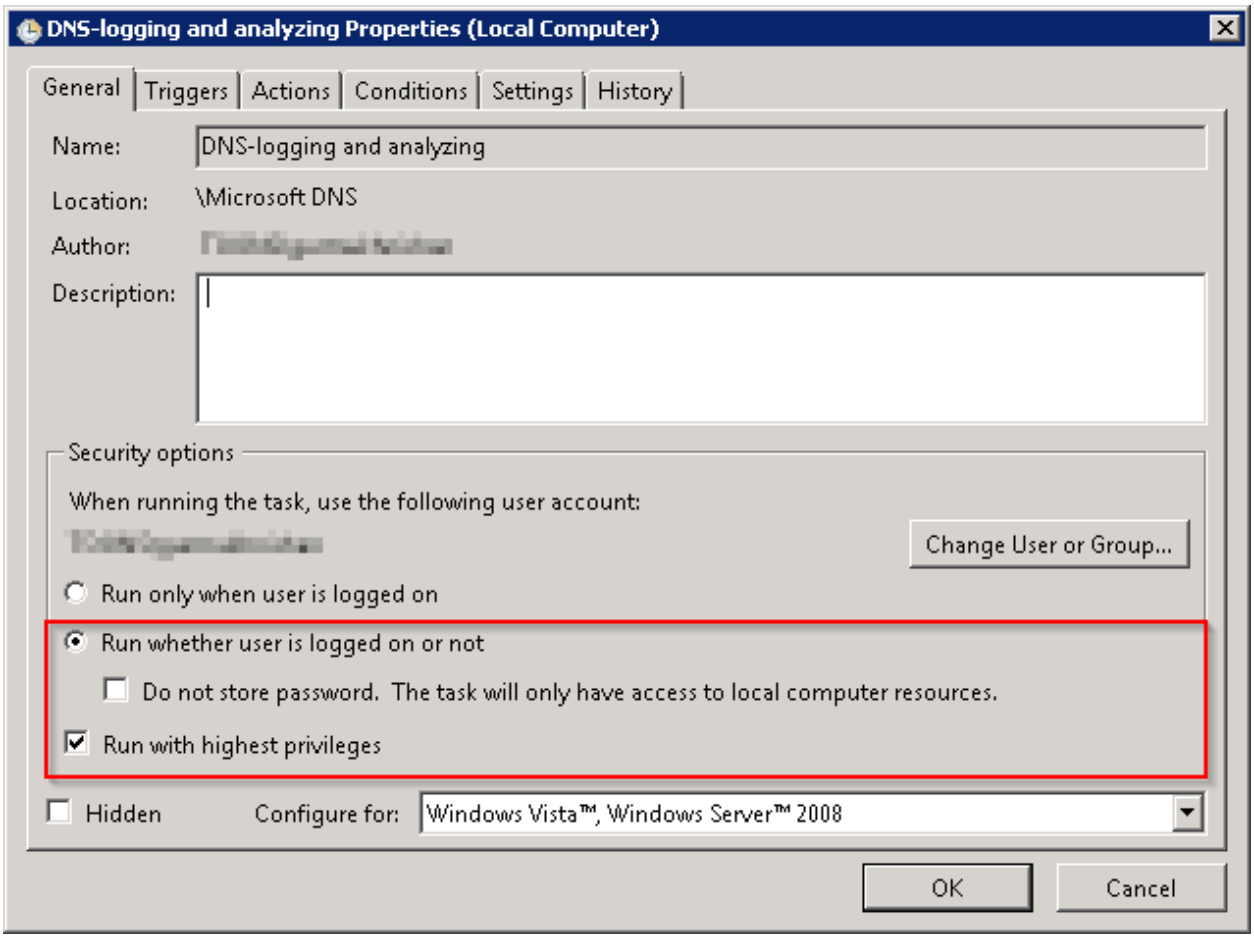

Figure 15

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.

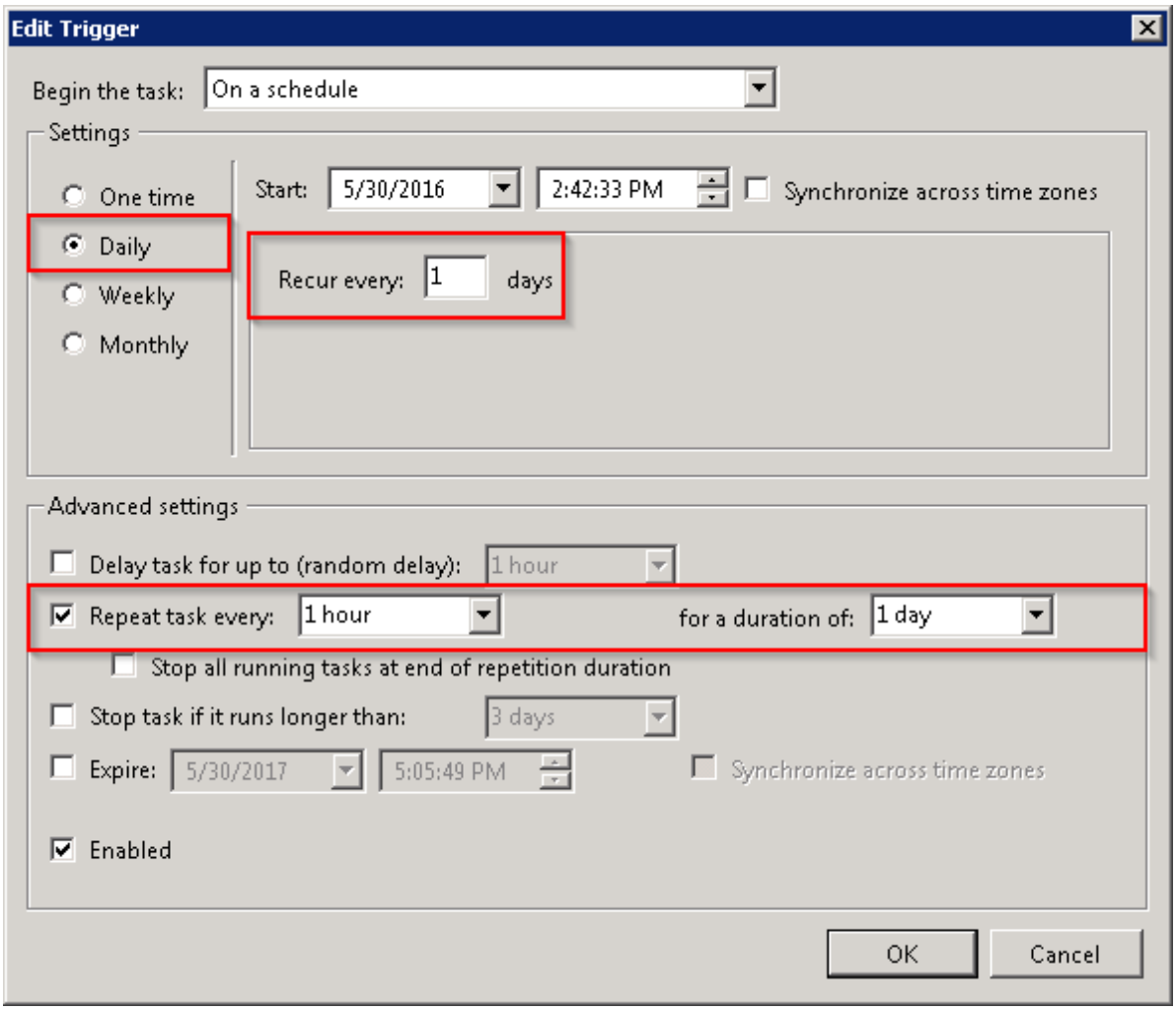

Figure 16

6. Select **Triggers** tab, select **Daily** with appropriate schedule settings to ensure hourly execution.

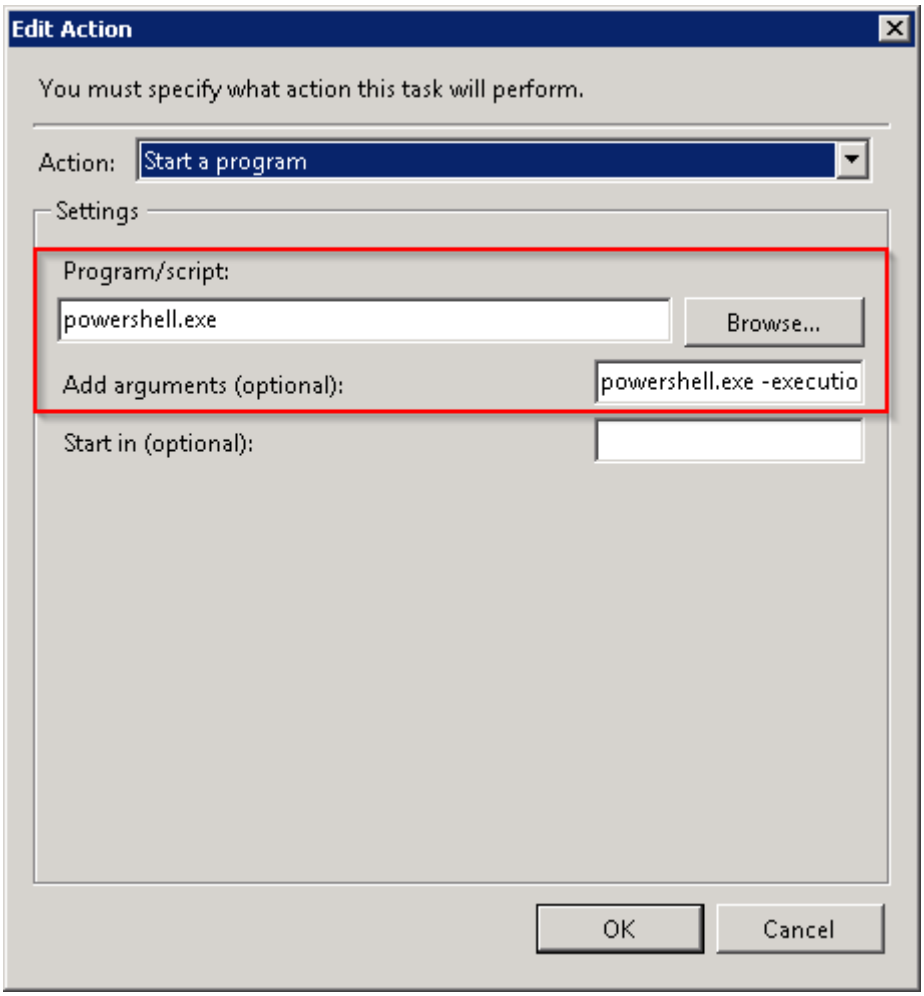

Figure 17

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
```

EventTracker installation folder

EventTracker agent workstation name

Threshold to trigger alerts for DNS error traffic parameters (i.e. domain, client, error types).

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.
2. Navigate to **Start>Administrative Tools>Task Scheduler**.

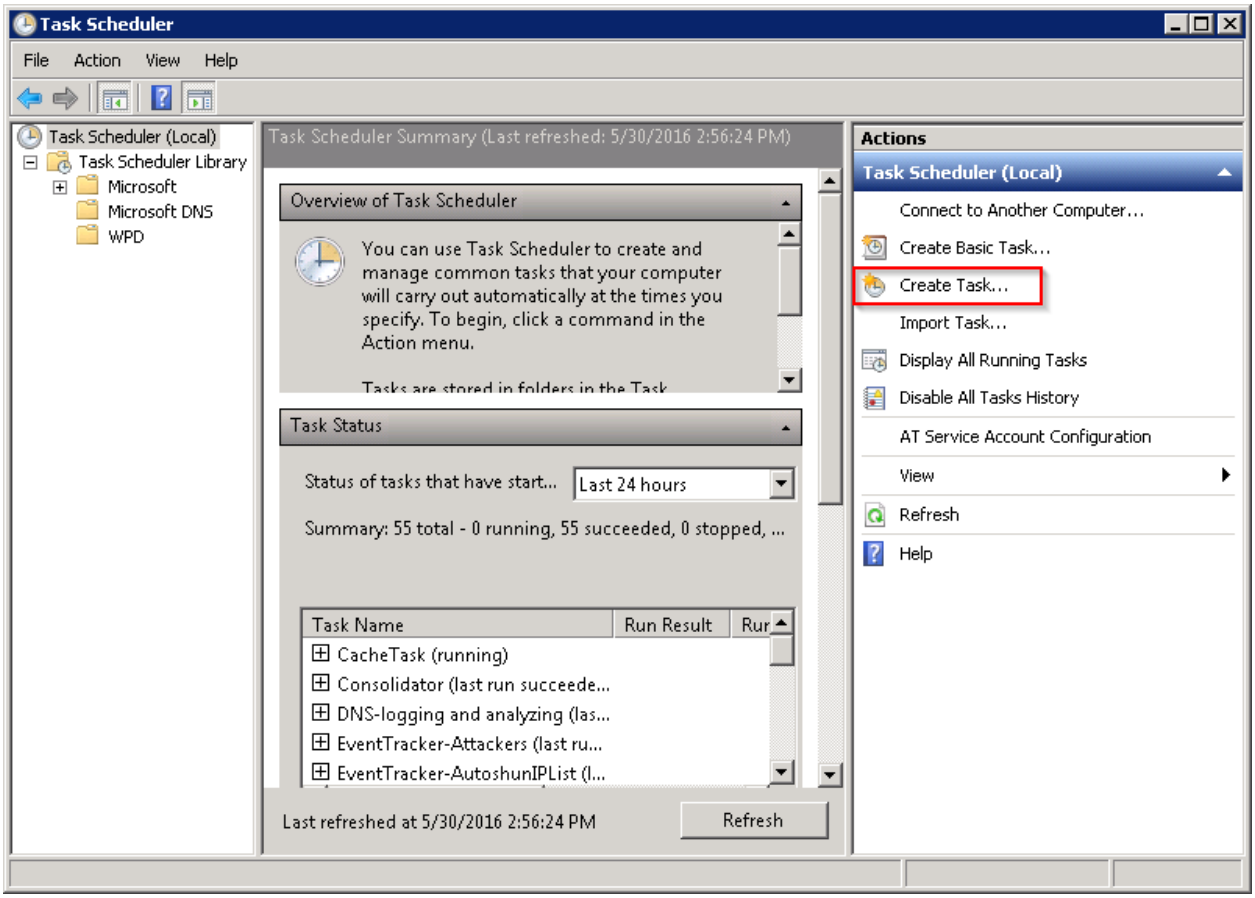

Figure 18

3. In the **Actions** tab select **Create task**.

4. Configure Task properties as shown below.

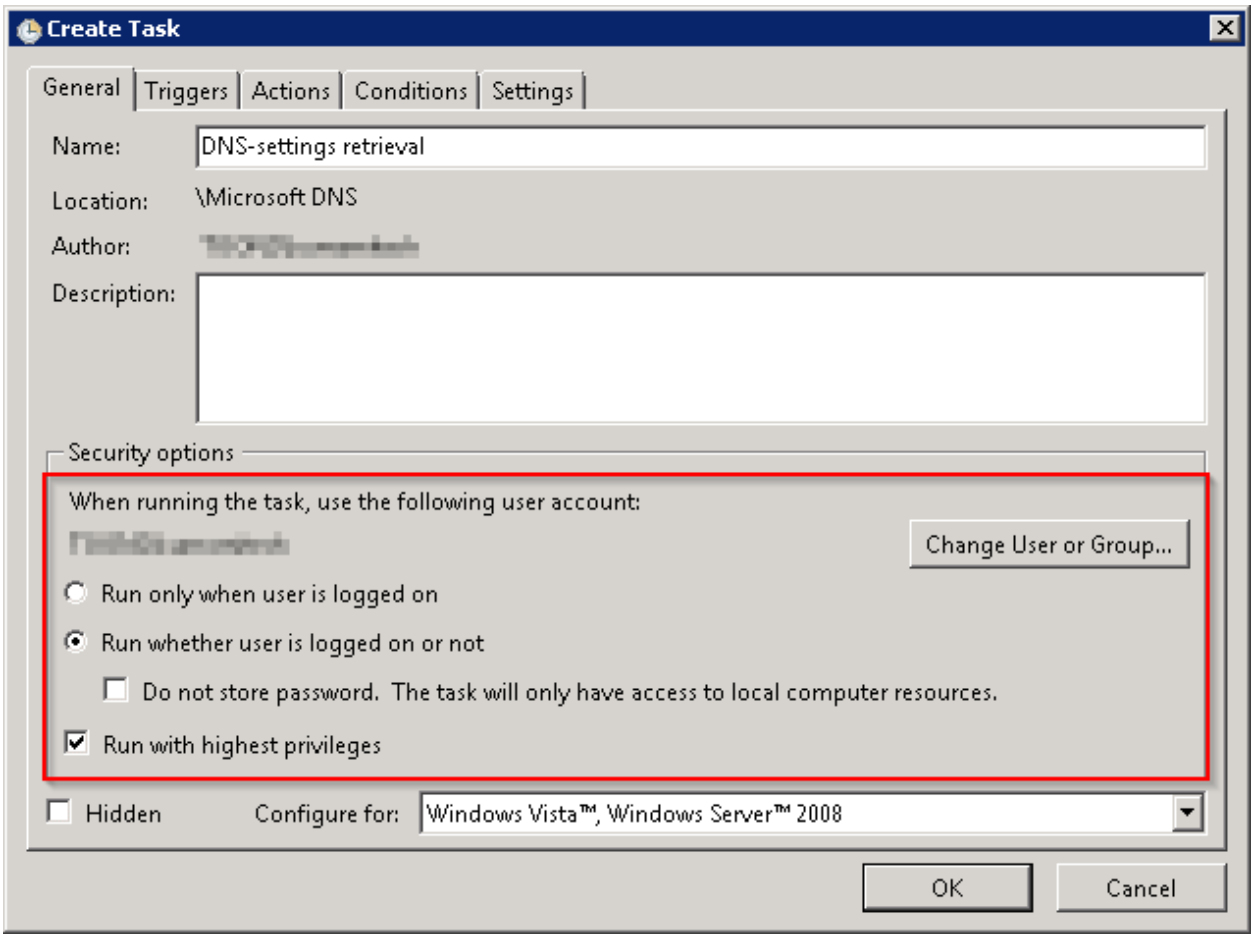

Figure 19

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.

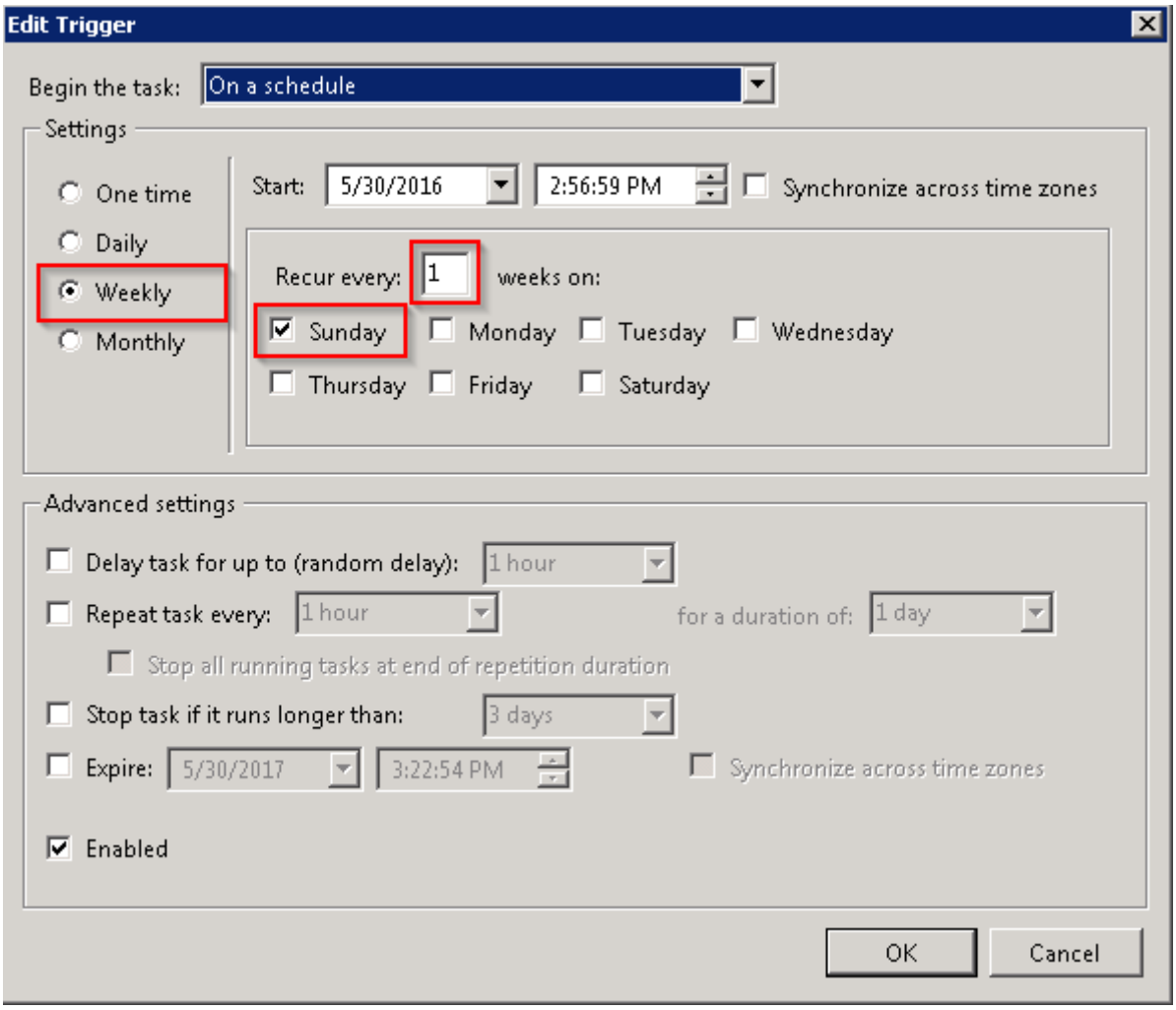

Figure 20

6. Select **Triggers** tab, select **Weekly** with appropriate schedule setting.

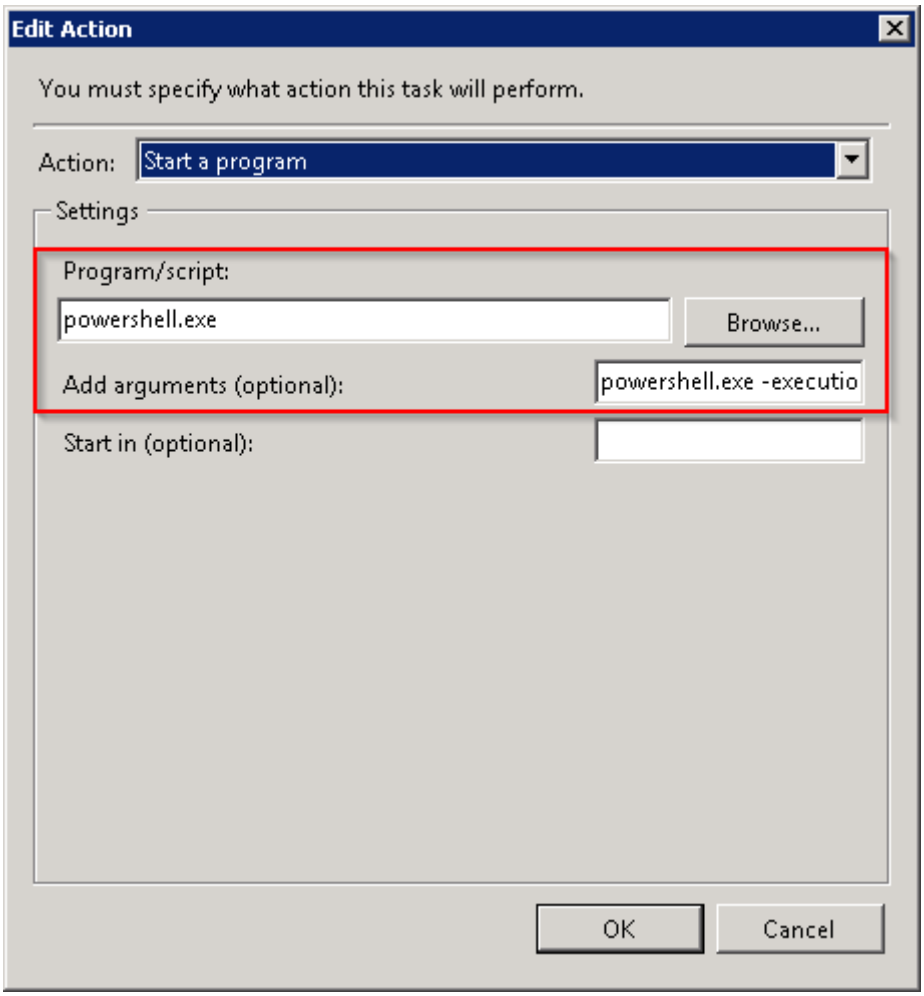

Figure 21

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-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.
2. Navigate to **Start>Administrative Tools>Task Scheduler**.

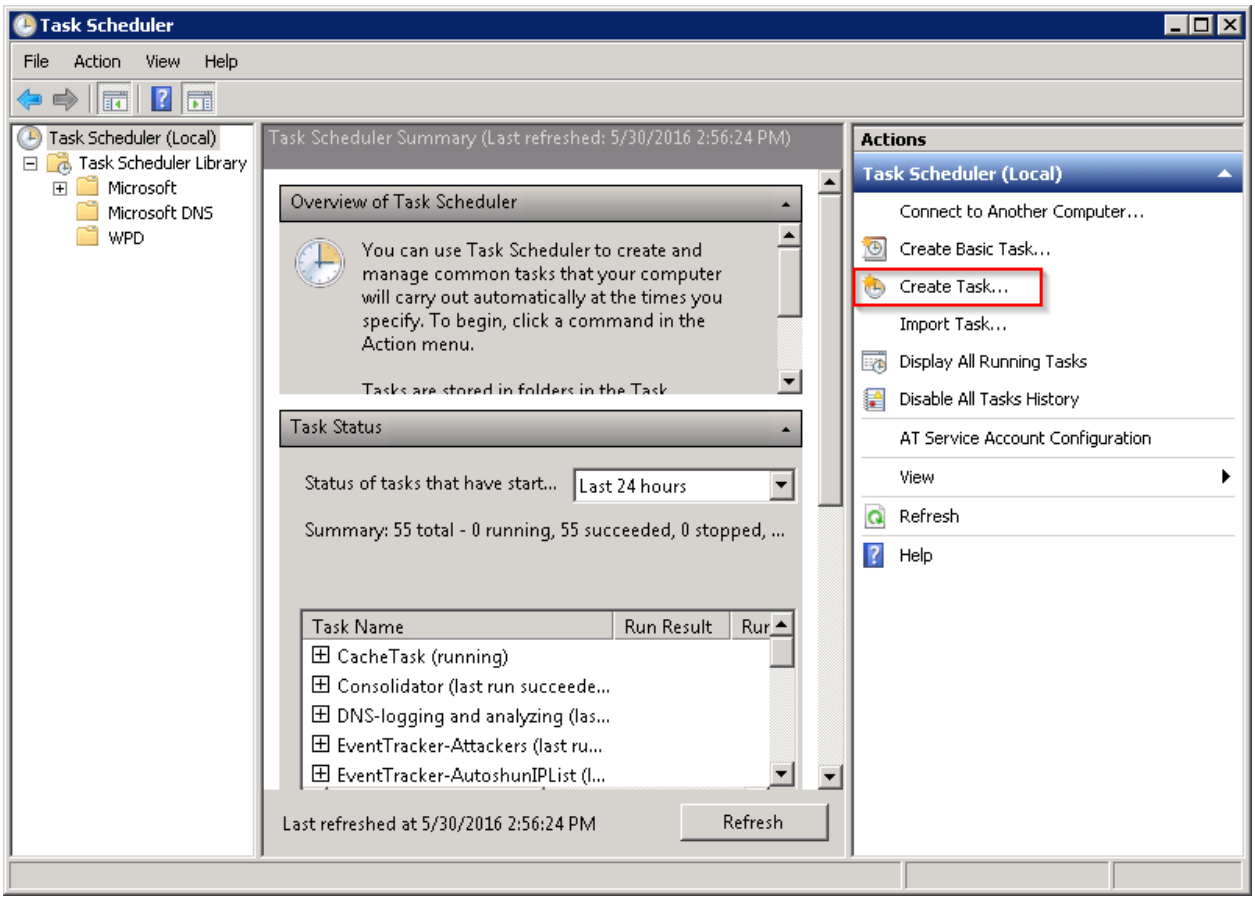

Figure 22

3. In the **Actions** tab select **Create task**.
4. Configure Task properties as shown below:

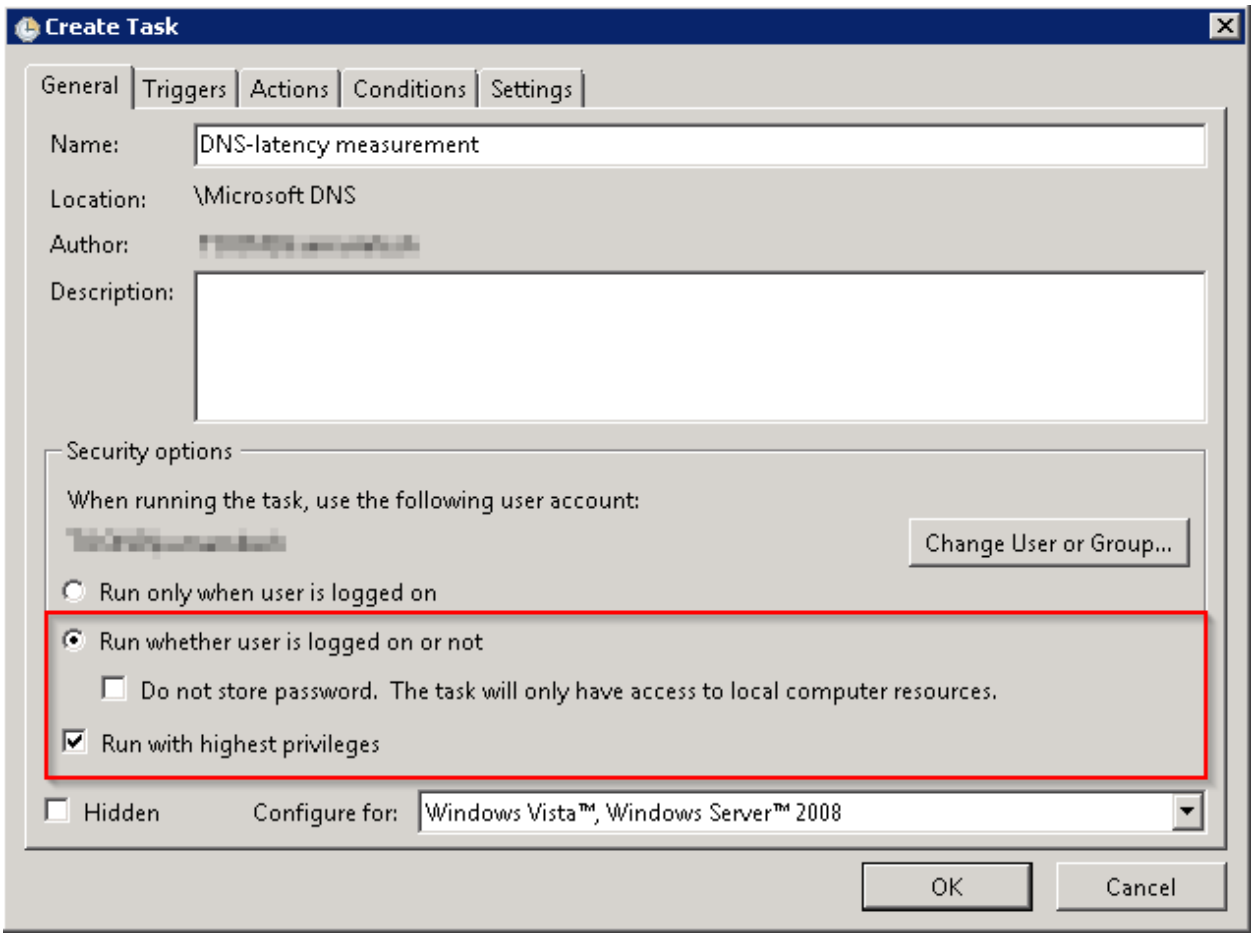

Figure 23

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.

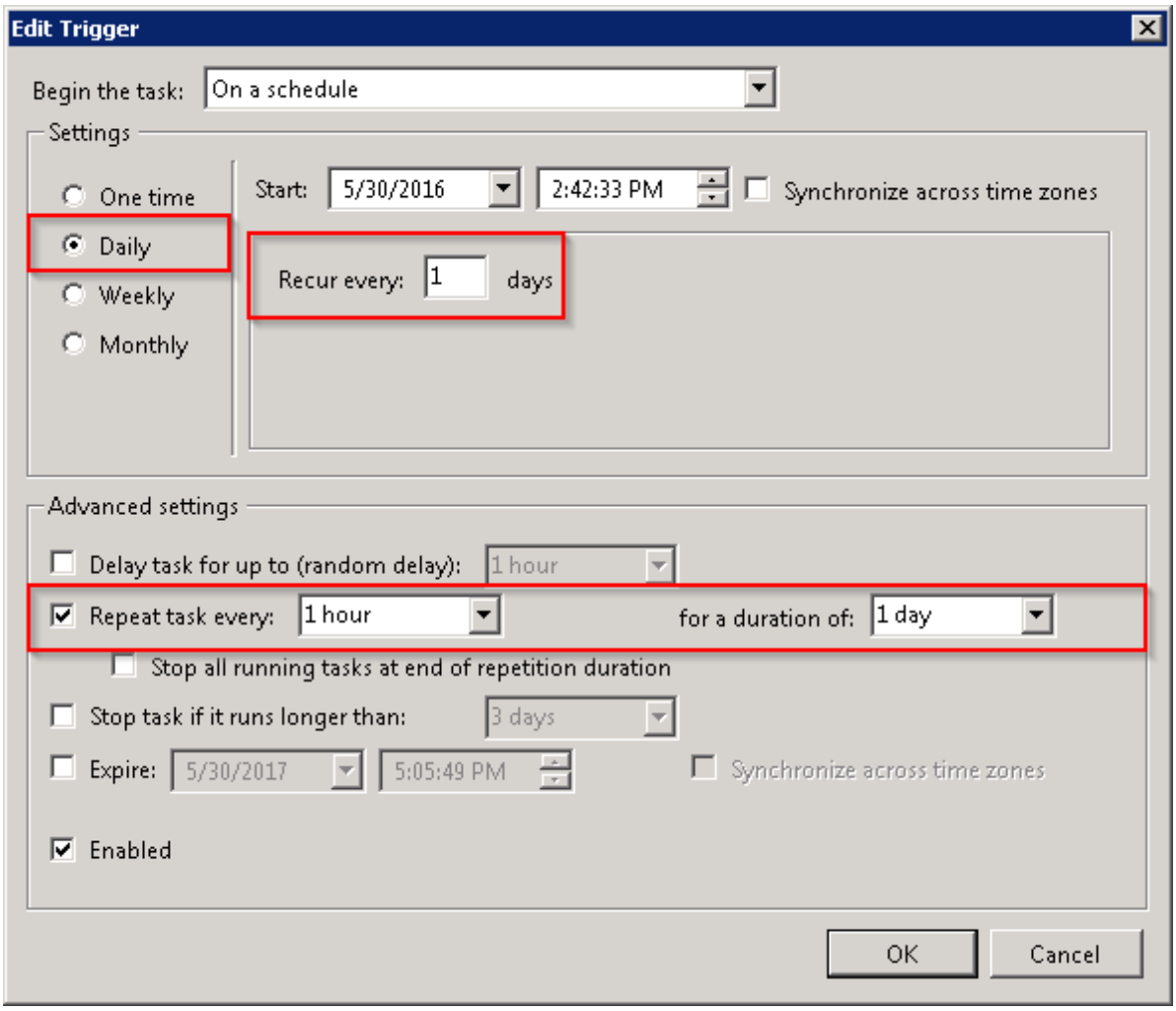

Figure 24

6. Select **Triggers** tab, select **Daily** with appropriate schedule settings to ensure hourly execution.

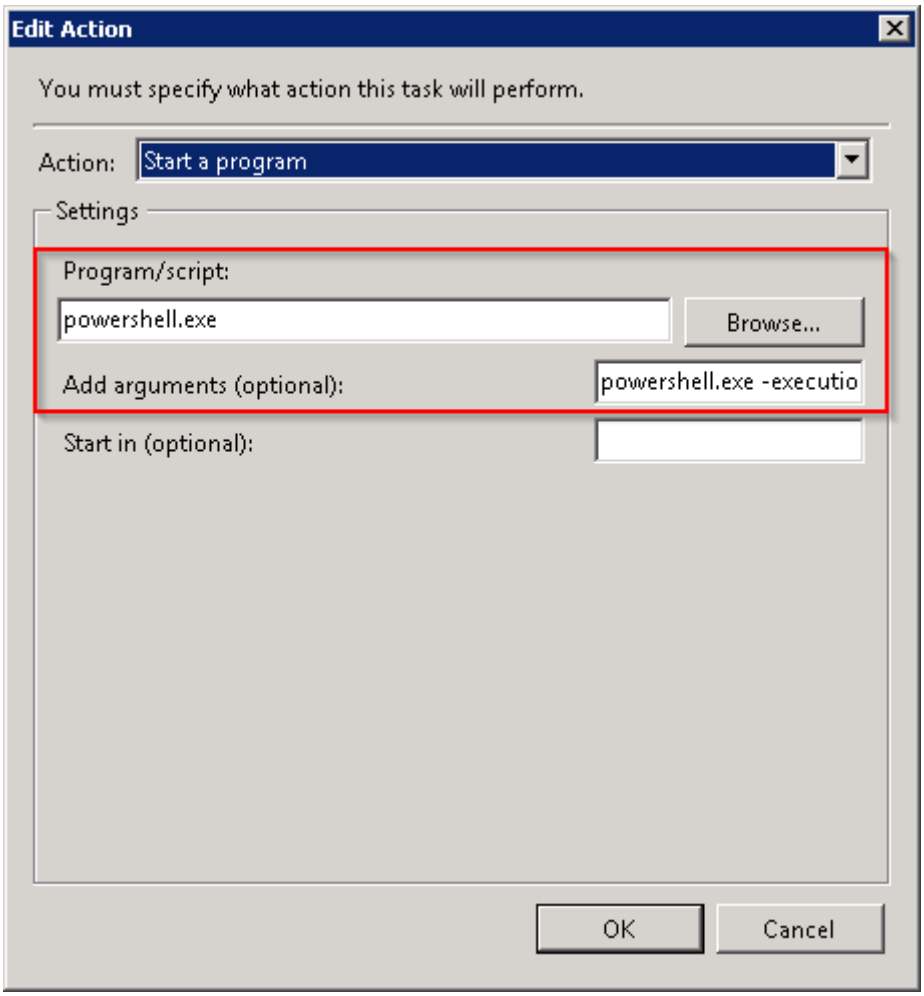

Figure 25

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-Dnslatency.ps1" –threshold 100
```

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.

Figure 26

- Open EventTracker control panel, click **EventTracker Agent Configuration**.

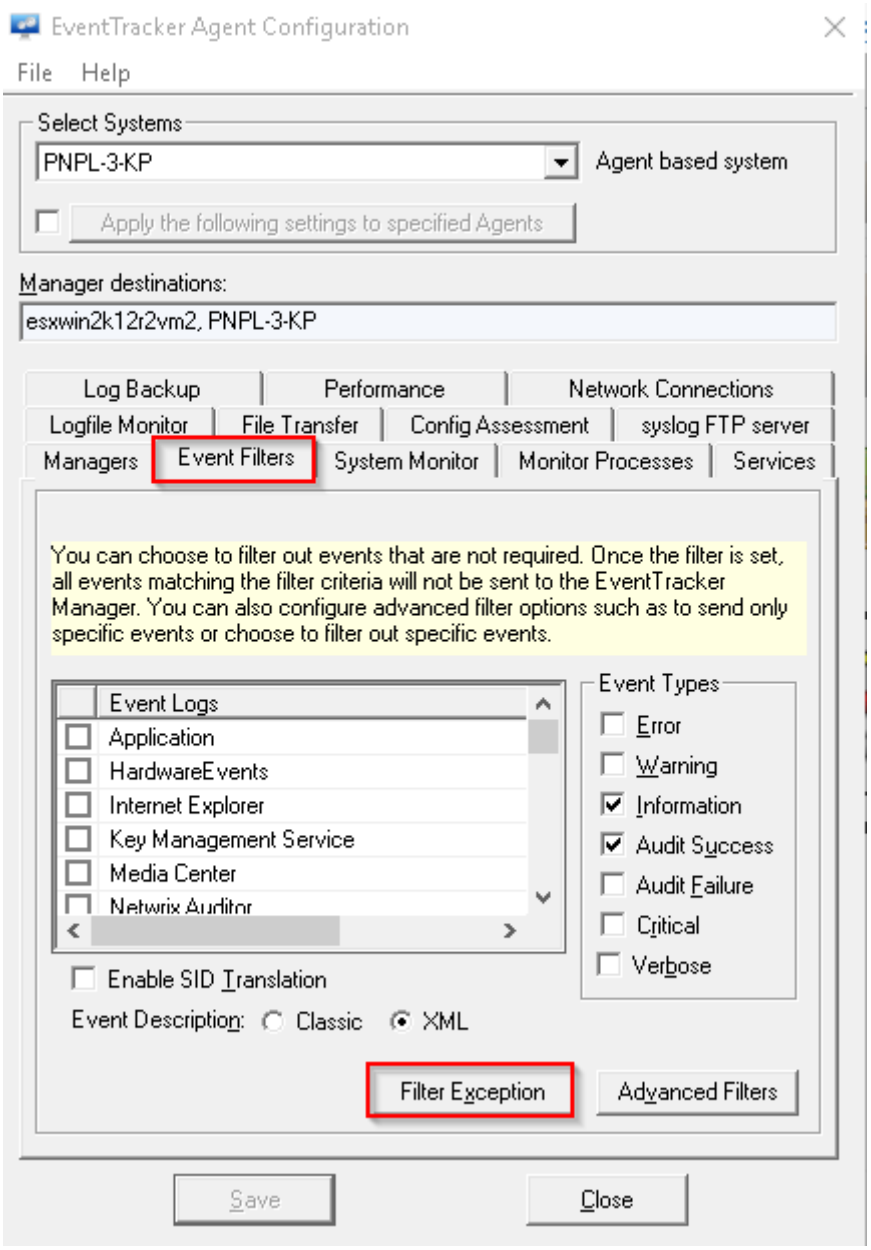

Figure 27

- Select **Event Filters** tab, click **Filter Exception**.

  Filter exception window opens,

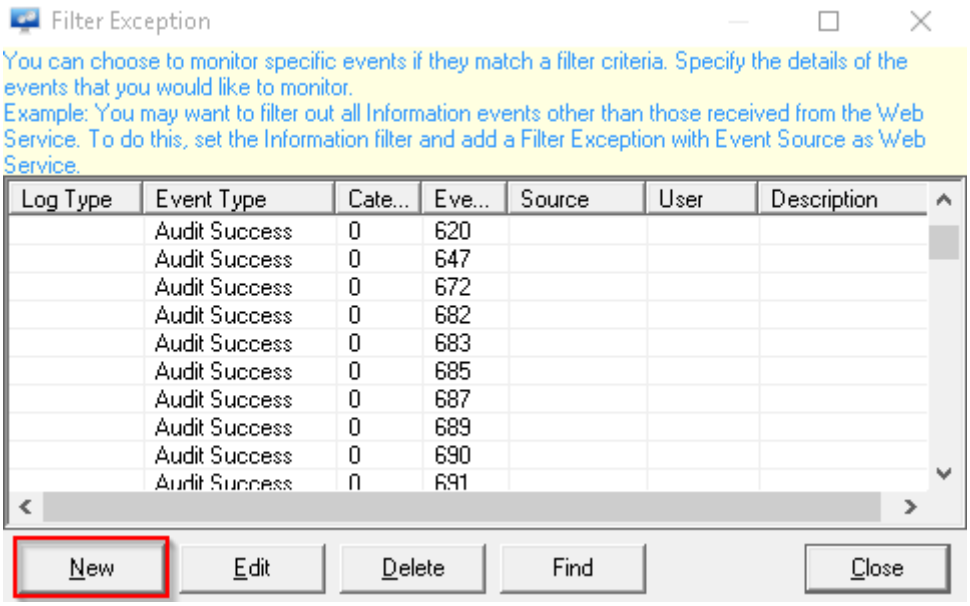

Figure 28

- 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.

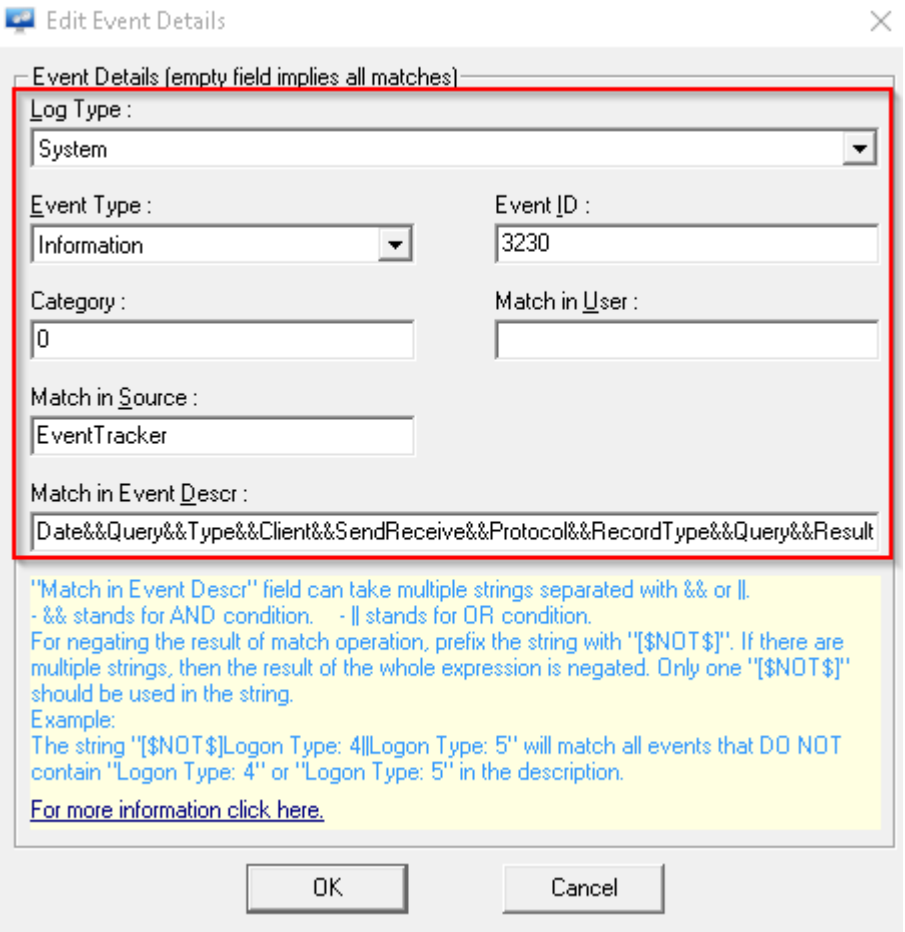

Figure 29

- Enter following as matching description.

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

- Click **OK** to apply.

DNS summary log filter

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

- Configure event filter details as shown below.

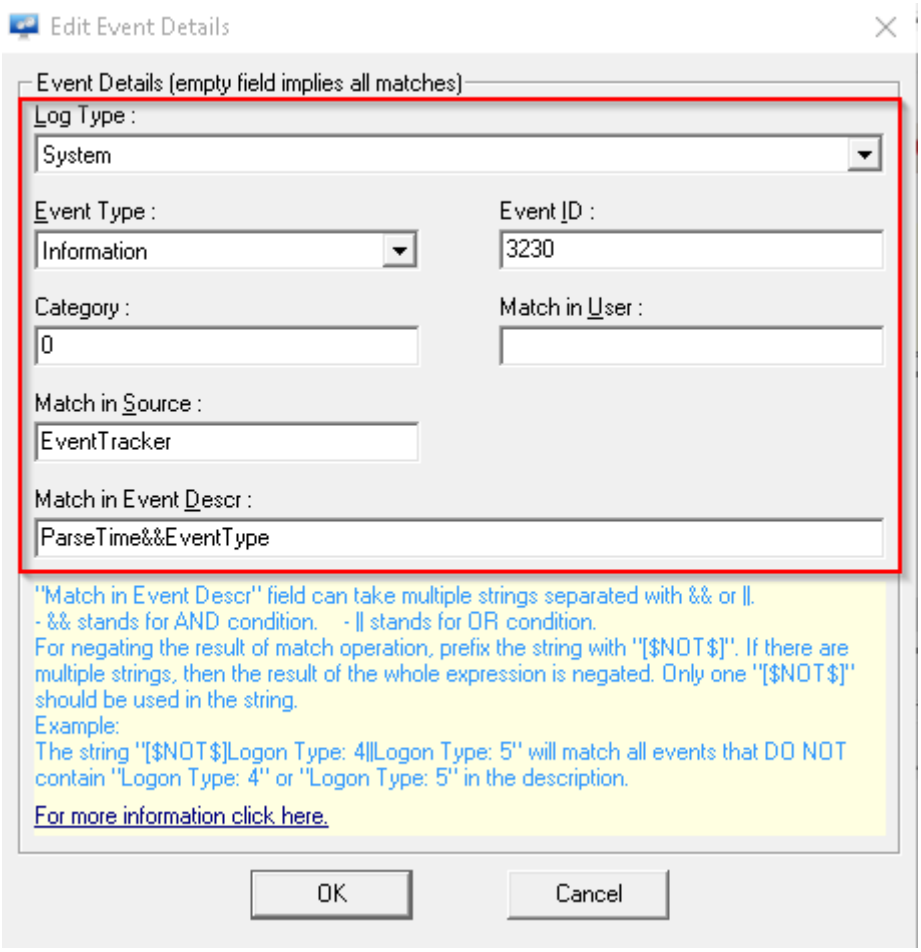

Figure 30

- 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.

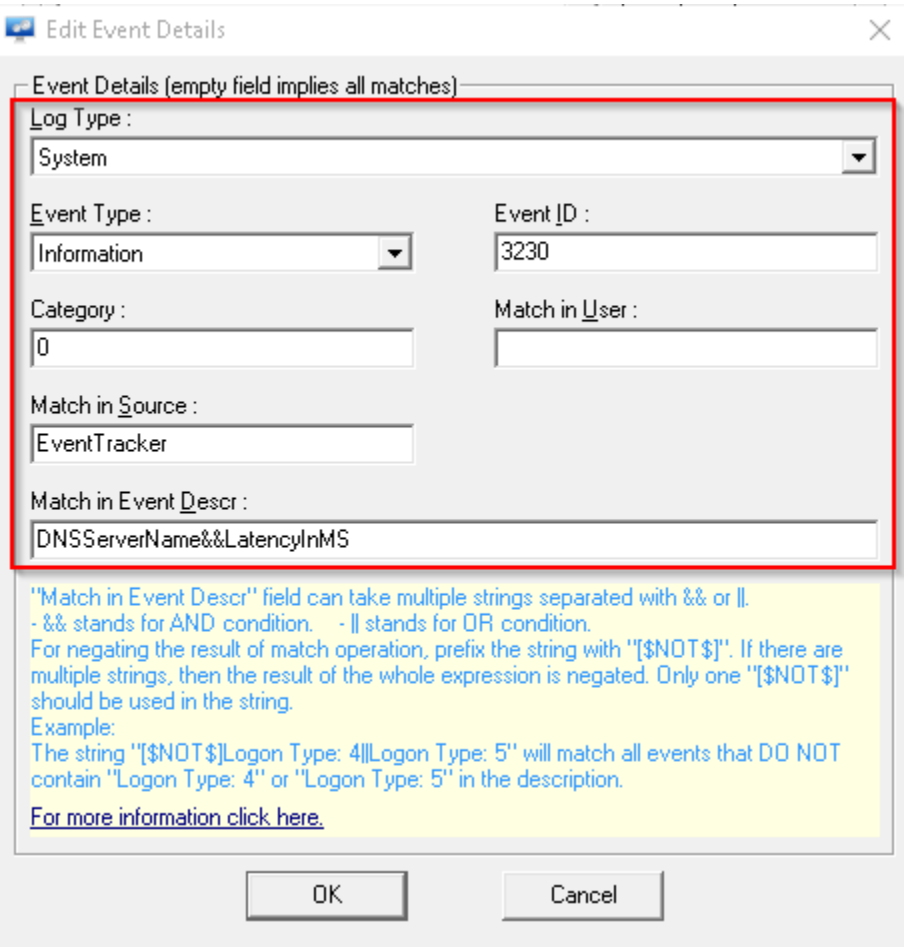

Figure 31

- 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.

Figure 32

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

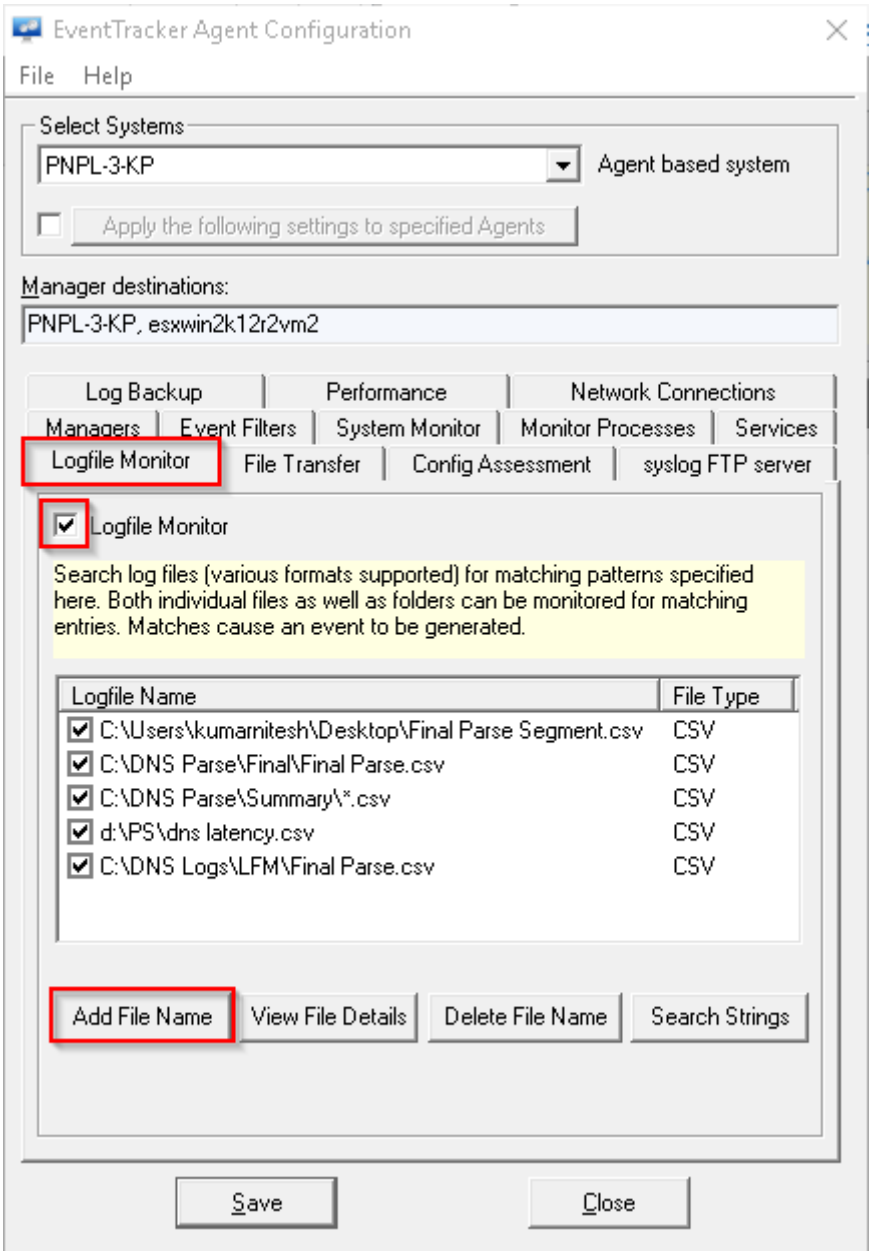

Figure 33

3. Click **Logfile Monitor** tab, select respective checkbox
4. Click **Add File Name**.

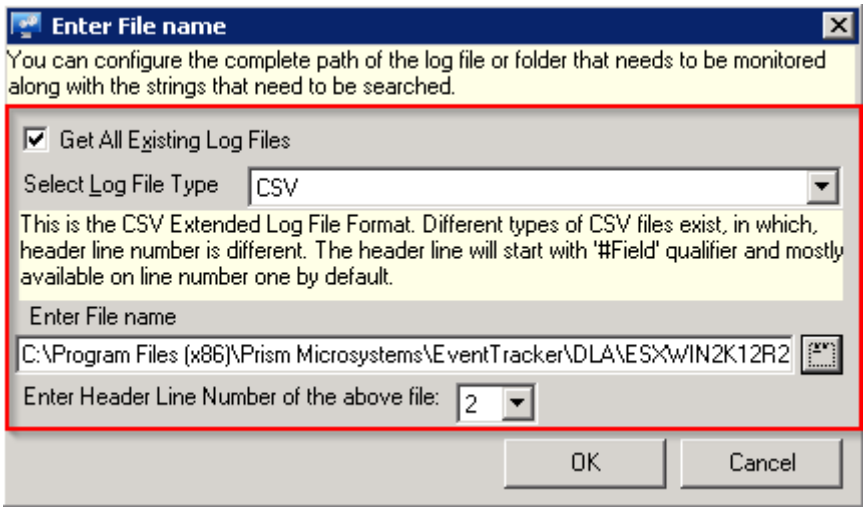

Figure 34

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.

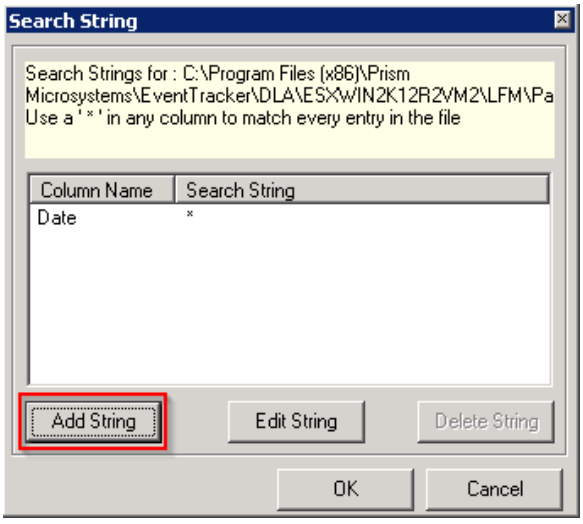

Figure 35

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**.

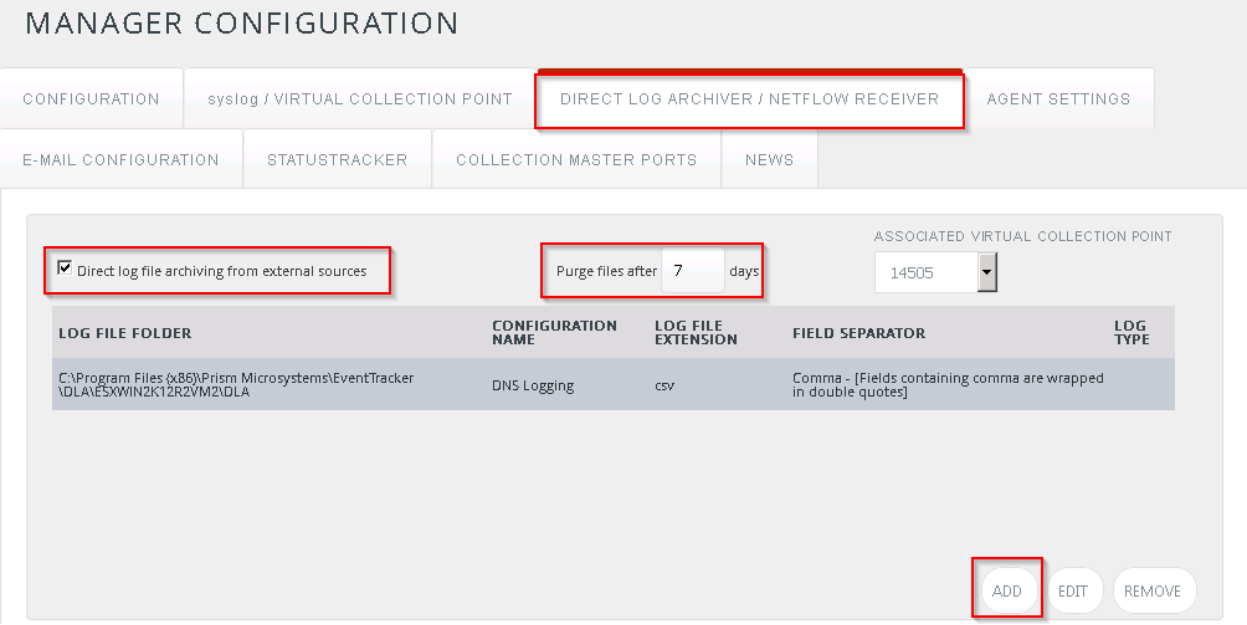

Figure 36

3. Select **Direct Log Archiver / NetFlow Receiver** tab, enable '**Direct log file archiving from external sources**".
4. Enter appropriate purge frequency and click **Add**.
5. Configure DLA options as shown below.

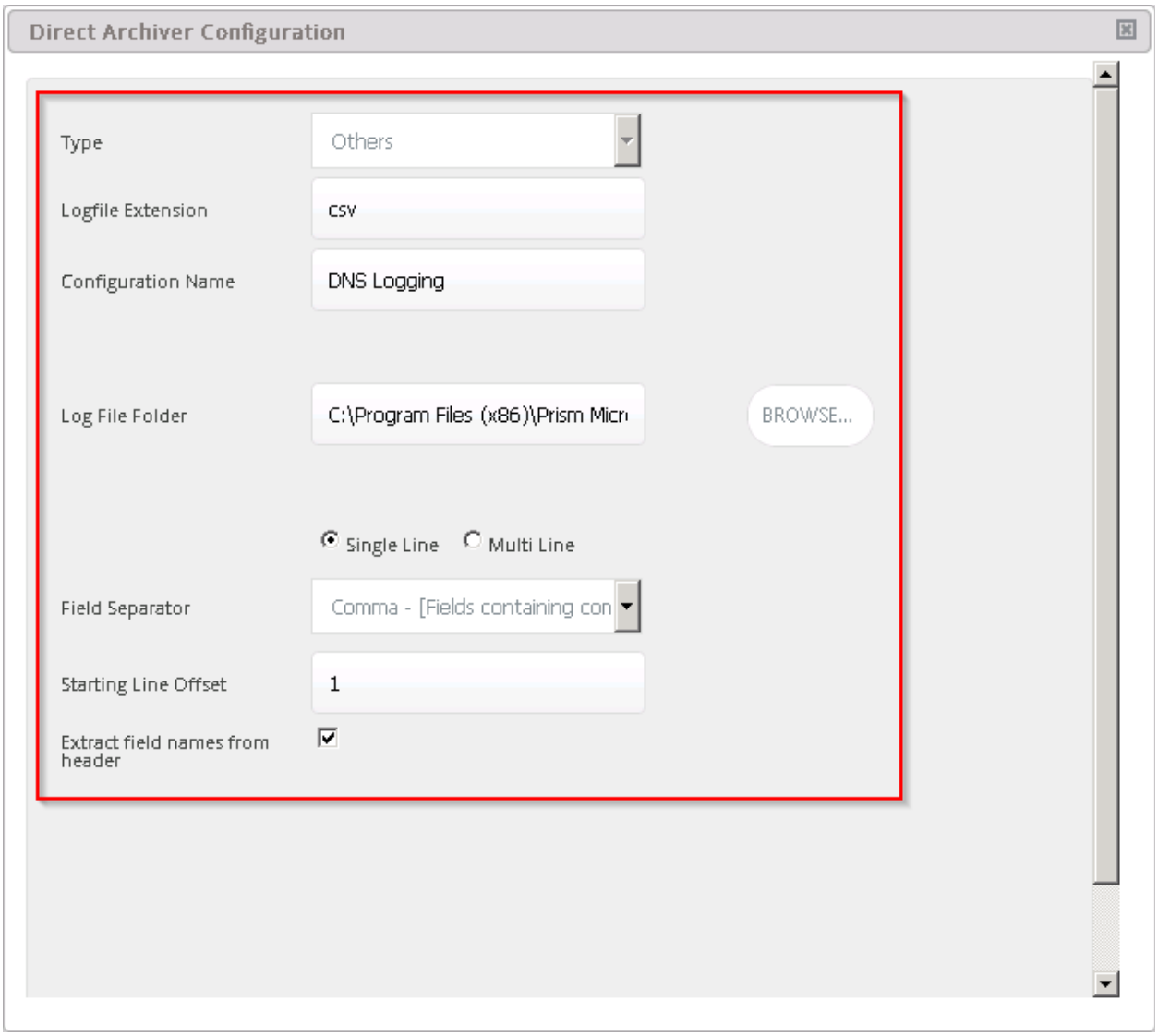

Figure 37

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.

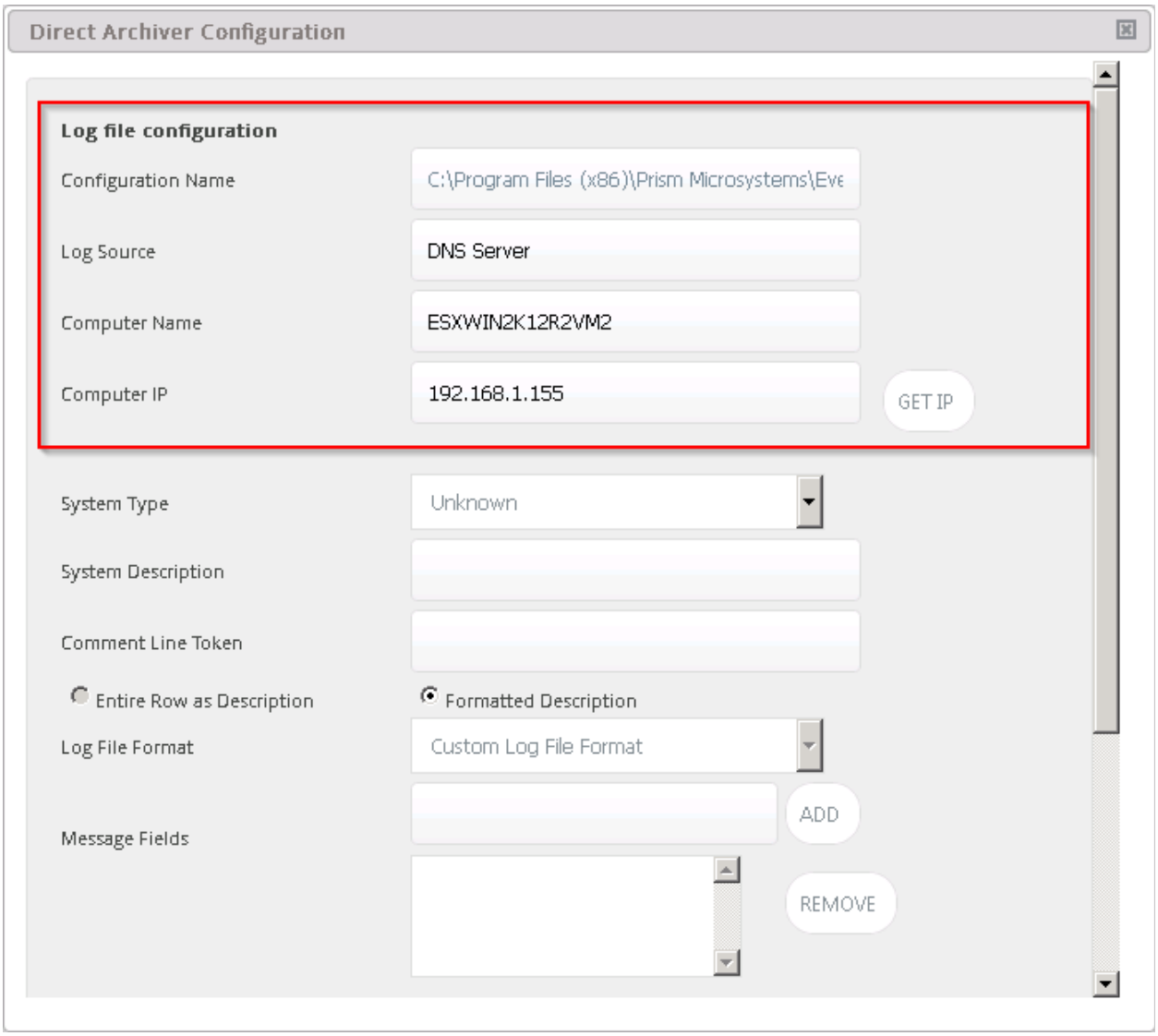

Figure 38

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.

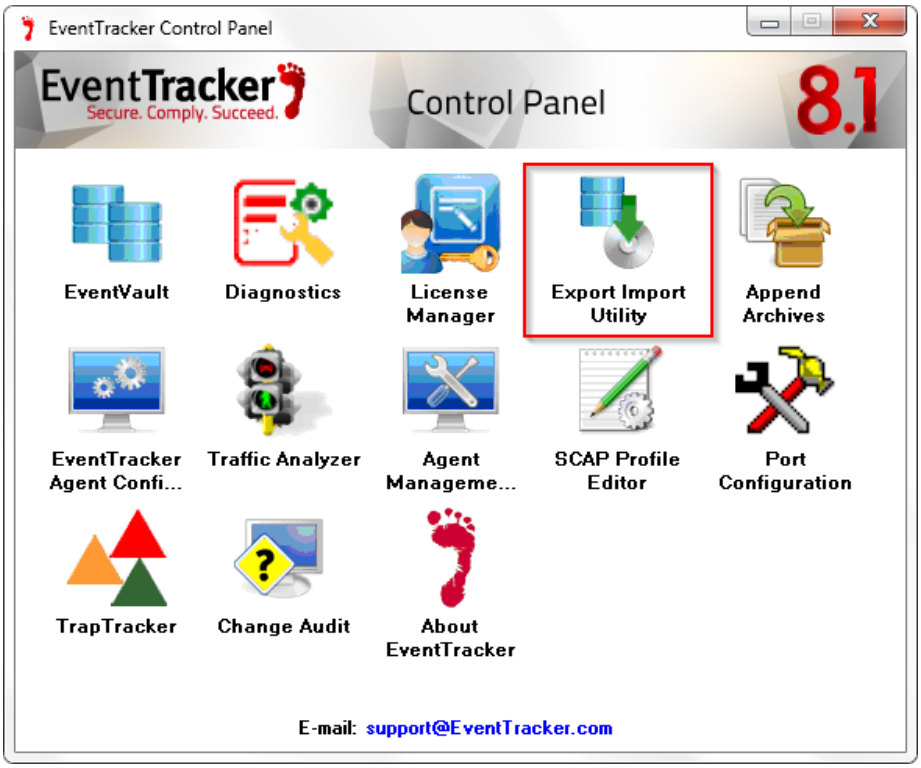

Figure 39

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.

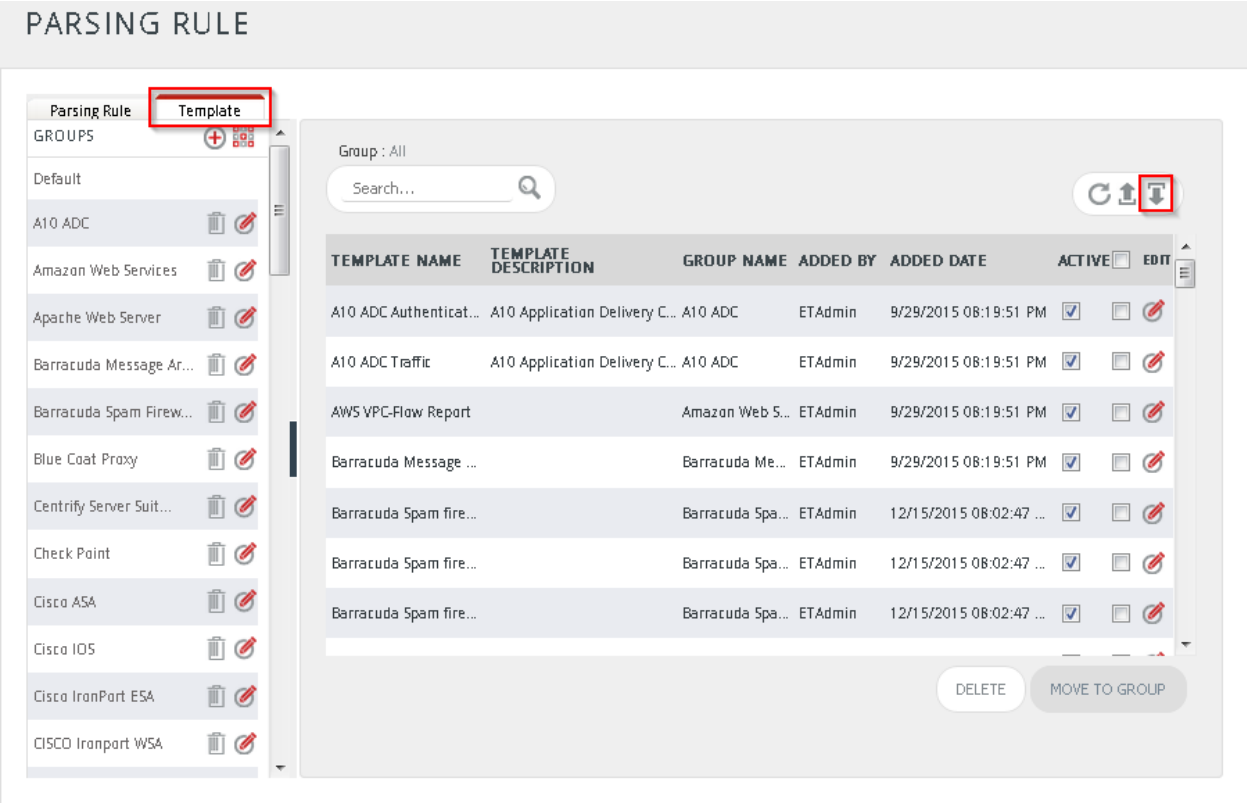

Figure 40

3. Click the **Browse** button.

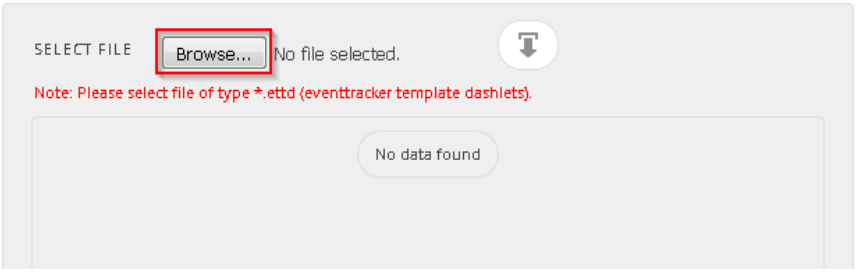

Figure 41

4. Locate **All Microsoft DNS token template.ettd** file, and then click the **Open** button.

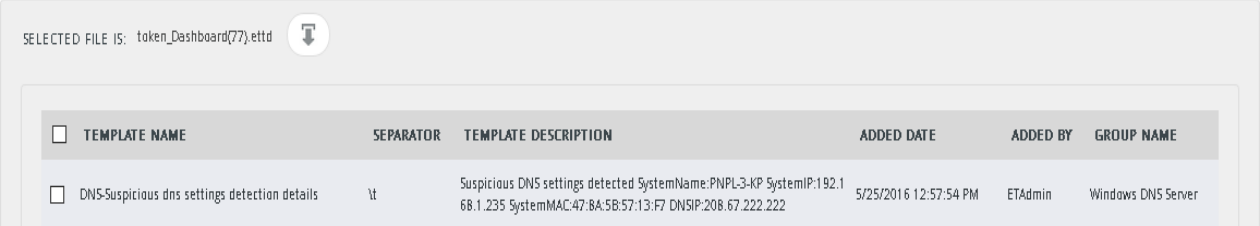

Figure 42

5. Now select the corresponding check boxes and then click on '**Import**' option.

   EventTracker displays success message.

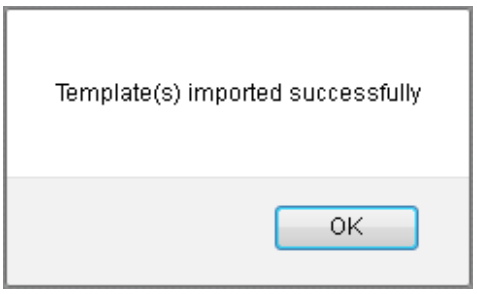

Figure 43

6. Click on **OK** button.

Import Parsing Rules

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

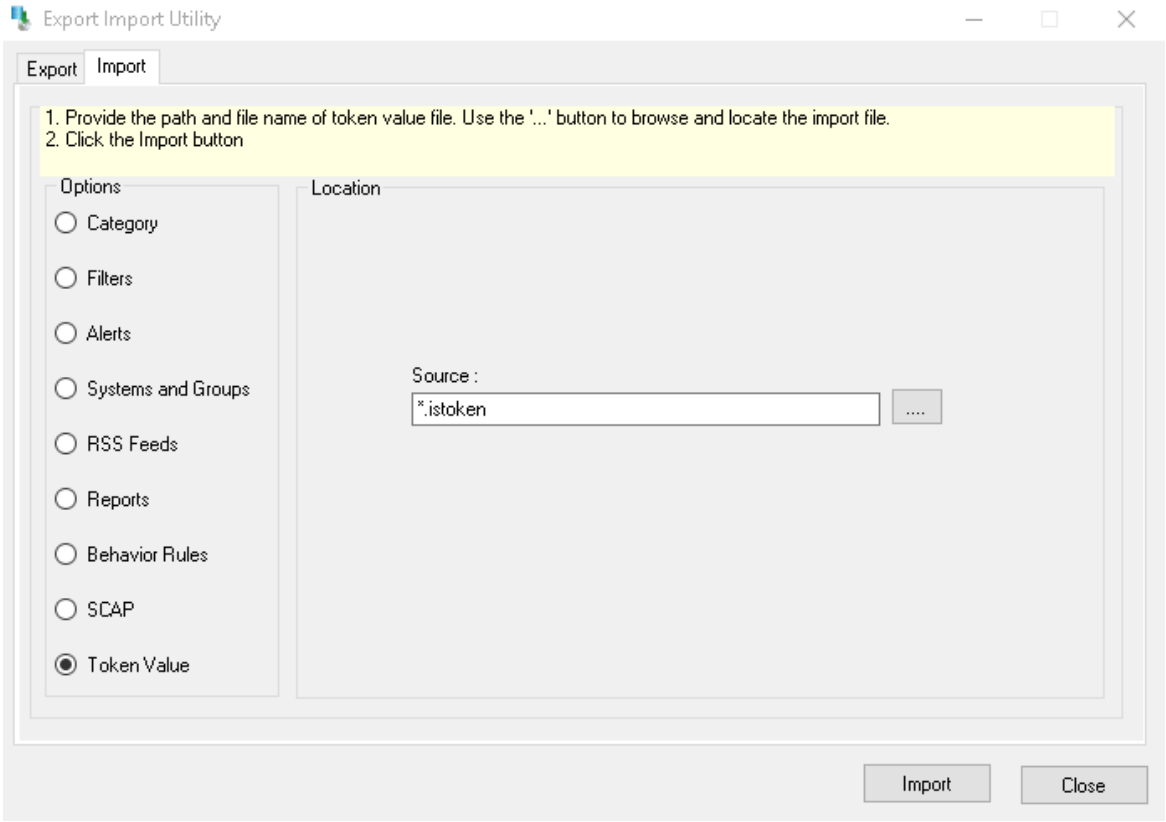

Figure 44

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.

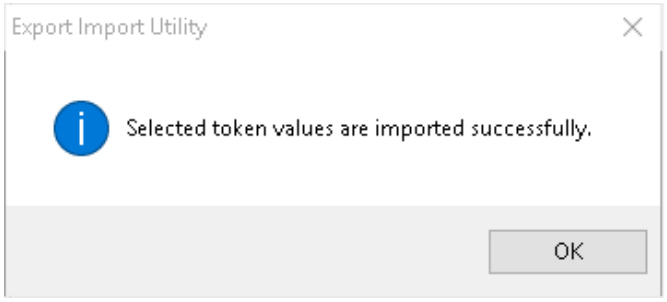

Figure 45

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

Import Behavior Rule

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

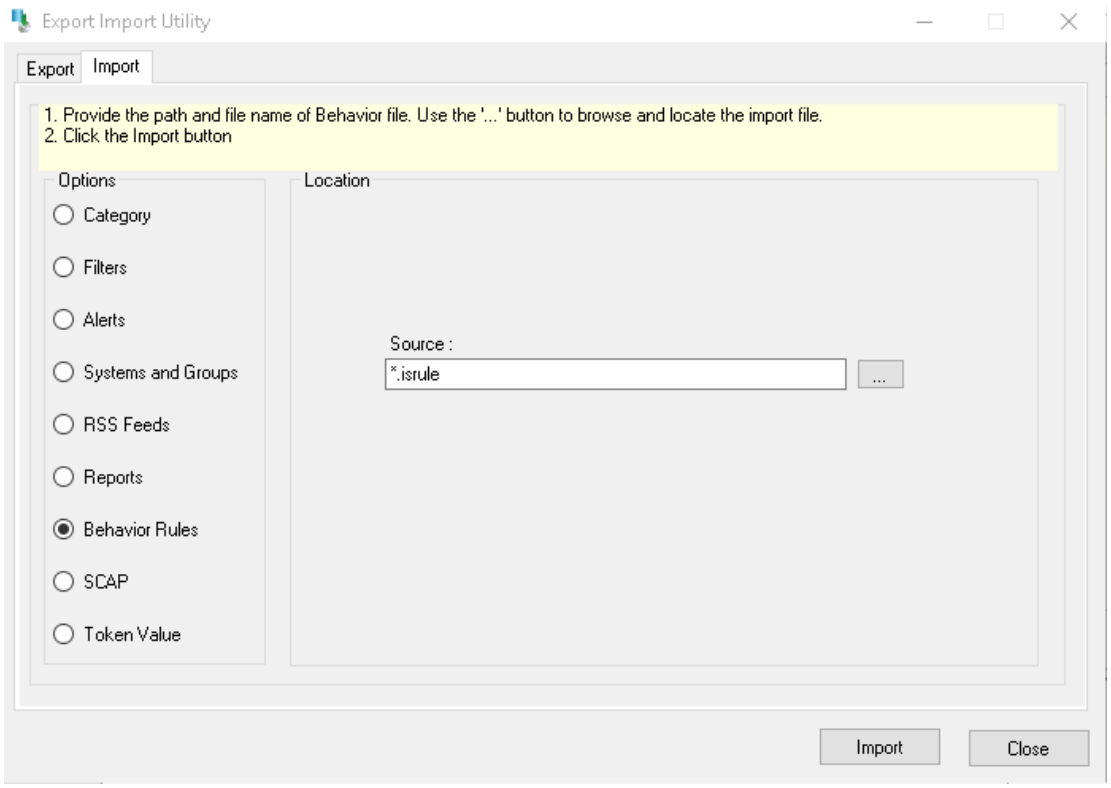

Figure 46

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.

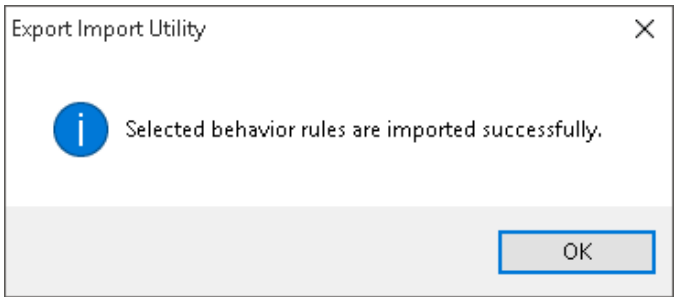

Figure 47

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.

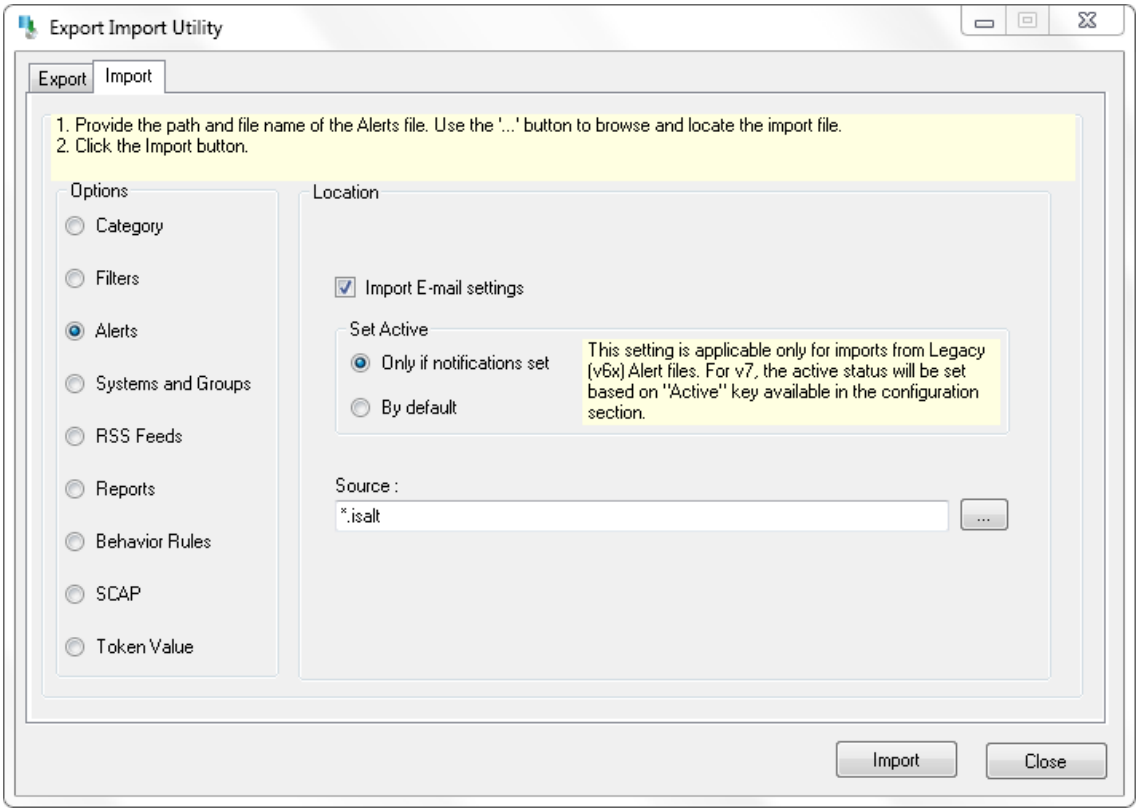

Figure 48

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

   EventTracker displays success message.

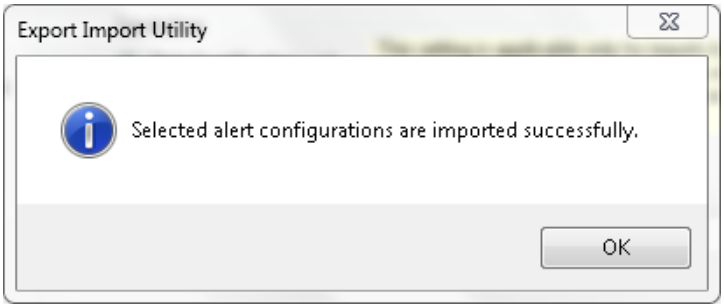

Figure 18

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.

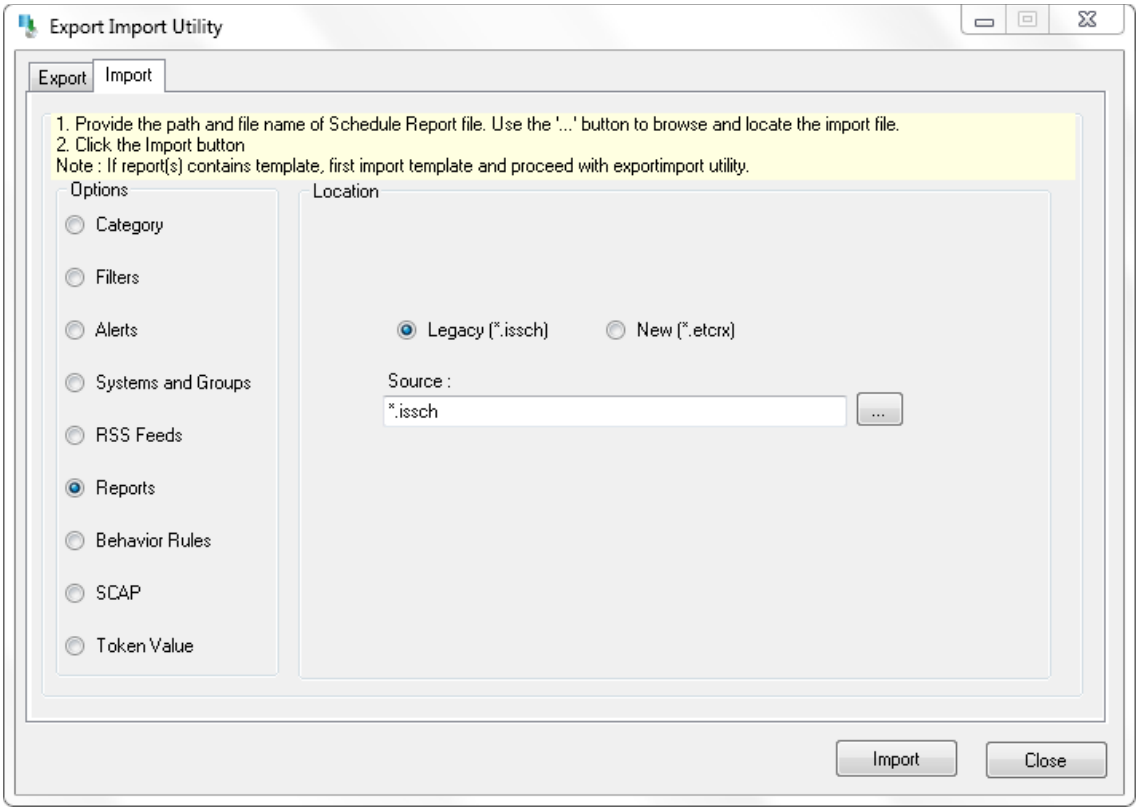

Figure 49

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

   EventTracker displays success message.

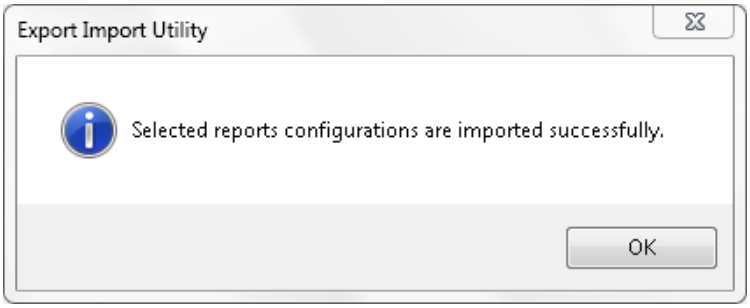

Figure 50

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.

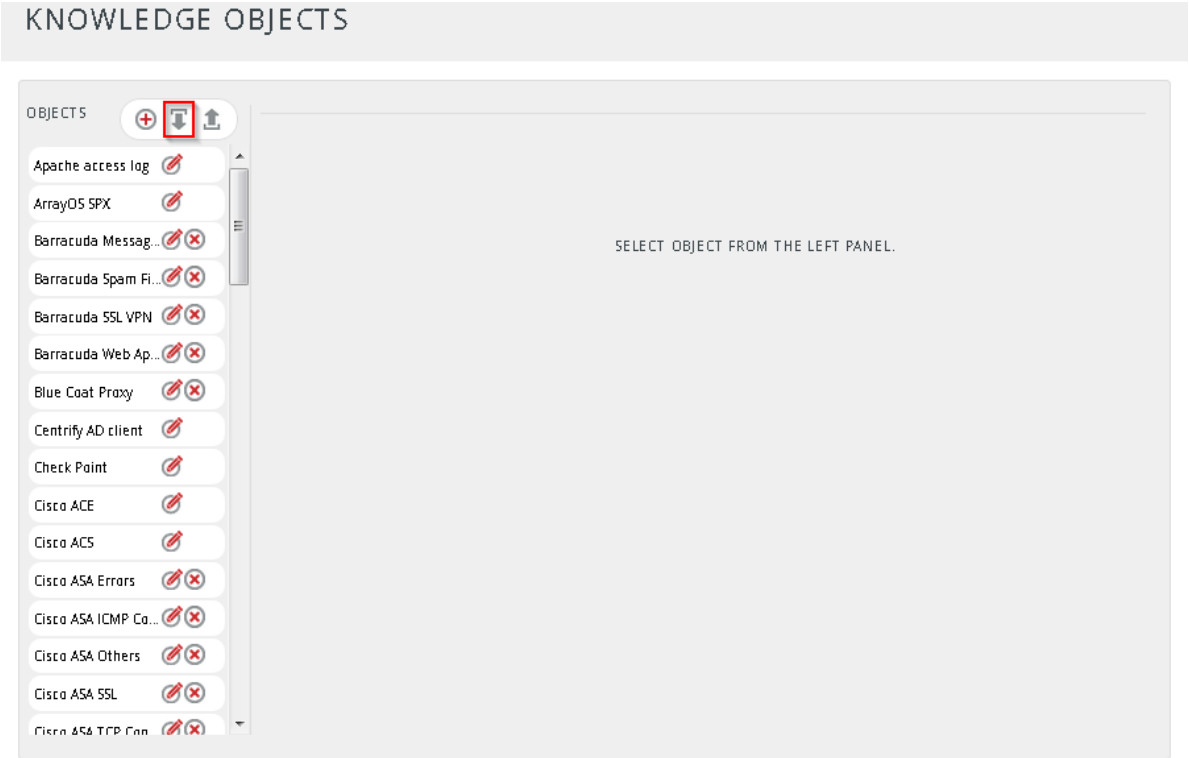

Figure 51

3. In **IMPORT** pane click on **Browse** button.

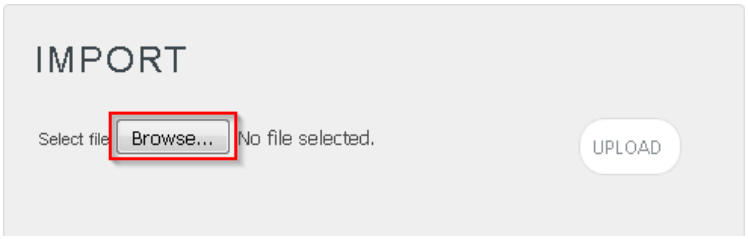

Figure 52

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

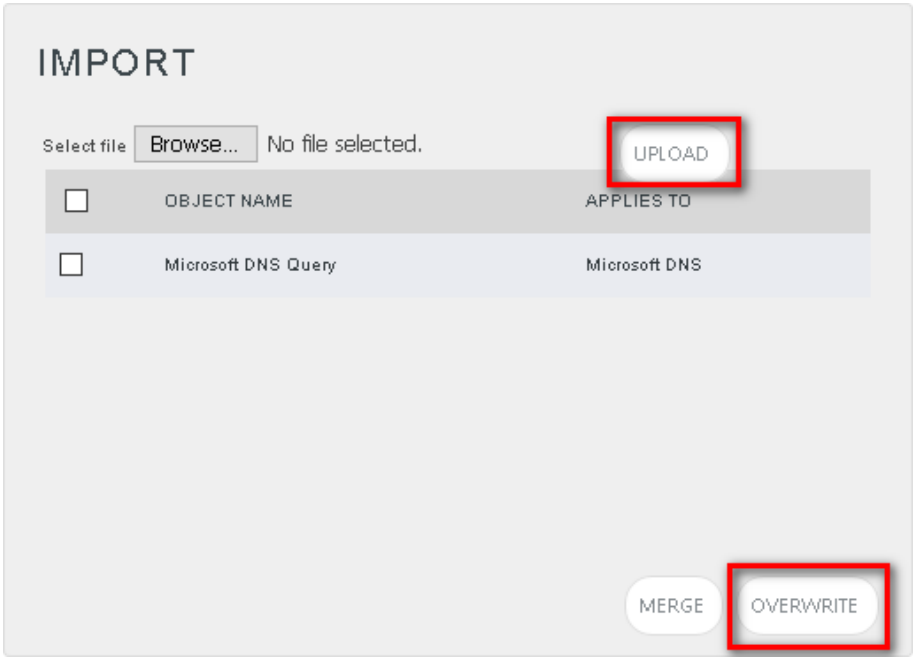

Figure 53

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

   EventTracker displays success message.

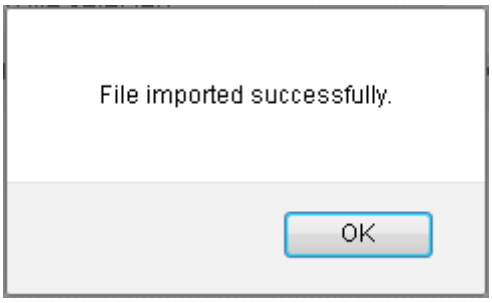

Figure 54

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.

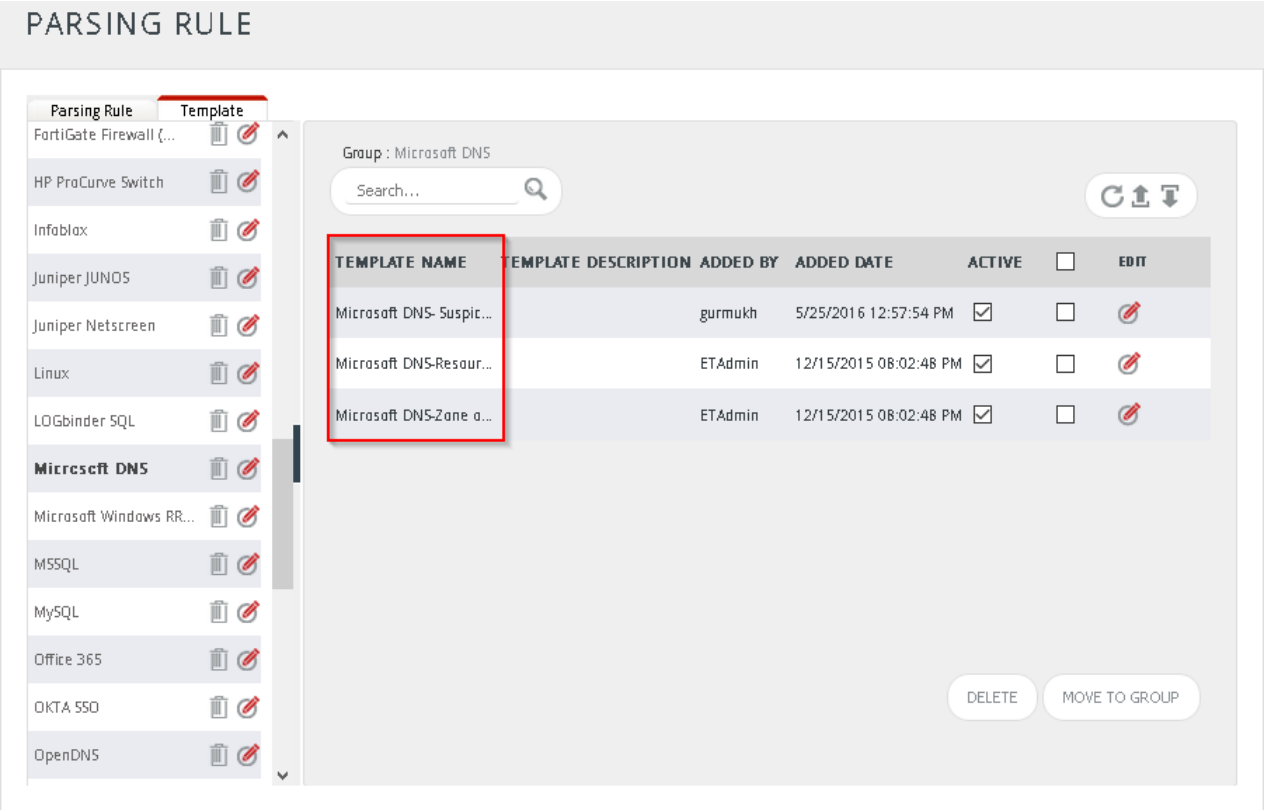

Figure 55

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.

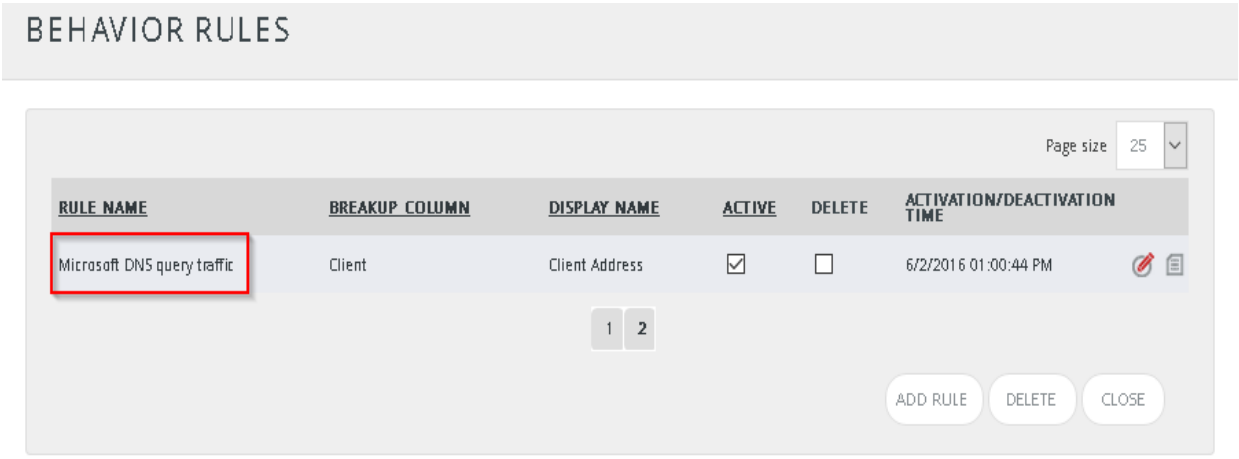

Figure 56

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.

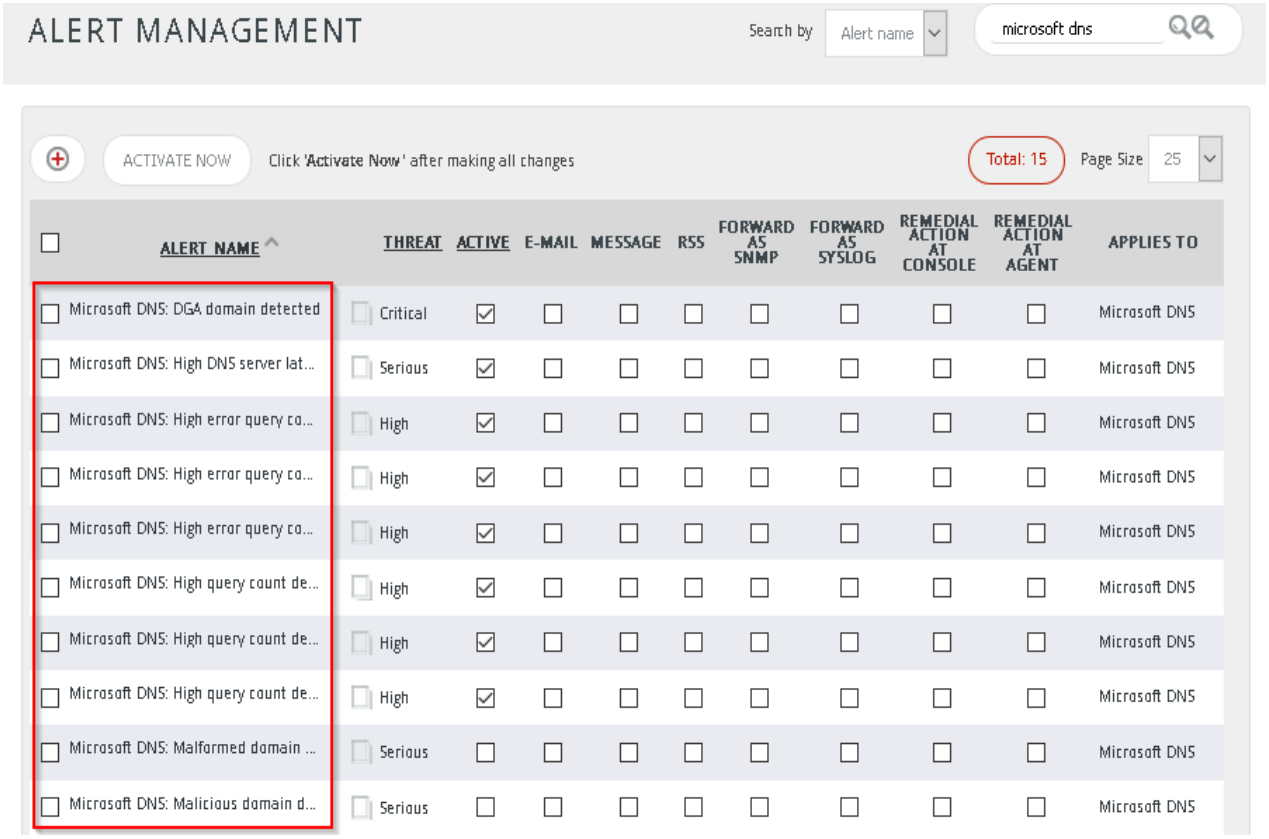

Figure 57

4. To activate the imported alerts, select the respective checkbox in the **Active** column.

   EventTracker displays message box.

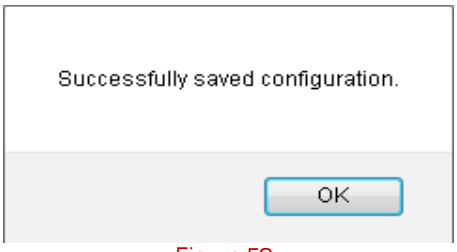

Figure 58

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.
4. In **Report Groups Tree**, select **Microsoft DNS group** folder.

Imported reports are displayed on the right pane.

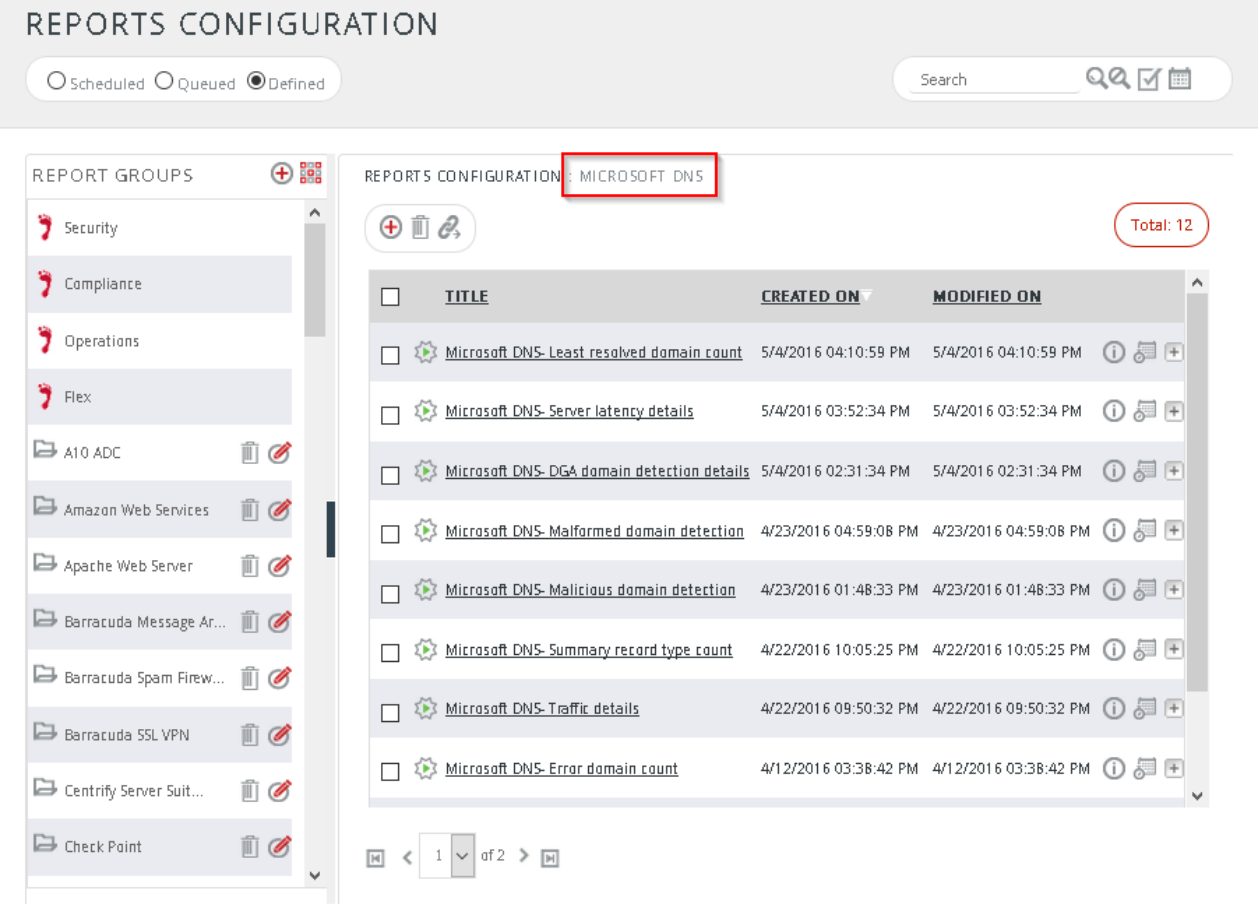

Figure 59

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.

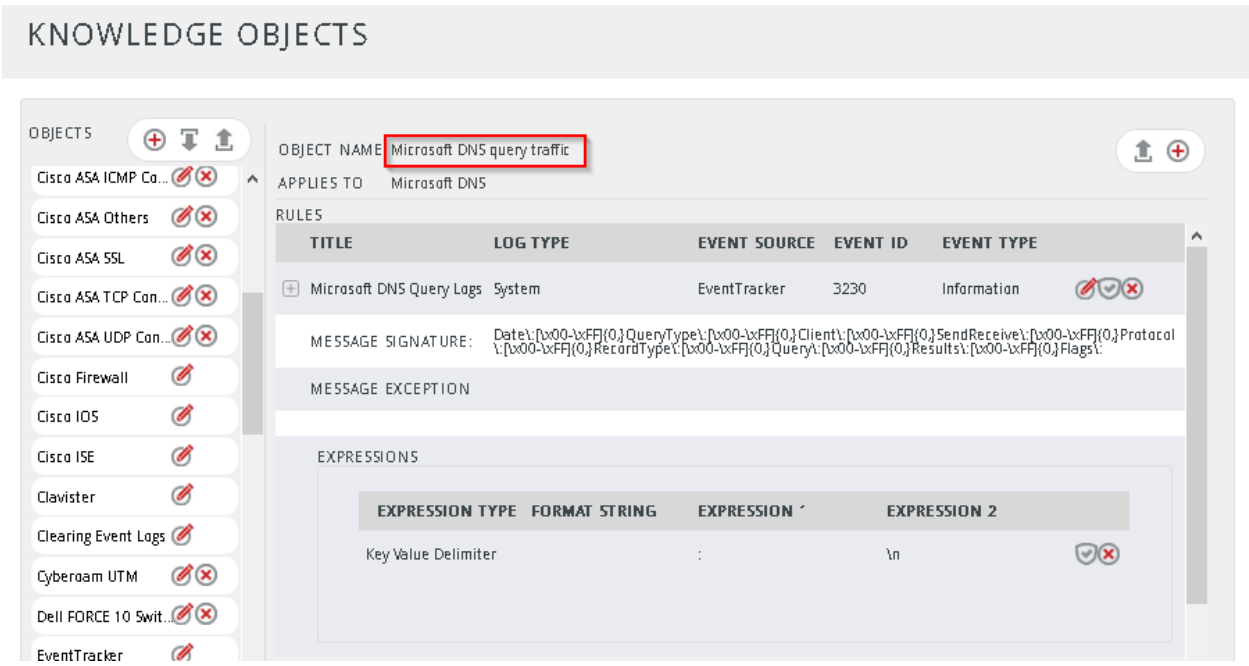

Figure 60

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.

Event Time	Computer	Client Address	Query Type	Action	Protocol Type	Domain Name	Result	Record Type	Flags
06/01/2016 17:48:18.16	CONTOSO-DNSSVR2	10.30.6.17	Forward	Snd	TCP	google.com	NOERROR	A	D
06/01/2016 17:48:26.59	CONTOSO-DNSSVR2	10.30.1.195	Forward	Snd	TCP	foxnews.com	NOERROR	A	D
06/01/2016 17:48:27.02	CONTOSO-DNSSVR2	10.30.1.195	Forward	Snd	TCP	delivery.josephsclothiers.com	NOERROR	A	D
06/01/2016 17:48:27.45	CONTOSO-DNSSVR2	10.30.1.195	Forward	Snd	TCP	litigators.esteroscreen.com	NOERROR	A	
06/01/2016 17:48:27.94	CONTOSO-DNSSVR2	10.30.1.195	Forward	Snd	TCP	qrwzoxcjatynejejsz.com	NOERROR	A	
06/01/2016 17:48:28.51	CONTOSO-DNSSVR2	10.30.1.195	Forward	Snd	TCP	gerrygraves.clientshostname.com	NOERROR	A	D
06/01/2016 17:48:36.04	CONTOSO-DNSSVR2	10.30.6.17	Forward	Rcv	TCP	google.com	NOERROR	A	

Figure 61

Date:06/01/2016 17:48:41.19
QueryType:Forward
Client:10.30.6.17
SendReceive:Snd
Protocol:TCP
RecordType: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.

Event Time	Computer	Error Type	Count
06/01/2016 17:48:25.92	CONTOSO-DNSSVR1	NXDOMAIN	77
06/01/2016 17:48:26.17	CONTOSO-DNSSVR1	REFUSED	63
06/01/2016 17:48:26.34	CONTOSO-DNSSVR1	SRVFAIL	28

Figure 62

Name: NXDOMAIN
Count: 77
ParseTime: 06/01/2016 17:48:25.92
EventType: DNS Error Type Summary

- **Microsoft DNS- Error client count**

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

Event Time	Computer	Client Address	Count
06/01/2016 17:48:25.32	CONTOSO-DNSSVR1	10.30.6.17	37
06/01/2016 17:48:25.74	CONTOSO-DNSSVR1	10.30.6.201	70
06/01/2016 18:04:43.64	CONTOSO-DNSSVR1	10.30.6.17	12
06/01/2016 18:04:44.04	CONTOSO-DNSSVR1	10.30.6.201	51

Figure 63

Name: 10.30.6.17
Count: 37
ParseTime: 06/01/2016 17:48:25.32
EventType: DNS Error Client Summary

- **Microsoft DNS- Error domain count**

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

Event Time	Computer	Domain Name	Count
06/01/2016 17:48:23.75	CONTOSO-DNSSVR1	ms2.google.com	71
06/01/2016 17:48:24.00	CONTOSO-DNSSVR1	contoso.local	37
06/01/2016 17:48:24.25	CONTOSO-DNSSVR1	download.com	77
06/01/2016 18:04:42.25	CONTOSO-DNSSVR1	jeremiaz.com	151

Figure 64

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.

Event Time	Computer	Record Type	Count
06/01/2016 17:48:22.33	CONTOSO-DNSSVR1	A	28
06/01/2016 17:48:22.53	CONTOSO-DNSSVR1	AAAA	37
06/01/2016 17:48:22.77	CONTOSO-DNSSVR1	SRV	70
06/01/2016 18:04:40.56	CONTOSO-DNSSVR1	A	100
06/01/2016 18:04:40.92	CONTOSO-DNSSVR1	AAAA	12
06/01/2016 18:04:41.09	CONTOSO-DNSSVR1	SRV	51

Figure 65

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.

Event Time	Computer	Client Address	Count
06/01/2016 17:48:24.43	CONTOSO-DNSSVR1	10.30.6.214	63
06/01/2016 17:48:24.67	CONTOSO-DNSSVR1	10.30.6.17	28
06/01/2016 17:48:24.82	CONTOSO-DNSSVR1	10.30.6.21	28
06/01/2016 17:48:25.07	CONTOSO-DNSSVR1	10.30.6.201	70

Figure 66

Name: 10.30.6.21
Count: 100
ParseTime: 06/01/2016 18:04:43.25
EventType: DNS Client Parse Summary

- **Microsoft DNS- Summary domain count**

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

Event Time	Computer	Domain Name	Count
06/01/2016 17:48:22.92	CONTOSO-DNSSVR1	mmexe.com	63
06/01/2016 17:48:23.16	CONTOSO-DNSSVR1	ocsp.usertrust.com	37
06/01/2016 17:48:23.41	CONTOSO-DNSSVR1	contoso.local	71
06/01/2016 17:48:23.61	CONTOSO-DNSSVR1	ocsp.comodoca.com	28

Figure 67

Name: mmexe.com
Count: 64
ParseTime: 06/01/2016 18:04:41.24
EventType: DNS Query Parse Summary

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

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

Event Time	Computer	Domain Name	Count	Client Address
06/01/2016 17:48:18.39	CONTOSO-DNSSVR1	l9ve.co	1	10.30.6.214
06/01/2016 17:48:21.91	CONTOSO-DNSSVR1	vacebook.net	1	10.30.6.17
06/01/2016 17:48:22.09	CONTOSO-DNSSVR1	amazon.o.org	1	10.30.6.21
06/01/2016 17:48:41.35	CONTOSO-DNSSVR1	l9ve.co	1	10.30.6.214

Figure 68

Domain: vacebook.net
Count: 1
Client: 10.30.6.17
ParseTime: 06/01/2016 18:04:45.08
EventType: Least Resolved Domain Summary

- **Microsoft DNS- Malicious domain detection**

This report provides information related to malicious domain detected in DNS logs.

Event Time	Computer	Client Address	Domain Name	Domain Category	Domain Address	Domain Country
06/01/2016 17:48:18.24	CONTOSO-DNSSVR2	10.30.6.201	jeremiaz.com	phishing	85.24.215.117	United States
06/01/2016 17:48:29.19	CONTOSO-DNSSVR2	10.30.1.195	litigators.esteroscreen.com	malware	209.126.120.8	United States
06/01/2016 17:48:34.23	CONTOSO-DNSSVR2	10.30.6.21	mmexe.com	attackpage	92.222.6.12	United States
06/01/2016 17:48:34.47	CONTOSO-DNSSVR2	10.30.6.17	softworksbd.com	malware	107.181.174.84	Bangladesh
06/01/2016 17:48:41.19	CONTOSO-DNSSVR2	10.30.6.201	jeremiaz.com	phishing	85.24.215.117	United States

Figure 69

Malicious domain detected
Date:06/01/2016 17:48:41.19
DomainName:jeremiaz.com
DomainIP:85.24.215.117
DomainCountry:United States
Category:phishing
ClientIP:10.30.6.201

- **Microsoft DNS- Suspicious DNS setting detection**

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

LogTime	Device Name	Device IP	Device MAC	Device DNS
06/01/2016 05:48:18 PM	Contoso-WRK01	10.30.6.17	00:0C:29:16:7D:A3	77.88.8.9
06/01/2016 05:48:33 PM	Contoso-WRK01	10.30.6.17	00:0C:29:16:7D:A3	77.88.8.8
06/01/2016 05:48:33 PM	Contoso-WRK25	10.30.6.21	47:8A:5B:57:13:F7	208.67.222.224
06/01/2016 05:48:33 PM	Contoso-WRK25	10.30.6.21	47:8A:5B:57:13:F7	208.67.222.222
06/01/2016 05:48:33 PM	Contoso-WRK13	10.30.6.201	00:0C:29:36:7D:A6	8.8.4.4
06/01/2016 05:48:34 PM	Contoso-WRK13	10.30.6.201	00:0C:29:36:7D:A6	8.8.8.8

Figure 70

Suspicious DNS setting detected
SystemName:Contoso-WRK01
SystemIP:10.30.6.17
SystemMAC:00:0C:29:16:7D:A3
DNSIP:77.88.8.9

- **Microsoft DNS- DGA domain detection**

This report provides information related to DGA domain, detected in DNS logs.

Event Time	Computer	Client Address	Domain Name	Domain Address	Domain Country	Record Type	Result
06/01/2016 17:48:18.33	CONTOSO-DNSSVR2	10.30.6.201	vmivkpqyunlqfpl.infor	Unknown	Unknown	A	NXDOMAIN
06/01/2016 17:48:20.64	CONTOSO-DNSSVR2	10.30.6.21	vmivkpqyunlqfpl.info	Unknown	Unknown	A	NXDOMAIN
06/01/2016 17:48:20.88	CONTOSO-DNSSVR2	10.30.6.17	googllerqwrwerwerwerw.net	2.111.70.28	China	A	NOERROR
06/01/2016 17:48:21.12	CONTOSO-DNSSVR2	10.30.6.214	googllerqwrwerwerwerw.net	37.59.14.201	China	A	NOERROR
06/01/2016 17:48:29.36	CONTOSO-DNSSVR2	10.30.1.195	qrwzoxcjatynejejsz.com	104.193.252.241	United States	A	NOERROR
06/01/2016 17:48:41.40	CONTOSO-DNSSVR2	10.30.6.201	vmivkpqyunlqfpl.infor	Unknown	Unknown	A	NXDOMAIN

Figure 71

DGA domain detected
Date:06/01/2016 17:48:41.40
DomainName:vmivkpqyunlqfpl.infor
DomainIP:Unknown
DomainCountry:Unknown
ClientIP:10.30.6.201
RecordType:A
Result:NXDOMAIN

- **Microsoft DNS- Server latency details**

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

Event Time	Computer Name	Computer IP	DNS Server Name	DNS Server IP	DNS Server Type	Latency in ms
06/01/2016 17:48:18.24	Contoso-WKS1	10.30.6.21	Contoso-DNSSVR2	10.30.6.12	Local DNS	100.19
06/01/2016 17:48:18.34	Contoso-WKS1	10.30.6.21	Contoso-DNSSVR2	10.30.6.12	Local DNS	8.9
06/01/2016 17:48:31.34	Contoso-WKS1	10.30.6.21	google-public-dns-b.google.com	8.8.4.4	Public DNS	5.16
06/01/2016 17:48:31.50	Contoso-WKS1	10.30.6.21	resolver4.opendns.com	208.67.220.222	Public DNS	6.19

Figure 72

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.

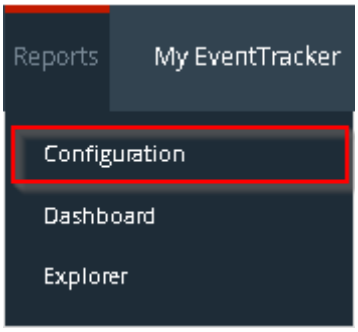

Figure 73

2. Navigate to **Reports>Configuration**.

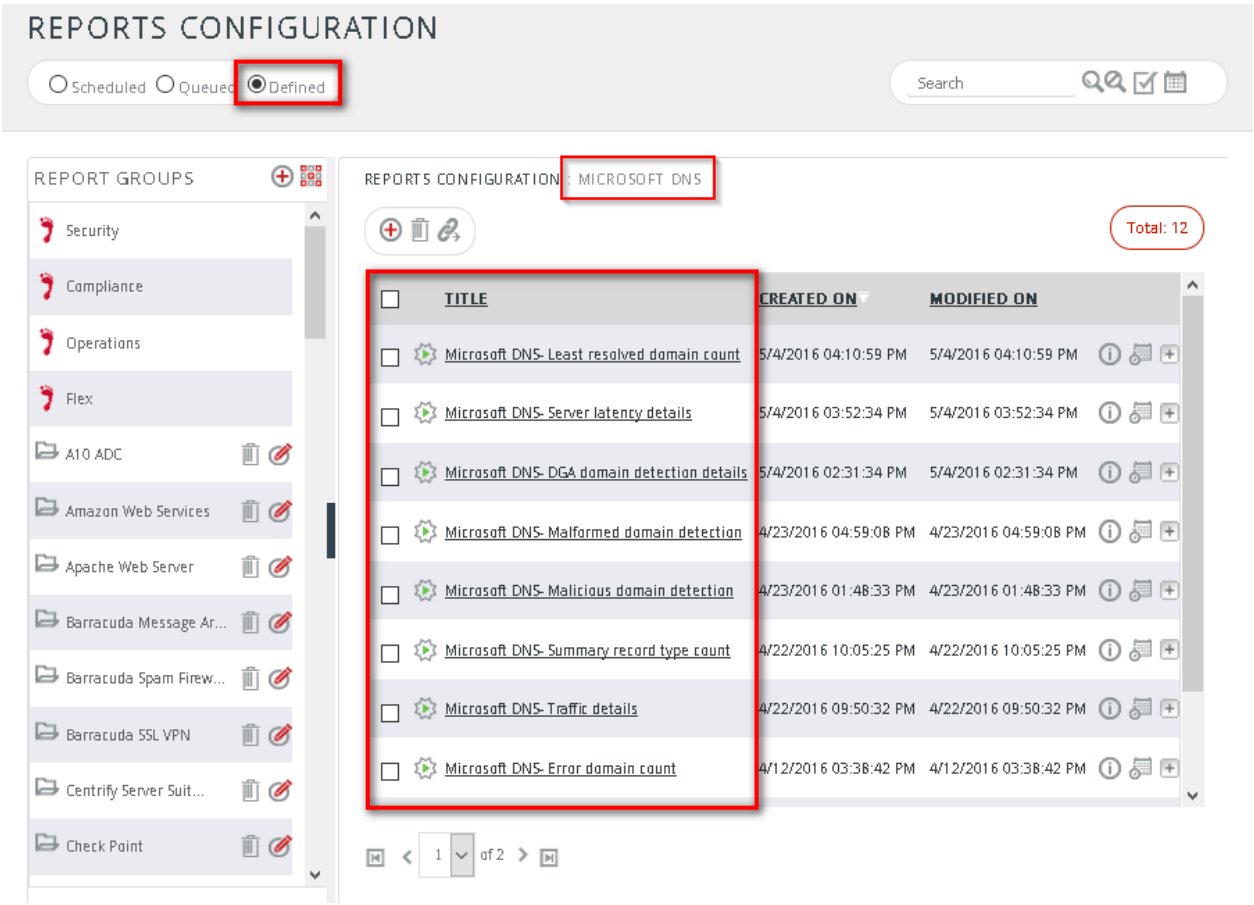

Figure 74

3. Select '**Microsoft DNS'** in report groups. Check **Defined** dialog box.
4. Click on '**schedule**'  to plan a report for later execution.

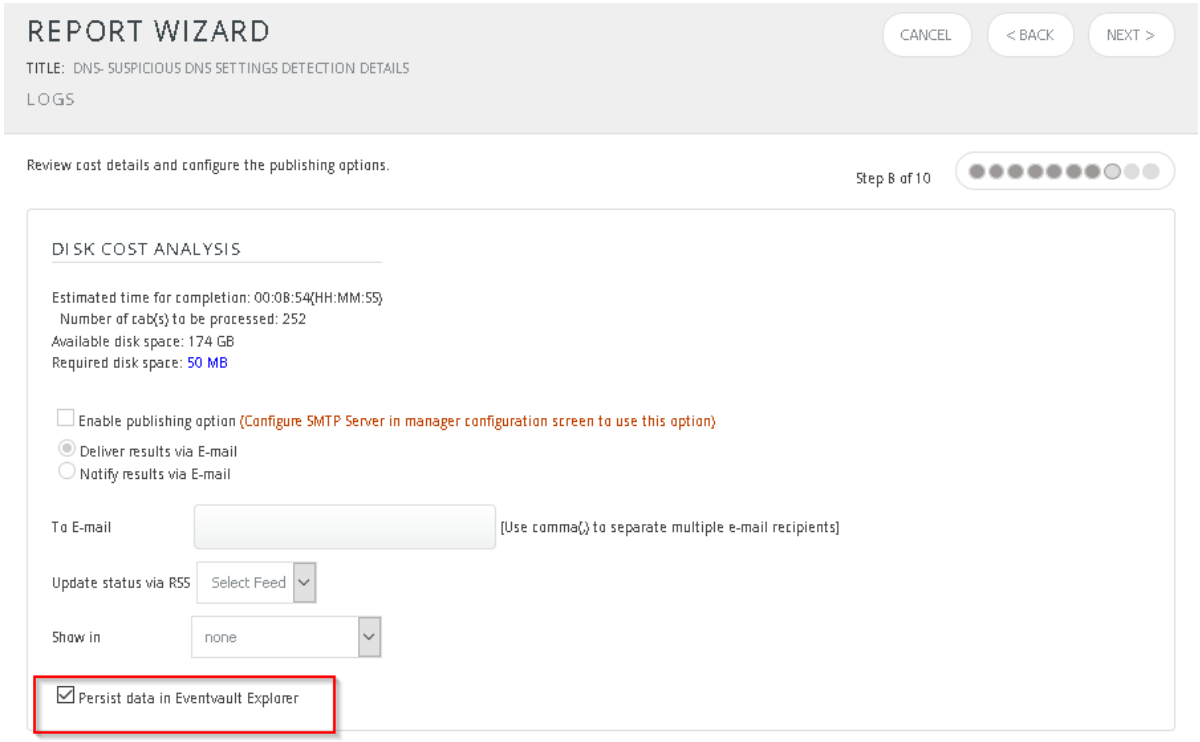

Figure 75

5. Choose appropriate time for report execution and in **Step 8** check **Persist data in Eventvault Explorer** box.

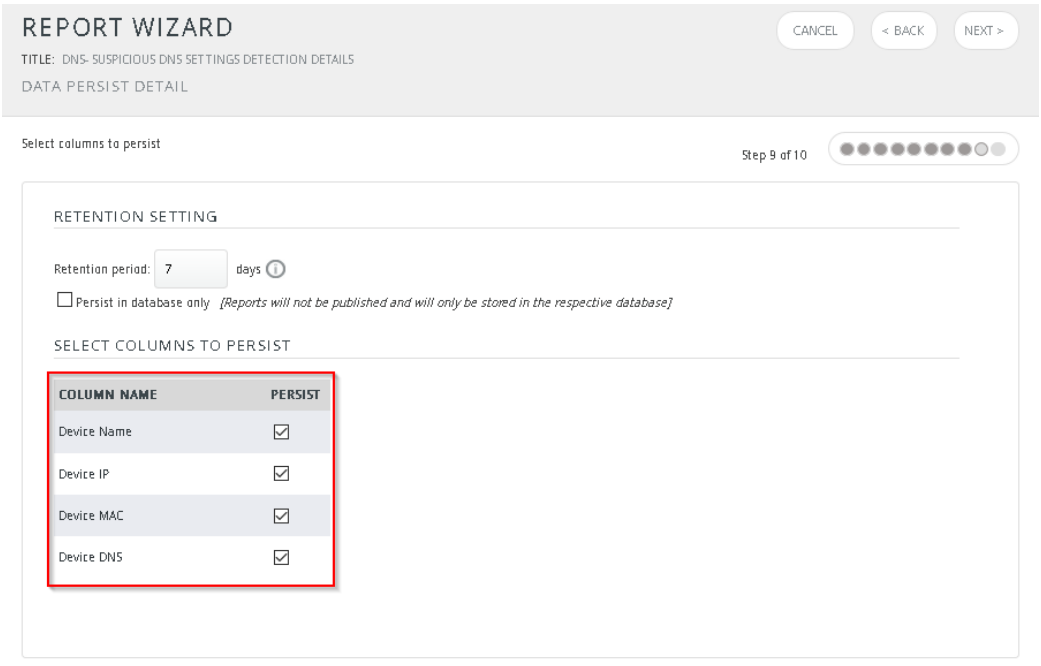

Figure 76

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.

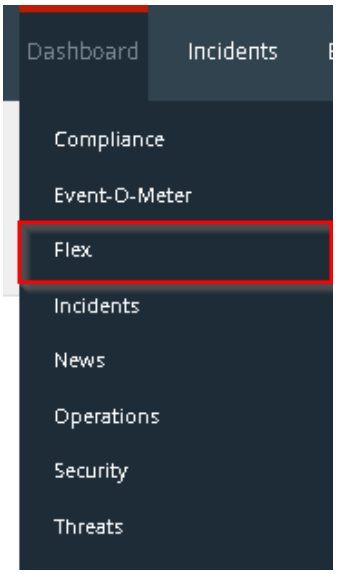

Figure 77

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

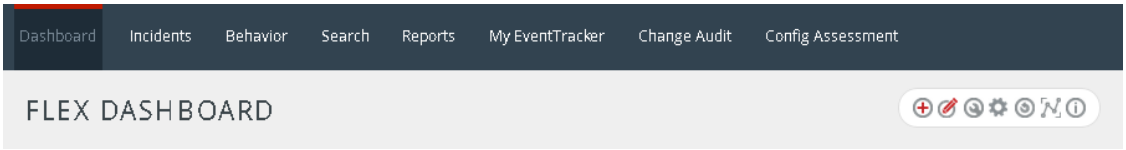

Figure 78

4. Click ⊕ to add a new dashboard.
   Flex Dashboard configuration pane is shown.

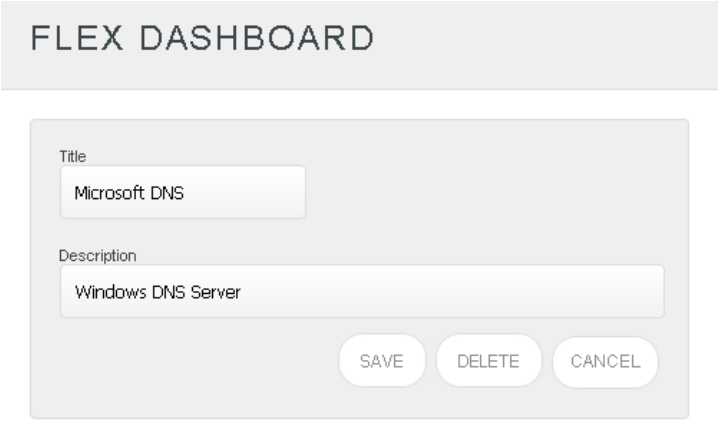

Figure 79

5. Fill appropriate title and description and click **Save** button.
6. Click ⚙ to configure a new flex dashlet.
   Widget configuration pane is shown.

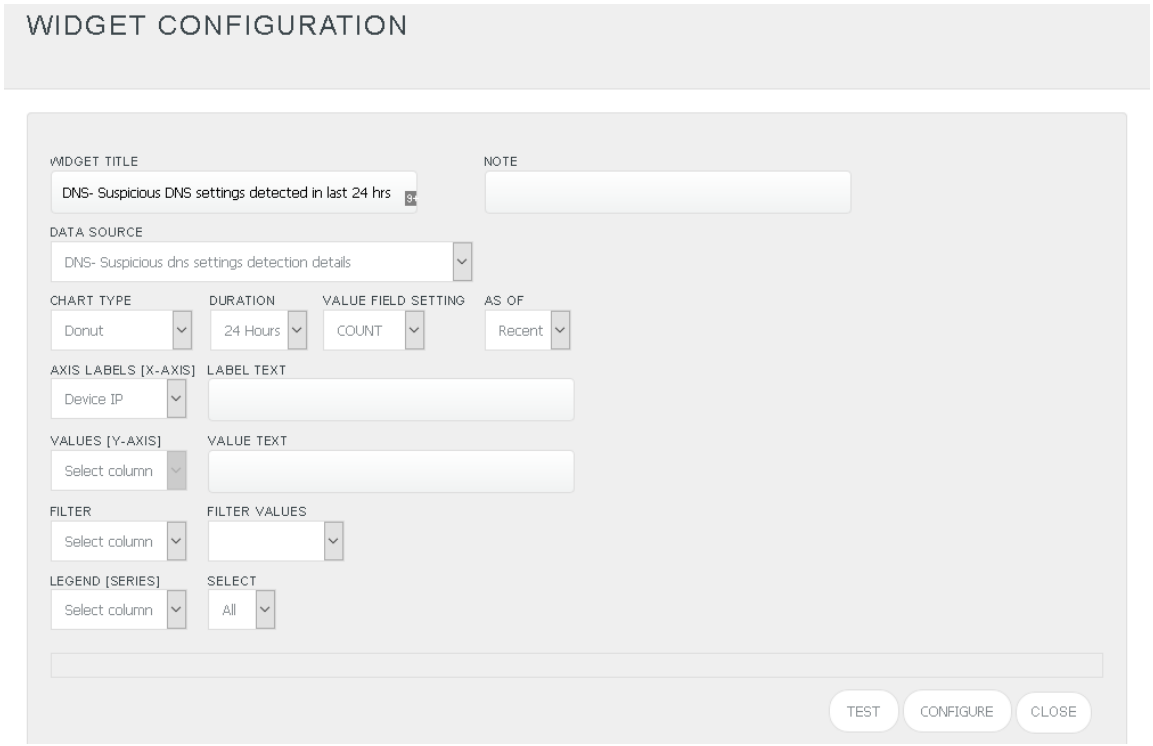

Figure 80

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.

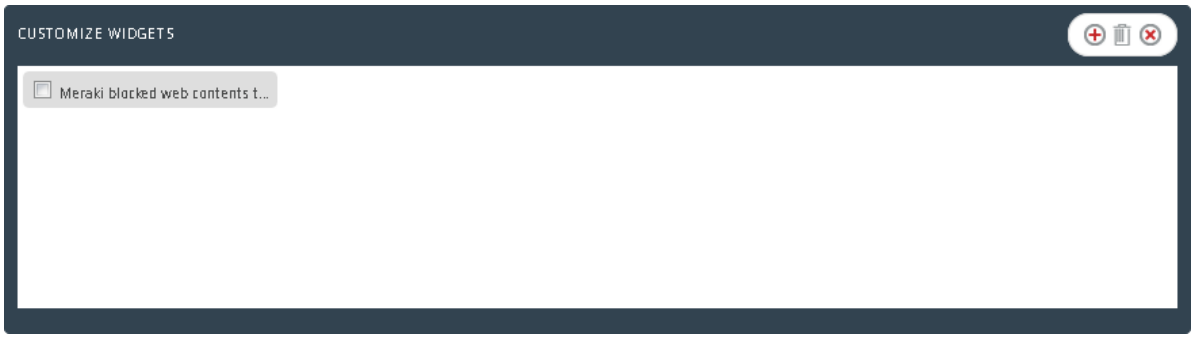

Figure 81

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**

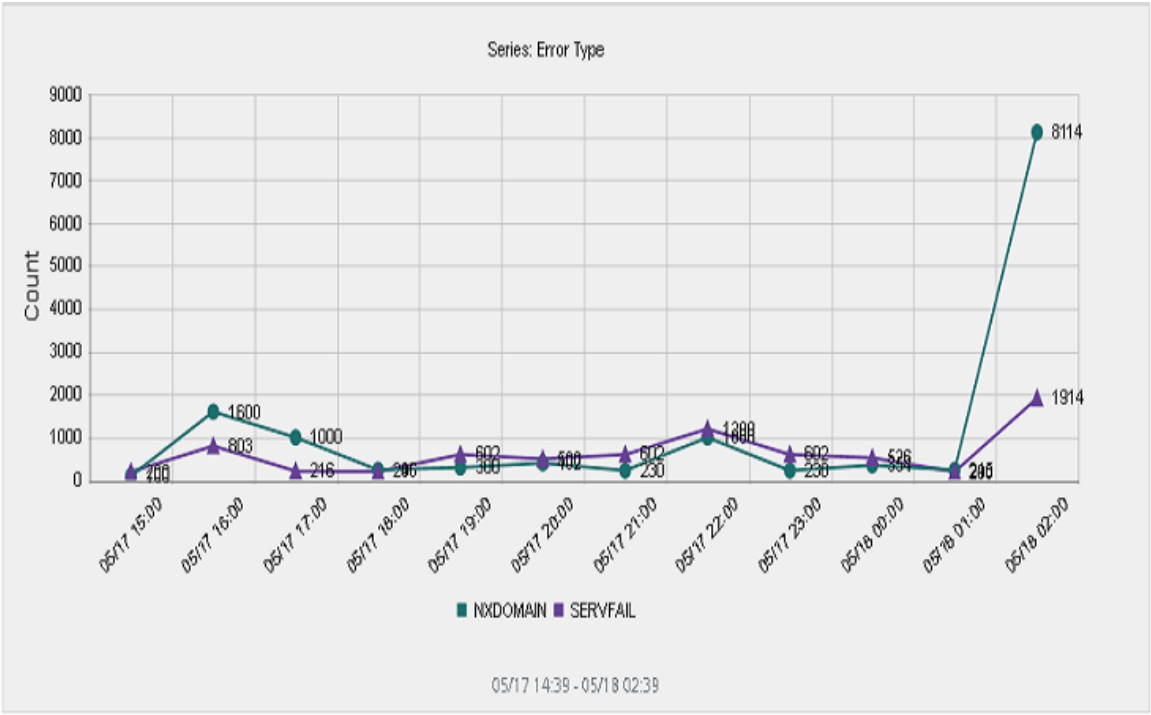

Figure 82

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

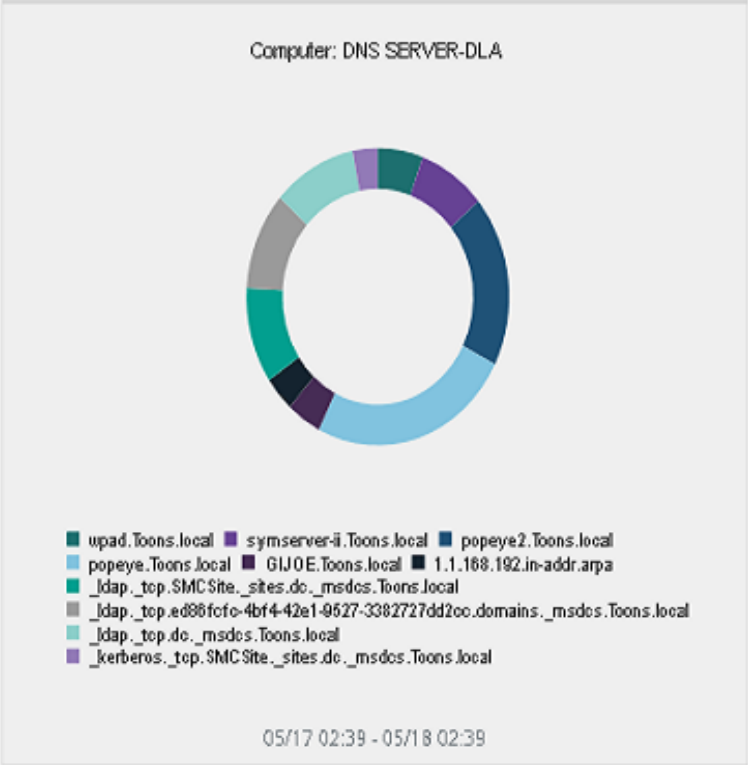

Figure 83

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

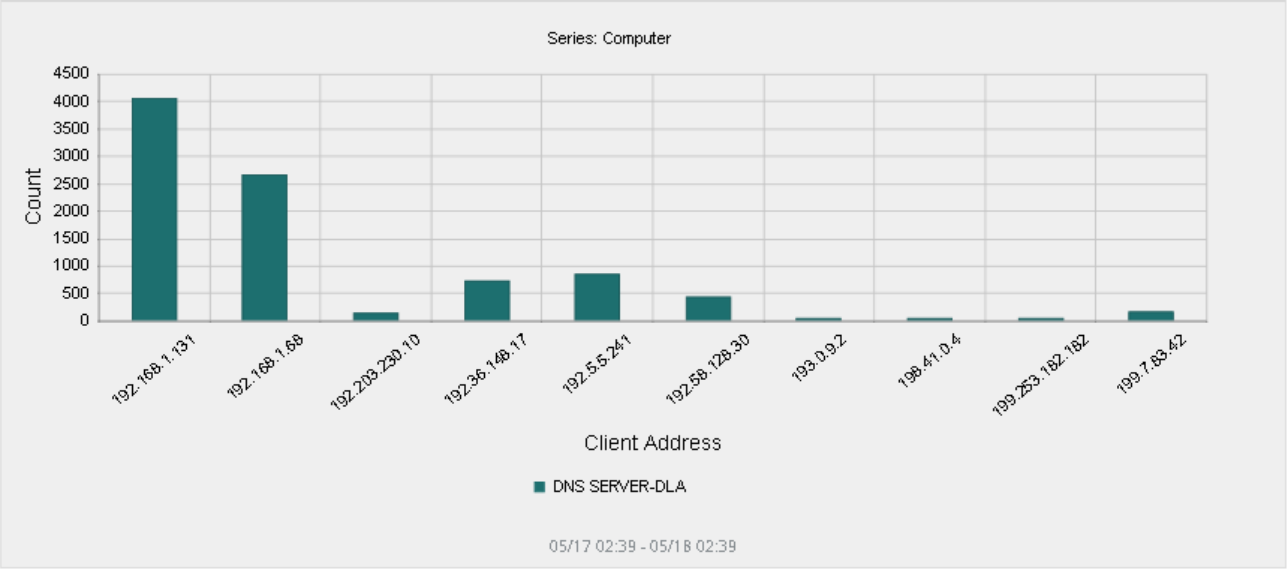

Figure 84

- **Microsoft DNS-Record type pattern in last 12 hrs**

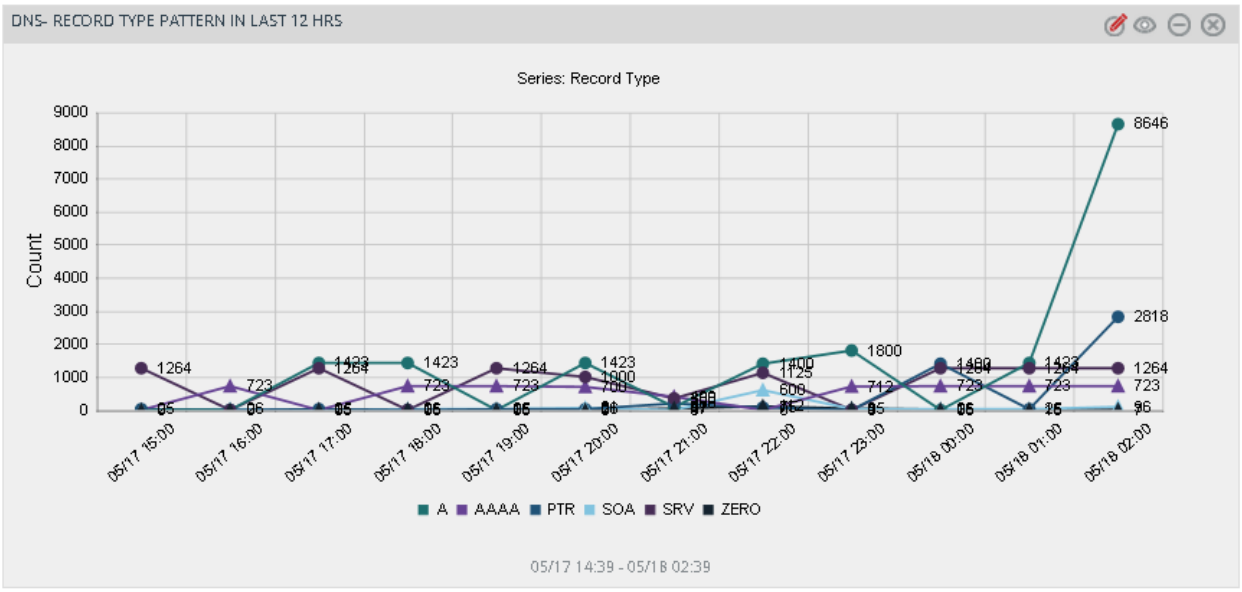

Figure 85

- **Microsoft DNS-Top queried domains in last 12 hrs**

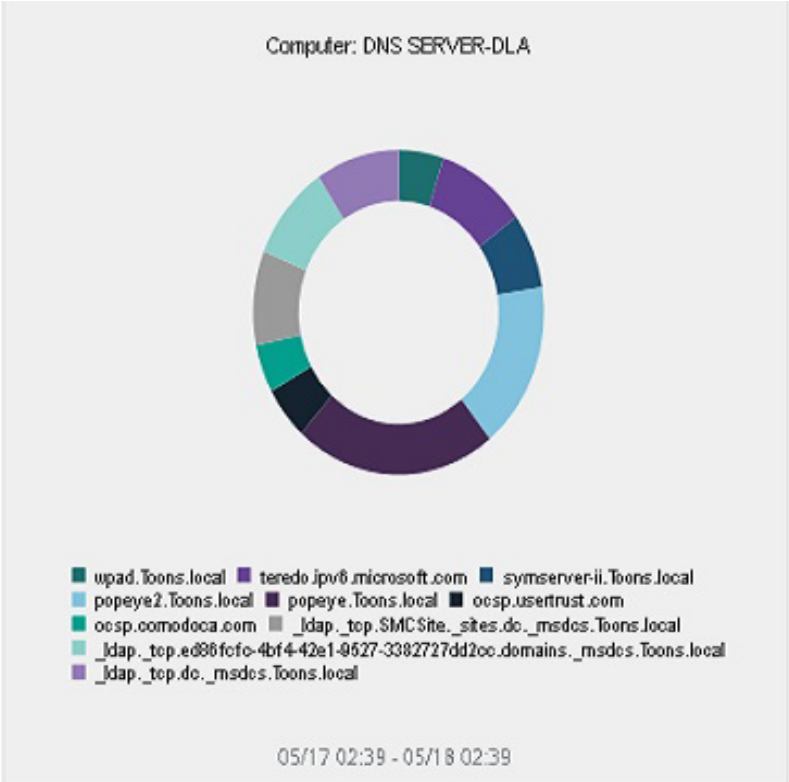

Figure 86

- **Microsoft DNS-Top querying clients in last 12 hrs**

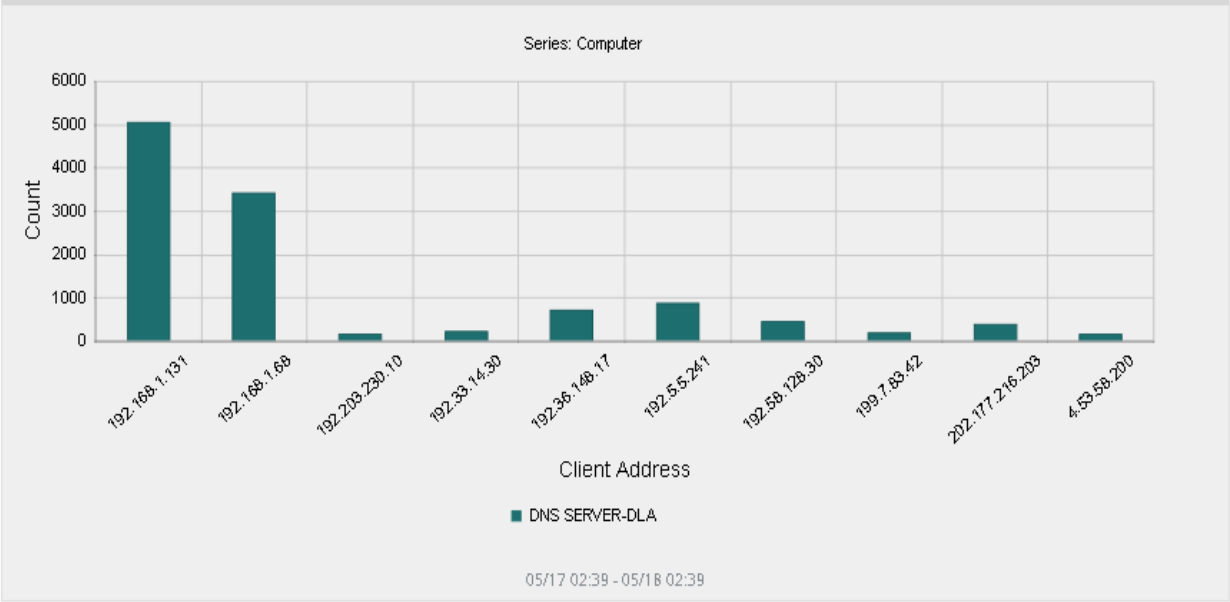

Figure 87

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

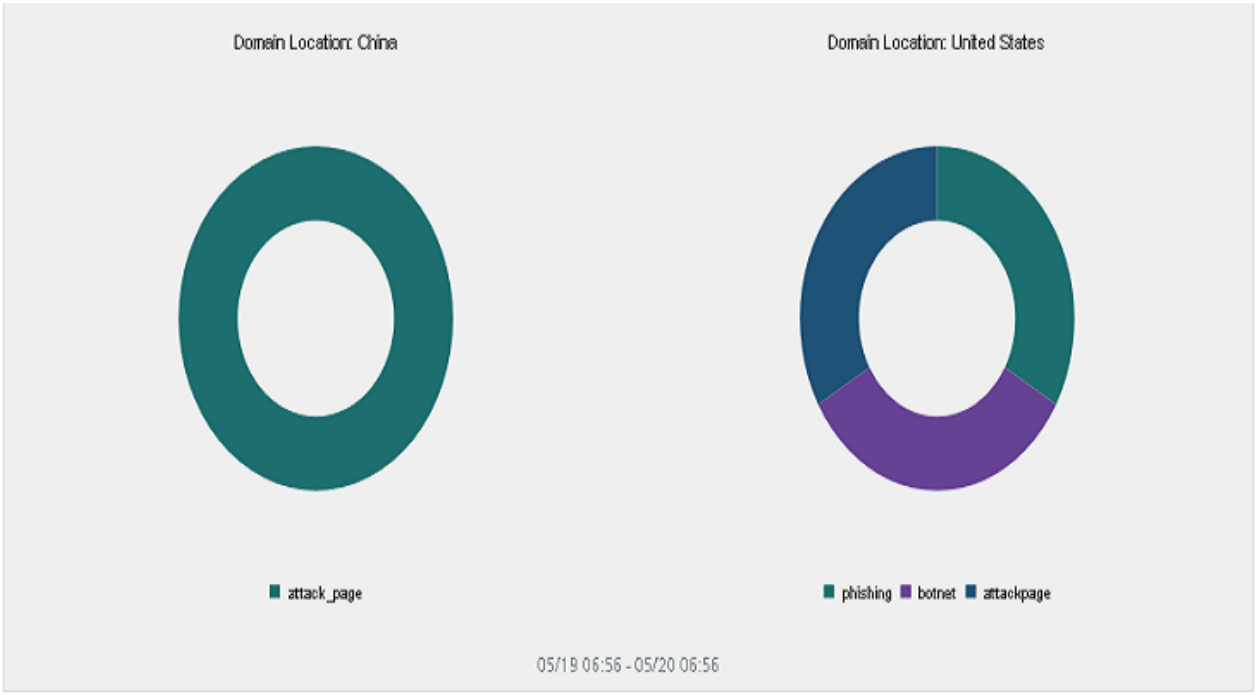

Figure 88

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

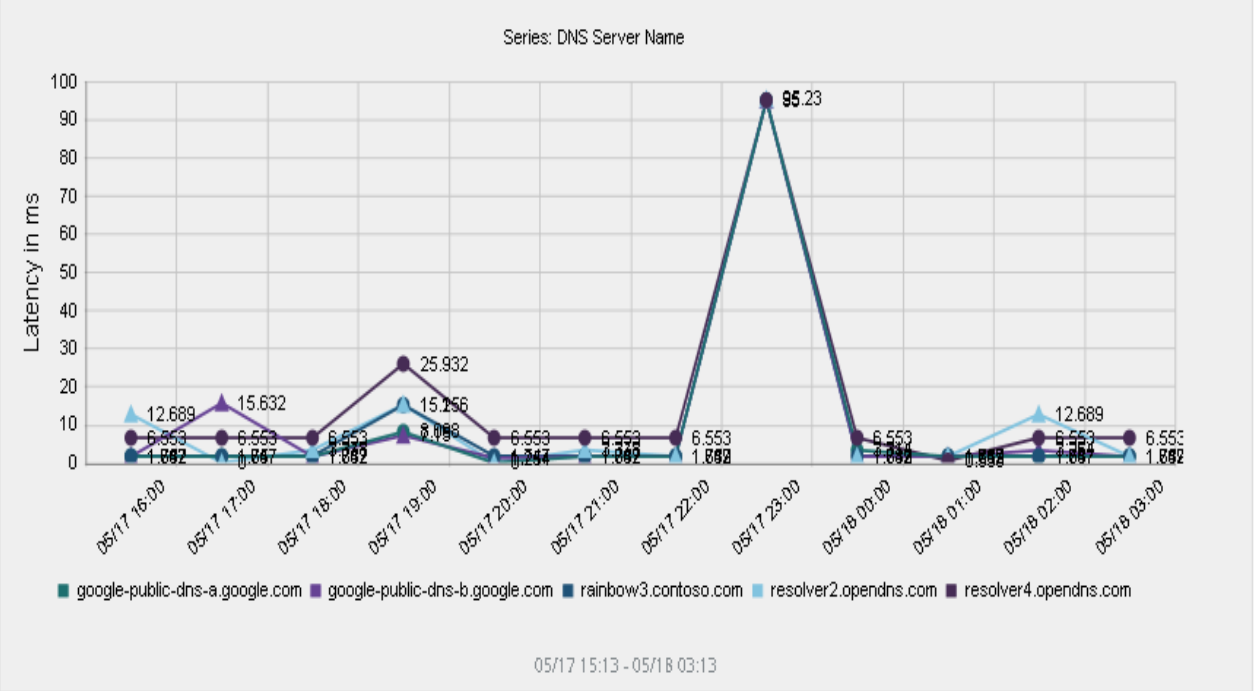

Figure 89

- **Microsoft DNS-DGA domains detected in last 12 hrs**

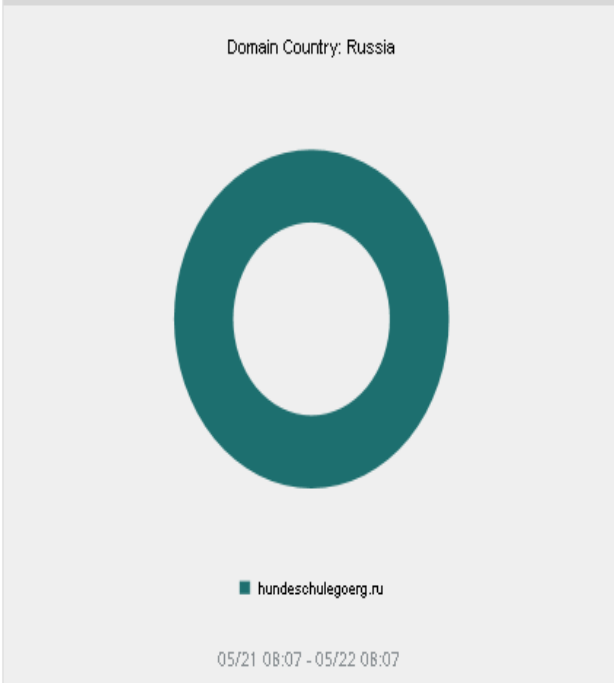

Figure 90

- **Microsoft DNS-Suspicious DNS settings detected in last 12 hrs**

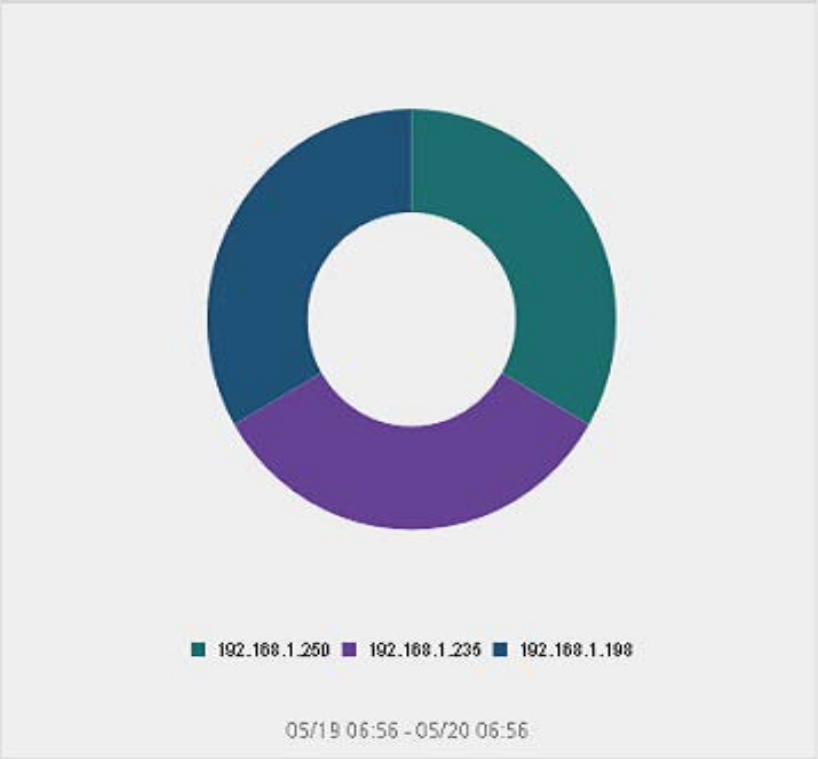

Figure 91

<-X->