Netsurion | EventTracker®

Integrate Microsoft DNS Server

EventTracker v9.2 and later

Publication Date: February 24, 2021

Abstract

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

Scope

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

Audience

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

Table of Contents

1. Overview

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

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

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

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

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

2. Prerequisites

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

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

3. Enabling Microsoft DNS Server Analytical logging

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

3.1 Install DNS diagnostic logging

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

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

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

3.2 Enable DNS diagnostic and analytical logging.

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

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

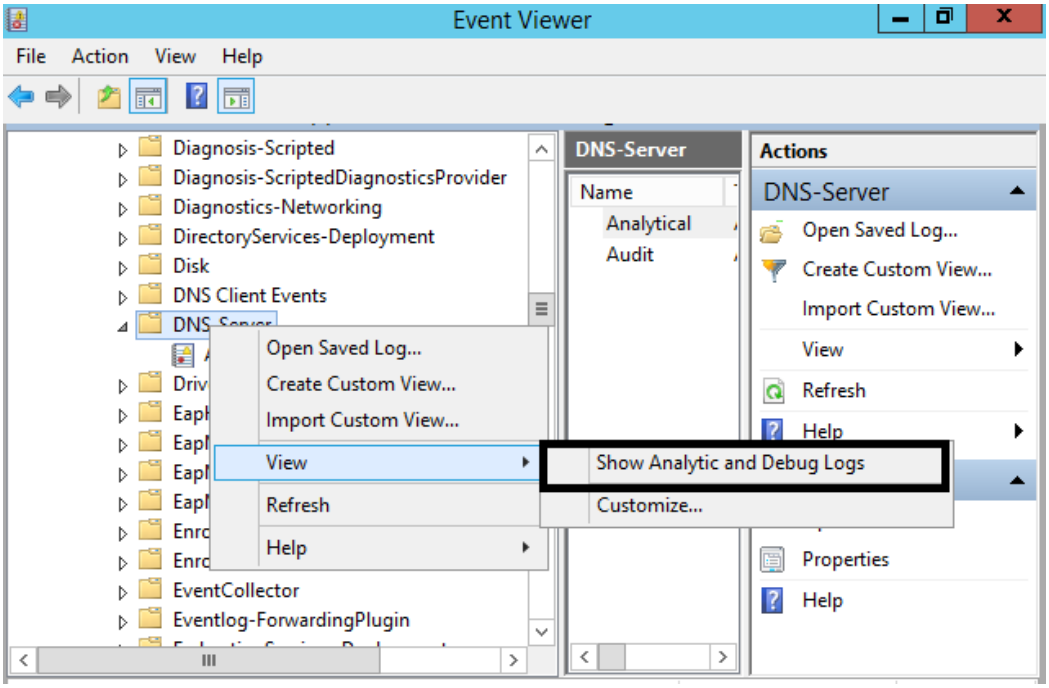

Figure 1

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

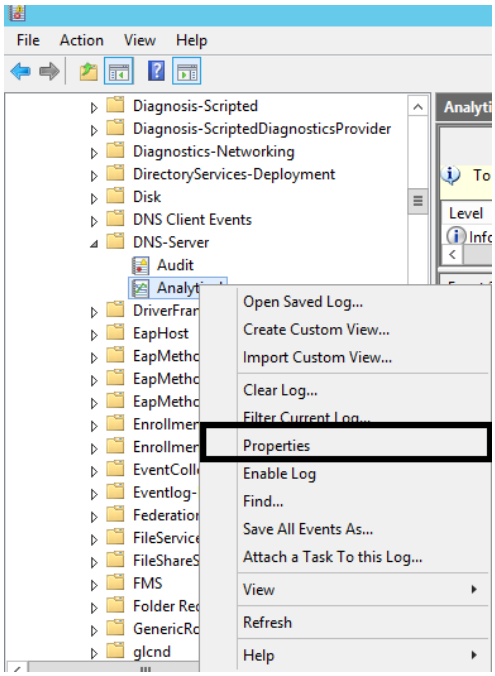

Figure 2

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

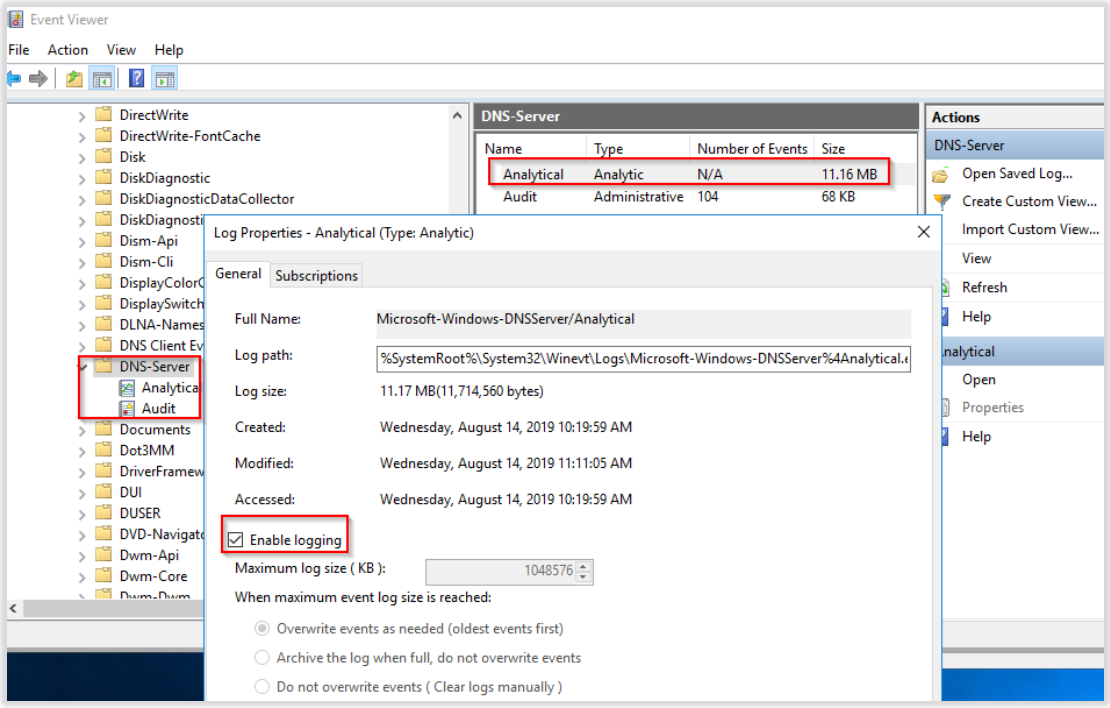

Figure 3

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

By default, analytic logs are written to the file:

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

4. Configuration for sending logs to EventTracker

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

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

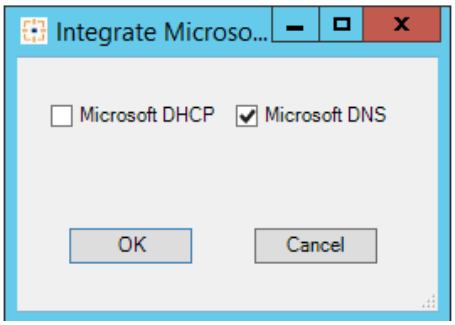

Figure 4

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

5. 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 to support Microsoft DNS Server.

5.1 Reports

- **Microsoft DNS-Zone creation, deletion and updating:** This report provides information related to zone creation, deletion, and updates in scope and by whom it was made.

- **Microsoft DNS-Resource record creation and deletion:** This report provides information related to resource record creation and deletion in zone and by whom it was made.

- **Microsoft DNS-Configuration changes:** This report provides information related to configuration name changes 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), query status, when query successfully resolve from DNS Server.

- **Microsoft DNS-Query resolution failed:** This report provides information related to FQDN or IP address, query type (forward lookup or reverse), query status, 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 and details of error type.

- **DNS- Error client count details:** This report provides information about error queries count for a client. and details of client IP address.

- **DNS- Summary client count details:** This report provides information about successful query count for a client and details of client IP address.

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

- **DNS- Error query count details:** This report provides information about error query for a FQDN resolution request and details of 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 is 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 about suspicious client DNS setting.

- **DNS-DGA domain detection details:** This report provides information on DGA domains detection details (FQDN and its IP) and client details from DNS logs.

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

- **DNS-Server latency details:** This report provides information about the provided DNS server (private and public DNS) and its latency.

5.2 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 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 detect 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 differs from the 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 domain threshold.
- **DNS: High error query count detected for type -** This alert is generated when error query count is greater than record type threshold.
- **DNS: High error query count detected from client -** This alert is generated when error query count is greater than client threshold.
- **DNS: High query count detected for record type -** This alert is generated when successful query count is greater than record type threshold.
- **DNS: High query count detected from client -** This alert is generated when successful query count is greater than client threshold.
- **DNS: High query count detected from domain -** This alert is generated when successful query count is greater than domain threshold.

5.3 Dashboards

- **Microsoft DNS: Top URL usage –** This dashboard gives information about usage of URL in the network.
- **Microsoft DNS: Resource record operations –** This dashboard gives information about the created and deleted resource record in a DNS zone.
- **Microsoft DNS: Zone operations –** This dashboard gives information about the creation, deletion, and the updates of DNS zone.

- **DNS: Error pattern –** This dashboard gives information about query count for an error type.
- **DNS: Top queried domains –** This dashboard gives information about query count for a domain.
- **DNS: Top queried domains with errors –** This dashboard gives information about error query count for a domain.
- **DNS: Top querying clients -** This dashboard gives information about query count for a client.
- **DNS: Top querying clients with errors –** This dashboard gives information about error query count for a client.
- **DNS: Record type pattern –** This dashboard gives information about the query count for a record type.
- **DNS: Suspicious domains detected -** This dashboard gives information on malware domain access from a client.
- **DNS: Received traffic –** This dashboard gives information on received traffic in DNS server.
- **DNS: Send traffic –** This dashboard gives information on send traffic from DNS server.
- **DNS: Malformed domains detected –** This dashboard gives information on typo-squatted domains access from a client.
- **DNS: Server latency –** This dashboard gives information about latency of a public and internal DNS server.
- **DNS: DGA domain detected –** This dashboard gives information on DGA domains access by a client.
- **DNS: Suspicious DNS settings detected –** This dashboard gives information about the client having suspicious DNS settings.
- **DNS: Least resolved domains –** This dashboard gives information about the least resolved domains over the network.

6. Importing 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**.

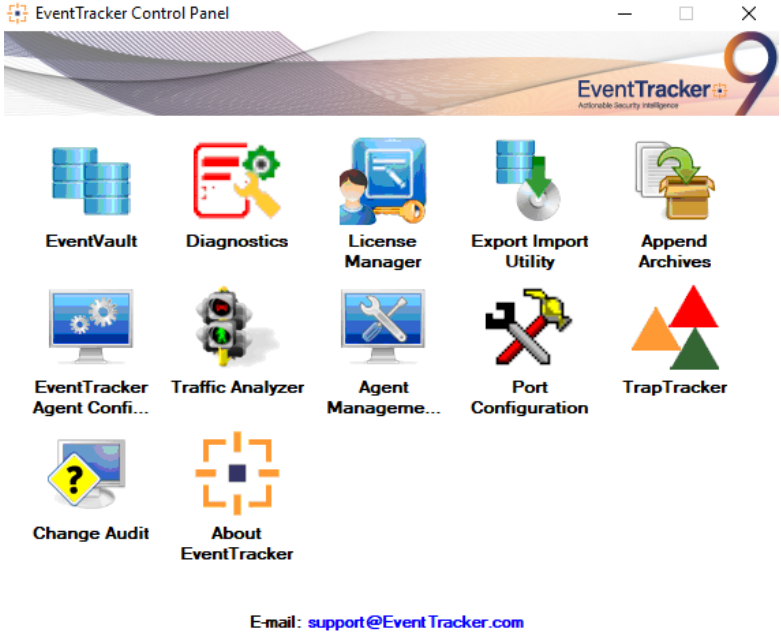

Figure 5

3. Click the **Import** tab.

6.1 Alerts

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

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

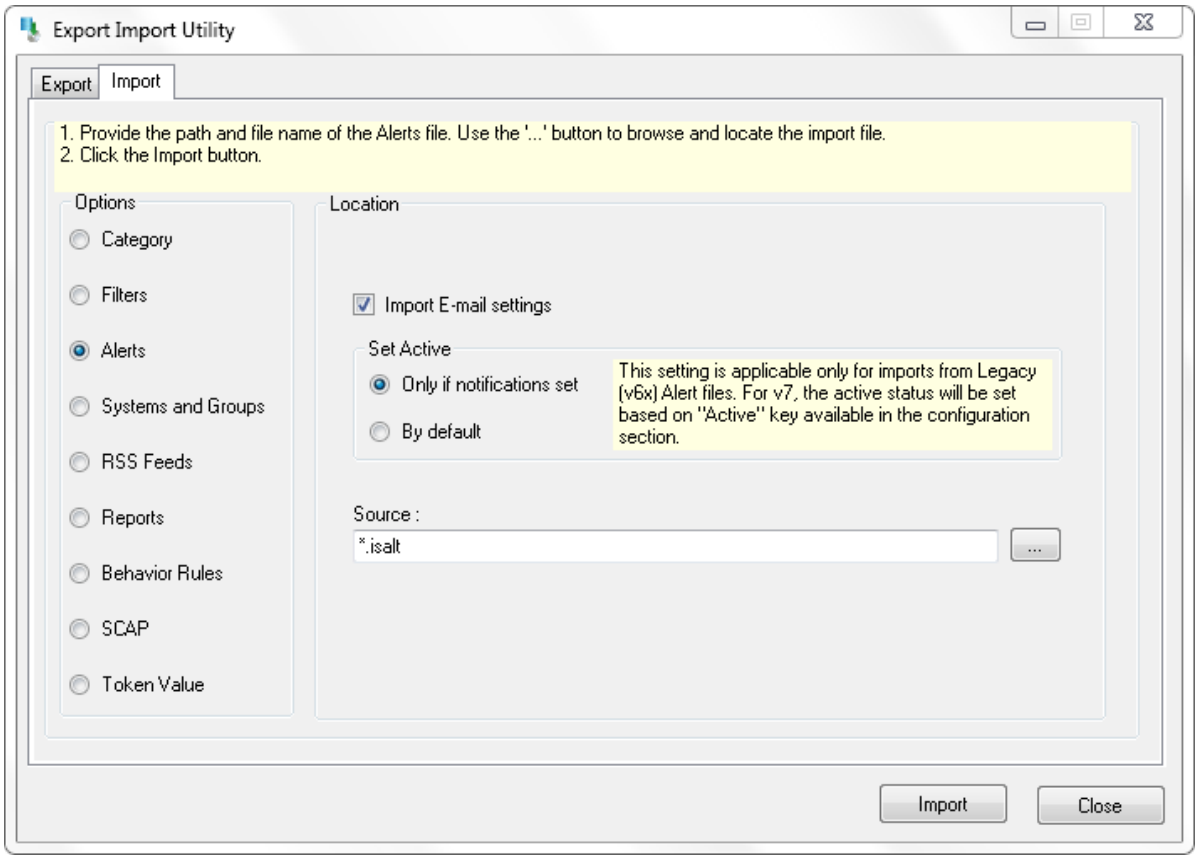

Figure 6

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

   EventTracker displays success message.

Figure 7

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

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

6. Logon to **EventTracker**.

7. Click **Admin** dropdown, and then click **Alerts.**

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

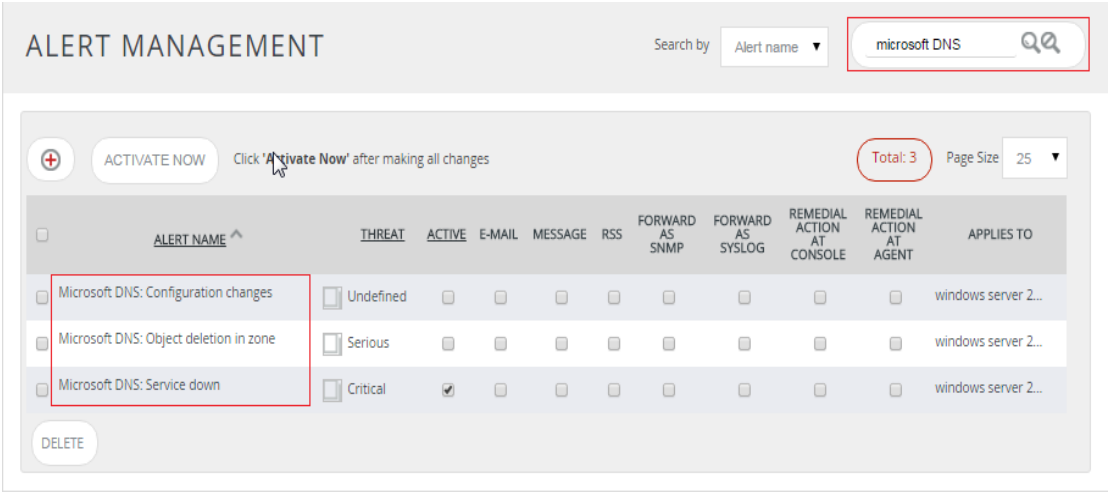

Figure 8

9. Click any **Microsoft DNS alert** and click **Systems** tab and then select the Window DNS server machine.

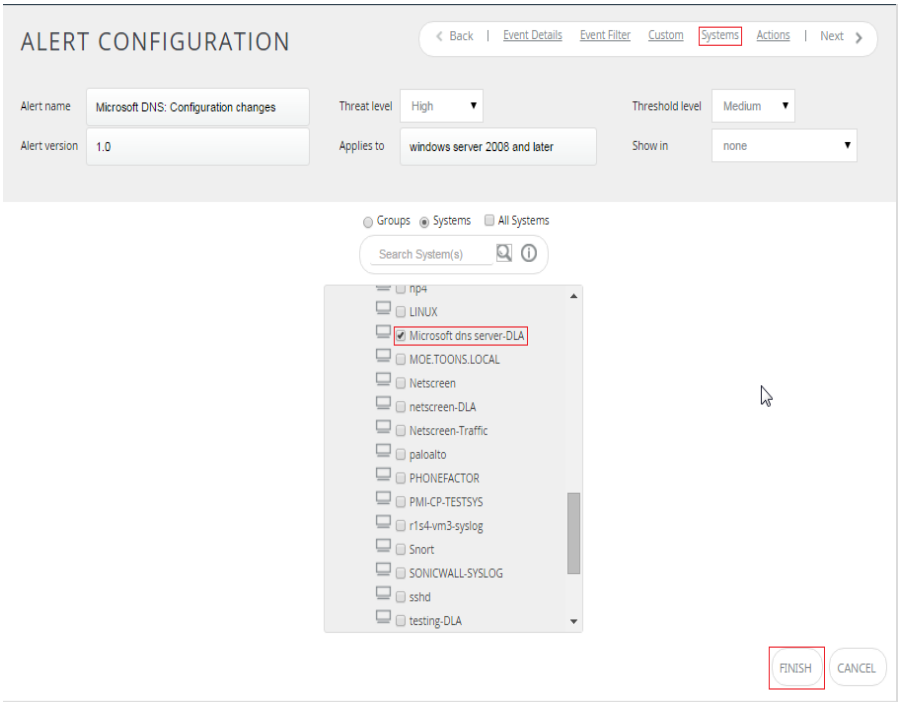

Figure 9

10. Click **FINISH** button to save the configuration.

6.2 Category

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

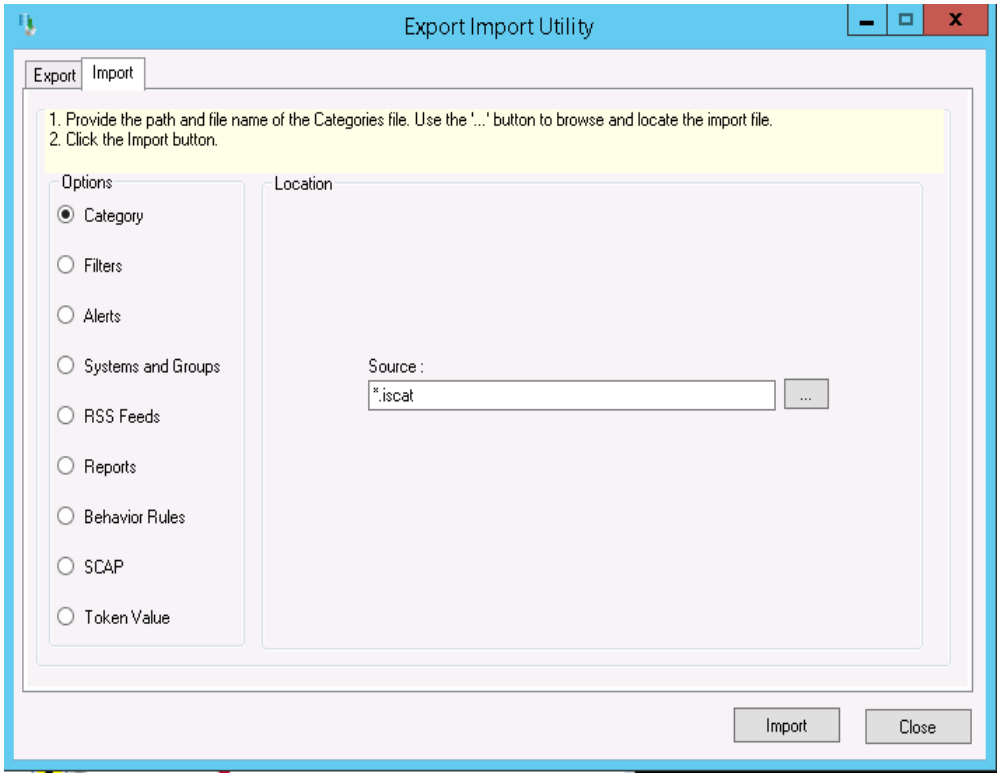

Figure 10

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

EventTracker displays success message.

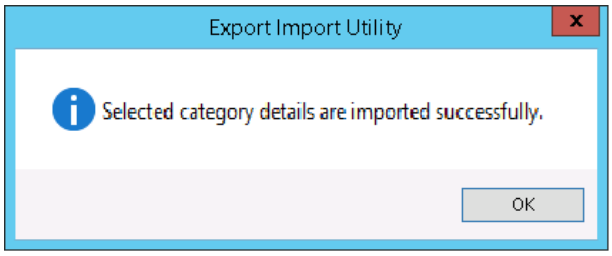

Figure 11

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

6.3 Tokens

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

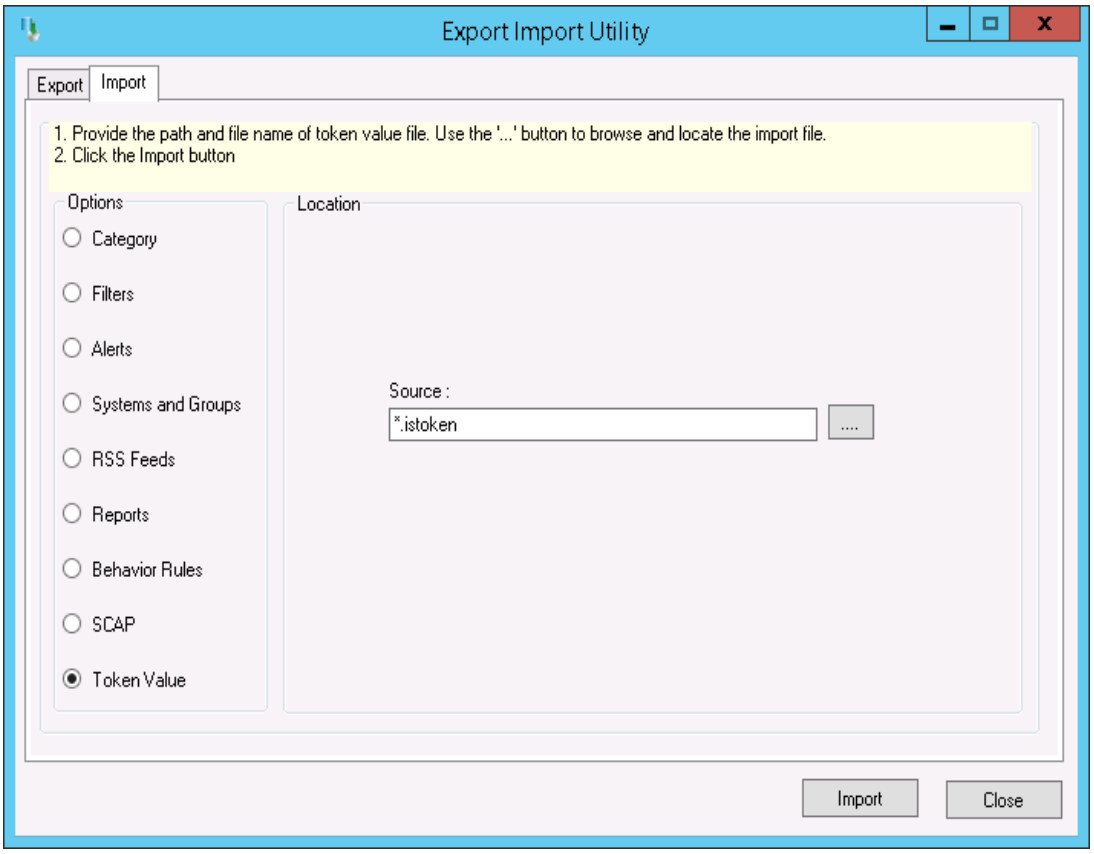

Figure 12

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

EventTracker displays success message.

Figure 13

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

6.4 Templates

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

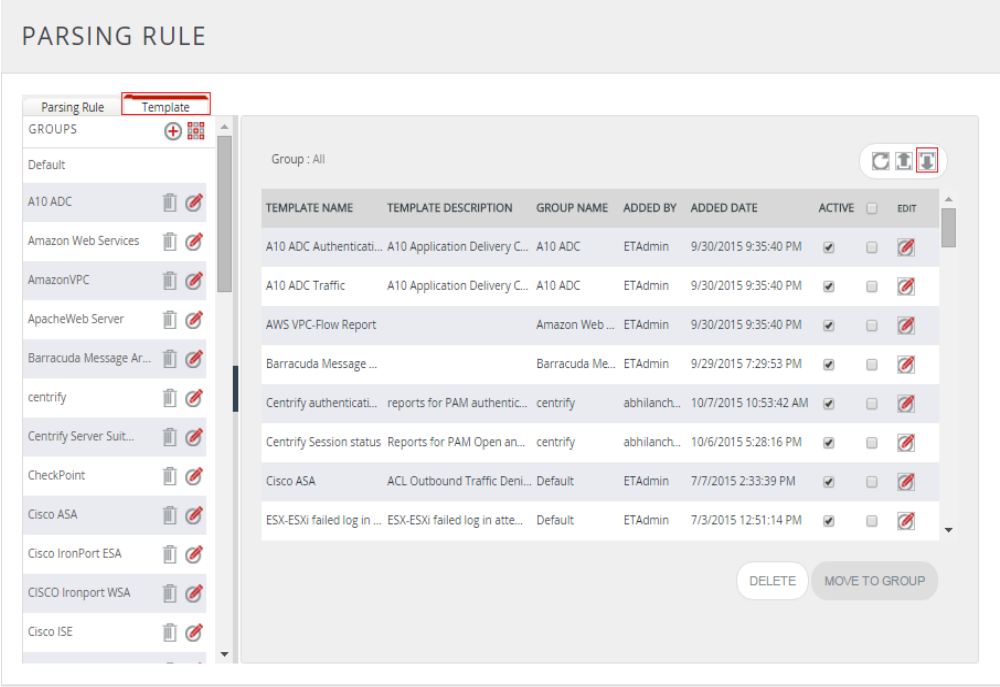

Figure 14

7. Locate and choose .ETTD file and then click the **Open** button.

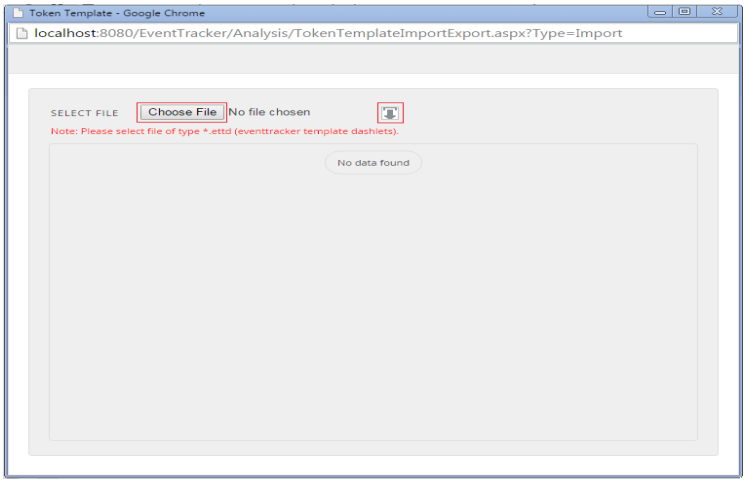

Figure 15

8. Select the template you want to upload.
9. Click **Import configuration** button.

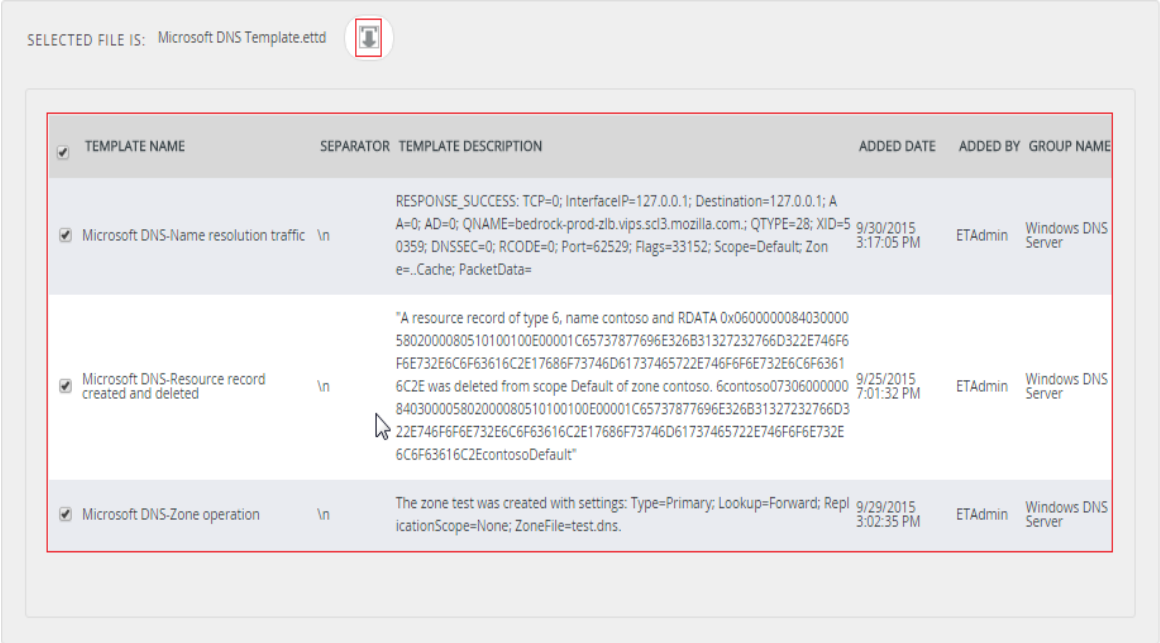

Figure 16

EventTracker displays success message.

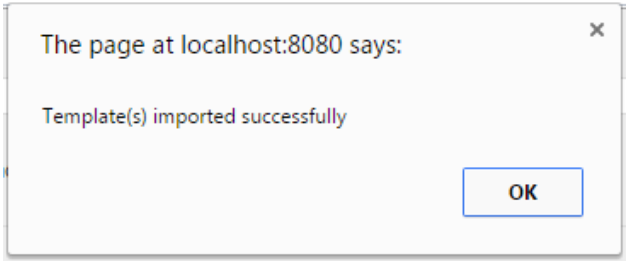

Figure 17

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

7. Verifying knowledge pack in EventTracker

7.1 Alerts

1. Logon to **EventTracker**.
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.

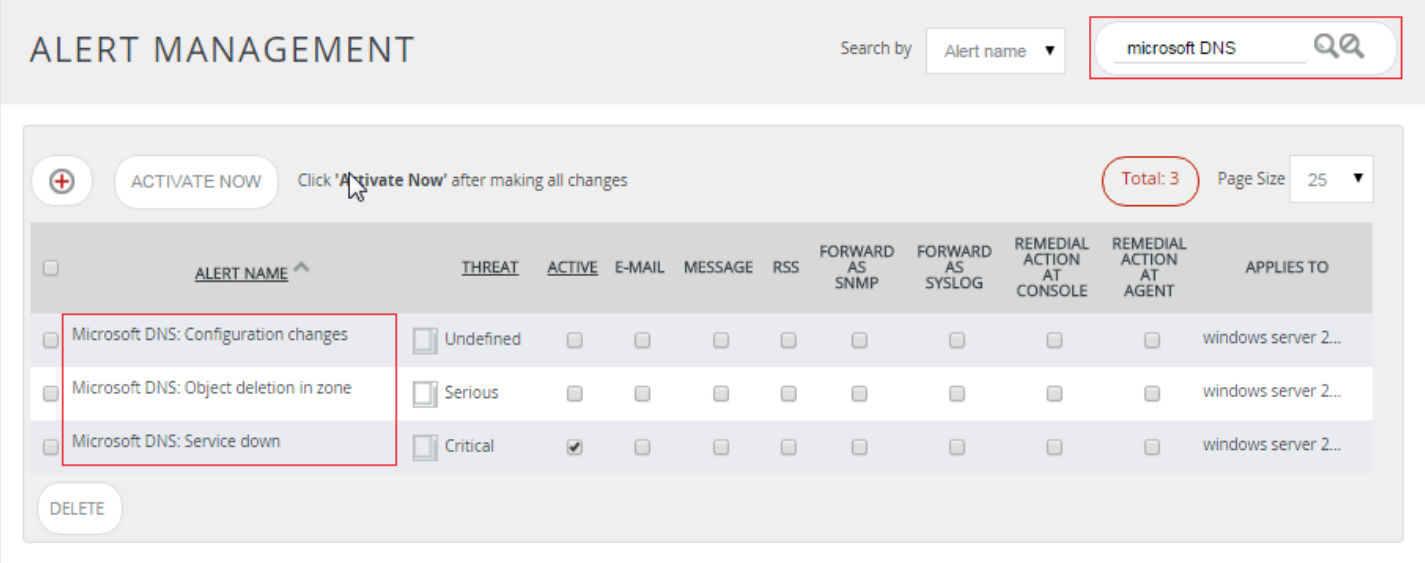

Figure 18

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

   EventTracker displays message box.

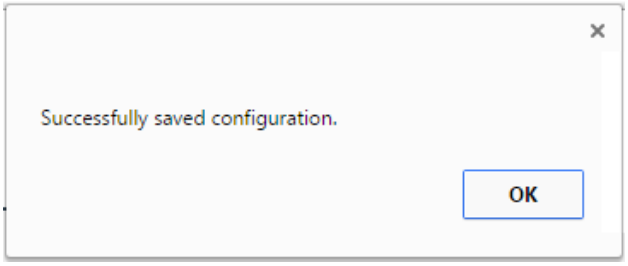

Figure 19

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.

7.2 Categories

1. Logon to **EventTracker**.
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.

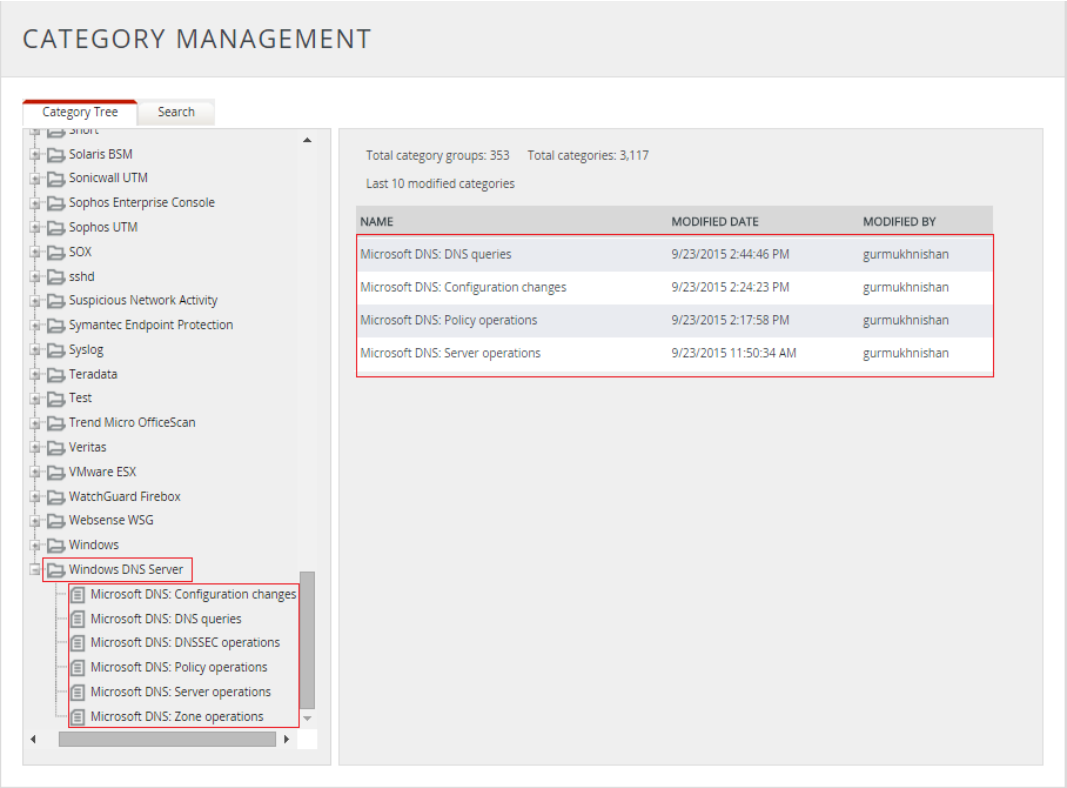

Figure 20

7.3 Tokens

1. Logon to **EventTracker**.
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 (as shown in below figure).

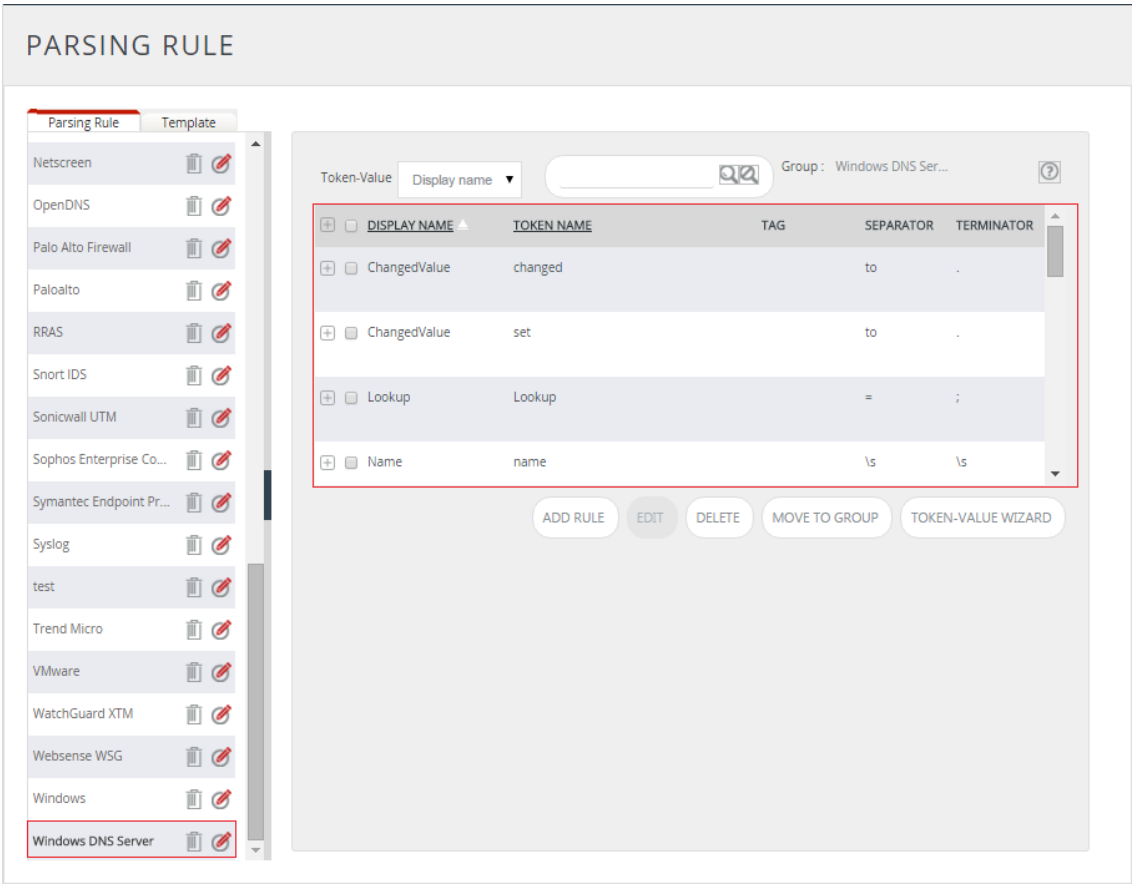

Figure 21

7.4 Templates

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

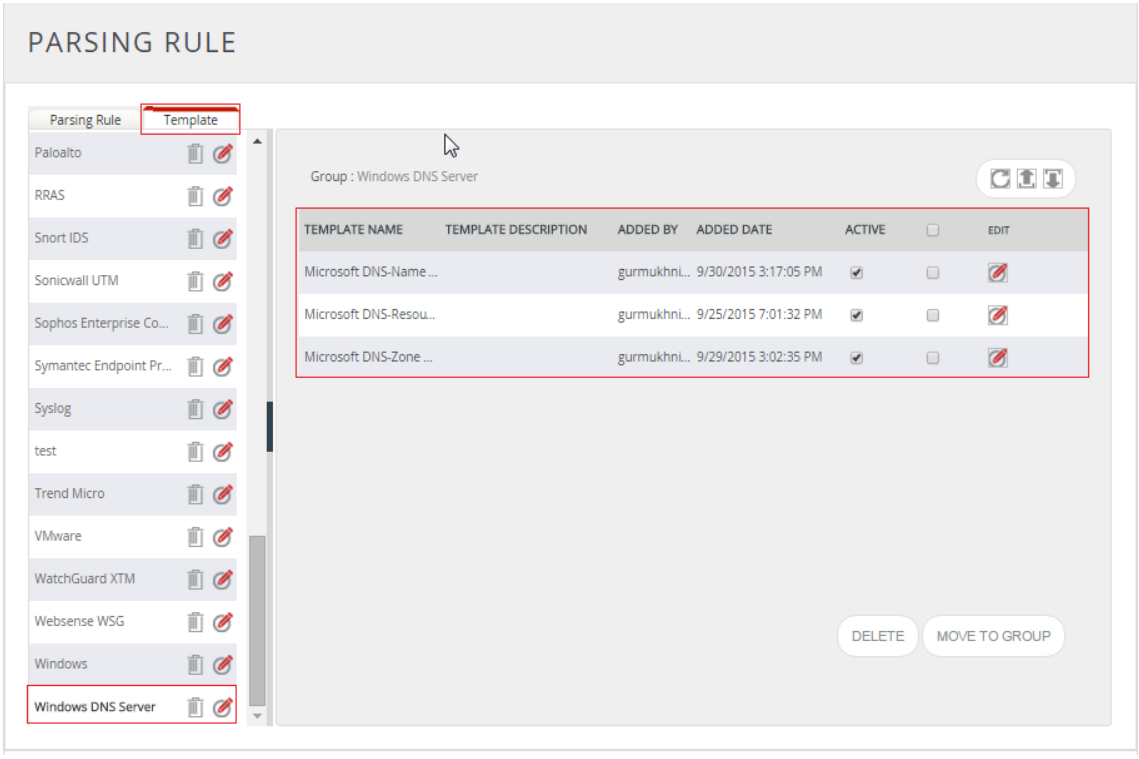

Figure 22

7.5 Flex Reports

1. Logon to **EventTracker**.
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.

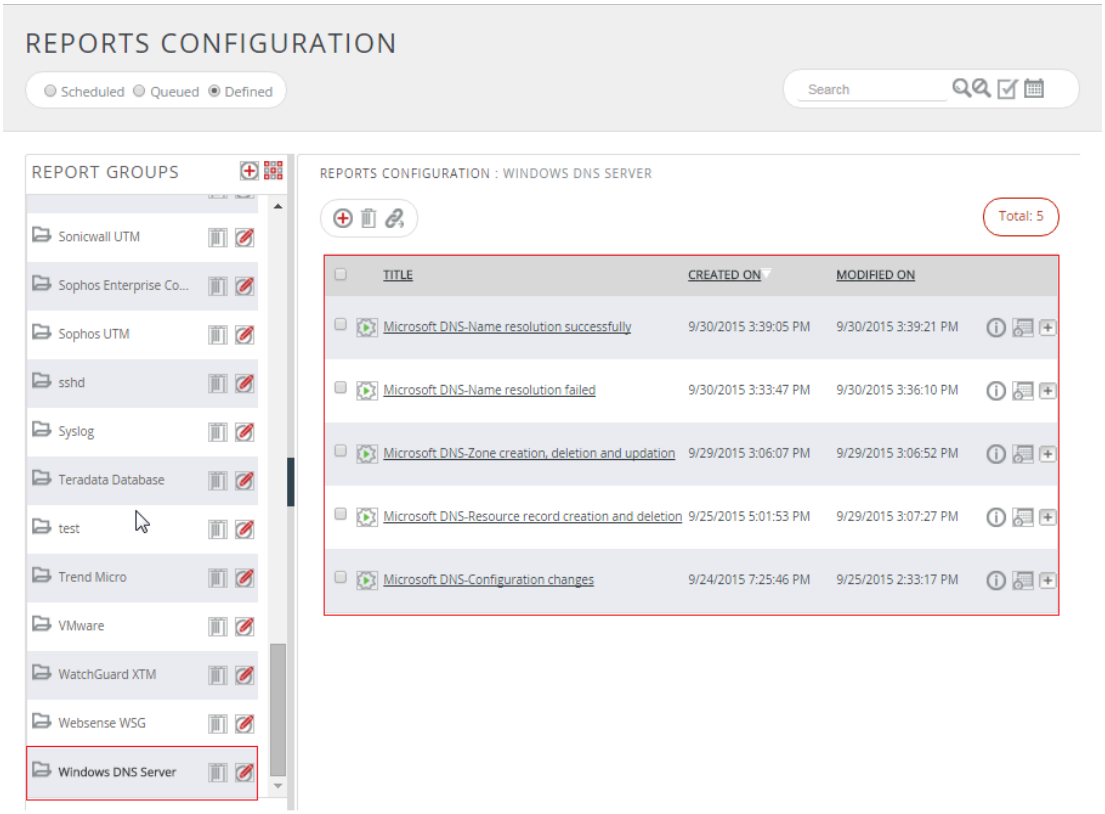

Figure 23

Here you can find imported defined reports such as Microsoft DNS-Name resolution successfully.

- **Microsoft DNS-Resource record creation and deletion**

Microsoft DNS-Resource record creation and deletion

LogTime	EventUser	Computer	Name	Action	Zone	Scope	Type	TTL
09/25/2015 04:06:06 PM	John	ESXWIN2K12R2VM2	www.contoso	deleted	contoso	Default	1	
09/25/2015 04:06:06 PM	Sam	ESXWIN2K12R2VM2	www.contoso	created	contoso	Default	1	3600

Figure 24

- **Microsoft DNS-Name resolution successfully.**

Microsoft DNS-Name resolution successfully

Date Time	Source Addre	Source Port	Interface IP	Query Name	Query Type	Status
2015-09-25T09:55:37.536813000Z	0	0	0.0.0.0	google.com.Toons.local.	RECURSE_QUERY	RECURSE_QUERY_OUT
2015-09-25T09:55:32.340676200Z	127.0.0.1	56723	127.0.0.1	1.0.0.127.in-addr.arpa.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:37.536813000Z	192.5.5.241	0	0.0.0.0	0	RECURSE_QUERY	RECURSE_QUERY_OUT
2015-09-25T09:55:37.536813000Z	192.5.5.241	0	0	google.com.Toons.local.	RECURSE_QUERY	RECURSE_QUERY_OUT
2015-09-25T09:55:37.536813000Z	192.5.5.241	0	0.0.0.0	google.com.Toons.local.	RECURSE_QUERY	RECURSE_QUERY_OUT
2015-09-25T09:55:32.340676200Z	127.0.0.1	56723	127.0.0.1	1.0.0.127.in-addr.arpa.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:32.340676200Z	127.0.0.1	56723	127.0.0.1	1.0.0.127.in-addr.arpa.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:32.340676200Z	127.0.0.1	56723	127.0.0.1	1.0.0.127.in-addr.arpa.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:32.340676200Z	127.0.0.1	56723	127.0.0.1	1.0.0.127.in-addr.arpa.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:32.340676200Z	127.0.0.1	56723	127.0.0.1	1.0.0.127.in-addr.arpa.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:32.340676200Z	127.0.0.1	56723	127.0.0.1	1.0.0.127.in-addr.arpa.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:37.536813000Z	192.5.5.241	0	0.0.0.0	google.com.Toons.local.	RECURSE_QUERY	RECURSE_QUERY_OUT
2015-09-25T09:55:32.340676200Z	127.0.0.1	0	127.0.0.1	1.0.0.127.in-addr.arpa.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:32.340676200Z	127.0.0.1	56723	0	1.0.0.127.in-addr.arpa.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:32.340676200Z	0	56723	127.0.0.1	1.0.0.127.in-addr.arpa.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:32.340676200Z	127.0.0.1	56723	127.0.0.1	1.0.0.127.in-addr.arpa.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:32.340676200Z	127.0.0.1	56723	127.0.0.1	0	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:32.340676200Z	127.0.0.1	56723	127.0.0.1	1.0.0.127.in-addr.arpa.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:32.340676200Z	127.0.0.1	56723	127.0.0.1	1.0.0.127.in-addr.arpa.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:32.340676200Z	127.0.0.1	56723	127.0.0.1	1.0.0.127.in-addr.arpa.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:32.340676200Z	127.0.0.1	56723	127.0.0.1	1.0.0.127.in-addr.arpa.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:37.608521200Z	192.5.5.241	0	0.0.0.0	google.com.Toons.local.	RECURSE_QUERY	RECURSE_RESPONSE_IN
2015-09-25T09:55:37.608768000Z	127.0.0.1	56727	127.0.0.1	google.com.Toons.local.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:37.608768000Z	127.0.0.1	56727	127.0.0.1	google.com.Toons.local.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:37.608521200Z	192.5.5.241	0	0.0.0.0	google.com.Toons.local.	RECURSE_QUERY	RECURSE_RESPONSE_IN
2015-09-25T09:55:37.608521200Z	192.5.5.241	0	0.0.0.0	google.com.Toons.local.	RECURSE_QUERY	RECURSE_RESPONSE_IN

Figure 25

7.6 Sample Dashboard

- **Microsoft DNS: Top URL usage**

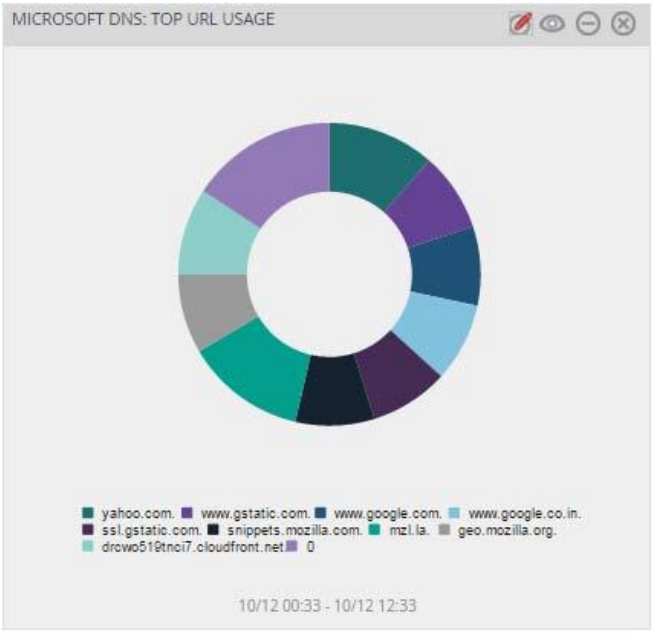

Figure 26

- **Microsoft DNS: Resource record and operations today**

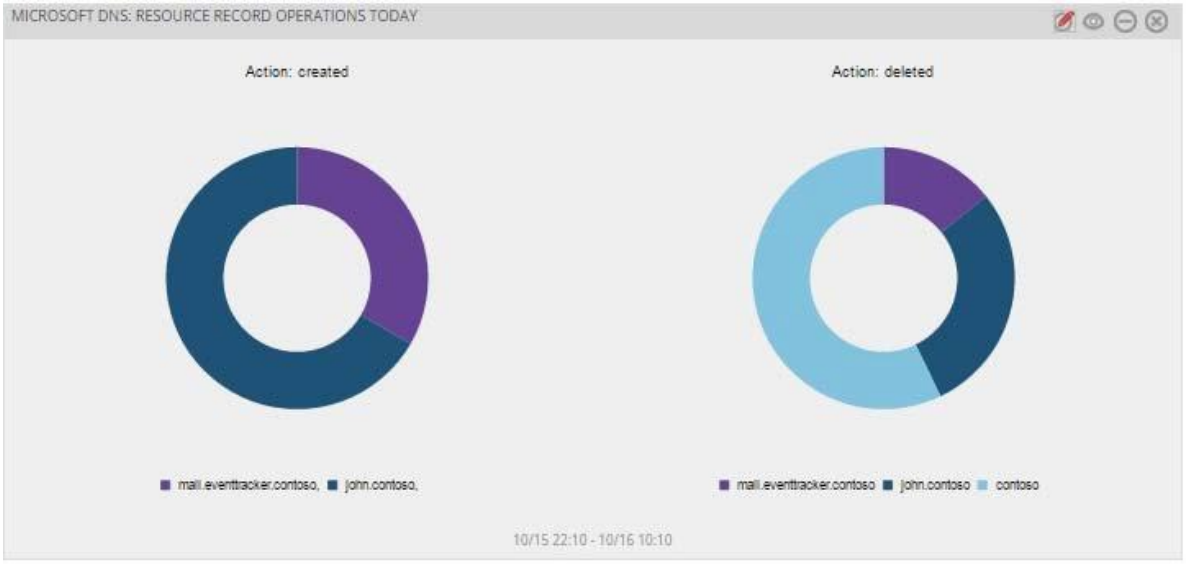

Figure 27

- **DNS-Error pattern**

Figure 28

- **DNS-Top queried domains**

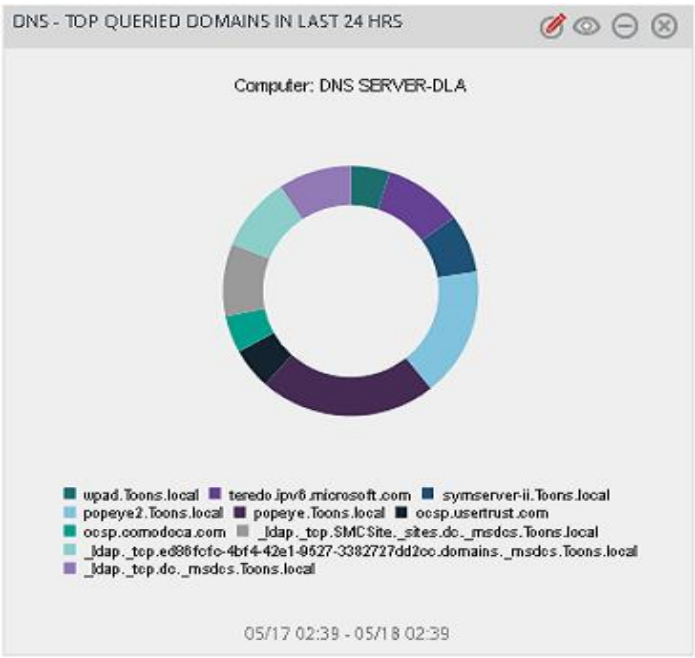

Figure 29

- **DNS-Top queried domains with errors**

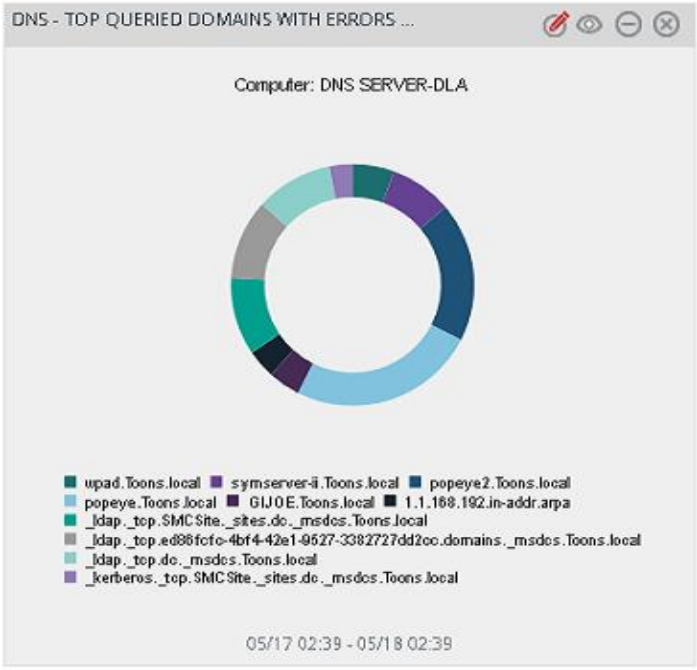

Figure 30

- **DNS-Top querying clients**

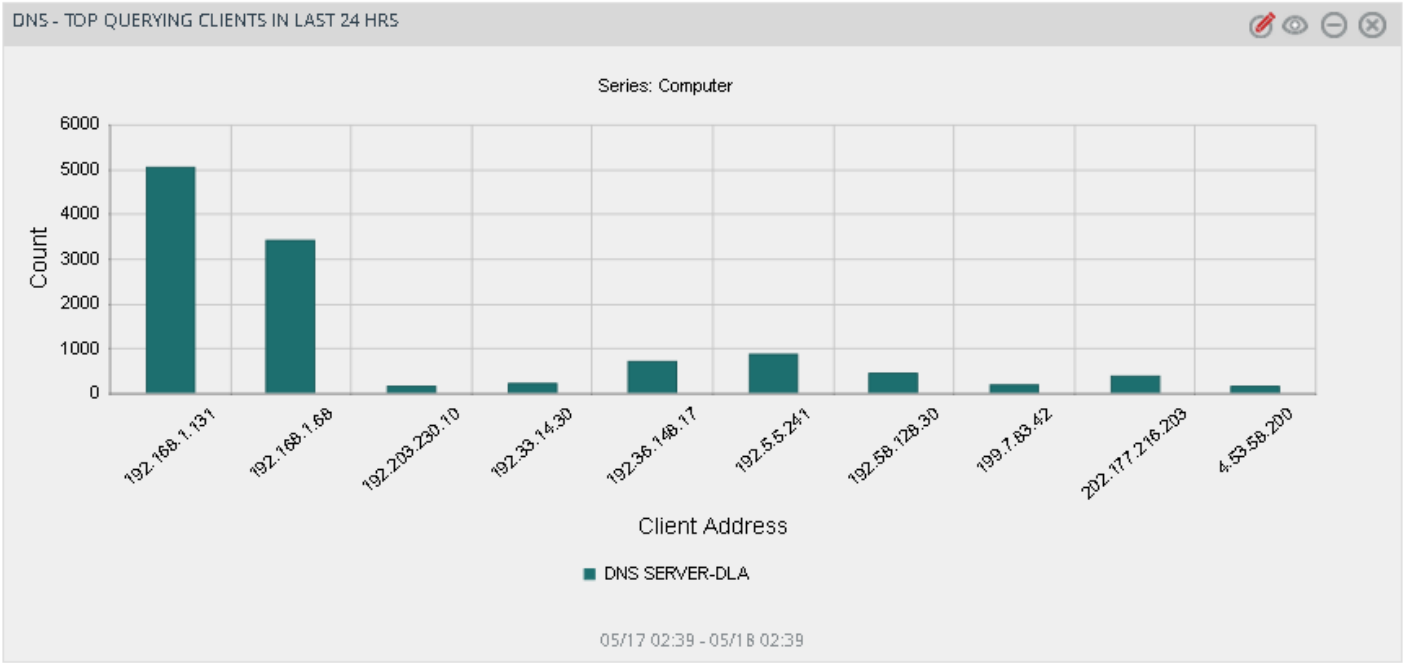

Figure 31

- **DNS-Top querying clients with errors**

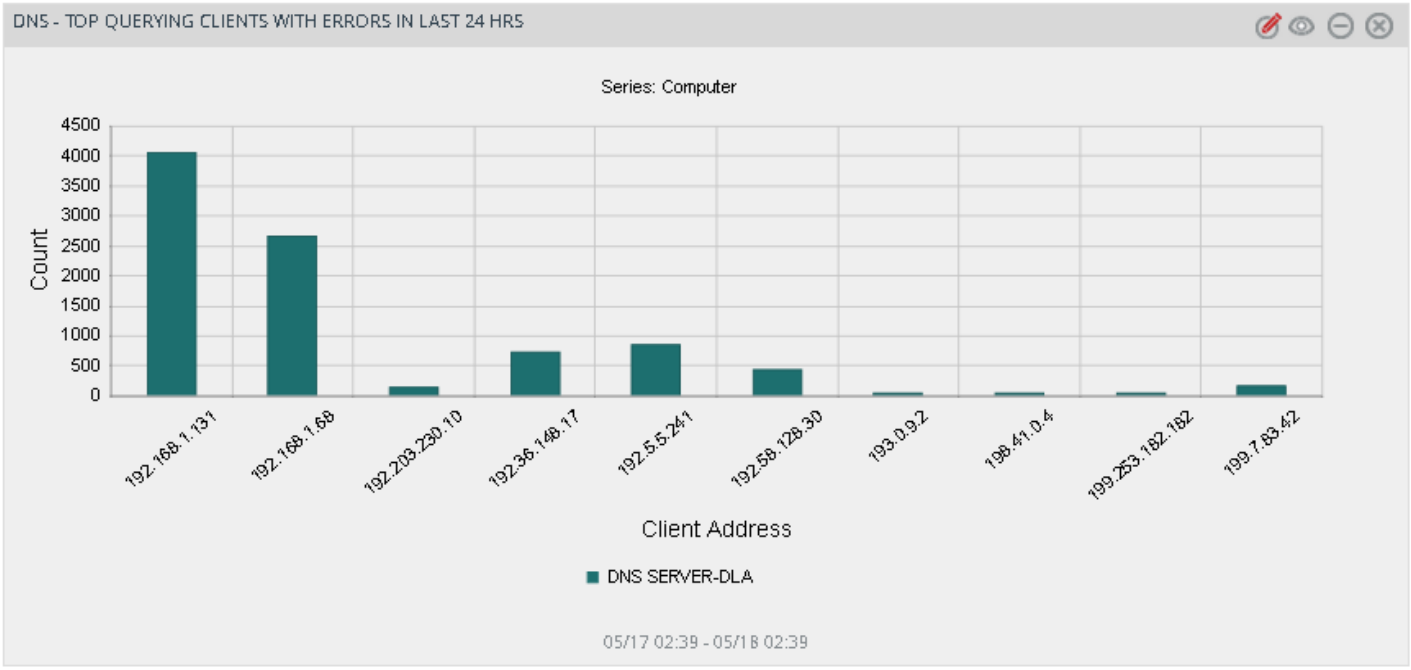

Figure 32

- **DNS-Record type pattern**

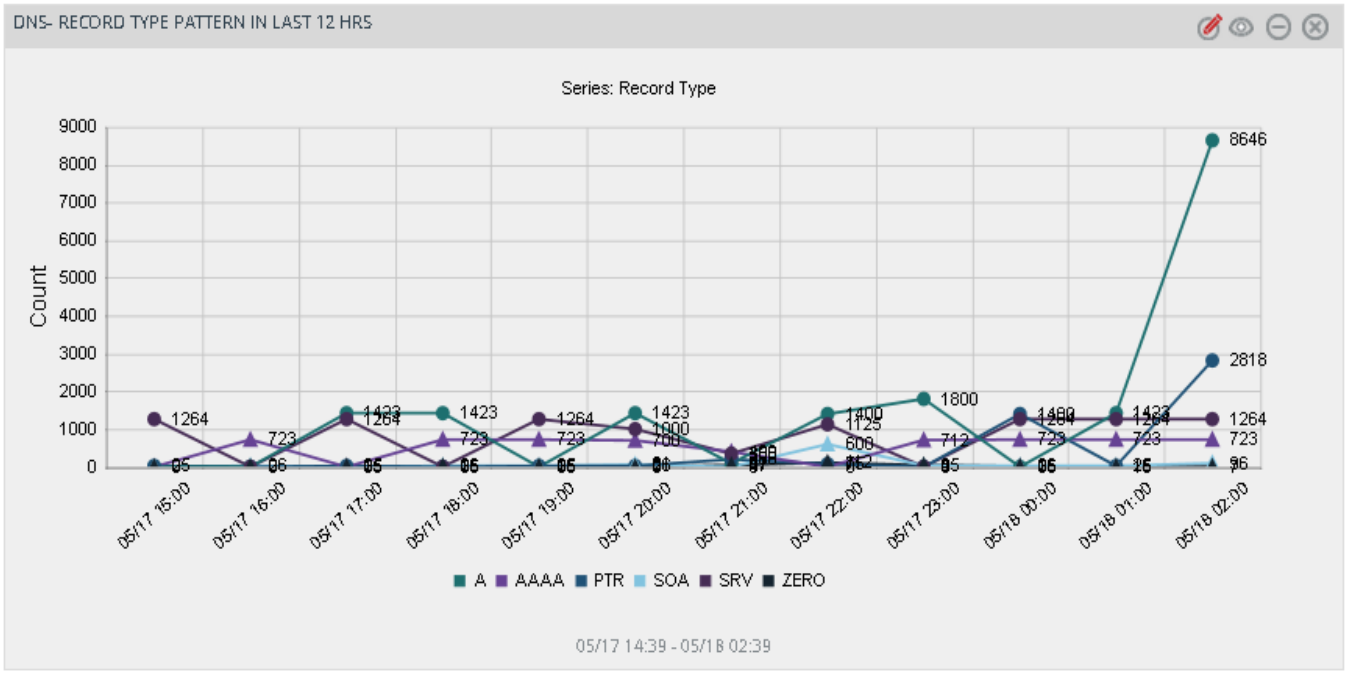

Figure 33