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.

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

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

Complying with all applicable copyright Zyxel firewall is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

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

© 2021 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

1.	Ove	erview	3
2.	Pre	requisites	3
3.	Ena 3.1	bling Microsoft DNS Server Analytical logging Install DNS diagnostic logging	3 4
	3.2	Enable DNS diagnostic and analytical logging.	4
4.	Cor	ifiguration for sending logs to EventTracker	6
5.	Eve 5.1	ntTracker Knowledge Pack Reports	6 6
	5.2	Alerts	8
	5.3	Dashboards	9
6.	Imp	porting knowledge pack into EventTracker	11
	6.1	Alerts	11
	6.2	Category	14
	6.3	Tokens	15
	6.4	Templates	16
7.	Ver	ifying knowledge pack in EventTracker	17
	7.1	Alerts	17
	7.2	Categories	18
	7.3	Tokens	19
	7.4	Templates	20
	7.5	Flex Reports	21
	7.6	Sample Dashboard	24

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.

8	Event	View	ver					
File Action View H	lelp							
🗢 🔿 🖄 📰 🛽			_					
 ▷ □ Diagno ▷ □ Diagno ▷ □ Diagno ▷ □ Discto ▷ □ Disk ▷ □ DNS C □ DNS C 	sis-Scripted sis-ScriptedDiagnosticsProvider stics-Networking ryServices-Deployment ient Events Open Saved Log	^ =	DNS-Server	Act DN ©	ions NS-Server ▲ Open Saved Log Create Custom View Import Custom View View ▶			
⊳ 🛄 Driv ⊳ 🚆 Eapl	Create Custom View Import Custom View			2	Refresh Help			
⊳ 📫 Eapl	View	•	Show Analytic and Debug Logs					
⊳ 🛄 Eapl	Refresh		Customize					
⊳ 🛄 Enro	Help	•			Properties			
▷ □ EventC	ollector og-ForwardingPlugin	~	<	?	Help			

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.

Event Viewer	
File Action View Help	
> DirectWrite DNS-Server	Actions
> DirectWrite-FontCache	DNS-Server
Disk Analytical Analytic N/A 1116 MR	 Open Saved Log
S DiskDiagnostic Data Collector Adult Administrative 104 68 KB	Crasta Curtam View
> DiskDianosti	Create Custom view
Dism-Api Log Properties - Analytical (Type: Analytic)	X Import Custom View
> Dism-Cli General Colocation	View
> DisplayColord Subscriptions	Refresh
DisplaySwitch Signal DisplaySwitch Microsoft-Windows-DNSServer/Analytical	2 Help
> DNS Client Ev	nalutical
DNS-Server Kog Path: %SystemRoot%System32\Winevt\Logs\Microsoft-Windows-DNSServer%4Analytical.	f norytical
Analytica Log size: 11.17 MB(11,714,560 bytes)	Open
	Properties
Documents Createa: Weanesday, August 14, 2019 10:19:39 AM	Help
> Doumin Modified: Wednesday, August 14, 2019 11:11:05 AM	
DUI Accessed: Wednesday, August 14, 2019 10:19:59 AM	
DUSER	
S DVD-Navigat Enable logging	
Maximum log size (KB): 1048576 ≑	
When maximum event log size is reached:	
Overwrite events as needed (oldest events first)	
Archive the log when full, do not overwrite events	
 Do not overwrite events (Clear logs manually) 	

Figure 3

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

By default, analytic logs are written to the file:

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

4. Configuration for sending logs to EventTracker

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

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

🕀 Integrate Microso 🗕 🗖 🗙
☐ Microsoft DHCP 🕑 Microsoft DNS
OK Cancel

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.

🗄 EventTracker Con	trol Panel			- 🗆	×
		Jan 1	EV	entTracker	9
	- ?		2		
EventVault	Diagnostics	License Manager	Export Import Utility	Append Archives	
00		X	*		
EventTracker Agent Confi	Traffic Analyzer	Agent Manageme	Port Configuration	TrapTracker	
?	13				
Change Audit	About EventTracker				
	E-mail: s	support@EventTra	cker.com		
		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.

 Options Category Filters Alerts Systems and Groups RSS Feeds Reports Behavior Rules 	Location Import E-mail settings Set Active Only if notifications set By default Source : *.isalt	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.
© SCAP		

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.

۹L	ERT MANAGEMEN		Search b	y Alert na	me 🔻	microsof					
ACTIVATE NOW Click 'A vivate Now' after making all changes Total: 3 Page Size 25											
	ALERT NAME	THREAT	<u>ACTIVE</u>	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
• '	licrosoft DNS: Configuration changes	Undefined									windows server 2
•	licrosoft DNS: Object deletion in zone	Serious									windows server 2
DEL	Vicrosoft DNS: Service down	Critical	۲								windows server 2

Figure 8

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

ALER	CONFIGURATION		K Back Event Detail	<u>s</u> <u>Event Filt</u>	<u>er Custom S</u> j	stems Actions Next >
Alert name Alert version	Microsoft DNS: Configuration changes	Threat level Applies to	High windows server 2008 and later		Threshold level Show in	Medium T
			Ps (Systems) All Systems rch System(s) Pq4 INUX MICS off dns server-DLA MOE TOONS LOCAL Netscreen netscreen-DLA Netscreen-Traffic paloalto PHONEFACTOR MILCP-TESTSYS 1154-Vm3-Systog Sonrt SONICWALL-SYSLOG shd testing-DLA	•		FINISH



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

6.2 Category

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

ц. Э	Export Import Utility	_ 🗆 X
Export Import		
1. Provide the path and file nam 2. Click the Import button.	e of the Categories file. Use the '' button to browse and locate the import file.	
Options	Location	
 Category 		
 Filters 		
 Alerts 		
 Systems and Groups 	Source :	
O RSS Feeds	*.iscat	
O Reports		
O Behavior Rules		
O SCAP		
O Token Value		
	Import	Close

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.

ц,	Export Import Utility	-		x
Export Import				
1. Provide the path and file na 2. Click the Import button	me of token value file. Use the '' button to browse and locate the import file.			
Options	Location			
Category				
⊖ Filters				
 Alerts 				
 Systems and Groups 	Source : *.istoken			
O RSS Feeds				
O Reports				
O Behavior Rules				
O SCAP				
Token Value				
	Import		Close	•

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.)

PARSING R	ULE										
Parsing Rule Tel GROUPS Default	mplate		Group : All						C	1 1	
A10 ADC	1		TEMPLATE NAME	TEMPLATE DESCRIPTION	GROUP NAME	ADDED BY	ADDED DATE	ACTIVE		EDIT	*
Amazon Web Services	1 🧭		A10 ADC Authenticati	A10 Application Delivery C	A10 ADC	ETAdmin	9/30/2015 9:35:40 PM	۲		0	
AmazonVPC	1 🧭		A10 ADC Traffic	A10 Application Delivery C	A10 ADC	ETAdmin	9/30/2015 9:35:40 PM			0	
ApacheWeb Server	1		AWS VPC-Flow Report		Amazon Web	ETAdmin	9/30/2015 9:35:40 PM			0	
Barracuda Message Ar	1 🧭	ł.	Barracuda Message		Barracuda Me	ETAdmin	9/29/2015 7:29:53 PM			0	
centrify	Ū 🧭	L.	Centrify authenticati	reports for PAM authentic	centrify	abhilanch	10/7/2015 10:53:42 AM			0	
Centrify Server Suit	1		Centrify Session status	Reports for PAM Open an	centrify	abhilanch	10/6/2015 5:28:16 PM			Ø	
CheckPoint	1		Cisco ASA	ACL Outbound Traffic Deni	. Default	ETAdmin	7/7/2015 2:33:39 PM			0	
Cisco ASA	1		ESX-ESXi failed log in	ESX-ESXi failed log in atte	Default	ETAdmin	7/3/2015 12:51:14 PM			0	-
Cisco IronPort ESA	1							MOVE	TOC	POUR	
CISCO Ironport WSA	1 🧭						DELETE	MOVE	TOG	ROUP	
Cisco ISE	100										

Figure 14

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

Token Template - Google Chrome							
localhost:8080/EventTracker/Analysis/TokenTemplateImportExport.aspx?Type=Import							
SELECT FUE Choose File No file chosen							
Note: Please select file of time & attd (eventtracker template dashlats)							
Hote, Heuse select me of type - setta (eventerbeker template dusmeta).							
No data found							
		_					

Figure 15



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

•	TEMPLATE NAME	SEPARATOR	TEMPLATE DESCRIPTION	ADDED DATE	ADDED BY	GROUP NAM
•	Microsoft DNS-Name resolution traffic	\n	RESPONSE_SUCCESS: TCP=0; InterfaceIP=127.0.0.1; Destination=127.0.0.1; A A=0; AD=0; QNAME=bedrock-prod-zlb.vips.scl3.mozilla.com.; QTVPE=28; XID=5 0359; DNSSEC=0; RCODE=0; Port=62529; Flags=33152; Scope=Default; Zon e=Cache; PacketData=	9/30/2015 3:17:05 PM	ETAdmin	Windows Dł Server
•	Microsoft DNS-Resource record created and deleted	\n \s	"A resource record of type 6, name contoso and RDATA 0x060000084030000 5802000080510100100E00001C65737877696E326831327232766D322E746F6 F6E732E6C6F63616C2E17686F73746D51737465722E746F6F6E732E6C6F6361 6C2E was deleted from scope Default of zone contoso. 6contoso07306000000 840300005802000080510100100E00001C65737877696E326B31327232766D3 22E746F6F6E732E6C6F63616C2E17686F73746D61737465722E746F6F6E732E 6C6F63616C2EcontosoDefault"	9/25/2015 7:01:32 PM	ETAdmin	Windows Dł Server
•	Microsoft DNS-Zone operation	\n	The zone test was created with settings: Type=Primary; Lookup=Forward; Repl icationScope=None; ZoneFile=test drs.	9/29/2015 3:02:35 PM	ETAdmin	Windows Di Server

Figure 16

EventTracker displays success message.

The page at localhost:8080 says:	3	ĸ
Template(s) imported successfully		
	ОК	
		_

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.

ALERT MANAGEMENT Search by Alert									me 🔻	microsof	
ACTIVATE NOW Click 'A givate Now' after making all changes Total: 3 Page Size 25											
o ,	ALERT NAME	THREAT	<u>ACTIVE</u>	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
Microsoft DNS: C	onfiguration changes	Undefined									windows server 2
Microsoft DNS: O	bject deletion in zone	Serious									windows server 2
Microsoft DNS: Se	ervice down	Critical	۲								windows server 2
DELETE											

Figure 18

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

EventTracker displays message box.

	×
Successfully saved configuration.	
	ОК



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.



Category Tree Search			
Solaris BSM Solaris BSM Sonicwall UTM Sophos Enterprise Console	Total category groups: 353 Total categories: 3,1 Last 10 modified categories	117	
Ca Sophos UTM	NAME	MODIFIED DATE	MODIFIED BY
Sox	Microsoft DNS: DNS queries	9/23/2015 2:44:46 PM	gurmukhnishan
sshd	Microsoft DNS: Configuration changes	9/23/2015 2:24:23 PM	gurmukhnishan
Symantec Endpoint Protection	Microsoft DNS: Policy operations	9/23/2015 2:17:58 PM	gurmukhnishan
Syslog	Microsoft DNS: Server operations	9/23/2015 11:50:34 AM	gurmukhnishan
- 🔁 Teradata			
Test			
Trend Micro OfficeScan			
Veritas			
- Cal VMware ESX			
WatchGuard Firebox			
Websense WSG			
Windows			
Windows DNS Server			
Microsoft DNS: Configuration changes			
Microsoft DNS: DNS queries			
Microsoft DNS: DNSSEC operations			
Microsoft DNS: Policy operations			
Microsoft DNS: Server operations			
Microsoft DNS: Server operations Microsoft DNS: Zone operations			

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).



PARSING F	RULE						
Parsing Rule Te Netscreen	emplate		Token-Value Display name	•	Group: W	/indows DNS Ser.	
OpenDNS	Ü Ø			TOKEN NAME	TAG	SEPARATOR	TERMINATOR
Palo Alto Firewall Paloalto	1 0 1 0		+ ChangedValue	changed		to	
RRAS	Ū 🏉		+ ChangedValue	set		to	
Snort IDS	i 🧭						
Sonicwall UTM	Ē 🏈		+ Lookup	Lookup		=	;
Sophos Enterprise Co	Ü 🧭	Ш	🕂 🔲 Name	name		\s	\s
Symantec Endpoint Pr	Ü 🏉	Ц		ADD RULE EDIT DELETE	MOVE TO G		N-VALUE WIZARD
Syslog	Ü 🧭						
test	Ū 🏉						
Trend Micro	Ü 🧭						
VMware	Ü 🏈						
WatchGuard XTM	Ü 🧭						
Websense WSG	Ü 🏈						
Windows	Ü 🏈						
Windows DNS Server	Û Ø .						

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.

PARSING R	ULE							
Parsing Rule Te Paloalto RRAS	emplate	•	Group : Windows DNS Server					
Snort IDS	İ 🏈		TEMPLATE NAME TEMPL	ATE DESCRIPTION ADDED	3Y ADDED DATE	ACTIVE		EDIT
Sonicwall UTM	Ē Ø		Microsoft DNS-Name	gurmuki	nni 9/30/2015 3:17:05 PM			Ø
Sophos Enterprise Co	Ū Ø		Microsoft DNS-Resou	gurmuki	nni 9/25/2015 7:01:32 PM	•		Ø
Symantec Endpoint Pr	Ū Ø		Microsoft DNS-Zone	gurmuki	nni 9/29/2015 3:02:35 PM			Ø
Syslog	1	11						
test	Ū Ø	1						
Trend Micro	1							
VMware	1 🧭							
WatchGuard XTM	1 🧭							
Websense WSG	Ū Ø					DELETE	MOVE	TO GROUP
Windows	1 🧭							
Windows DNS Server	Ū Ø	•						

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.



REPORTS CC	ONFIGUE	RATION			
Scheduled OQueue	d Defined			Search Q	Q [] []
REPORT GROUPS	+	REPORTS CONFIGURATION : WINDOWS DNS SERVER			
Sonicwall UTM	▲ ■ Ø	⊕ Î 𝔅,			Total: 5
Sophos Enterprise Co			CREATED ON	MODIFIED ON	
Sophos UTM	1	Microsoft DNS-Name resolution successfully	9/30/2015 3:39:05 PM	9/30/2015 3:39:21 PM	() 🖉 🕂
🔁 sshd	1	Microsoft DNS-Name resolution failed	9/30/2015 3:33:47 PM	9/30/2015 3:36:10 PM	() 🖉 +
Syslog	1	Microsoft DNS-Zone creation, deletion and updation	9/29/2015 3:06:07 PM	9/29/2015 3:06:52 PM	() A F
D Teradata Database	1				
🔁 test 🔓	1	Microsoft DNS-Resource record creation and deletion	n 9/25/2015 5:01:53 PM	9/29/2015 3:07:27 PM	1 🗐 Ŧ
Trend Micro	1	<u>Microsoft DNS-Configuration changes</u>	9/24/2015 7:25:46 PM	9/25/2015 2:33:17 PM	() 🖉 🕂
VMware					
🔁 WatchGuard XTM	1				
🕒 Websense WSG					
🕒 Windows DNS Server					

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	Туре	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	RECURSE_QUERY	RECURSE_QUERY_OUT
2015-09-25T09:55:37.536813000Z	192.5.5.241	6	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	6	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	6	1.0.0.127.in-addr.arpa.	LOOK_UP	RESPONSE_SUCCESS
2015-09-25T09:55:32.340676200Z	6	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	6	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







DNS - ERROR PATTERN IN LAST 12 HRS Ø 🛛 🖓 🖉 Series: Error Type 9000 8114 8000 7000 6000 tuno 4000 3000 2000 1914 1600 1886 1000 ▲1000 **80**3 216 290 0 BEAT 15:00 0517 17.00 B511723.00 65/18/09/00 051716:00 B517718:00 00,017 19:00 05172000 0517221:00 051722.00 051001:00 05/18/02:00 NXDOMAIN SERVEAIL 05/17 14:39 - 05/18 02:39

• DNS-Error pattern



• DNS-Top queried domains



Figure 29





DNS-Top queried domains with errors

Figure 30



• DNS-Top querying clients



• DNS-Top querying clients with errors





• DNS-Record type pattern



