

Integrate Microsoft DNS Server (Advanced)

EventTracker Enterprise

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

Publication Date: Jun 8, 2016

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.

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

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

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

Prism Microsystems 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 Prism Microsystems, 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.

© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

Abstract1
Scope1
Audience1
Introduction
General Prerequisites
Configuration on DNS server workstation
Prerequisites
DNS Server Configuration
EventTracker Agent Configuration7
Configuration on EventTracker Manager workstation8
Prerequisites
Configure Malware domain watch list9
Prerequisites9
Malware script schedule9
Watch List Verification14
Configure DGA detection script14
Prerequisites14
Python script configuration
Python script verification15
Configure DNS log parse script15
DNS log script schedule15
Configure DNS settings script
Prerequisites
DNS settings script schedule20
Configure DNS latency script24
DNS latency script schedule
Configuration on EventTracker
Create Event Filters



DNS log filter	
DNS summary log filter	31
DNS latency filter	32
Configure Log Consumption	34
Prerequisites	
Configure LFM for DNS query log	34
Configure DLA for DNS miscellaneous logs	
Configure Microsoft DNS KP	
Import Token Templates	
Import Parsing Rules	42
Import Behavior Rule	43
Import Alerts	44
Import Flex Reports	45
Import Knowledge Object	46
Verify Microsoft DNS KP	48
Token Templates	48
Behavior Rule	49
Alerts	50
Flex Reports	51
Knowledge Object	52
EventTracker Knowledge Pack (KP)	53
Reports	53
Behavior Rule	58
Alerts	
Knowledge Object	59
Create Dashboards in EventTracker	59
Schedule Reports	59
Create Dashlets	62
Sample Dashboards	64



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;



Å	DNS Manager
File Action View Help	
🧢 🔿 🖄 🖬 🕻	
DNS ESXWIN2K12R2VM ² Sim Global Logs Global Logs Global Logs Forward Looku Find Reverse Looku Conditional Fo Conditional Fo	Name Configure a DNS Server New Zone Set Aging/Scavenging for All Zones Scavenge Stale Resource Records Update Server Data Files Clear Cache Launch nslookup All Tasks View Delete Refresh Export List Properties Help
Opens the properties dialog box	for the current selection.

Figure 1

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

DNS server properties window opens:



E	SXWIN	I2K12R2\	/M2 Propert	ies ? X
Interfaces	Forw	arders	Advanced	Root Hints
Debug Loggin	g	Event	Logging	Monitoring
To assist with debugging, you can record the packets sent and received by the DNS server to a log file. Debug logging is disabled by default. Compackets for debugging Packet direction: Transport protocol:				
	- {	least one		least one
✓ Incoming) least one ✓ TCP) least one Packet contents: Packet type: ✓ Queries/Transfers ✓ Request > select at least one ✓ Updates > select at least one ✓ Response > select at least one ○ Notifications > Image: Select at least one ✓ Response > select at least one ○ Notifications > > Select at least one > > ○ Notifications > > > > > > > ○ Updates > > > > > > > > > > ○ Updates ><				
Log file File path and name: c:\dns\dns.txt Maximum size (bytes): 100000				
	OK	Cance	l Apply	/ Help

- 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

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.
PS C:\Windows\system32> Set-DnsServerDiagnostics -EnableLogFileRollover $true
PS C:\Windows\system32>
```

Figure 3



 To verify log file rollover setting, open registry editor and navigate to HKEY_LOCAL_MACHINE>SYSTEM>CurrentControlSet>Services>DNS>Parameters. Check if registry name EnableLogFileRollover has value set as '1".

EventTracker Agent Configuration

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

EventTracker Agent Configuration	x	
File Help		
C Select Systems		
ESXWIN2K12R2VM2 Agent based system		
Apply the following settings to specified Agents		
<u>M</u> anager destinations:		
192.168.1.174, ESXWIN2K12R2VM2, pnpl-2-kp.Toons.local, pnpl-3-kp.Toons.loca	al	
Log Backup Performance Network Connections		
Managers Event Filters System Monitor Monitor Processes Service	s	
Logfile Monitor File Transfer Config Assessment syslog FTP server		
This feature allows file transfer of selected Windows and application log files at scheduled times. Windows logs that are filtered out by the real-time settings are translated and cached for transfer (further filtering is available). Application log files placed in the folder are transferred.		
Manager Port Encrypted Add	1	
ESXWIN2K12B2VM2 14505 No	4	
PNPL-TEST4 14505 Yes <u>Edit</u>		
< III > <u>R</u> emove		
Send Windows events via <u>File</u> Transfer Fil <u>t</u> ers		
✓ Send other log files C:\dns		
All files placed in this folder will be transferred to the configured manager(s). Frequency Purge Transferred Files Advasced		
○ Daily at: 2:22:15 PM → Set 0 to disable purging Send Now		
	-	
Save Close		

Figure 4



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

DLA Manager pane opens;

DLA Manager	x			
For successful processing of Windows logs that are filtered out by the real-time settings, an instance of EventTracker Receiver MUST be running on the configured port. Please make sure that a Virtual Collection Point is configured on the target system with appropriate Receiver port number.				
<u>System:</u> 192.168.1.174				
Port 14505				
Encrypt: No				
<u> </u>				

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.
- 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.



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.



Malware list update Properties (Local Computer)	×			
General Triggers Actions Conditions Settings History				
Name: Malware list update				
Location: \Microsoft DNS				
Author:				
Description:				
Security options				
When running the task, use the following user account:				
P TOTATA annualizada	Change User or Group			
Run only when user is logged on A second secon				
Run whether user is logged on or not				
Do not store password. The task will only have access to local computer resources.				
Run with highest privileges				
☐ Hidden Configure for: Windows Vista™, Windows Server™ 2008	•			
	OK Cancel			

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.



Edit Trigger
Begin the task: On a schedule Settings One time Start: 5/30/2016 Start: 2:56:59 PM Synchronize across time zones
C Daily Weekly Monthly Recur every: Weeks on: Sunday Monday Wednesday Tuesday Friday Saturday
Advanced settings
Delay task for up to (random delay): 1 hour
Repeat task every: 1 hour for a duration of: 1 day
Stop all running tasks at end of repetition duration
Stop task if it runs longer than:
Expire: 5/30/2017 Synchronize across time zones
✓ Enabled
OK Cancel

Figure 9

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



dit Action You must specify what action this task wi	Il perform.
Action: Start a program	
Program/script: powershell.exe	Browse
Start in (optional):	
	OK Cancel

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

Dashboard Incidents Behavior Searc	h Reports My EventTrad	ker Change Audit Config Asse	essment
ACTIVE WATCH LISTS			 ⊕ ☆
GROUPS 🕑 🍘 🗓	DOMAINS/MALWAREL	IST	Page size 20 ▼ 2 ① ⑦ ⑦ ⑧ ∂, ∂, ◎
IP Address AutoshunbadlPList	+ PATTERN	ADDED BY	
EmergingThreatBlocked	①.net@phishing	ETAdmin	5/27/2016 5:58:24 PM 🕜 🗖
Processes FO: KnownExeW/hitelist	+ 0000mps.webpreview.dsl.n	et@malicious ETAdmin	5/27/2016 5:56:28 PM 🧭 🗖
······································	+ 007.com@Kronos	ETAdmin	5/27/2016 5:58:24 PM 🕜 🗖
Unsafe List Services	+ 03574cd.netsolhost.com@l	ocky ETAdmin	5/27/2016 5:58:24 PM 🕜 🗖
Port No	+ 0735sh.com@malicious	ETAdmin	5/27/2016 5:56:28 PM 🕜 🗖
Domains	+ 101.boquan.net@malicious	s ETAdmin	5/27/2016 5:56:28 PM 🕜 🗖



 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

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





Python script verification

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

python .\dga_detector.py

PS C:\Program Files (x86)\Pytho	on35-32> python .\dga_detector.py
7_/-/ / / 7_/ 7	;_/-//(/_; {/ (/_; (/_//,_/))
usage: aga_aetector.py [-n] [-a	I DUMAINJ [-T FILE]
DGA domain detection	
ontional arguments:	
-h,help show th	is help message and exit
-d DOMAIN,domain DOMAIN	
Domain frug file gur gile wi	to check
-T FILE,TTIE FILE FILE WI	th domains. One per line



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.



🕒 DNS-logging	and analyzing Propertie	es (Local Computer)		×	
General Triggers Actions Conditions Settings History					
Name:	DNS-logging and analy	zing			
Location:	\Microsoft DNS				
Author:	Filling providents	e			
Description:					
_ Security op	tions				
When runr	ing the task, use the follo	owing user account:			
Change User or Group					
Run only when user is logged on					
Run wh	Run whether user is logged on or not				
🗖 Do i	Do not store password. The task will only have access to local computer resources.				
Run with highest privileges					
🗖 Hidden	Configure for: 🛛	Vindows Vista™, Windows Server™ 2008	•		
			OK Cancel		

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.



Edit Trigger
Begin the task: On a schedule Settings One time Start: 5/30/2016 2:42:33 PM Synchronize across time zones August Recur every: 1 days Monthly
Advanced settings Delay task for up to (random delay): 1 hour Repeat task every: 1 hour for a duration of: 1 day
 Stop all running tasks at end of repetition duration Stop task if it runs longer than: 3 days Expire: 5/30/2017 Stop task if it runs longer than: 5:05:49 PM Expire: 5/30/2017 Stop task if it runs longer than: 5:05:49 PM Expire: 5/30/2017 Enabled
OK Cancel

Figure 16

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



Edit Action	X
You must specify what action this task will perf	orm.
Action: Start a program	•
- Settings	
Program/script:	
powershell.exe	Browse
Add arguments (optional):	powershell.exe -executio
Start in (optional):	
	OK Cancel



7. Select **Actions** tab, enter '**powershell.exe**" as program name and compose argument as given below:

powershell.exe -executionpolicy bypass -file "<mark>C:\Program Files (x86)\Prism</mark> 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.

🕑 Task Scheduler		
File Action View Help		
🗢 🔿 📊 🛿 🗊		
Task Scheduler (Local) Task Scheduler Library Task Scheduler Library Microsoft Microsoft DNS WPD	Task Scheduler Summary (Last refreshed: 5/30/2016 2:56:24 PM) Overview of Task Scheduler You can use Task Scheduler to create and manage common tasks that your computer will carry out automatically at the times you specify. To begin, click a command in the Action menu. Tasks are stored in folders in the Task Task status Status of tasks that have start Last 24 hours Summary: 55 total - 0 running, 55 succeeded, 0 stopped, Task Name Run Result Run Cache Task (running) Consolidator (last run succeede DNS-logging and analyzing (las EventTracker-Attackers (last ru EventTracker-AutoshuniPList (l Last refreshed at 5/30/2016 2:56:24 PM	Actions Task Scheduler (Local) Connect to Another Computer Create Basic Task Tmport Task Import Task Display All Running Tasks Disable All Tasks History AT Service Account Configuration View Refresh Help

Figure 18

3. In the Actions tab select Create task.



4. Configure Task properties as shown below.

🕒 Create Task	×			
General Trig	gers Actions Conditions Settings			
Name:	DNS-settings retrieval			
Location:	\Microsoft DNS			
Author:	70000 constant			
Description:				
	<u></u>			
Security opt	ions			
When runni	ing the task, use the following user account:			
100.014	Change User or Group			
C Run only when user is logged on				
• Run whether user is logged on or not				
Do not store password. The task will only have access to local computer resources.				
Run with highest privileges				
🗖 Hidden	Configure for: Windows Vista™, Windows Server™ 2008 💌			
	OK Cancel			

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.



Edit Trigger				
Begin the task: On a schedule Settings One time Start: 5/30/2016 2:56:59 PM Image: Synchronize across time zones				
C Daily Weekly Monthly C Monthly Friday Friday Saturday				
Advanced settings				
Delay task for up to (random delay): 1 hour				
■ Repeat task every: 1 hour ■ for a duration of: 1 day ■				
Stop all running tasks at end of repetition duration				
Stop task if it runs longer than:				
Expire: 5/30/2017 🔄 3:22:54 PM 🚔 🔲 Synchronize across time zones				
☑ Enabled				
OK Cancel				

Figure 20

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



dit Action You must specify what action this task wi	Il perform.
Action: Start a program	
Program/script: powershell.exe	Browse
Start in (optional):	
	OK Cancel

Figure 21

7. Select **Actions** tab, enter **'powershell.exe**" as program name and compose argument as given below:

powershell.exe -executionpolicy bypass -file "<mark>C:\Program Files (x86)\Prism</mark> 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:



🕒 Create Task	×			
General Trig	gers Actions Conditions Settings			
Name:	DNS-latency measurement			
Location:	\Microsoft DNS			
Author:	T TO THE ANY AND A STATE OF A STA			
Description:				
E Security opt	tions			
When runn	ing the task, use the following user account:			
100009-0	Change User or Group			
Run only when user is logged on				
💿 Run whe	ether user is logged on or not			
Do not store password. The task will only have access to local computer resources.				
🔽 Run with	h highest privileges			
🗖 Hidden	Configure for: Windows Vista™, Windows Server™ 2008 💌			
	OK Cancel			

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.



Edit Trigger
Begin the task: On a schedule Settings One time Start: 5/30/2016 • 2:42:33 PM • Synchronize across time zones Daily Weekly Monthly
Advanced settings Delay task for up to (random delay): 1 hour Repeat task every: 1 hour for a duration of: 1 day
Stop all running tasks at end of repetition duration
Stop task if it runs longer than:
Expire: 5/30/2017 💽 5:05:49 PM 🚔 🗖 Synchronize across time zones
Enabled
OK Cancel

Figure 24

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



dit Action	×
You must specify what action this task will p	perform.
Action: Start a program	
Settings	
Program/script: powershell.exe	Browse
Add arguments (optional):	powershell.exe -executio
Start in (optional):	



7. Select **Actions** tab, enter **'powershell.exe**" as program name and compose argument as given below:

powershell.exe -executionpolicy bypass -file "<mark>C:\Program Files (x86)\Prism Microsystems</mark>\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.



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



🜠 EventTracker Agent Configuration File Help	×
Select Systems PNPL-3-KP Apply the following settings to specified Agents Manager destinations: esxwin2k12r2vm2, PNPL-3-KP Log Backup Performance Log Backup File Transfer Config Assessmer	Agent based system
Managers Event Filters System Monitor Monitor You can choose to filter out events that are not required all events matching the filter criteria will not be sent to the Manager. You can also configure advanced filter options specific events or choose to filter out specific events. Event Logs • Application • HardwareEvents • Internet Explorer • Key Management Service • Media Center • Netwrix Aurlitor • Enable SID Translation • Event Description: •	Once the filter is set, e EventTracker s such as to send only Event Types Error Warning ✓ Information ✓ Audit Success Audit Failure Critical Verbose
Filter Exception	Advanced Filters

Figure 27

• Select Event Filters tab, click Filter Exception.

Filter exception window opens,



록 Filter Exc	ception						\times
You can choose to monitor specific events if they match a filter criteria. Specify the details of the events that you would like to monitor. Example: You may want to filter out all Information events other than those received from the Web Service. To do this, set the Information filter and add a Filter Exception with Event Source as Web							
Log Type	Event Type	Cate	Eve	Source	User	Description	^
	Audit Success	0	620				
	Audit Success	0	647				
	Audit Success	0	672				
	Audit Success	0	682				
	Audit Success	0	683				
	Audit Success	0	685				
	Audit Success	0	687				
	Audit Success	0	689				
	Audit Success	0	690				
	Audit Success	Π	691				×
<							>
<u>N</u> ew	<u>E</u> dit	<u>D</u> el	ete	Find		<u>C</u> los	e

• 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.



🚅 Edit Event Details	×		
Event Details (empty field implies all matche Log Type :	35]		
System	•		
Event Type : Information	Event ID : 3230		
Category : 0	Match in <u>U</u> ser :		
Match in <u>S</u> ource : EventTracker Match in Event <u>D</u> escr : Date&&Query&&Type&&Client&&SendRece	ive&&Protocol&&RecordType&&Query&&Result		
"Match in Event Descr" field can take multiple strings separated with && or . - && stands for AND condition stands for OR condition. For negating the result of match operation, prefix the string with "[\$NOT\$]". If there are multiple strings, then the result of the whole expression is negated. Only one "[\$NOT\$]" should be used in the string. Example: The string "[\$NOT\$]Logon Type: 4 Logon Type: 5" will match all events that DO NOT contain "Logon Type: 4" or "Logon Type: 5" in the description. For more information click here.			
OK	Cancel		

• Enter following as matching description.

Date&&Query&&Type&&Client&&SendReceive&&Protocol&&RecordType&&Query&&Results&&R esponse&&Flags

• Click **OK** to apply.

DNS summary log filter

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

• Configure event filter details as shown below.



🚅 Edit Event Details	×
Event Details (empty field implies all match Log Type : System	ies)
Event Type :	Event <u>I</u> D : 3230
Category : 0	Match in <u>U</u> ser :
Match in <u>S</u> ource : EventTracker Match in Event <u>D</u> escr :	
"Match in Event Descr" field can take mul - && stands for AND condition stands For negating the result of match operation, multiple strings, then the result of the whole should be used in the string. Example: The string "[\$NOT\$]Logon Type: 4 Logon contain "Logon Type: 4" or "Logon Type: For more information click here.	Itiple strings separated with && or . for OR condition. , prefix the string with "[\$NOT\$]". If there are e expression is negated. Only one "[\$NOT\$]" n Type: 5" will match all events that DO NOT 5" in the description.
ОК	Cancel

• 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.



록 Edit Event Details	×
Event Details (empty field implies all matche Log Type :	es]
System	•
Event Type : Information	Event ID : 3230
Category : 0	Match in <u>U</u> ser :
Match in <u>S</u> ource : EventTracker Match in Event <u>D</u> escr : DNSServerName&&LatencyInMS	
"Match in Event Descr" field can take mult - && stands for AND condition stands For negating the result of match operation, multiple strings, then the result of the whole should be used in the string. Example: The string "[\$NOT\$]Logon Type: 4 Logon contain "Logon Type: 4" or "Logon Type: 4 For more information click here.	tiple strings separated with && or . for OR condition. prefix the string with ''[\$NOT\$]''. If there are expression is negated. Only one ''[\$NOT\$]'' Type: 5'' will match all events that DO NOT 5'' in the description.
ОК	Cancel

• Enter following as matching description.

DNSServerName&&LatencyInMS

- Click **OK** to apply.
- Click **Save** to apply configured filters.



Configure Log Consumption

Prerequisites

1. Administrative privileges to EventTracker Manager workstation.

Configure LFM for DNS query log

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

1. Logon to EventTracker manager workstation.



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



🚅 EventTracker Agent Configuration	×
File Help	
Select Systems	
PNPL-3-KP Agent	based system
Apply the following settings to specified Agents	
<u>M</u> anager destinations:	
PNPL-3-KP, esxwin2k12r2vm2	
Log Backup Performance Network (Managers Event Filters System Monitor Monitor Proces	Connections
Logfile Monitor File Transfer Config Assessment sy	slog FTP server
Search log files (various formats supported) for matching patterns here. Both individual files as well as folders can be monitored for entries. Matches cause an event to be generated.	specified matching
Logfile Name	File Type
C:\Users\kumarnitesh\Desktop\Final Parse Segment.csv	CSV
C:\DNS Parse\Final\Final Parse.csv	CSV
C:\DNS Parse\Summary*.csv	CSV
d:\PS\dns latency.csv	CSV
C:\DNS Logs\LFM\Final Parse.csv	CSV
Add File Name View File Details Delete File Name S	earch Strings
<u>S</u> ave <u>C</u> lose	

Figure 33

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



Tou can configure the complete path of the log file or folder that needs to be monitored
along with the strings that need to be searched.
Get All Existing Log Files
Select Log File Type CSV
This is the CSV Extended Log File Format. Different types of CSV files exist, in which, header line number is different. The header line will start with '#Field' qualifier and mostly available on line number one by default.
Enter File name
C:\Program Files (x86)\Prism Microsystems\EventTracker\DLA\ESXWIN2K12R2
Enter Header Line Number of the above file: 2
OK Cancel



5. Configure DNS log file as shown above. Compose log file path as given below.

C:\Program Files (x86)\Prism Microsystems\EventTracker\DLA\ESXWIN2K12R2VM2<mark>\LFM\</mark> 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.

Search String Search Strings for Microsystems\Eve Use a '*'in any co	: C:\Program Files (x86)\Prisr ntTracker\DLA\ESXWIN2K olumn to match every entry in	n 12R2VM2\LFM\Pa the file
Column Name	Search String	
Date	x	
Add String	Edit String	Delete String
	OK	Cancel

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.

MANAGER CONFIGURATIO	N			
CONFIGURATION Syslog / VIRTUAL COLLECTION	ON POINT	LOG ARCHIVER /	NETFLOW RECEIVER	AGENT SETTINGS
E-MAIL CONFIGURATION STATUSTRACKER	COLLECTION MASTER	R PORTS NE	WS	
☑ Direct log file archiving from external sources	Purge files	after 7 days	ASSOCIATED V 14505	VIRTUAL COLLECTION POINT
LOG FILE FOLDER	CONFIGURATION NAME	LOG FILE EXTENSION	FIELD SEPARATOR	LDG TYPE
C:\Program Files (x86)\Prism Microsystems\EventTracker \DLA\\ESXWIN2K12R2VM2\DLA	DNS Logging	CSV	Comma - [Fields containing in double quotes]	comma are wrapped
				ADD EDIT REMOVE

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.



vpe	Others		
orfile Extension			
ogine extension			
onfiguration Name	DNS Logging		
og File Folder	C:\Program Files (x86)\Prism Micn	BROWSE	
	⊙ Single Line ⊂ Multi Line		
ield Separator	Comma - [Fields containing con 💌		
tarting Line Offset	1		
xtract field names from leader	V		
leader			

6. Configure DNS log file as shown above. Compose log file path as given below.

C:\Program Files (x86)\Prism Microsystems<mark>\EventTracker\DLA\</mark>ESXWIN2K12R2VM2<mark>\DLA\</mark>

EventTracker installation folder

EventTracker agent workstation name

7. Scroll down and click **Save** to proceed.



Log file configuration		
Configuration Name	C:\Program Files (x86)\Prism Microsy:	stems\Eve
Log Source	DNS Server	
Computer Name	ESXWIN2K12R2VM2	
Computer IP	192.168.1.155	GET IP
System Type	Unknown	•
System Description		_
Comment Line Token		
C Entire Row as Description	● Formatted Description	
Log File Format	Custom Log File Format	*
Manager Fields		ADD
Message Fields	A	REMOVE



- 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 I **'Import**' option.



PARSING R	JLE									
Parsing Rule Ter GROUPS Default A10 ADC	nplate (+) ::::	E	Group : All Search	Q.				C	; 1 T])
Amazon Web Services	Ē Ø		TEMPLATE NAME	TEMPLATE DESCRIPTION	GROUP NAME	ADDED BY	ADDED DATE	ACTIVE	ED T	Ê
Apache Web Server	Ü 🏉		A10 ADC Authenticat	A10 Application Delivery C	A10 ADC	ETAdmin	9/29/2015 08:19:51 PM	V	. Ø	
Barracuda Message Ar	Ü 🏉		A10 ADC Traffic	A10 Application Delivery C	A10 ADC	ETAdmin	9/29/2015 08:19:51 PM	V	. Ø	
Barracuda Spam Firew	Ü Ø		AWS VPC-Flaw Repart		Amazon Web S	ETAdmin	9/29/2015 08:19:51 PM	V	. Ø	
Blue Coat Proxy	Ü 🖉	L.	Barracuda Message		Barracuda Me	ETAdmin	9/29/2015 08:19:51 PM	v	. 0	
Centrify Server Suit	1		Barracuda Spam fire		Barracuda Spa	ETAdmin	12/15/2015 0B:02:47		🗆 🧭	
Check Paint	Ü Ø		Barracuda Spam fire		Barracuda Spa	ETAdmin	12/15/2015 0B:02:47	v	. 🏈	
Cisco ASA	1		Barracuda Spam fire		Barracuda Spa	ETAdmin	12/15/2015 0B:02:47	V	. Ø	
Cisca IOS	Ш́ Ø							_		
Cisco IronPart ESA	1						DELETE	MOVE TO	GROUP	
CISCO Iranpart WSA	11 🧭	-								

Figure 40

3. Click the **Browse** button.



Figure 41

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

SELECTI	ED FILE IS: token_Dashboard(77).ettd T					
	TEMPLATE NAME	SEPARATOR	TEMPLATE DESCRIPTION	ADDED DATE	ADDED BY	GROUP NAME
	DNS-Suspicious dns settings detection details	`t	Suspicious DNS settings detected SystemName:PNPL-3-KP SystemIP:192.1 68.1.235 SystemMAC:47:8A:58:57:13:F7 DNSIP:208.67.222.222	5/25/2016 12:57:54 PM	ETAdmin	Windows DNS Server





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

EventTracker displays success message.

Template(s) import	ied successfully
	ОК



6. Click on **OK** button.

Import Parsing Rules

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

Uptions Category Filters Alerts Systems and Groups RSS Feeds Reports Behavior Rules SCAP Token Value	Location Source : *.istoken	
---	-----------------------------------	--



- 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.



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

Import Behavior Rule

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

Click the Import button	ame or benavior nie. Ose the buttor to browse and locate the import nie.	
Options Category Filters Alerts Systems and Groups RSS Feeds	Location Source : *.isrule	
Reports Behavior Rules SCAP Token Value		





- 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.



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.

1. Provide the path and file na 2. Click the Import button. Options Category	ame of the Alerts file. Use the '' button	to browse and locate the import file.
Filters	Import E-mail settings	
Alerts	Set Active	This setting is applicable only for imports from Legacy
Systems and Groups	 By default 	(v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section
RSS Feeds	0 -,	SCUOIL
Reports	Source :	
Behavior Rules	*.isalt	
SCAP		
💿 Token Value		

Figure 48



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

EventTracker displays success message.





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.

lote : If report(s) contains temp	plate, first import template and proceed with exportimport utility.
Category	Location
Filters	
Alerts	egacy (*.issch)
Systems and Groups	Source :
RSS Feeds	*.issch
Reports	
Behavior Rules	
SCAP	
Token Value	





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

EventTracker displays success message.





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.

KNOWLEDGE	OBJECTS
-----------	---------

O BJECT S	Ð T 1	
Apache access lo,	g 🧭	
ArrayOS SPX	Ø	
Barracuda Messa	g 🧭 🙁	=
Barracuda Spam I	Fi 🧭 🗵	
Barracuda SSL VP	N 🔗 🗵	
Barracuda Web A	р 🧭 🗵	
Blue Coat Proxy	8 🗵	
Centrify AD client	1	
Check Paint	0	
Cisco ACE	0	
Cisco ACS	1	
Cisco ASA Errors	8	
Cisco ASA ICMP C	a 🧭 🗵	
Cisco ASA Others	Ø ×	
Cisco ASA SSL	8	
Circle AEA TOD Cor		-

Figure 51



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



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

IMPORT	
Select file Browse No file selected.	UPLOAD APPLIES TO
Microsoft DNS Query	Microsoft DNS
	MERGE



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.



PARSING RI	JLE							
Parsing Rule Ter FortiGate Firewall (nplate	Graup : Microsoft DNS						
HP ProCurve Switch	1	Search	Q					CIT
Infablax	Î Ø	TEMPLATE NAME	TEMPLATE DESCRIPTION	ADDED BY	ADDED DATE	ACTIVE		EDIT
Juniper Netscreen	iii Ø	Microsoft DNS- Suspic		gurmukh	5/25/2016 12:57:54 PM			1
Linux	Ē Ø	Micrasaft DNS-Resaur		ETAdmin	12/15/2015 0B:02:48 PM			0
LOGbinder SQL	1	Microsoft DNS-Zane a		ETAdmin	12/15/2015 08:02:48 PM	I 🗹		Ø
Microsoft DNS	1	1						
Microsoft Windows RR	11 🧭							
M55QL	1							
My5QL	Ü 🧭							
Office 365	Ū 🏉							
OKTA 550	Î 🧭					DELETE	MOVE	TO GROUP
OpenDN5	1							



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.



BEHAVIOR RULES	•					
					Page si	ze 25 🗸
RULE NAME	BREAKUP COLUMN	DISPLAY NAME	<u>ACTIVE</u>	DELETE	ACTIVATION/DEACTIVATI TIME	ON
Microsoft DNS query traffic	Client	Client Address			6/2/2016 01:00:44 PM	Ø 🗉
		1 2				
					ADD RULE DELETE	CLOSE
		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 Q button.

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



ALERT MANAGEMEN	١T	Search I	Y Alert na	ame 🗸	microsoft dr	ns QQ				
		(Total: 15	Page Size 25 🗸						
ALERT NAME	<u>THREAT</u>	<u>ACTIVE</u>	E-MAIL	MESSAGE	R55	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
Microsoft DNS: DGA domain detected	Critical	\checkmark								Microsoft DN5
Microsoft DN5: High DN5 server lat	Serious	\checkmark								Microsoft DN5
Microsoft DNS: High error query co	🗌 High	\checkmark								Microsoft DN5
Microsoft DNS: High error query co	🔲 High	\checkmark								Microsoft DN5
Microsoft DNS: High error query co	🗌 High	\checkmark								Microsoft DN5
Microsoft DN5: High query count de	🔲 High	\checkmark								Microsoft DN5
Microsoft DN5: High query count de	🗌 High	\checkmark								Microsoft DN5
Microsoft DN5: High query count de	🔲 High	\checkmark								Microsoft DN5
Microsoft DN5: Malformed domain	Seriaus									Microsoft DN5
Microsoft DNS: Malicious domain d	Serious									Microsoft DNS

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

EventTracker displays message box.



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

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

Flex Reports

1. Logon to **EventTracker Enterprise**.



- 2. Click the **Reports** menu and select **Configuration**.
- 3. Select **Defined** in report type.
- 4. In Report Groups Tree, select Microsoft DNS group folder.

Imported reports are displayed on the right pane.

REPORTS CONFIGURATION											
O Scheduled O Queueo	d 🔘 Defi	ned				Search (20 1				
REPORT GROUPS	+		RE P O RT 5	CONFIGURATION : MICROSOFT DNS							
🍞 Security		^	🕀 🗓	e,			Total: 12				
🍞 Compliance				TITLE	CREATED ON	MODIFIED ON	^				
🍞 Operations				Microsoft DNS- Least resolved damain count	5/4/2016 04:10:59 PM	5/4/2016 04:10:59 PM	() 河 🛨				
🍞 Flex				<u>Microsoft DNS- Server latency details</u>	5/4/2016 03:52:34 PM	5/4/2016 03:52:34 PM	() 🖉 +				
🔁 A10 ADC	Ü Ø			Microsoft DNS- DG4 domain detection details	5/4/2016 02:31:34 PM	5/4/2016 02:31:34 PM	() 🎘 +				
🔁 Amazon Web Services	1 🧭	Т.		<u>Microsoft DNS- Malformed domain detection</u>	4/23/2016 04:59:08 PM	4/23/2016 04:59:08 PM	() 🖉 🕂				
🕞 Apache Web Server	Ü Ø			<u>Microsoft DNS- Malicious domain detection</u>	4/23/2016 01:48:33 PM	4/23/2016 01:48:33 PM	() 🗐 🗉				
🕞 Barracuda Message Ar	1 0			Microsoft DNS- Summary record type count	4/22/2016 10:05:25 PM	4/22/2016 10:05:25 PM	() 🎜 🕂				
Barracuda Spam Firew	1			Microsoft DNS- Traffic details	4/22/2016 09:50:32 PM	4/22/2016 09:50:32 PM	() 🖉 🛨				
🗃 Barracuda SSL VPN	1 0			Microsoft DNS- Error domain count	4/12/2016 03:38:42 PM	4/12/2016 03:3B:42 PM	() 🗐 F				
🔁 Centrify Server Suit	Ü 🏈						¥				
🕞 Check Paint	Ü 🏉		н <	1 🗸 af 2 🕻 🕨							

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.



KNOWLEDGE OBJECTS

DBJECT S) T 1	OBJECT	T NAME Microsoft DNS	query traffic				1	÷
Cisca ASA Others	8	RULES							
Cisco ASA SSL	Ø×	TI	TLE	LOG TYPE	EVENT SOURCE	EVENT ID	EVENT TYPE		
Cisco ASA TCP Con		± Mi	crasaft DNS Query Lags	5ystem	EventTracker	3230	Information	✐⊴⊗	
Cisca ASA UDP Car	🧭 🗵	м	ESSAGE SIGNATURE:	Date\:[\x00-\xFF]{0,}QueryTy \:[\x00-\xFF]{0,}RecordType\:	pe\:[\x00-\xFF]{0,}Clie [\x00-\xFF]{0,}Query\:	nt\:[\x00-\xFF]{0 [\x00-\xFF]{0,}Re	}SendReceive\:[\x00 sults\:[\x00-\xFF]{0,}	I-\xFF]{0,}Protoco Flags\:	.1
Cisco Firewall	0	MI	ESSAGE EXCEPTION						
Cisca IOS	0								
Cisca ISE	0	E	XPRESSION 5						
Clavister	0		EXPRESSION T	YPE FORMAT STRING	EXPRESSION '	EXPR	E55ION 2		
Clearing Event Log	s 🧭								
Cyberoam UTM	8		Key value Delimiti	2F	:	١n			
Dell FORCE 10 Swi	tØX								
EventTracker	Ø								

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	ТСР	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	Rev	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

_			
Fi	σι	Iro	67
	ъu	пс	02

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: do				
Court 77				

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	А	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





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

- 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.



EventTracker: Microsoft DNS Server (Advanced)

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	А	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.







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

REPORTS COI	NFIG	URA	TIC	ΟN				
	o 💿 Defi	ned					Search	QQ []
	_							
REPORT GROUPS	÷		REPO	RT 5 C	ONFIGURATION : MICROSOFT DNS			
🍞 Security		^	€	Ô 🗓	2			Total: 12
🍞 Compliance]	TITLE	CREATED ON	MODIFIED ON	^
🍞 Operations				٤	Microsoft DNS- Least resolved domain count	5/4/2016 04:10:59 PM	5/4/2016 04:10:59 PM	() 🎜 🗉
🍞 Flex				٤	Microsoft DNS- Server latency details	5/4/2016 03:52:34 PM	5/4/2016 03:52:34 PM	() 🎜 🕂
🔁 A10 ADC	1 🧭			<u>ي</u>	Microsoft DNS- DGA domain detection details	5/4/2016 02:31:34 PM	5/4/2016 02:31:34 PM	() 🎘 +
🕞 Amazon Web Services	1 🧭	н		<u>ي</u>	Microsoft DNS- Malformed domain detection	4/23/2016 04:59:08 P	A 4/23/2016 04:59:08 PM	() 💭 +
🕞 Apache Web Server	1 🧭			<u>ي</u> ي	Microsoft DN5- Malicious domain detection	4/23/2016 01:48:33 PI	M 4/23/2016 01:48:33 PM	() / =
🕞 Barracuda Message Ar	1 🧭			<u>ب</u>	Microsoft DN5- Summary record type count	4/22/2016 10:05:25 PI	И 4/22/2016 10:05:25 PM	• 5
Barracuda Spam Firew	1			<u>ي</u>	Microsoft DNS- Traffic details	4/22/2016 09:50:32 Pl	M 4/22/2016 09:50:32 PM	() 🖉 🛨
🕞 Barracuda SSL VPN	Ü Ø			577	Mirrosoft DNS, Error domain count	4/10/2016 03:38:42 P	4 . 4/12/2016 03:38:42 PM	
🕞 Centrify Server Suit	Ü 🧭		Ľ	~~~ .		12/2010 00.00.42 FI	N	¥
🕞 Check Paint	1 🧭	~	M 4	¢ 1	✓ af 2 > ►			

Figure 74

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



REPORT WIZARD TITLE: DNS- SUSPICIOUS DNS SETTINGS DETECTION DETAILS LOGS		CANCEL < BACK NEXT >
Review cost details and configure the publishing options.		Step B of 10
DISK COST ANALYSIS Estimated time for completion: 00:08:54(HH::MM:55) Number of cab(s) to be processed: 252 Available disk space: 174 GB Required disk space: 50 MB Enable publishing option (Configure SMTP Server in manager co Deliver results via E-mail Notify results via E-mail	nfiguration screen to use this option)	
To E-mail	[Use comma(;) to separate multiple e-mail recipients]	
Update status via RSS Select Feed 🗸		
Shaw in none 🗸		
Persist data in Eventvault Explorer		

Figure 75

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

PORT WIZAH : DNS- SUSPICIOUS DNS SET A PERSIST DETAIL	D		CANCEL < BACK NEXT >
t calumns ta persist			Step 9 af 10
RETENTION SETTIN Retention period: 7	G days ①	lished and will only be stored in the respective d.	(atabase]
SELECT COLUMNS T	O PERSIST		
Device Name			
Device IP			
Device MAC			





- 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.



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



FLEX DASHBOA	RD
Title Microsoft DNS	
Description Windows DNS Server	
	SAVE DELETE CANCEL



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

WIDGET CONFIGURATION

WIDGET TITLE				NOTE		
DNS- Suspicious DNS s	ettings detected i	n last 24 hrs 🔐				
DATA SOURCE						
DNS- Suspicious dns s	ettings detection (details	~			
Donut	24 Hours	COUNT	TING	AS OF Recent 🗸		
AXIS LABELS [X-AXIS] Device IP	LABEL TEXT					
VALUES [Y-AXIS]	VALUE TEXT					
Select column 🗸						
FILTER Select column	FILTER VALUES	~				
LEGEND [SERIES]	SELECT					
Select column 🗸	All 🗸					
						TE

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.

CUSTOMIZE WIDGETS		€ İ 🖲
Meraki blacked web contents t		
1		
	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



• Microsoft DNS-Top queried domains in last 12 hrs



Figure 86





• Microsoft DNS-Top querying clients in last 12 hrs





• Microsoft DNS-Malicious domains detected in last 12 hrs

Figure 88





• Microsoft DNS-Server latency in last 12 hrs



• Microsoft DNS-DGA domains detected in last 12 hrs







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

Figure 91

<-X->

