

Enhancement in Log Search and System Manager

Publication Date: May 6, 2019

Abstract

This document provides enhancements in EventTracker v9.0 log search result and system manager.

Audience

EventTracker v9.0 user(s) who wish to refine the log search result by selecting multiple normalized data and also given an option to pivot the log search results, by selecting multiple CIM fields.

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 laws 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.

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

Abstract	. 1
Audience	. 1
Options to add multiple CIM fields for pivoting	. 3
Option to add multiple normalized data by using include/exclude options in log search.	. 5
Option to move systems from one group to other in System Manager	. 8

Netsurion... EventTracker

Options to add multiple CIM fields for pivoting

After performing log search, the user can see new enhancements in the log search result window.

User is provided with an option to filter multiple interesting fields for pivoting the log search results.

To perform multiple CIM field for pivoting.

1. Click **"Add multiple fields for Pivoting"** icon in the **Interesting** field tab.





2. "Add multiple fields for pivoting" dialog box appears.

Interesting fields	Selected fields	
action	+ ^	
addl_date	+	
addl_info	+	
addl_info1	+	
addl_info4	+	
addl_info5	+	
addl_info6	+	
addl_info7	+	
application_name	+	
application_type	+	
	~	

Figure 2



3. Select the CIM fields by clicking **Add field** (+ sign) icon and click **Add Field** button to add multiple fields for pivoting.

Interesting fields		Selected fields	
dest_user_name	+ ^	1 event_computer	
event_log_type	+	‡ event_id	
event_source	+	<pre></pre>	
event_type	+	<pre></pre>	
event_user_domain	+		
event_user_name	+		
file_path	+		
log_direction	+		
log_info	+		
og_source	+		
log status	+ ~		
			Add Field Clos

4. The selected fields are displayed in the tabular form as a pivot column as well as under the **Selected field** tab.

and and EventTracker a										
A datameter a training of the second se										
Name: No 01211 M - 10y 0121 M - 10y 0121 M -										
Search criteria: *										
and commission			0							
Top 10 (src_host_name)	Top 10 (dest_host_name)	Top 10 (dest_user_name)	Top 10 (event_computer)							
224.0.0.252										
M02::1:3		and the second								
r1s5-vm3.rdpt										
ristomitate										
ac20:985::	and and a second and a second start of the second start from the second start and the second	sugumaran.k	Conformation Conformation							
ac20:98e::78	■r1s5-vm5 ■ 172.28.9.146 ■ phartom2 ■ r1s6-vm2 mtpl3cal									
Top 10 (event_id)	Top 10 (src_user_name)	Top 10 (log_source)	Top 10 (taps)							
3516										
3514		evertisation								
1609										
4688		eventingine								
4674										
3515										
3244	🖬 et authoritylynetwork service 🧧 sugumaran k 📓 system 📕 r1s5-vm35 📕 r1s5-vm155	windows secur	eventtracker events in nom events in traffic activities in security in windows							
3246	Tocal service Int authority/local service network service									
			1 Segment = 1 Hour							
< 1 of 200 CO >	Page state 50 V									
Selected Selfs	event_computer	event_id event_category	event_type							
event, computer C x + May 03 GL11:30 PM	R155-VM15-OLA	3221 2	Information							
+ May 03 04.11:08 PM	R155-VM15-DLA	3221 2	information							
+ May 03 04:11:08 PM	R155-VM15-OLA	3221 2	information							
	RISI-VMIL-OLA	3221 2	information							
• May 03 04 100 PM	R155-VMIS-DUA R155-VMIS-DUA	1221 2	information							
Interesting fields × May 03 04:10:08 PM	R155-VM15-DLA	3221 2	information							
action C + May 03 04:10:08 PM	R155-VM15-OLA	3221 2	information							
addl_dane C + May 03 04.09.40 PM	R155-VM15-DLA	3221 2	information							
addLinfo C + May 03 04:09:28 PM	R155-VMG-DLA	3221 2	Information							
add_info1 C + May 03 04:09:22 PM	R155-VM3-OLA	3221 2	Information							
addLinfo# Cf + May 03 04:09:21 PM	R155-VMS-CLA	3221 2	information							
add_ivfo5 C + May 03 04 00:17 PM	R155-VM3-CLA	3221 2	information							

Figure 4

NOTE: The exported log search result file will contain pivoted columns with respect to columns selected for pivoting.



Option to add multiple normalized data by using include/exclude options in log search.

To add the multiple CIM field values or data and get the results based on it

1. Click the **View field values** icon for the respective CIM field. In this example "event_id" is chosen.

Selected fields		Time	Description
Interesting fields	+	May 06 11:30:17 AM	A new binary file, which is not available in safe list, has been detected by EventTracker. Hash (MDS): 7488:2b009a/f886537952ea2:393847fc Image Rame: pcr4.dll Image File Name: C\Windows/System32\pcr4.dll Acco
action 🖸 +	+	May 06 11:30:17 AM	A new binary file, which is not available in safe list, has been detected by EventTracker. Hash (MD5): deb33d08/bf708caac08080054d4c7cc Image Name: imm32.dll Image File Name: C:\Windows\System32\imm32.dll Acc
addl_date 🖸 🕇	+	May 06 11:30:17 AM	A new binary file, which is not available in safe list, has been detected by EventTracker. Hash (MD5): 03e5c13fdc60d31fb71bb36918ac898e Image Name: sspicit.idll Image File Name: C\Windows\System32\sspicit.idll Acco
addl_info 🖸 🕇	+	May 06 11:30:16 AM	A new binary file, which is not available in safe list, has been detected by EventTracker. Hash (MD5): 421b695412fe0d5b0c0db00c51eaba1b Image Name: user32.dll Image File Name: C\Windows\System32 user32.dll Ac
addl_info1 🕑 +	+	May 06 11:30:16 AM	A new binary file, which is not available in safe list, has been detected by EventTracker. Hash (MD5): 8/Tbda89ae433bdbc950/463bac845b9 Image Name: KernelBase.dll Image File Name: C:\Windows\System32\KernelBa
addl_info4 🕑 +	+	May 06 11:30:16 AM	A new binary file, which is not available in safe list, has been detected by EventTracker. Hash (MD5): d5669294178a7d48c318ef22d5685ba7 Image Name: conhost.exe Image File Name: C:\Windows\System32\conhost.ex
addl_info5 🗹 +	+	May 06 11:30:16 AM	Network connection opened. Type: TCP IP Version: 4 Local Address: 172329.133 Local Hostname: R1S5-VM3.ntpl.local Local Port: 62088 Remote Address: 172329.133 Remote Hostname: R1S5-VM3.ntpl.local Remote P
addl_info6 🖸 +	+	May 06 11:30:16 AM	Network connection opened. Type: TCP IP Version: 4 Local Address: 172.32.9.133 Local Hostname: R1S5-VM3.ntpLlocal Local Port: 62088 Remote Address: 172.32.9.133 Remote Hostname: R1S5-VM3.ntpLlocal Remote P
addLinfo7 🗹 +	+	May 06 11:30:16 AM	Network connection opened. Type: TCP IP Version: 4 Local Address: 172.329.133 Local Hostname: R155-VM3.ntpl.local Local Port: 62088 Remote Address: 172.329.133 Remote Hostname: R155-VM3.ntpl.local Remote P
application_name C +	+	May 06 11:30:16 AM	A new binary file, which is not available in safe list, has been detected by EventTracker. Hash (MD5): 6494e2865cb2b360Hc355e2ff1cb8d7 Image Name: qdi32.dll Image File Name: ClWindows/System32(qdi32.dll Acco

Figure 5

2. Choose the required values to be displayed from the "Values for event_id" dialog box window that appears and click Include.

Values for event_id				×
Search for cim field v	values		0, 0	2
3516	3524	☑ 3512		\sim
3514	4674	4688		
4689	3221	2008		
3222	3515	3244		
3246	102	4672		
100	200	129		
201	4648	4624		
4634	107	17137		
16	3507	3513		
4017	40961	40962		
5017	2065	8013		
4985	7036	2046		
2072	2038	30800		
3418	140	3279		
4670	318	4016		
5016	4006	4326		\sim
		Include	Exclude	ose
	Figure 6	5		

Netsurion. EventTracker

EventTracker @ • Add search to Q 1 O G Close Duration: May 05 11:55:04 AM - May 06 11:55:04 AM Total co int: 244,912 Search criteria: * ne querv Top 10 (src_host_name) Top 10 (dest_host_na Top 10 (event_computer) Top 10 (event_id) r1s5-vm3.ntpl.. 351 224.0.0.252 ff02::1:3 3524 r1s5-vm15.ntp... r1s5-vm32 r1s5-vm3.ntpl.local r1s5-vm5 172.28.9.146 phanto 📕 r1s5-vm3 📕 r1s5-vm3-dla 📕 r1s5-vm15-dla 📕 r1s5-vm15 3512 r1s5-vm15 📕 r1s6-vm1 📕 r1s6-vm1.ntpl.local 📕 et-testing-do Top 10 (src user name) Top 10 (log_source) Top 10 (tags) 📕 nt authority\network service 📒 system 📕 sugumaran.k 📕 eventtracker events 📕 ncm events 📕 traffic activities network service nt authority\system local service





To exclude the values, in the result page.

1. Click the **View field values** icon for the "event_id" CIM field.

Selected fields	(2)	lime	event_id
and id	Ť, t	• May 06 11:30:17 AM	3524
eventja	^ +	• May 06 11:30:17 AM	3524
Interesting fields	*	• May 06 11:30:17 AM	3524
addl_info C	1 + 4	• May 06 11:30:16 AM	3524
addl_info1 C	; + 4	- May 06 11:30:16 AM	3524
addl info4	. + 4	- May 06 11:30:16 AM	3524
		- May 06 11:30:16 AM	3524
addl_intob	4	May 06 11:30:16 AM	3524
addl_info6	+ +	• May 06 11:30:16 AM	3524



2. Choose the values from the "Values for event_id" dialog box window and click Exclude option.



Values for event_id							
Search for cim field values			Q	Q			
3516	3524	☑ 3512					



3. The excluded value is highlighted in orange color.

ELASTIC CACHE			Event Tracker a
Duration: May 05 11:5504 AM - May 06 11:5504 AM Search criteria: " Show Learner query Care filters event Jel: 3516 X event Jel: 3534	X event (dd: 3512 X	revent, lift. 3512 X	Add search to Q E O E O Coar Total count: 155,174
Top 10 (src, host_name) 224.0.0.252 102::1:3 r1s5-ym3.ntpi 1155-ym15.ntp	Top 10 (dest,heat_name)	Top 10 (event, computer)	Top 10 (event_3d)
Top 10 (src.user,name)	Top 10 (log_source) eventtrasker eventtrasker	eventiracker events a traffic activities	Activate Windows Go to Settings to activate Windows.



NOTE: The same changes apply for both Cache Search and Archive search.



Option to move systems from one group to other in System Manager.

User is provided with an option to select the system and move to any other groups.

To move the system to other groups.

1. Click Admin option from the Home page and choose Systems.

+	-> O @ O rtd-and total territories age						日 ☆	白尾的
=	EventTracker B						🖉 Admire	Sale 💿
	Home		E Active Webs Link	Dependo Gil Gent Files (1)	Manager Planter Manager Planter	/ Battored / Hyree		
	1 Indications of Compromise URL adviction, have any orthogon many	3 Network Standar Denati International Control of Standard Standar		1887.7K Non datlet	Behavior Constantion Rul Constantion Text Constantion Constantion Ser Constantion Configuration + Constantion Configuration	In Statistics Activity of the State	Conservation Conse	
	Nay 12 EP	0	Catch of the Day I Catcherer The Network A Mine Revenience A Mine Revenience A Mine Revenience A Mine as a Society Minage Mine A Mine A Mine Mine A Mine A Mine A Mine Mine A Mine A Mine A Mine A Mine A Mine Mine A Mine A Mine A Mine A Mine A Mine Mine A Mine A Mine A Mine A Mine A Mine Mine A Mine A Mine A Mine A Mine A Mine A Mine Mine A Mine A Mine A Mine A Mine A Mine Mine A Mine A Mine A Mine A Mine A Mine A Mine Mine A Mine A Mine A Mine A Mine A Mine A Mine Mine A Mine A	gg common from CDR optohes Empore at MSP1 and the CDR to model CDR to allower Born CDR and SIMM To discuss Service worder at managed retroom Common or Information Common of Information Common and Teoparop of Information and Incoded.				
	Incident Trand	() - Unknows Process			0 - Targe			0 +
			Data for		o			8
			Figure 1	11				

2. In the Systems Manager Page, click **Groups** icon.



≡	EventTracker 🕀							•	Admin + Tools + 🔘 +
	Systems								🕈 / Admin / Systems
Q R	9 Non Reporting Systems Systems not reporting since the last 24 hours		0 Popper1Satus Popper1satus			Managed anaged system count	a Even Versio	53 - foor 16 51 - load 13 Tracker Sensor Version	
	< Groups	Systems							
	Create Group Delete Group	Request Status Non Reporting Systems Search All Domain Computers Type hore	Computers System Report Auto Discover	Q			Page size 25	Sort by columns	Managed: 20
	All Groups O Default Ó	< 1 of1 > 60							
	Domain Controllers	Computer		Туре	Port	EventTracker version	Change audit version	Asset value	
	EventTracker Ö	192.168.1.55-syslog		Syslog	514	Managed	-NA-	Low	9
	Firewall Devices	json-DLA		2003	14505			Undefined	0
	Network Devices	NTPLDTBLR33		Win 8.1	14505	9.0 - Build 18		Low	9
	NTPL Ö	NTPLDTBLR33-DLA		Win 8.1	14505	-		Low	Q
	VmWare Ö	R1		Unknown	14590	9.0 - Build 18	-	Undefined	<u>Q</u>
	Win 7 and Server 2008 Above	R1S3VM1~Netsurion		2008 R2	14555	9.0 - Build 18	-	High	Q
	Win XP and Server 2003	R1S3VM1~Netsurion-DLA		2008 R2	14555	-	-	High	9
		R1S4-VM1~Netsurion		Win 7	14505	9.1 - Build 19	-	Low	9
		R1S4-VM1~Netsurion-DLA		Win 7	14505	-	-	Low	9
		R1S4-VM3-Prism		Win 8.1	14505	9.1 - Build 19	-	Low	Q
		R1S4-VM3-Prism-DLA		Win 8.1	14505	-	-	Low	Q
		R1SS-VM15		2012 R2	14505	9.0 - Build 18		High	Q
		R1SS-VM1S-DLA		Unknown	14505			Undefined	Q
		R155-VM3		2012 R2	14505	9.0 - Build 18	9.0 - Build 18	Serious	Q
		R1SS-VM3-DLA		2012 R2	14505			Serious	Q
		KISS-VM/~lesong		2016	14525	9.0 - 8010 18		High	Q
		KIDO-VM1~Prism		2016	14505	yu - suid 18	-	High	0
		R156-VM1~Phsm-DLA		2016	14505	-	-	High	Q
		TESTOLACSV-DLA		2003	14505	-	-	Undefined	9
		vcentertesto-s.ntpt.local@R1SS-VM3-VMWARE		VMWare	14505	9.0 - Suid 18	-	High	Q.

Figure 12

3. Click [©] **Tools** icon and choose **Move System** option.

₽ €	EventTracker :: Home	2	TechSmith Snagit, Screen (How to Edit a Screenshot !	EventTracker :: System C $ imes $	EventTracker ::	Home	+ ~			- 0
\leftarrow	→ Ŭ ŵ O) r1s5-v	n3:8080/EventTracker/Admin/Syst	tems/Default.aspx						□ ☆	\$ L &
Ev	entTracker⊕									4	👂 Admin+ Tools+
■ Sy	stems										🔒 / Admin /:
) Kon Reporting Systems stems not reporting since the last 24 hours Groups	Details Folia Move sy Install a	stems perufstant pol	0 Request Status Satus of wirksa werear requests			20 Managed vs Unm Managed/Unmanaged	Margard R anaged system towel	10 state State Wester by court	uid 19	
	Croups Create Group Delete Group	Uninsta Upgrad Restart : Agent s Query fi C Remove TOOIS ^{® 1} Manage Query fi	I agent/Stop poll agent service envice status e agent cervision agent components ystems asset value of 1 > CO	Search Computers System Report Auto Di	cover C				Page tite 25	Sort by columns	Managed: 20
	Jefault	9	Computer			Туре	Port	EventTracker version	Change audit version	Asset value	
	Jornain Controllers ventTracker	0	192.168.1.55-syslog			Syslog	514	Managed	-NA-	Low	
	irewall Devices	0	json-DLA			2003	14505	-		Undefined	
	letwork Devices	0	NTPLDTBLR33			Win 8.1	14505	9.0 - Build 18	-	Low	
	ITPL	0	NIPLDIBLR3S-DDA			Win 8.1	14505			LOW	
	fmWare	0	R1S3VM1-Naturity			2008 82	14555	9.0 - Build 18		High	
	Vin 7 and Server 2008 Above	0	R1S3VM1~Netsurion-DLA			2008 R2	14555			High	
	Vin XP and Server 2003	9	R1S4-VM1-Netsurion			Win 7	14505	9.1 - Build 19		Low	
			R1S4-VM1~Netsurion-DLA			Win 7	14505	-		Low	
			R1S4-VM3~Prism			Win 8.1	14505	9.1 - Build 19		Low	
			R1S4-VM3-Prism-DLA			Win 8.1	14505			Low	
			R155-VM15			2012 R2	14505	9.0 - Build 18		High	
			R1SS-VM15-DLA			Unknown	14505	-	-	Undefined	
			R155-VM3			2012 R2	14505	9.0 - Build 18	9.0 - Build 18	Serious	
			R1SS-VM3-DLA			2012 R2	14505	••		Serious	
			R1S5-VM7~Testing			2016	14525	9.0 - Build 18		High	
			K150-VM1~Prism			2016	14505	9.0 - Bulla 18	-	High	
			K150-VM1+Phsm-DLA			2010	14505			High	
			vrantartatt6-5 nml local@R155 UM2 UMA	4.05		VMWara	14005	00 - Build 18		High	
			record testor a mprovenen rad-VMD-VMM			- MINTER C	14000	2.0 0000 t0		cigit	

Figure 13

Netsurion... EventTracker

4. "Move Systems from group" window opens.

elect group	
Domain Controllers	~
elect Systems	
Search	Q
192.168.1.55-syslog	
json-DLA	
NTPLDTBLR33	
NTPLDTBLR33-DLA	
R1	
R1S3VM1~Netsurion	
R1S3VM1~Netsurion-DLA	
R1S4-VM1~Netsurion	

Figure 14

- 5. Select Group from the drop-down option you want to move from and Select Systems from the list.
- 6. Click **Move** button to move the systems from the selected group.

