Netsurion. EventTracker

Terminal Services Gateway

EventTracker v9.2 and above

Publication Date: July 2, 2020

Abstract

The purpose of this document is to help users to monitor Microsoft Windows **Terminal Services Gateway** by deploying Windows Agent.

Scope

The configuration details in this guide are consistent with **EventTracker** version 9.2 and later, **Terminal Services Gateway**.

Audience

Administrators who want to monitor the Terminal Services Gateway 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 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.

© 2020 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.	Introduction	3
2.	Pre-requisite	3
3.	EventTracker Agent configuration	3



1. Introduction

Windows Server 2008 Terminal Services Gateway (TS Gateway) is a role service that enables authorized remote users to connect to resources on an internal corporate or private network, from any Internet-connected device that can run the Remote Desktop Connection (RDC) client. The network resources can be terminal servers, terminal servers running RemoteApp programs, or computers with Remote Desktop enabled.

EventTracker gathers and examines acquired logs to identify terminal server configurations, terminal server connections, terminal server desktop host activity. It generates reports for terminal services user session connected, user session disconnected, user authentication success, user authentication failed, and network traffic activity. It displays authentication success and failed with username's, user session connected, and network traffic by systems. It alerts the users when terminal services gateway is shutting down and user authentication fails.

2. Pre-requisite

Prior to configuring Windows Server 2008 and later and EventTracker 9.2 and later, ensure that you meet the following prerequisites.

- Administrative access on EventTracker.
- User should have Administrative rights on Microsoft Windows Terminal Server.

3. EventTracker Agent configuration

- 1. Deploy EventTracker Agent in Terminal Services Server, please follow the steps mentioned in <u>How to</u> <u>Install EventTracker and Change Audit</u>.
- 2. Click Start >All Programs>Prism Microsystems> EventTracker.
- 3. In EventTracker Control Panel, double-click EventTracker Agent Configuration.
- 4. Select Event Filters tab, and then click the Filter Exception button.

Terminal Services Gateway

🗳 EventTracker Agent Configuration	×
File Help	
C Select Systems	
ETMANGER Agent based system	
Apply the following settings to specified Agents	
Apply the following settings to specified Agents	
Manager destinations:	_
ETMANGER	
Services Log Backup Processes Network Connections	
Logfile Monitor File Transfer Config Assessment syslog FTP server	i.
Managers Event Filters System Monitor Monitor Apps	ĺ
Event Logs Event Types Application Error Cisco AnyConnect VPN Client Warning HardwareEvents Information Internet Explorer Audit Success Media Center Audit Eailure Enable SID Translation Verbose	
Event Description: O Classic C XMI	
Filter Exception Advanced Filters	
<u>S</u> ave <u>Close</u>	

Figure 1

5. Filter Exception window displays. Click **<u>N</u>ew**.

Filter Exception 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 Service.									
Log Type	Event Type	Cate	Eve	Source	User	Description	*		
		0	102	Microsoft					
		0	100	Microsoft					
	Audit Success	0	593						
	Audit Success	0	592						
	Audit Success	0	512						
	Audit Success	0	513						
	Audit Success	0	516						
	Audit Success	0	517						
	Audit Success	0	520						
	Audit Success	Π	552				Ψ.		
4 III >									
<u>N</u> ew	<u>E</u> dit	Dele	ete	Find		<u>C</u> lose			





6. Event Details window opens. In Match in <u>Source</u> box enter 'Microsoft-Windows-TerminalServices-Gateway'.

📮 Edit Event Details	×						
Event Details (empty field implies all matches Log Type :]						
<u>E</u> vent Type :	Event <u>I</u> D :						
•							
Category :	Match in <u>U</u> ser :						
0							
Match in <u>S</u> ource :							
Microsoft-Windows-TerminalServices-G-							
Match in Event <u>D</u> escr :							
"Match in Event Descr", "Match in User" and "Match in Source" 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 D0 NOT contain "Logon Type: 4" or "Logon Type: 5" in the description. For more information click here.							
OK	Cancel						

Figure 3

- 7. Click **OK**.
- 8. Save the configuration and Close the EventTracker Agent Configuration window.



🖙 EventTracker Agent Configuration	83
File Help	
Select Systems ETMANGER Agent based systems Apply the following settings to specified Agents 	stem
<u>M</u> anager destinations: ETMANAGER	
Services Log Backup Processes Network Connec Logfile Monitor File Transfer Config Assessment syslog FTP Managers Event Filters System Monitor Monitor You can choose to filter out events that are not required. Once the filter is	ctions server Apps set,
all events matching the filter criteria will not be sent to the Event Fracker Manager. You can also configure advanced filter options such as to send specific events or choose to filter out specific events. Event Logs Application Cisco AnyConnect VPN Client HardwareE vents Internet Explorer Key Management Service Media Center Citical Enable SID Iranslation Event Description: Classic © XML	ess e
Filter Exception Advanced Fil	ters
<u>Save</u>	

Figure 4

