EventTracker:

Actionable Security Intelligence

Integrate Citrix Access Gateway

Publication Date: September 3, 2015

Abstract

This guide provides instructions to configure Citrix Access Gateway to transfer logs to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 7.X and later.

Audience

Citrix Access Gateway users, who wish to forward event logs to EventTracker Manager and monitor events using EventTracker.

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

This document is for informational purposes only. EventTracker 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 EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker 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 EventTracker, 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.

© 2017 EventTracker Security LLC. 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
Scope	. 1
Audience	. 1
Overview	. 3
Configuring Citrix Access Gateway Event Logging To Configure the Remote Server:	. 3 . 3
To transfer log files to the remote server	. 5
Configure DLA for Log transfer into EventTracker:	. 6
Configure Freesshd server for log transfer in EventTracker Machine.	. 6
DLA Configuration for log transfer in EventTracker Machine	. 8



Overview

Citrix NetScaler Gateway is a secure application access solution that provides administrators granular application-level policy and action controls to secure access to applications and data while allowing users to work from anywhere. The solution gives IT administrators a single point of control and tools to help ensure compliance with regulations and the highest levels of information security across and outside the enterprise. At the same time, NetScaler Gateway empowers users with a single point of access—optimized for roles, devices, and networks—to the enterprise applications and data they need. This unique combination of capabilities helps maximize the productivity of today's mobile workforce.

Configuring Citrix Access Gateway Event Logging

You can archive Access Gateway event logs to an external server. You can also manually save and archive the files or can automatically archive the files at scheduled intervals.

To Configure the Remote Server:

- 1. In the Access Gateway Management Console, click Management.
- 2. Under System Administration, click Logging.

	Here working								
letworking									
Appliance Failover	You can configure A: the P address of the	ccess Gate appliance.	way settings specific Configure the P addres	to this appliance. Click an IP as as internet Protocol versi	address in the Netw on 4 (IPv4).	ork adapters list to	change		
Vame Service Providers									
itatic Routes									
ddress Pools	Host name		citrile.net						
Jeployment Mode									
assword	Network adapters:					Adar	ater Boles		
Date and Time		Name	IP address	Subnet mask	Internal	External	Appliance Failo	Management	
icensing		eth0	192.168.2.2	255 255 255 0	1	~		1	
ogging					had	Los	End	had .	
		Edit							
Access Control									
Access Control									
Interstant Control Interstant Co	Acc	ess Gatev	vay Properties	t	efault Gateway				
Iobal Options uthentication Profiles letwork Resources	ACC	ess Gatev	vay Properties	I Network Interface:	efault Gateway eth0 🛛 👻				
In the set of the set	Secure port 443	ess Gatev	vay Properties	I Network Interface	eth0 •				
Access Control Clobal Options Authentication Profiles Vetwork Resources Device Profiles Logon Points	Secure port + 443	ess Gatev	vay Properties	I Network Interface: IP address: •	ethul (•) 92.168.2.1				
Interface Control Interface Co	Acc Secure port + 443	ess Gatev New ICMP Inable supp Redirect HT	vay Properties requests ort access IP to HTTPS	I Network Interface IP address. ●	eth0 • 92 168 2 1				
In the second se	Acc Secure port # 443 V # V #	ess Gatev Now ICMP inable supp Redirect HT	vay Properties requests orf access TP to HTTPS	I Network Interface: IP address: +	eth0 • 92.168.2.1				
kccess Control Ilobal Options uthentication Profiles letwork Resources voice Profiles ogon Points imartGroups pplications and Desktops enApp or XenDesktop	Acc Secure port # 443 V F	ess Gatev Now ICMP Inable supp Redirect HT	vay Properties requests off access TP to HTTPS	I Network Interface: Paddress: +	efault Gateway eth0 • 92.168.2.1				

Figure 1



- 3. In the Access Gateway Logging panel, under **Remote Server Settings**, set the following options:
 - a. In **Server**, type the IP address or host name of the remote server (EventTracker Machine).
 - b. In **Username**, type the user name.
- 4. In **Password**, type the user's password.
- 5. In **Confirm password**, retype the password.
- 6. In Transfer protocol, select one of the following:
 - a. **SCP**. The Secure Copy Protocol (SCP) allows you to transfer files from one computer to another with encryption through the Secure Shell (SSH) protocol.
 - b. **FTP**. The File Transfer Protocol (FTP) allows you to transfer files from one computer to another without encryption.
- 7. In **Por**t, type the port number for the server.
- 8. In **Remote directory**, type the path of the directory in which you want to store the log files on the remote server.
- 9. In **Log type**, select one or more types of log file that you want to archive on the remote server: EPA, Info, and Audit.
- 10. Click Save.

Access Gateway		Help Logout	CITRI2
Monitor Management Certificates	Snapshots	Search Restart	Shut Down
System Administration Networking Appliance Failover	Access Gateway Logging frequency of archiving log files automatically or logs, click Monitor, and then click Show.	you can manually save and transfer the logs. To view	i
Name Service Providers Static Routes Address Pools Deployment Mode	Log Settings Use local time in logs Archive logs every:	Remote Server Settings Server:	
Password Date and Time Licensing Logging	✓ Transfer archived log files automatically Transfer logs every. 8 + hours	Password:	-m
Access Control Global Options Authentication Profiles Network Resources		Port:	
Device Profiles Logon Points SmartGroups	Transfer llow	Save C	ancel

Figure 2



To transfer log files to the remote server

You can transfer log files to the remote server manually or you can schedule automatic archives.

- 1. In the Access Gateway Management Console, click Management.
- 2. Under System Administration, click Logging.
- 3. In the Access Gateway Logging panel, under Log Settings, set the following options:
 - a. To use the local time in the log files, select the Use local time in logs check box.
 - b. To change the scheduled intervals in hours at which log files are archived locally, in **Archive logs every**, select 4 or 8 hours.
 - c. To archive log files automatically, select the **Transfer archived log files automatically** check box and then in **Transfer logs every**, select the frequency with which you want the archived files transferred to the remote server, 4, 8, or 16 hours.
 - d. To manually save and transfer the log files immediately, click Transfer Now button.

Access Gateway		Help L	ogout CiTR Close this mes
Monitor Management Certificates	Snapshots	Search Res	start Shut Dow
System Administration Networking Appliance Failover Networking	Access Gateway Logging frequency of archiving log files automatically or logs, click Monitor, and then click Show.	you can manually save and transfer the logs. To view	i i
Static Routes Address Pools Deployment Mode Password Date and Time Licensing Logging Access Control Global Options	Log Settings Use local time in logs Archive logs every: Transfer archived log files automatically Transfer logs every: Image: Constraint of the set	Remote Server Settings Server: 192.168.1.118 Username: root Password: ******* Confirm password: ******* Transfer protocol: SCP Port: * 22 Remote directory: *	
Authentication Profiles Network Resources Device Profiles Logon Points	Transfer How	Log type: V EPA V Info Audit * Indicates required field	T
SmartGroups			

Figure 3



Configure DLA for Log transfer into EventTracker:

Configure Freesshd server for log transfer in EventTracker Machine.

Follow the below mentioned steps for the configuration of log transfer into EventTracker:

- 1. Download and install <u>freesshd</u> server in EventTracker Machine.
- 2. Configure User (e.g root) in freesshd server setting
- 3. Click the Add... button

nreeSSHd set	tings				• 💌
Server status Users	Telnet SSH Host restrictions	Authentication Logging On	Encryption line users	Tunneling	SFTP
Add	Change	Remove]		2
Login		Shell	SFTP	Tunnel	
🤱 root		۲	۲	۲	^
	\$				
		ОК		Cancel	Apply



4. Enter the Login (e.g root), select the Authorization type, and enter the Password and select the Option User can use.



🚨 User properties	
General	
	•
ß	🍝
Login:	root
Authorization:	Password stored as SHA1 hash
Password:	*****
Password (again):	XXXXXX
Domain:	
User can use:	 ✓ Shell ✓ SFTP ✓ Tunneling
	OK Cancel Apply

Figure 5

5. Please specify the directory where you want to stored logs by going to **SFTP** tab.



n freeSSHd settings	- • •
Users Host restrictions Logging Online users Server status Telnet SSH Authentication Encryption	Automatic u <u>pdates</u> Tunneling SFTP
	<i>i</i>
SFTP home path: SFTP home path:	
OK Can	cel Apply

Figure 6

6. Please use Same User and directory for Citrix Access Gateway log transfer configuration.

DLA Configuration for log transfer in EventTracker Machine

- 1. Login to EventTracker Enterprise.
- 2. Click Admin dropdown, and then click Manager.
- 3. Click Direct Log Archiver tab.
- 4. Click Direct log file archiving from external sources option.
- 5. Click the Add button.



N	MANAGER CONFIGURATION							
cc	NFIGURATION	sysiog / VIRTUAL COLLE	CTION POINT	DIRECT LOG ARCHIVER	AGENT SETTINGS	E-MAIL CONFIGURATION		
ST	ATUSTRACKER	COLLECTION MASTER F	PORTS					
[Direct log file arch	iving from external sources	Ρ	Purge files after 0 days	ASSOCIATED	VIRTUAL COLLECTION POINT		
		CONFIGURATION NAME	LOC EILE EXTENSIO	IN CIFLID SEDADATOD		LOG TYPE		
	G:\TVReportoutput	teamviewerreports	CSV	Comma - [Fields containing	comma are wrapped in doub	LOG TYPE		

Figure 7

EventTracker displays Direct Archiver Configuration window.

Direct Archiver Configurati	on	×
Туре	•	Â
Configuration Name		
Log File Folder	BROWSE	
Field Separator	Comma - [Fields containing cc 🔻	
Starting Line Offset	0	
Extract field names from header		
	CONFIGURE	CANCEL

Figure 8

6. In **Type** dropdown, select the type as **Others**.



- 7. Enter Logfile Extension as TXT.
- 8. Enter Configuration Name.
- Click the Browse... button to select the Log File Folder path. (OR)

Type the Log File Folder path in the text box.

- 10. Select Single Line Radio Button.
- 11. In Starting Line Offset let it be zero by default.

Direct Archiver Configuration					
Туре	Others •				
Logfile Extension	ТХТ				
Configuration Name	Çittix access gateway]			
Log File Folder	C:\Users\gurmukhnishan\logs	BROWSE			
Field Separator	● Single Line ○ Multi Line				
Starting Line Offset	0				
	C ₂	CONFIGURE CANCEL			



12. Click the **Configure** button.

Logfile configuration pane displays.



Direct Archiver Configuration		×
l og file configuration		^
Configuration Name	C:\Users\shalendra\Desktop\Linux Monitoring'	
Log Source		
Computer Name		
Computer IP		
	GET IP	
System Type	Unknown	
System Description		
Comment Line Token		
O Entire Row as Description	In Formatted Description	
Log File Format	•	
Message Fields	ADD	
	A	
	•	-

Figure 10

- 13. Enter Log Source, Computer Name, Computer IP, System Type and System Description.
- 14. Leave blank the **Comment Line Token** field.
- 15. Select Entire Row as Description option, if not selected.



Direct Archiver Configuration		(X)
Log file configuration		
Configuration Name	C:\Users\gurmukhnishan\logs\Citrix access gate	
Log Source	Citrix Access Gateway	
Computer Name	CAG	
Computer IP	192.168.1.85	
	GET IP	
System Type	Win 7 T	
System Description	OS	
Comment Line Token		
Entire Row as Description	O Formatted Description	
Log File Format		
Message Fields	ADD	
	PEMOWE	-

Figure 11

16. Click the Save & Close button.

The relevant folder is configured in the DLA folder.



NEIGURATION	syslog / VIRTUAL COLLECTION POINT		DIRECT LOG ARCHIVER	AGENT SETTINGS	E-MAIL CONFIGURATION
ATUSTRACKER	COLLECTION MA	STER PORTS			
B Direct log file an	chiving from external sou	#oes	Purge files after 0 days	ASSOCIA 14505	TED VIRTUAL COLLECTION POIN
LOG FILE FOLDER		CONFIGURATION NAME	LOG FILE EXTENSIO	N FIELD SEPAR	ATOR LOG TYPE
C/Users/L **	in Nogs 🔓	Citrix access gateway	TXT		

Figure 12

17. Click the Save button.

Now Direct Log Archiver (DLA) has been created successfully. Check the logs in search option of EventTracker.

- 18. Click the **Search** menu, and then select **Advanced Search**. Advanced Log Search window displays.
- 19. Select the required systems.
- 20. In Custom Criteria pane, select Add custom criteria.
- 21. In Search in drop down, select Description.
- 22. In **Operator** drop down, select **contains**.
- 23. In **Search for** box, enter **any key word** related to log description like DiskMon, and then click the **Search** button.





Figure 13

Log Search results display.

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE			
Collapse all 1:02:39 AM	<u>3230</u>	BENDER / <u>CAG-DLA</u>	SYSTEM	NT AUTHORITY	Citrix Access Gateway	<u>^</u>		
Event Type: Information	Descript sessio	tion: on						
Category Id: 2	201508271031.58 AG: (error): Failed to transfer info 20150825_2000.txt to citrix@10.0.30.56:22: Failure establishing ssh session							
	20150	08271032.03 AG: (error): Faile	ed to transfer info_20	150825_1600.txt to citrix(@10.0.30.56:22: Failure establishing ssh session			
	20150	08271032.08 AG: (error): Faile	ed to transfer info_20	150825_1200.txt to citrix@	@10.0.30.56:22: Failure establishing ssh session			
	20150	08271032.13 AG: (error): Faile	ed to transfer info_20	150825_0800.txt to citrix@	@10.0.30.56:22: Failure establishing ssh session			
	20150	08271032.18 AG: (error): Faile	ed to transfer info_20	150825_0400.txt to citrix(@10.0.30.56:22: Failure establishing ssh session			
	20150	08271032.23 AG: (error): Faile	ed to transfer info_20	150825_0000.txt to citrix(@10.0.30.56:22: Failure establishing ssh session			
	20150	08271032.28 AG: (error): Faile	ed to transfer info_20	150824_2000.txt to citrix(፬10.0.30.56:22: Failure establishing ssh session			
	20150	08271032.33 AG: (error): Faile	ed to transfer info_20	150824_1600.txt to citrix(@10.0.30.56:22: Failure establishing ssh session			
	20150	08271032.38 AG: (error): Faile	ed to transfer info_20	150824_1200.txt to citrix(@10.0.30.56:22: Failure establishing ssh session			
	20150	08271032.43 AG. (error): Fail	ed to transfer info_20	150824_0800.txt to citrix(@10.0.30.56.22: Failure establishing ssh session			
	20150	08271032.48 AG: (error): Faile	ed to transfer info_20	150824_0400.txt to citrix(a10.0.30.56:22: Failure establishing ssh session			
	20150	08271032.58 AG: (error): Faile	ed to transfer info_20	150823_2000.txt to citrix(@10.0.30.56:22: Failure establishing ssh session			
	20150	08271033.03 AG: (error): Faile	ed to transfer info_20	- 150823_1600.txt to citrix(@10.0.30.56:22: Failure establishing ssh session			



