

How to Configure NetWrix File Server Change Reporter to Monitor NetApp Filer CIFS Shares

TECHNICAL ARTICLE

April/2012

Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from NetWrix Corporation of any features or functions discussed. NetWrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice.

NetWrix is a registered trademark of NetWrix Corporation. The NetWrix logo and all other NetWrix product or service names and slogans are registered trademarks or trademarks of NetWrix Corporation. Active Directory is a trademark of Microsoft Corporation. All other trademarks and registered trademarks are property of their respective owners.

Disclaimers

This document may contain information regarding the use and installation of non-NetWrix products. Please note that this information is provided as a courtesy to assist you. While NetWrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-NetWrix product and contact the supplier for confirmation. NetWrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-NetWrix products.

© 2012 NetWrix Corporation.

All rights reserved.

www.netwrix.com

Table of Contents

1.	INTRODUCTION
	1.1. Overview
	1.2. How This Guide is Organized 4
2.	MANAGEMENT ACCOUNTS
	2.1. File Server Change Reporter Access Account
	2.2. NetApp Management Account 5
3.	NETAPP FILER COMMAND PROMPT OVERVIEW
	3.1. Accessing the Command Prompt
	3.2. Basic Configuration Commands 6
4.	CONFIGURING NETAPP FILER SETTINGS
	4.1. Configuring Qtree Security
	4.2. Configuring Admin Web Access
	4.3. Configuring CIFS Auditing
	4.3.1 Configuring Audit Events Categories
	4.3.2 Configuring the Security Log
	4.3.3 Specifying the Security Log Shared Folder
5.	CONFIGURING AUDIT SETTING FOR THE CIFS FILE SHARES
6.	CONFIGURING NETWRIX FILE SERVER CHANGE REPORTER
7.	CONFIGURING AUTOMATIC DELETION OF SECURITY LOG AUTO ARCHIVES
Α	Appendix: Related Documentation

1. INTRODUCTION

1.1. Overview

This article is intended to help you configure NetWrix File Server Change Reporter and set up reporting on modifications and access events to the files, folders and shares of your NetApp[®] filer instance.

NetWrix File Server Change Reporter supports auditing of NetApp[®] filer CIFS shares since version 2.0. If you are running an older version, you can download the latest product edition from <u>NetWrix File Server Change Reporter website</u>.

Note: NetApp Filer is only configurable and available in the NetWrix File Server Change Reporter Standard configuration mode of the Enterprise Edition.

1.2. How This Guide is Organized

This section explains how this guide is organized and provides a brief overview of each chapter.

- Chapter <u>1 Introduction</u>: the current chapter. It explains the purpose of this document and outlines its structure.
- Chapter <u>2 Management Accounts</u>: lists all privileges and access rights required for NetWrix File Server Change Reporter access account and the NetApp management account.
- Chapter <u>3 NetApp Filer Command Prompt Overview</u>: explains how to access the NetApp filer command line and lists the basic configuration commands.
- Chapter <u>4 Configuring NetApp Filer Settings</u>: provides instructions on how to configure your NetApp filer to be monitored by NetWrix File Server Changer Reporter.
- Chapter <u>5 Configuring Audit Setting for the CIFS File Shares</u>: explains how to configure audit settings for the CIFS file shares.
- Chapter <u>6 Configuring NetWrix File Server Change Reporter</u>: provides instructions on how to configure NetWrix File Server Change Reporter to monitor NetApp filer CIFS shares.
- Chapter <u>7 Configuring Automatic Deletion of Security Log Auto Archives</u>: explains how to enable automatic deletion of your security log archives.
- <u>A Appendix: Related Documentation</u>: lists all documentation published to support NetWrix File Server Change Reporter.

2. MANAGEMENT ACCOUNTS

This chapter explains the requirements to the NetWrix File Server Change Reporter access account and the NetApp filer management account. Please ensure that these accounts have the necessary access permissions and rights listed below.

2.1. File Server Change Reporter Access Account

On NetWrix File Server Change Reporter configuration, you are prompted to enter an account that will be used by the system for data collection and report generation. This must be a domain user account with the Domain Administrator rights, or with the following access permissions:

- Access to the file shares you are going to monitor ('read' access at least);
- Access to the security log shared folder ('read' access at least; 'write' access is required for automatic log deletion (for details, see Chapter <u>7</u> <u>Configuring Automatic Deletion of Security Log Auto Archives</u>).

2.2. NetApp Management Account

The NetApp management account is required to perform the operations related to the security log, and to validate audit settings against NetWrix File Server Change Reporter requirements.

This must be a domain or a NetApp filer local account with the following set of capabilities:

- login-http-admin;
- api-system-cli;
- api-options-get;
- cli-cifs.

These capabilities can be configured using the NetApp filer command prompt (for instructions on how to access the command prompt, refer to Chapter <u>3_NetApp Filer</u> <u>Command Prompt Overview</u>):

Figure 1: Management Account Configuration

```
apphost01> useradmin user list fscr_user

Name: fscr_user

Info:

Rid: 131077

Groups: fscr_group

Full Name:

Allowed Capabilities: login-http-admin,api-system-cli,api-options-get,cli-cifs

Password min/max age in days: 0/4294967295

Status: enabled

apphost01>
```

3. NETAPP FILER COMMAND PROMPT OVERVIEW

3.1. Accessing the Command Prompt

The NetApp filer command prompt is accessible through SSH/Telnet connection (depending on your NetApp filer settings), or via the web interface.

To access it via the web interface, open the NetApp filer web GUI, and navigate to FilerView > Filer > Use Command Line:

	Internet Explorer			
🔇 💭 👻 🙋 http://apphost01/na	a_admin/		💌 🍫 🗙 Live Search	P -
File Edit View Eavorites Tools	Help			
	. inste	1		Pres (2) Tesla >>
🔀 🐼 🌽 apphost01: FilerView			🔟 T 🖸 T 🖷 T 🗹	Page + Or Tools +
LeC NetworkAppliance		000 ⁰¹¹¹¹⁰⁰⁰¹¹¹¹		Search About
	Data	ONTAP ^{III}	1	
FilerView® helps	s you configure and mo	nitor your filer.		
Filer At-A-Gland	ce monitors the perform	ance of your file	er.	
Operations Man	nager links are not ena	bled. <u>Click here</u>	to enable links.	
Documentation ROM or the NOV	n is not installed . <u>Click</u> <u>V site</u> .	<u>here t</u> o install t	ne ZIP file from the Data ONT	AP™ CD-
Simulator Docu	umentation is installed			-1
Done			Local intrapet	100%
<u>v</u> e			100100100 6001111	VIEW
Network Appliance*			aaddaf []]] [] 8899]	11160001
Network Appliance*			**************************************	Search About
NetworkAppliance*		l line @		Search About
NetworkAppliance*	Use Command Filer → Use Command	J Line ⑦		Search About
NetworkAppliance*	Use Command	1 Line ⑦ Line	1999,831,111,14599, [Search About
NetworkAppliance*	Use Command Filer → Use Command	1 Line ⑦ Line		Search About
NetworkAppliance*	Use Command Filer → Use Command connect ion open Data CMT#P (d Line @		Search About
NetworkAppliance*	Use Command Filer → Use Command connect i on open Dat = CMTAP (Call of the ROT_	d Line @ Line		Search About
NetworkAppliance*	Use Command Filer → Use Command connection open Det a Cht/#P (cogin: REOT apphost 01>	J Line ⑦ Line)		Search About
NetworkAppliance*	Huse Command Filer → Use Command connection open Det a CMT#PC(opin KPC(apphost 01>	J Line ® Line		Search About
NetworkAppliance*	Use Command Filer → Use Command connect ion open Dat a CMT#P (login: RCOT apphost 01>	1 Line ® Line		(Search) About
NetworkAppliance*	Her → Use Command Filer → Use Command connect ion open Dat a CMTAP (Login: ROOT apphost 01>	J Line (9) Line		Search About
NetworkAppliance*	Use Command Filer → Use Command connect i on open Det a CMTAP (Cogin: RCOT apphoet 01>	J Line ⑦ Line		Search About
NetworkAppliance* Filer © Show Status Manage Licenses Report Syslog Messages Audit Logs Use Command Line Configure Syslog Configure File System Configure Autosuport Test Autosuport	Use Command Filer → Use Command connect i on open bet a CMTAP (Logi n: ROOT apphost 01>]	J Line ® Line		Search About
NetworkAppliance*	Use Command Filer → Use Command connection open Data CMT#P (Login: ROOT apphost 01>]	1 Line ® Line		Search About
NetworkAppliance*	Huse Command Filer → Use Command connection open Det a CMT#P (ogin R ROT apphost 01>]	1 Line (® Line)		Search About
NetworkAppliance*	■ Use Command Filer → Use Command connect ion open Data CMT#P (opin ref (apphost 01>]	1 Line (® Line		Search About
NetworkAppliance*	Use Command Filer → Use Command connect i on open bet a CMTAP (Log in: RCOT apphost 01>	J Line ⑦ Line		Search About
NetworkAppliance*	Use Command Filer → Use Command connect i on open bet a CMTAP (Log in: ROOT apphost 01>]	J Line ® Line		Search About
NetworkAppliance* Eiler ① Show Status Manage Licenses Report Syslog Messages Audit Logs Use Command Line Configure Syslog Configure Syslog Configure File System Configure Miscellaneous Shut Down and Reboot Show System Status Volumes ② Aggregates ②	Use Command Filer → Use Command connect ion open Det a CMT#P (Login, ROCT apphost 01> []	J Line ® Line		Search About
NetworkAppliance*	Use Command Filer → Use Command connection open Data CMT#P (Cogin: RCOT apphost 01>]	1 Line ® Line		Search About
NetworkAppliance*	Use Command Filer -> Use Command connect ion open Det a CMT#P (opin: ROOT apphost 01>]	1 Line (® Line		Search About
NetworkAppliance*	Use Command Filer → Use Command connect i on open Det a CMTAP (to a CMTAP (opphost 01>]	Line ()		Search About

Figure 2: Accessing the Command Prompt

Note: The appearance of your NetApp filer instance may vary slightly from the screenshots used in this document.

3.2. Basic Configuration Commands

To perform the configuration procedures described in Chapter <u>4 Configuring NetApp</u> <u>Filer Settings</u> of this document, the following commands must be used: • To get an option value:

options <option name>

• To set option value:

options <option name> <option value>

For example, to enable the cifs.audit.enable option, execute the following command:

options cifs.audit.enable on

Note: For a full list of commands and their detailed descriptions, please refer to <u>NetApp command line reference document</u>.

4. CONFIGURING NETAPP FILER SETTINGS

This section explains how to configure the NetApp filer for audit by NetWrix File Server Change Reporter. The instructions in this section apply to the default VFiler. If you wish to audit several VFiler instances, you must perform these configuration steps for each of them.

The settings described in this chapter are performed via NetApp filer command line. For instructions on how to access NetApp Filer command line, and for description of some basic configuration commands, please refer to Chapter <u>3 NetApp Filer</u> <u>Command Prompt Overview</u>.

Note: It is assumed that CIFS shares have already been set up on your NetApp filer.

4.1. Configuring Qtree Security

For auditing to function properly, the volume where the monitored file shares are located must have the security style set to 'ntfs':

Figure 3: Qtree Security

```
apphost01> qtree status

Volume Tree Style Oplocks Status

vol0 ntfs enabled normal

vol0 test ntfs enabled normal

vol1 unix enabled normal

vol2 ntfs enabled normal

apphost01>
```

4.2. Configuring Admin Web Access

NetWrix File Server Change Reporter uses the NetApp API to obtain the current CIFS audit configuration and force the audit data flush from the internal filer format to the MS Event Viewer compatible format.

NetWrix File Server Change Reporter supports both the SSL and non-SSL HTTP access, trying HTTPS first, and falling back to HTTP if it is unavailable.

Make sure that httpd.admin.enable or httpd.admin.ssl.enable is set to 'on'. For security reasons, it is recommended to configure SSL access and enable the httpd.admin.ssl.enable option:

Figure 4: HTTPD. ADMIN Access

```
apphost01> options httpd.admin
httpd.admin.access legacy
httpd.admin.enable off
httpd.admin.hostsequiv.enable off
httpd.admin.max_connections 512
httpd.admin.ssl.enable on
httpd.admin.top-page.authentication on
apphost01>
```

If non-default configuration for httpd.admin.access is set (i.e. 'limit access to trusted host only' or 'allow admin web access for specific Ethernet interfaces'), make sure that the Web Filer UI is accessible by the name of the audited file server.

For example, the audit share \\file_server\my_share\ must be viewed with the NetApp filer WebUI at http(s)://file_server/na_admin/.

4.3. Configuring CIFS Auditing

4.3.1. Configuring Audit Events Categories

To configure audit event categories, perform the following steps:

- 1. Set the following options to 'on':
 - cifs.audit.enable
 - cifs.audit.file_access_events.enable
- 2. Unless you are going to audit logon events, set the following options to 'off':
 - cifs.audit.logon_events.enable
 - cifs.audit.account_mgmt_events.enable

4.3.2. Configuring the Security Log

NetWrix File Server Change Reporter supports processing of auto-saved audit logs. In order to avoid overwriting of the security logs, the following settings are recommended:

- cifs.audit.logsize 300 000 (300 MB)
- cifs.audit.autosave.onsize.enable
 on
- cifs.audit.autosave.file.extension timestamp

Also, you must disable the cifs.audit.liveview.enable option, since it interferes with the normal security log behavior and prevents NetWrix File Server Change Reporter from processing audit data properly.

Figure 5: Security Log Settings

```
apphost01> options cifs.audit
cifs.audit.account_mgmt_events.enable off
cifs.audit.autosave.file.extension timestamp
cifs.audit.autosave.file.limit 0
cifs.audit.autosave.onsize.enable on
cifs.audit.autosave.onsize.threshold 75%
cifs.audit.autosave.ontime.enable off
cifs.audit.autosave.ontime.interval 1d
cifs.audit.enable
                            on
cifs.audit.file access events.enable on
cifs.audit.liveview.enable off
cifs.audit.logon_events.enable off
cifs.audit.nfs.enable off
cifs.audit.nfs.filter.filename
cifs.audit.saveas
                          /etc/log/adtlog.evt
apphost01>
```

Note: Due to Windows Server 2003 limitations, a security log larger than 300 MB cannot be processed. If you wish to have a log that exceeds 300 MB, NetWrix File Server Change Reporter must be installed on Windows Server 2008 / Windows Vista / Windows 7. However, even on these

Windows versions, it is not recommended to set security log size to a value that exceeds 300 MB, since this may slow down security log conversion and cause performance issues.

Make sure there is enough disk space allotted to the security logs archives. Depending on the file access activity, audit data may grow rapidly, and the location specified for the security log (and security log auto archives) must be large enough to hold data until it is processed by NetWrix File Server Change Reporter (by default, data collection runs every 24 hours). To set up old logs deletion, you can configure the cifs.audit.autosave.file.limit option by specifying the maximum number of files to be stored, or enable the built-in automatic log deletion option in NetWrix File Server Change Reporter (for instructions on how to do this, refer to Chapter <u>7 Configuring Automatic Deletion of Security Log Auto Archives</u>).

4.3.3. Specifying the Security Log Shared Folder

NetWrix File Server Change Reporter accesses audit logs via a specified file share. This may be either the default administrative share (ETC\$, C\$, etc.), or a custom file share.

Use the ${\tt cifs}$ ${\tt shares}$ command to create a new file share or configure an existing share:

apphost01> c Name	ifs shares Mount Point	Description
		·
ETC\$	/etc	Remote Administration
	BUILTIN\Administrators	/ Full Control
C\$	/	Remote Administration
	BUILTIN\Administrators	/ Full Control
share1	/vol/vol0/shares/share1	
	everyone / Full Contro	1

Figure 6:	Cifs Shares	Configuration
-----------	-------------	---------------

Note: For a detailed description of the cifs shares command, please refer to <u>NetApp command line reference document</u>.

5. CONFIGURING AUDIT SETTING FOR THE CIFS FILE SHARES

To configure audit settings for the CIFS file shares, perform the following steps on the monitored file share:

- 1. Navigate to the root share folder.
- 2. Right-click it and select **Properties** from the popup menu.
- 3. Open the **Security** tab.
- **Note:** If there is no such tab, it means a wrong security style has been specified for the volume holding this file share. For instructions on how to configure the file share, please refer to Section <u>4.1 Configuring Qtree Security</u>.
- 4. Click the Advanced button, and then select the Auditing tab.
- 5. Click Edit. The following dialog will be displayed:

📕 📶	vanced Se	curity Settings for share0	(\\apphost01)			×
Audit	ting					
To v Obj	To view or edit details for an auditing entry, select the entry and then click Edit. Object name: \\apphost01\share0					
Aud	liting entries	:	(
<u>_</u>	ype	Name	Access	Inherited From	Apply To	1
Su	JCCESS	Everyone	Special	<not inherited=""></not>	This folder, subfolder	
	Add	Edit	Remove			
	Include inhe	ritable auditing entries from t	nis object's parent			
⊡ <u>Wh</u> a	Replace all e at are the re	existing inheritable auditing en	tries on all descendants <u>t access?</u>	with inheritable auditing	entries from this object	
				ОК	Cancel Apply	

Figure 7: Advanced Security Settings

6. Select the 'Success Everyone' entry, click **Edit** and make sure it is configured as shown in the figure below:

Auditing Entry for share0 (\\app	ohost01)	×
Name: Everyone		Change
Apply onto: This folder, subfolders a	nd files	•
Access:	Successful	Failed
Read attributes Read attributes Read extended attributes Create files / write data Create folders / append data Write attributes Write extended attributes Delete subfolders and files Delete Read permissions Change permissions Take ownership Annly these audition entries to ob	v V V V V V V V V V V V	
and/or containers within this cont only <u>Managing auditing</u>	ainer _	
Do Not Check	OK	Cancel

Figure 8: Auditing Entry Configuration

7. Click **OK** to save the changes.

6. CONFIGURING NETWRIX FILE SERVER CHANGE REPORTER

This chapter explains how to configure NetWrix File Server Change Reporter to monitor NetApp Filer CIFS shares.

To do this, perform the following steps:

- Launch NetWrix File Server Change Reporter Standard configuration mode (Start > All Programs > NetWrix > File Server Change Reporter > File Server Change Reporter (Standard Edition)).
- 2. Select the Enable large server support option, and deselect the Enable network traffic compression option:

Figure 9: NetWrix File Server Change Reporter Standard Configuration Main Window

	List of UNC pal	ths to check	for chang	jes:	
	UNC Path FileServer				Add
					Edit
	-				Remove
					Import
	Store data to:	C:\Program	Data\Ne	(Wrix\Mar	nagement
	Enable long-ten	m archiving f	or: 24	mont	h(s)
-1	Enable network	traffic comp	ression 🖡	2	
	Enable network traffic compression				
_				-	
7	Enable large se	rver support			
7	Enable large se NOTE: This opt	rver support	mended to	o speed u	
7	Enable large se NOTE: This opl processing of fil	rver support tion is recom le servers wit	mended to h 500 000	o speed up) files or m	p iore
~	Enable large se NOTE: This op processing of fil	rver support tion is recom le servers wit	mended to	o speed up) files or m	p lore
•	Enable large se NOTE: This opl processing of fil File Version Cor	rver support tion is recom le servers wit ntrol (based o	mended to h 500 001 on Volume	o speed up) files or m : Shadow	p iore Copy)
د	Enable large se NOTE: This opl processing of fil File Version Cor Attach the ema	rver support tion is recom le servers wit ntrol (based o il reports as a	mended to h 500 001 on Volume a CSV file	o speed up) files or m : Shadow	p iore Copy)
. <	Enable large se NOTE: This op processing of fil File Version Cor Attach the ema	rver support tion is recom le servers wit ntrol (based o il reports as a	mended tr h 500 000 n Volume a CSV file	o speed up) files or m : Shadow	p iore Copy)
	Enable large se NOTE: This op processing of fil File Version Cor Attach the ema- vanced reporting	rver support tion is recom le servers wit ntrol (based o il reports as a I (SQL SRS):	mended to h 500 000 on Volume a CSV file	o speed up) files or m : Shadow	p iore Copy) Configure
✓ ✓	Enable large se NOTE: This op processing of fil File Version Cor Attach the ema vanced reporting	rver support tion is recom le servers wit ntrol (based o il reports as a I (SQL SRS):	mended tr h 500 001 on Volume a CSV file	o speed up) files or m : Shadow	p lore Copy) Configure
⊽ Adv	Enable large se NOTE: This op processing of fil File Version Cor Attach the ema vanced reporting ail report delivery	rver support tion is recomi le servers wit ntrol (based o il reports as a (SQL SRS):) settings —	mended to h 500 001 on Volume a CSV file	o speed up) files or m : Shadow	p lore Copy) Configure
⊽ Adv Ema	Enable large se NOTE: This op processing of fil File Version Cor Attach the ema vanced reporting ail report delivery Report on mod	rver support tion is recomi le servers wit ntrol (based o il reports as a (SQL SRS):) settings — lifications:	mended to h 500 000 n Volume h CSV file	o speed up) files or m : Shadow trator@en	Copy)
▼ Adv Ema	Enable large se NOTE: This op processing of fil File Version Cor Attach the emai vanced reporting ail report delivery Report on mod Report on read	rver support tion is recomm le servers wit htrol (based of il reports as a g (SQL SRS): o settings	mended to h 500 000 m Volume a CSV file	o speed up) files or m : Shadow trator@en trator@en	Copy) Configure terprise.com terprise.com
⊽ Adv Em∂	Enable large se NOTE: This opp processing of fil File Version Cor Attach the ema vanced reporting ail report delivery Report on read SMTP Server:	rver support tion is recomme servers wit ntrol (based o il reports as a 1 (SQL SRS): 9 settings — ilifications: 1s: enterprise.c	mended to h 500 001 on Volume a CSV file adminis adminis	o speed up Diles or m Shadow trator@en trator@en Po	Configure Configure terprise.com terprise.com
▼ Adv Ema	Enable large se NDTE: This op processing of fil File Version Cor Attach the emai vanced reporting ail report delivery Report on mod Report on read SMTP Server: From address:	rver support tion is recomm le servers wit htrol (based o il reports as a (SQL SRS): settings	mended to h 500 000 m Volume a CSV file adminis adminis om r@enterp	o speed up files or m shadow trator@en trator@en Po rise.cor	Copy) Configure terprise.com terprise.com rt [25 Verify
▼ Adv Eme	Enable large se NOTE: This op processing of fil File Version Cor Attach the ema vanced reporting ail report delivery Report on read SMTP Server: From address: ditional product of	rver support tion is recomm le servers wit ntrol (based of il reports as a g (SQL SRS): p settings	mended to h 500 000 on Volume a CSV file adminis adminis om r@enterp	o speed up) files or m s Shadow trator@en trator@en Po rise.cor	Copy) Configure terprise.com terprise.com tr [25 Verify Advanced
Adv Ema Addu	Enable large se NDTE: This op processing of fil File Version Cor Attach the ema- vanced reporting ail report delivery Report on mod Report on mod SMTP Server: From address: ditional product o rt NetWrix Enterp integrated repo poter collection	rver support tion is recomm le servers wit htrol (based of il reports as a settings	mended to h 500 00 on Volume a CSV file adminis adminis adminis om r@enterp	o speed up) files or m s Shadow trator@en trator@en trator@en en rise.cor	Configure Copy) terprise.com terprise.com rt: [25 Verify Advanced Start

3. Click the **Add** button to add a UNC path. Specify the path and select NetApp Filer as the file server platform:

Figure 10: Add UNC Path Dialog

Specify the	UNC path to the folder	you want to	o audit.
JNC Path:	\\apphost01\share0		
Select file s	(example: \\server\sha erver platform	re\folder)	5978
C Micro	osoft Windows		
C EMC	VNX/VNXe/Celerra		
Net ^A	pp Filer		Configure
Select type	s of access you want to	monitor-	-
Suce	essfull modifications		
🗖 Faile	d modification attempts		
E Suce	essfull reads		
E Faile	d read attempts		

4. Click **Configure**. The following dialog will be displayed:

Figure 11: NetApp Filer Conne	ection Settings
-------------------------------	-----------------

Configure NetApp Fi	iler auditing.
NetApp server web	interface credentials:
Username:	root
Password:	1
Full path to event log	g file generated by NetApp:
	The second s
Local filename:	/etc/log/adtlog.evt
Local filename: Network filename:	/etc/log/adtlog.evt ETC\$\log\adtlog.evt
Local filename: Network filename: Click to check NetA	/etc/log/adtlog.evt ETC\$\log\adtlog.evt pp Filer settings: Verify

5. Specify the following parameters:

Tabl	le 1	: NetApp	Filer	Parameters
------	------	----------	-------	------------

Parameter	Description
Username	Specify the NetApp management account. For a detailed description of a management account, please refer to Section <u>2.2 NetApp Management Account</u> .
Password	Enter the NetApp management account password.
Local filename	Specify the local path in the NetApp filer to the file where the event log files are to be saved. This file must be in .evt format. Example /etc/log/adtlog.evt.
Network filename	Specify the network path to the event log file. NOTE: The path must be entered without the server name, for example, \ETC\$\log\adtlog.evt.

6. Click **Verify** to ensure that the values you have entered are correct. If errors are returned, check that:

- A valid filer DNS name or IP address were specified in the UNC Path;
- HTTP or HTTPS admin access has been enabled on the NetApp filer (for instructions on how to do this, please refer to Section <u>4.2</u> <u>Configuring Admin Web Access</u>);
- The Network filename you have specified is valid and the UNC path is accessible from the machine where NetWrix File Server Change Reporter is installed.

7. CONFIGURING AUTOMATIC DELETION OF SECURITY LOG AUTO ARCHIVES

NetWrix File Server Change Reporter can be configured to automatically delete old EVT log files. To do this, perform the following steps:

- 1. Open the Registry Editor (go to Start > Run and type regedit).
- 2. Expand HKEY_LOCAL_MACHINE\SOFTWARE\NetWrix\File Server Change Reporter (for 64 bit operating systems the path is HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NetWrix\File Server Change Reporter).
- 3. Set the 'CleanAutoBackupLogs' value to 1 and click **OK**.
- 4. Create a new DWORD value, if it does not exist.

With such configuration, log files older than 1 hour will be removed automatically. If the value is set to 0 or is not specified, log files will be kept forever.

A APPENDIX: RELATED DOCUMENTATION

The table below lists all documents available to support NetWrix File Server Change Reporter:

Document Name	Overview
How to Configure NetWrix File Server Change Reporter to Monitor NetApp Filer CIFS Shares	The current document provides detailed instructions on how to configure NetWrix File Server Change Reporter and NetApp filer CIFS shares for auditing.
NetWrix File Server Change Reporter Administrator's Guide	The guide provides detailed instructions on how to configure and use NetWrix File Server Change Reporter.
NetWrix File Server Change Reporter Quick Start Guide for the Enterprise Edition	The guide provides instructions on how to start working with the program quickly and easily.
NetWrix File Server Change Reporter Quick Start Guide (Freeware Edition)	The document is intended for evaluation of the product Freeware Edition. It provides instructions on how to start working with the program quickly and easily.
NetWrix File Server Change Reporter Troubleshooting Guide	The guide provides step-by-step instructions on troubleshooting incorrect reporting.
How to Perform File System Backup and Restore with NetWrix File Server Change Reporter	The technical article provides instructions on how to roll back to a previously saved back-up point using NetWrix File Server Change Reporter.
Installing Microsoft SQL Server and Configuring the Reporting Services	The technical article provides instructions on how to install Microsoft SQL Server 2005/2008/2008 R2 Express and configure the Reporting Services.
How to Configure NetWrix File Server Change Reporter to Monitor EMC VNX/VNXe/Celerra CIFS Shares	The technical article provides detailed instructions on how to configure NetWrix File Server Change Reporter and the EMC VNX/VNXe/Celerra CIFS shares for auditing.
Subscription to SQL Server Reports	The article provides step-by-step instructions on how to configure subscription to SSRS reports.
Installing SQL Express on Windows Vista Technical Article	The article provides detailed instructions on how to install SQL 2005 with Advanced Services on Windows Vista.
How to Configure Granular Audit Policy on a File Server Monitored by NetWrix File Server Change Reporter	The technical article provides instructions on how to configure granular Audit policy on a file server monitored by NetWrix File Server Change Reporter.
NetWrix File Server Change Reporter Release Notes	The document provides a list of known issues that customers may experience while using the release version 3.3.

Table 2: Product Documentation