FileSure ByStorm Software

www.bystorm.com

877-BYSTORM

Network-attached storage appliances are great things; offering an easy way to expand or consolidate your file servers onto a stand-alone device that just plugs into your network.

But how do you audit or secure it?

NAS appliances run streamlined operating systems and for the most part, implement Microsoft Windows-styled (NTFS) auditing and security systems. On NAS devices based on Windows Storage Server, the underlying file system actually is NTFS; but on UNIX-based NAS devices, they usually emulate NTFS.

On Windows-based NAS appliances, you can install FileSure directly on the NAS and make use of all its features.

On UNIX-based NAS devices (e.g. NetApp Filer), FileSure can't be installed directly on the server and your only option for server-based file auditing and security is to rely on the emulated NTFS access control list model...which is troublesome at best.

But, there is a way to benefit from the power of FileSure with your UNIX-based NAS and that's by using **FileSure for Workstations** instead. FileSure can handle file operations when they occur **on** the machine where FileSure is installed and file operations made **from** the machine where FileSure is installed.

In this 'How-to', I'm going to show you to audit a Network-attached storage appliance using FileSure for Workstations.

1. Start the FileSure console and click the 'Rules management' tab, then click the 'Audit access' button.

3/11 9:07 AM allengb Read \\win2008x64\marketing\how tos\gene old how tos only for	emergency/how to install and se
	4
Common tasks Rule management Analysis, Reports and Alerts	
Local rules Master rules (read-only)	-
Auditing Rule - Monitor AutoCAD files	Quick audit
🛛 🗹 Auditing Rule - Trial Rule for Local Machine - Audit Access to Microsoft Office Files	Audit access
Auditing Rule - Watch a file	Abdit access
Auditing Rule - watch exe writes and deletes	Block access
Auditing Rule - Watch File Accesses	
Auditing Rule - Watch Folder Moves	Event log monitoring
Auditing Rule - Watch temp	
Deny Rule - Block CD writes	/ Edit Rule
Deny Rule - Block malware	
Deny Rule - Block read access to the FileSure Console	Delete rule
ByStorm Software	🛚 Close

- 2. On the Auditing rule screen, make the following changes (see figure next page):
 - a. For the 'Rule name' enter 'Watch NAS'
 - b. Under 'Operations to Audit' click the 'Select All' button.
 - c. In the 'User name filters' section, click the 'Add' and add an include filter of '*' to cover all users
 - d. In the 'File name filters' section, click the 'Add' button and enter the UNC path to the NAS share you want to audit. [Note: you have to use a UNC since mapped drives can be different for each user.]

🏠 Edit File Filter		
Please enter file or folder name fil	ter:	6
\\BYSTORM01\Marketing*		▼ 📄 Browse
 Include matching Files in C Exclude Files in Filter 	Filter	✓ OK Sancel

e. In the 'Rule applies to' area, uncheck everything except 'Network drives', 'Files' and 'Workstations'.

When all these changes are made, your rule should look something like this:

矝 FileSure - Auditing Rule	X
Pule name: Watch ByStom NAS File name filters Include: \\BYSTORM01\Marketing* Include: \\BYSTORM01\Marketing* Include: * Include: * <td>Operations to Audit Deselect All Access checks ✓ Read access ✓ Write access ✓ Delete access Status changes ✓ Create ✓ Delete ✓ Rename ✓ Security Changes Content operations ✓ File read ✓ File write</td>	Operations to Audit Deselect All Access checks ✓ Read access ✓ Write access ✓ Delete access Status changes ✓ Create ✓ Delete ✓ Rename ✓ Security Changes Content operations ✓ File read ✓ File write
File size filters Other Options Program name filters Group name filters Machine name filters Time slot Rule applies to Image: Send e-mail on rule match Send to: Send to: Image: Senvers Image: More servers Image: Servers Image: Servers Image: Only apply rule after a threshold has been Activate rule when the threshold of Image: Driveless (VSS) Image: Servers Image: Only apply rule after a threshold of	filters Signature filters n reached. iminutes is reached.
Comment:	Cancel

3. Click 'OK' to close the rule screen and find the newly created rule and click the checkbox to turn it on.

3/11 9:07 AM 3/11 9:07 AM	allengb allengb 	Opened for Read Read	\\WIN2008X64\N \\win2008x64\ma	
Common tasks	Rule management	Analysis, Reports	and Alerts	
Local rules Ma	ster rules (read-only)			
Auditing Rule	- Watch ByStorm NAS	5		
Auditing Pule	 Watch cike writes an Watch File Accesse 	d-defetes s		
Auditing Rule - Watch Folder Moves				
Auditing Rule - Watch temp				
🗌 🗌 Deny Rule - B	lock CD writes			
🖌 Deny Rule - B	lock malware			
Deny Rule - B	lock read access to th	e FileSure Console		

Now we have a workstation rule defined to watch all files on the Marketing share on our NAS (<u>\\ByStormO1\Marketing</u>), but we need to deploy FileSure to the workstations that access that share.

4. On the main console screen, select the 'Common tasks' and click the 'Manage workstations' button.



5. This will bring up the 'Manage Deployments' screen, click 'Add workstations.'

🐴 Manage Deployments				
		Workstations	0	Add workstation
Name	Manage	Status		
XP2PROVM		Machine unreachable		Total Licenses: 10
XPPROVM		Managed Workstation v.2.5.3858.36012 Instal		Managed: 2
				Deploy to: 0
				Remove from: 0
			Work	station options ide FileSure Service ide Non-Owned Processes nable Desktop Alerts er FileWall estrict Access to anaged Workstations Exceptions Request license release Build disconnected config. pdate workstation credentials Deploy / Remove

6. This will bring up the 'Add Managed Workstation' screen. On this screen enter the workstations you want to monitor and click OK.

わ Add Managed Workstation				- D X
Please type in the name of the computer	to manage.	Separate co	mputers with	n a semicolon.
BYTELESS; DUAL32; QUADPROC2				
			🗸 ок	Cancel

7. Click the 'Deploy/Remove' to install FileSure for Workstation on the workstations you have listed.

The managed workstations will pull their rules, configuration and summaries from the server and push their back logs to the server so they can be used for searching, researching or reporting. All activity from that NAS will be monitored.