netwrix

Top 5 NetApp Filer Incidents You Need Visibility Into

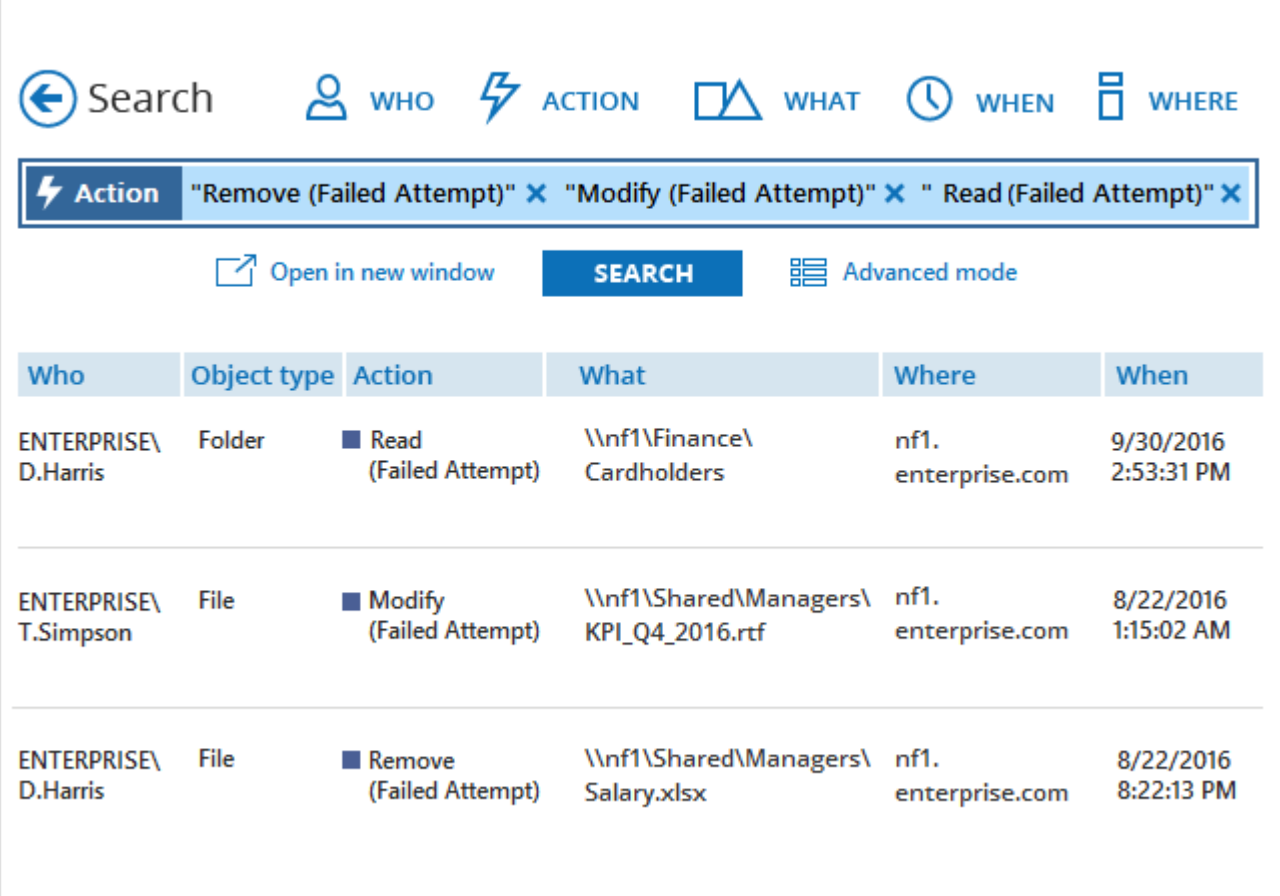
www.netwrix.com | **Toll-free**: 888-638-9749

Table of Contents

#1: Failed NetApp Filer Activity

An unusually large number of failed attempts to access or modify files during normal business operations can indicate an attack. So can a steady increase in this number of overtime. Netwrix Auditor delivers complete visibility into all failed NetApp filer actions and helps answer the following questions:

- **Who** attempted but failed to add, read, modify or remove files or folders?
- **What** actions did each user attempt?
- **What object** was each user trying to add, read, modify or remove?
- **On which NetApp filer** did each user attempt the failed action?
- **When** was each failed action attempted?



#2: Activity Involving Potentially Harmful Files

Malicious insiders and outsider attackers often place harmful files on file shares. Netwrix Auditor tracks suspicious file extensions that could be malware, viruses or other dangerous executables, and provides answers to the following questions:

- **What suspicious executables** were created, modified or deleted across your NetApp filer?
- **Where** is each potentially harmful file stored?
- **Who** created, modified or deleted each suspicious file?
- **What action** did the user take with each potentially harmful file?
- **When** did each action take place?

Potentially Harmful Files – Activity

Shows the creation, modification, and deletion of potentially harmful files, such as executables, installers, scripts, and registry keys on your file shares and SharePoint sites. These files may be malware, viruses, or inappropriate distributives, and should not be stored on shared resources. Use this report to track incidents and prevent security threats.

Audited System: File Servers

Action	What	Who	When
Read	\\NF1\shared\Dev\crss.hta	ENTERPRISE\J.Carter	08/22/2016 11:12:09 PM
Read	\\NF1\shared\Managers\nvcpl.exe	ENTERPRISE\T.Simpson	08/24/2016 2:56:49 PM
Added	\\NF1\shared\Managers\nvcpl.exe	ENTERPRISE\T.Simpson	08/24/2016 3:10:45 PM
Modified	\\NF1\shared\PM\crss.hta	ENTERPRISE\G.Brown	08/22/2016 6:31:59 AM

#3: Anomalous Spikes in User Activity

A high number of successful or failed attempts to access, modify or delete files can be a sign of malicious activity. Timely detection of this activity is critical for thwarting attacks in their early stages. Netwrix Auditor shows the most active user accounts and helps answer the following questions:

- **Who** made most changes in your IT environment?
- **Which user accounts** attempted the most failed actions?
- **How many files** were deleted by a particular user?
- **Has there been any abnormal growth** in the number of file reads on your NetApp filer?

User Activity Summary

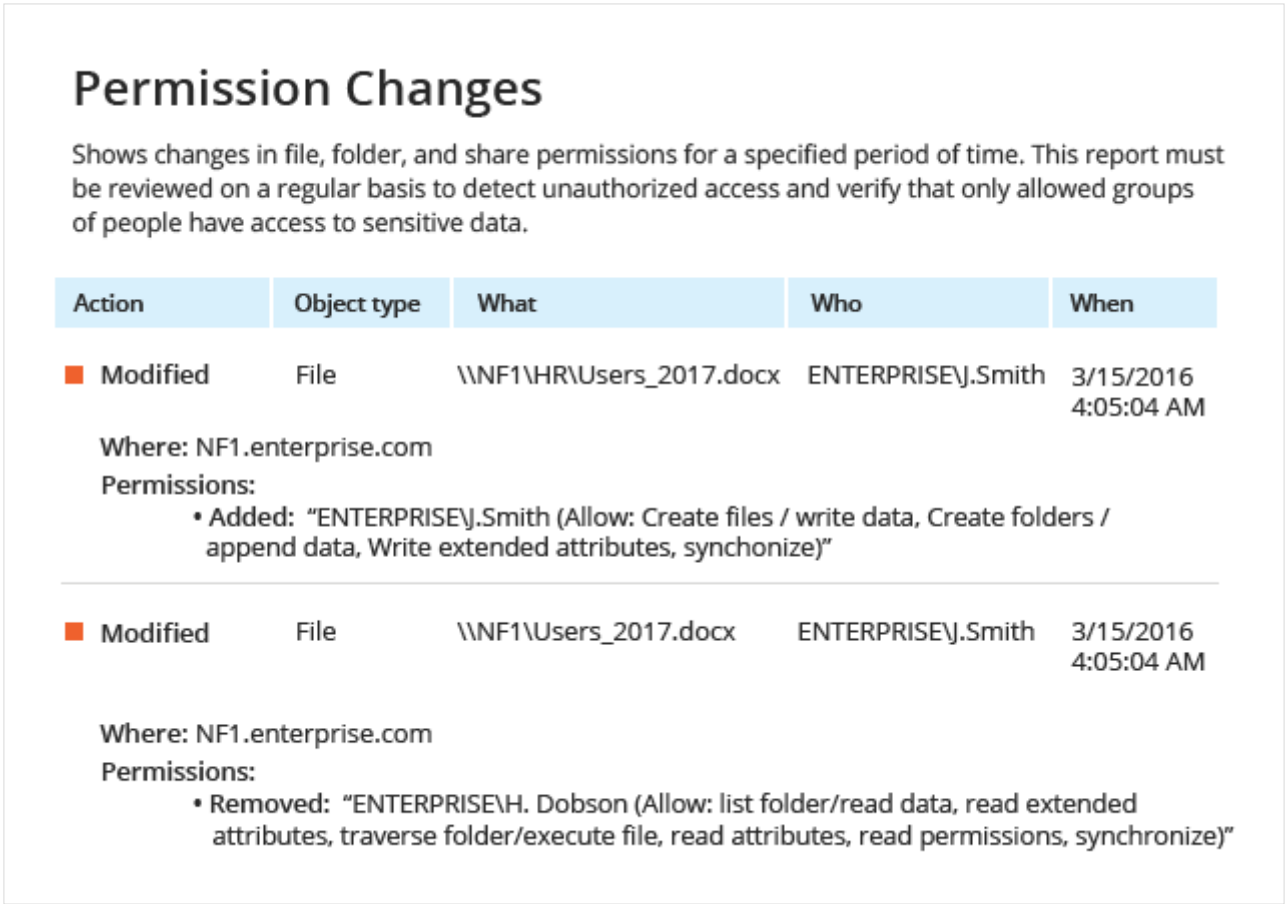
Shows the most active users. Use this report to detect suspicious user activity, such as high numbers of failed access attempts or file reads.

Who	Changes	Reads	Failed Attempts	Deletions
ENTERPRISE\J.Carter	0	12	0	1
ENTERPRISE\M.Spenser	0	18	0	0
ENTERPRISE\F.Ramirez	4	20	1	0
ENTERPRISE\Y.Chong	24	346	569	34
ENTERPRISE\I.Franko	5	19	1	1

#4: Changes to Access Permissions

Strict control over changes to access permissions for sensitive data is required in order to minimize the risk of a data breach. Netwrix Auditor delivers deep insights into changes to access rights and helps answer the following questions:

- **Who** made changes to access rights?
- **Which objects** had their permissions changed?
- **What are the "after" values** for the changed permissions?
- **When** were the permissions changed?



Permission Changes

Shows changes in file, folder, and share permissions for a specified period of time. This report must be reviewed on a regular basis to detect unauthorized access and verify that only allowed groups of people have access to sensitive data.

Action	Object type	What	Who	When
Modified	File	\\NF1\HR\Users_2017.docx	ENTERPRISE\J.Smith	3/15/2016 4:05:04 AM

Where: NF1.enterprise.com
Permissions:
• Added: "ENTERPRISE\J.Smith (Allow: Create files / write data, Create folders / append data, Write extended attributes, synchonize)"

Action	Object type	What	Who	When
Modified	File	\\NF1\Users_2017.docx	ENTERPRISE\J.Smith	3/15/2016 4:05:04 AM

Where: NF1.enterprise.com
Permissions:
• Removed: "ENTERPRISE\H. Dobson (Allow: list folder/read data, read extended attributes, traverse folder/execute file, read attributes, read permissions, synchronize)"

#5: Excessive Permissions Granted

Best practices require granting the users access to only data they need. Granting a user account excessive permissions to sensitive data increases your risk of a security breach. Netwrix Auditor helps you detect and revoke excessive access rights before data exfiltration occurs, and answers the following questions:

- **Are there any users** who have access to data they don't work with?
- **What privileges** does each user account hold?
- **How were the permissions granted:** directly or through group membership?
- **How frequently** has each user accessed a particular file or folder?

Excessive Access Permissions

Shows accounts with permissions for infrequently accessed files and folders. Use this report for spotting unnecessary permissions and preventing data leaks. Track permissions assigned to accounts directly or by group membership.

Object: \\NF1\Accounting (Permissions: Different from parent)

Account	Permissions	Means Granted	Times Accessed
ENTERPRISE\D.Harris	Full Control	Directly	0
ENTERPRISE\A.Watson	Full Control	Group	0
ENTERPRISE\J.Carter	Full Control	Group	0
ENTERPRISE\K.Miller	Write and List folder content	Directly	0
ENTERPRISE\T.Simpson	Read (Execute, List folder content)	Group	0

About Netwrix Auditor

Netwrix Auditor is a **visibility and governance platform** that enables control over changes, configurations and access in hybrid cloud IT environments to protect data regardless of its location. The unified platform provides security analytics for detecting anomalies in user behavior and investigating threat patterns before a data breach occurs.

Netwrix Auditor includes applications for Active Directory, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware and Windows Server. Empowered with a RESTful API, Netwrix Auditor provides **endless integration, auditing and reporting capabilities** for security and compliance.

Unlike other vendors, Netwrix focuses exclusively on providing complete visibility and governance for hybrid cloud security. The sharp focus enables us to offer much more robust functionality than legacy change auditing solutions. Netwrix Auditor has been already honored with more than **100 awards** and recognized by almost **160,000 IT departments** worldwide.

Deploy Netwrix Auditor Wherever You Need It

- Free 20-Day Trial for On-Premises Deployment: netwrix.com/freetrial
- Free Virtual Appliance for Hyper-V and VMware Hypervisors: netwrix.com/go/appliance
- Free Cloud Deployment from the AWS, Azure and CenturyLink Marketplaces: netwrix.com/go/cloud

netwrix.com/social

Netwrix Corporation, 300 Spectrum Center Drive, Suite 1100, Irvine, CA 92618, US

Toll-free: 888-638-9749

Int'l: +1 (949) 407-5125

EMEA: +44 (0) 203-318-0261