NetWrix
#1 for Change Auditing and Compliance™

#1 for Change Auditing™
Simple, Efficient, Affordable

NetWrix Top 10 Change Auditing Reports

The hit list of the most popular change auditing reports among IT security professionals

Netwrix Corporation, 12 N. State Route 17, Suite 104, Paramus, NJ 07652, USA

netwrix.com

New York: (201) 490-8840
Tampa: (813) 774-6472
Los Angeles: (949) 407-5125
Boston: (617) 674-2157
London: +44 (0) 203 318 0261
Toll-free: (888) 638-9749

twitter.com/netwrix
youtube.com/netwrix
netwrix.com/linkedin
netwrix.com/googleplus
facebook.com/netwrix
spiceworks.com/netwrix

How to Keep your IT Infrastructure Secure

When dealing with Microsoft's native auditing, one can't help noticing that event data in the logs simply is not provided in a way that is either actionable or easy to understand. It's common practice that a couple of dozen events need to be filtered through to find a single one that shows an actual change. For example, updated security details are shown in the internal Windows format which could be difficult to read and understand. This could lead to failing an IT audit.

With NetWrix Change Reporter Suite there is no need to deal with cryptic and unreliable event logs spread across the IT infrastructure. Thanks to the patent-pending NetWrix **AuditIntelligence™** technology that transforms raw audit data into meaningful and actionable intelligence to drive security and compliance, NetWrix change auditing solution allows to easily track and report on the **"4W detail": who changed what, where and when**. NetWrix Change Reporter Suite provides easy-to-read, informative and well-structured reports that show exactly what is needed at that specific moment of time. Moreover, audit reports and alerts can be automatically sent to administrators via email. This document provides an overview of the most popular NetWrix change auditing reports among IT security professionals.

The change audit data is automatically archived and can be stored for years, so that the **full audit trail of changes can be recreated**. These changes can be made to any environment in an IT infrastructure such as Active Directory and Group Policy during any period and drilled down to detailed information if necessary. The AD audit trail archiving allows organizations to analyze any policy violations occurred in the past and maintain ongoing compliance with internal and external regulations.

Even if a third-party change auditing solution is already deployed in an organization, chances are that it requires agents which are intrusive to the operating system putting servers at risk. The biggest problem with intrusive agents inventing their own audit stream is that they can hang working for some period of time, so the audit data is not created and there's no way to recreate it. This could be enough to fail an audit. Unlike many third-party auditing products, NetWrix unified auditing platform is built with NetWrix **AuditAssurance™** technology which avoids the problem of lost data by constructing audit data from multiple sources including native event data. Therefore, intrusive agents are never required and the NetWrix solution can be deployed with or without agents.

NetWrix Corporation's core competency is in unifying change and configuration auditing of critical systems across the entire IT infrastructure. With the broadest platform coverage available in the industry, innovative technology and strategic roadmap aiming to support different platforms, devices and applications, NetWrix offers **award-winning** auditing solutions and **superior customer service** at affordable prices. Founded in 2006, NetWrix has evolved as **#1 for Change Auditing** as evidenced by **thousands of satisfied customers** worldwide. The company is headquartered in Paramus, NJ, and has regional offices in Los Angeles, Boston, Tampa and the UK. NetWrix is #33 among the fastest growing software companies in America according to Inc. 500 list published by Inc. Magazine in 2012.

Table of Contents

1. Active Directory

Organizational Units Removed

This report shows deleted AD organizational units. It can be used for early detection of accidentally deleted OUs. Active Directory Object Restore Wizard allows you to quickly recover OUs and their child objects. Active Directory Change Reporter automatically creates change audit reports and real-time alerts that show **who changed what, when, and where** for all changes in human-readable form without having to resolve complicated native identifiers.

Filter	Value
Date/Time From:	4/1/2012 5:02:20 AM
Date/Time To:	8/28/2012 5:15:20 PM
Domain name:	netwrix-test.local
Where removed:	%
Who removed:	%
What changed:	%
Sort by:	What Removed

Who removed: NETWRIX-TEST\administrator

What Removed	Where Removed	When Removed
\local\netwrix-test\Accounting	dc1.netwrix-test.local	8/28/2012 5:00:08 AM
\local\netwrix-test\Development\ou1	dc1.netwrix-test.local	4/13/2012 8:51:02 AM
\local\netwrix-test\Key User Group	dc1.netwrix-test.local	8/28/2012 5:01:00 AM
\local\netwrix-test\Marketing	dc1.netwrix-test.local	8/28/2012 4:59:53 AM
\local\netwrix-test\NY	dc1.netwrix-test.local	8/28/2012 5:00:28 AM

2. Active Directory (continued)

Administrative Group Membership Changes

Administrative groups such as Domain Admins and Enterprise Admins should be very well-defined and rarely changed. Changes to group memberships must be closely monitored. This report shows **who** added, removed or modified **which** group members, **where** and **when** across administrative groups.

Filter	Value
Date/Time From:	8/15/2012 2:15:55 PM
Date/Time To:	8/15/2012 2:40:55 PM
Domain name:	netwrixdemo.local
Where changed:	%
Who changed:	%
Exclude who changed:	
Sort by:	Member
Group name:	Domain Admins, Enterprise Admins

Group name: \local\NetWrixDemo\Users\Domain Admins

Action	Member	Who Changed	Where Changed	When Changed
Added	NetWrixDemo.local/ OU for deletion/AG1	NETWRIXDEMO\TMoore	WINRNE4GDCO683.NetWrix Demo.local	8/15/2012 2:18:33 PM
Removed	NetWrixDemo.local/ OU for deletion/AG4	NETWRIXDEMO\TMoore	WINRNE4GDCO683.NetWrix Demo.local	8/15/2012 2:18:54 PM
Removed	NetWrixDemo.local/ OU for deletion/AG5	NETWRIXDEMO\TGarvin	WINRNE4GDCO683.NetWrix Demo.local	8/15/2012 2:19:55 PM

Group name: \local\NetWrixDemo\Users\Enterprise Admins

Action	Member	Who Changed	Where Changed	When Changed
Added	NetWrixDemo.local/ OU for deletion/AG3	NETWRIXDEMO\JMelnik	WINRNE4GDCO683.NetWrix Demo.local	8/15/2012 2:21:09 PM

3. Group Policy

All Password Policy Changes

A password policy implies password history, expiration date, complexity and other settings that affect password security as mandated by an organization's policy. Microsoft's native Group Policy management tools don't have any auditing and change reporting capabilities and you just can't track the "**4W detail: who, what, when and where**" data for critical modifications. NetWrix Group Policy Change Reporter fills the gap in native auditing by clearly providing the "4W detail".

Filter	Value
Date/Time From:	8/14/2012 2:02:21 PM
Date/Time To:	8/15/2012 2:02:21 PM
Domain name:	netwrixdemo.local
Where changed:	%
Who changed:	%
What changed:	%
Sort by:	What Changed

Action	Who Changed	What Changed	Where Changed	When Changed
Modified	NETWRIXDEMO\TMoore	Default Domain Controllers Policy	WINRNE4GDCO683.NetWrix Demo.local	8/15/2012 1:57:11 PM
	Action	**Path**		
	Added	Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Account Policies/ Password Policy		
		Policy: Maximum password age; Setting: 42 days;		
		Policy: Minimum password age; Setting: 30 days;		
Modified	NETWRIXDEMO\JMelnik	Netwrix for Test	WINRNE4GDCO683.NetWrix Demo.local	8/15/2012 2:00:06 PM
	Action	**Path**		
	Modified	Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Account Policies/ Password Policy		
		Policy: Enforce password history; Setting: 2 passwords remembered -> 1 passwords remembered;		
		Policy: Maximum password age; Setting: 42 days -> 50 days;		
		Policy: Minimum password length; Setting: 9 characters -> 5 characters;		

4. Exchange Server

Mailboxes Created

Microsoft Exchange is one of the most important IT infrastructure components in an organization. Even one hour of email downtime can cost millions of dollars of lost revenue and credibility. Auditing changes to configuration settings in an Exchange environment is critical to ensure reliable email operation, security and compliance. The below report shows **who** created **what** mailboxes, **where** and **when**. These changes usually take place when new employees are hired. Newly created mailboxes must be reviewed to detect unauthorized activity.

Filter	Value
Date/Time From:	3/1/2012 6:32:37 PM
Date/Time To:	8/20/2012 6:32:37 PM
Domain name:	wks166.local
Where changed:	%
Who changed:	%
What changed:	%
Sort by:	Object Type
Who created:	WKS166\Administrator

Object Type	What Changed	Where Created	When Changed
User	\local\wks166\Users\4567890	DC01.wks166.local	8/3/2012 7:16:54 PM
Exchange Proxy Addresses set to 'SMTP:4567890@wks166.local'			
Mailbox Created			
Mailbox Database set to '\local\wks166\Configuration\Services\Microsoft Exchange\WKS166\Administrative Groups\Exchange Administrative Group (FYDIBOHF23SPDLT)\Servers\EXCH07-WKS166\InformationStore\First Storage Group\Mailbox Database'			
User	\local\wks166\Users\all	DC01.wks166.local	6/25/2012 11:07:54 PM
Exchange Proxy Addresses set to 'SMTP:all@wks166.local'			
Mailbox Created			
Mailbox Database set to '\local\wks166\Configuration\Services\Microsoft Exchange\WKS166\Administrative Groups\Exchange Administrative Group (FYDIBOHF23SPDLT)\Servers\EXCH07-WKS166\InformationStore\First Storage Group\Mailbox Database'			
User	\local\wks166\Users\DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852}	DC01.wks166.local	7/6/2012 5:37:16 PM
Exchange Proxy Addresses set to 'SMTP:DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}@wks166.local'			
Mailbox Created			
Mailbox Database set to '\local\wks166\Configuration\Services\Microsoft Exchange\WKS166\Administrative Groups\Exchange Administrative Group (FYDIBOHF23SPDLT)\Databases\Mailbox Database 0957855029'			

5. Exchange Server (continued)

Non-Owner Mailbox Access Daily Changes

This report shows **who** accessed **what** mailboxes, what items inside mailboxes (e.g. emails, appointments, tasks) and what items **were** viewed, edited or deleted. This allows detecting any unauthorized activity from users who may be trying to steal confidential information from sensitive mailboxes belonging to other users.

Filter	Value
Date/Time From:	6/26/2012 12:00:00 AM
Date/Time To:	6/26/2012 11:59:00 PM
Domain name:	wks166.local
Who changed:	%
What changed:	%
Where changed:	%
When changed:	%
Date:	8/15/2012
Sort by:	Who Accessed
Who created:	WKS166 \ Administrator

Who Accessed	When Accessed	Mailbox	Server	Access Type	Details
WKS166\ Administrator	6/26/2012 3:44:04 PM	all@wks166.local	exch07-wks166	Folder opened	Folder **/** was opened.
	6/26/2012 3:44:04 PM	all@wks166.local	exch07-wks166	Folder opened	Folder **/Inbox** was opened.
	6/26/2012 3:44:04 PM	all@wks166.local	exch07-wks166	Message opened	The message located in **/Inbox** with the subject **sdf** was opened.
	6/26/2012 3:44:18 PM	all@wks166.local	exch07-wks166	Folder opened	Folder **/Drafts** was opened.
	6/26/2012 3:44:18 PM	all@wks166.local	exch07-wks166	Message created and saved	A message was created in **/Drafts** with the subject **a**.
	6/26/2012 3:44:27 PM	all@wks166.local	exch07-wks166	Message saved	Changes were saved in the message located in **/Drafts** with the subject **a**.
	6/26/2012 3:44:27 PM	all@wks166.local	exch07-wks166	Message opened	The message located in **/Inbox** with the subject **sdf** was opened.
WKS166\ JSmith	6/26/2012 3:49:42 PM	all@wks166.local	exch07-wks166	Folder opened	Folder **/Inbox** was opened.
	6/26/2012 3:49:43 PM	all@wks166.local	exch07-wks166	Message opened	The message located in **/Inbox** with the subject **sdf** was opened.

6. Windows Server

Local User and Group Changes

This report shows **who** made **what** change to a local user/group on a server and **when**. Find out who added, modified or removed a user from a group and see new object attributes after the change (e.g. status, members, description and more). This type of report allows catching even the slightest configuration changes made to servers. These changes can potentially impact your users and cause major disruptions to businesses.

Filter	Value
Date/Time From:	8/2/2012 12:00:00 AM
Date/Time To:	8/2/2012 11:59:00 PM
Domain name:	vfs2.vdomain.local
Who changed:	%
What changed:	%
Where changed:	%
When changed:	%
Date:	8/15/2012
Sort by:	Change Type
Who created:	VDOMAIN\Super Administrator

Change Type	Who Changed	When Changed	Server	Object Type	Resource Path	Details
Removed	VDOMAIN\ Administrator	8/2/2012 3:17:52 PM	VFS1	Local Group	System Information\Local Groups\ SomeTestGroup	Object attributes before deletion: **Status:** "OK" **Members:** "VFS1\SomeTest" **Description:** "TestGroup" **Name:** "SomeTestGroup"
Modified	VDOMAIN\ Administrator	8/2/2012 3:03:01 PM	VFS1	Local User	System Information\Local Users\	An account's password was reset.
Added	VDOMAIN\ Administrator	8/2/2012 3:05:47 PM	VFS1	Local User	System Information\Local Users\ SomeTest	Object attributes after addition: **Password Expires:** "Yes" **Password can be changed:** "No" **Status:** "OK" **Password Required:** "Yes" **Name:** "SomeTest" **Disabled:** "No" **Description:** "TestUser" **Lockout:** "No" **Full Name:** "TestUser"

7. File Server

All File Server Changes by Date

Unauthorized and accidental changes in files and folder structure, permissions, file shares, and other objects can significantly impact your users and infrastructure by facilitating data theft and security threats. Native file system auditing lacks many important features and doesn't have reporting capabilities. The below report shows all created, deleted, and modified files, folders, shares, and permissions, grouped by the modification date. This report is very useful for compliance audits to show that all data modifications are traceable and auditable.

Filter	Value
Date/Time From:	7/28/2009 6:19:53 PM
Date/Time To:	7/29/2009 6:19:53 PM
Who changed:	%
Sort by:	Where
UNC Path:	%

Action	Where	Object Type	Who Changed	What Changed	When Changed
Modified	nyw35	Share	WIDGETS\administrator	\finance	7/28/2009 9:20:48 PM
Root Folder Permissions added: 'Permissions: Users (Deny: Delete Subdirectories And Files, Delete, Write Extended Attributes, Read Attributes, Take Ownership, Traverse Folder/Execute File, Read Extended Attributes, Read Permissions, Create Folder/Append Data, Write Attributes, Create Files/Write Data, List Folder/Read Data, Change Permissions); Finance (Allow: Delete, Write Extended Attributes, Read Attributes, Traverse Folder/Execute File, Read Extended Attributes, Read Permissions, Create Folder/Append Data, Write Attributes, Create Files/Write Data, List Folder/Read Data)'					
Modified	nyw35	File	WIDGETS\JSmith	\finance\CurrentResponsibilities.doc	7/28/2009 9:20:41 PM
Permissions added: 'Permissions: Users (Allow: Delete, Write Extended Attributes, Read Attributes, Traverse Folder/Execute File, Read Extended Attributes, Read Permissions, Create Folder/Append Data, Write Attributes, Create Files/Write Data, List Folder/Read Data)'					
Size changed from '0' to '170'					
Added	nyw35	File	WIDGETS\PJohnson	\finance\Financial Report 2008-1.pdf	7/28/2009 9:18:45 PM
Removed	nyw35	File	WIDGETS\JSmith	\finance\Privileged Access.xls	7/28/2009 9:16:22 PM
Added	nyw35	File	WIDGETS\MCrown	\finance\Quote Template.doc	7/28/2009 9:18:45 PM

8. SQL Server

Login Changes & Server Role Changes

This report shows changes made to SQL server roles and logins. This and similar reports help administrators timely detect all unauthorized and unwanted changes that can lead to server and database downtime. They can also help ensure compliance with regulatory and security requirements such as GLBA, SOX, HIPAA and PCI.

Filter	Value
Date/Time From:	8/27/2012 7:31:03 PM
Date/Time To:	8/28/2012 7:31:03 PM
Object type:	%
What changed:	%
Where:	%
Who changed:	%
Sort by:	Where

Action	Where	Object Type	Who Changed	What Changed	When Changed	Workstation
Added	sirius	Login	ANDROMEDA\adm	Security\Logins\ [Tes]	8/28/2012 7:27:41 PM	sirius
Added	sirius	Login	ANDROMEDA\adm	Security\Logins\ [Tester]	8/28/2012 7:02:07 PM	sirius
Removed	sirius	Login	ANDROMEDA\adm	Security\Logins\ [Tester]	8/28/2012 7:27:32 PM	sirius
Modified	sirius	Server Role	ANDROMEDA\adm	Security\Server Roles\setupadmin	8/28/2012 7:02:27 PM	sirius
Role Members: 'Tester'						
Modified	sirius	Server Role	ANDROMEDA\adm	Security\Server Roles\setupadmin	8/28/2012 7:27:21 PM	sirius

9. VMware

All VMware Infrastructure Changes

This report shows **who** made **what** changes to VMware Infrastructure 3 objects and settings, including hosts, containers, resource pools, virtual machines. The data in the report is filtered by the object that was changed ('What changed'). Such changes can cause failures and outages in your virtual infrastructure and significantly contribute to virtual machine sprawl. It is therefore essential for VMware administrators to be constantly aware of these changes. This type of reports is also suitable for IT compliance auditors, such as SOX, HIPAA, GLBA and others.

Filter	Value
Date/Time From:	7/27/2009 4:00:24 PM
Date/Time To:	7/27/2009 5:00:24 PM
Sort by:	What Changed
WHo changed:	%

Action	Object Type	Who Changed	What Changed	When Changed
Modified	HostSystem	netwrix\JSmith	\Datacenters\NetWrixCorporation\NJ_Office\host\production_cluster\Virtual Server1	7/27/2009 4:43:11 PM
Service Console IP Address of port Service Console 2 changed from '212.192.24.1' to '212.192.24.2'				
Modified	HostSystem	netwrix\JSmith	\Datacenters\NetWrixCorporation\NJ_Office\host\VirtualServer2\Virtual Server2	7/27/2009 4:42:35 PM
NTP running changed from 'True' to 'False'				
Port Group Virtual Machine Network Allow Promiscuous changed from 'False' to ''				
Port Group Virtual Machine Network Attached uplink adapter changed from 'vmnic0' to ''				
Port Group Virtual Machine Network Forged Transmits changed from 'True' to ''				
Port Group Virtual Machine Network MAC Address Changes changed from 'True' to ''				
Virtual Switch vSwitch0 Number of Ports changed from '128' to '64'				
Virtual Switch vSwitch1 Allow Promiscuous changed from 'False' to ''				
Virtual Switch vSwitch1 Attached uplink adapter changed from 'vmnic0' to ''				
Virtual Switch vSwitch1 Forged Transmits changed from 'True' to ''				
Virtual Switch vSwitch1 MAC Address Changes changed from 'True' to ''				
Virtual Switch vSwitch1 Number of Ports changed from '64' to ''				
Removed	VirtualMachine	netwrix\Administrator (7/27/20093:36:07 PM), netwrix\JSmith (7/27/2009 4:20:34 PM)	\Datacenters\NetWrixCorporation\NJ_Office\vm\testers\JackHuntington\w2k3_for_test	7/27/2009 4:20:34 PM
Modified	VirtualMachine	netwrix\Administrator (7/27/2009 3:40:09 PM), netwrix\MPeterson (7/27/2009 4:21:00 PM)	\Datacenters\NetWrixCorporation\NJ_Office\vm\testers\MaryPeterson\mp_w2k3	7/27/2009 4:21:00 PM
Network Adapter 1 Connected changed from 'True' to 'False'				
Power State changed from 'Powered On' to 'Suspended'				
Added	VirtualMachine	netwrix\MCrown	\Datacenters\NetWrixCorporation\NJ_Office\vm\testers\Michael Crown\mc_w2k3	7/27/2009 4:21:26 PM

10. User Logon/Logoffs

Logon Reporter Daily Report

This report shows both successful and failed (invalid) logon and logoff events across the network. These events can be really difficult to track with built-in Active Directory tools. Logon Reporter is a tool capable of consolidating, archiving and reporting successful and failed logons and logoffs for such event types as: interactive, network, batch, service, account lockouts, unlocks and many others.

Filter	Value
Date/Time From:	3/13/2012 12:00:00 AM
Date/Time To:	3/13/2012 11:59:00 PM
Domain name:	wks166.local
Target computer:	%
User:	%
Subject computer:	%
Audit type:	%
Date:	3/13/2012
Sort by:	Target Computer
Who created:	WKS166 \ Administrator

Target Computer	User	Date	Subject Computer	Audit Type	Description
WIN-DTH7E16F1AU	WIN-DTH7E16F1AU\ Administrator	3/13/2012 4:17:01 AM	127.0.0.1	Interactive	An account failed to log on (The specified account's password has expired)
WIN-DTH7E16F1AU	WIN-DTH7E16F1AU\ Administrator	3/13/2012 4:17:20 AM	N/A	N/A	An account was logged off
WIN-DTH7E16F1AU	WIN-DTH7E16F1AU\ Administrator	3/13/2012 4:17:22 AM	127.0.0.1	Interactive	An account was successfully logged on
WIN-DTH7E16F1AU	WIN-DTH7E16F1AU\ Administrator	3/13/2012 4:19:36 AM	N/A	N/A	User initiated logoff
WIN-DTH7E16F1AU	WIN-DTH7E16F1AU\ Administrator	3/13/2012 4:23:11 AM	127.0.0.1	Interactive	An account was successfully logged on
WIN-DTH7E16F1AU. wks166.local	WKS166\Administrator	3/13/2012 5:43:11 AM	N/A	N/A	User initiated logoff

Get Top 10 Change Auditing Reports Now

Download a free 20-day trial of NetWrix Change Reporter Suite to try all of the top 10 change auditing reports for free. See for yourself how simple and efficient change auditing can be!

Alternatively, test NetWrix integrated solution for **automated auditing of the IT infrastructure** in a web-based virtual environment, evaluate the functionality of the product and try change auditing reports for free, **without the need to install and configure the product**. You will quickly see how it works in a sample test environment.

Take the TestDrive Now

Find out more at netwrix.com

Click to share this document with others: