netwrix

Keeping Tabs on the Top 5 Critical Windows Server Changes with Netwrix Auditor

www.netwrix.com | **Toll-free**: 888.638.9749

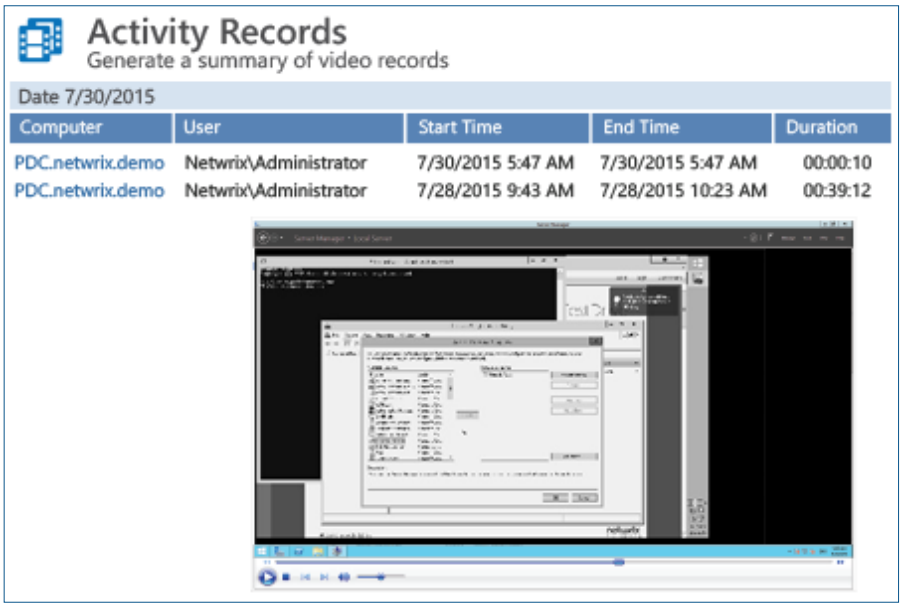
Table of Contents

#1: Software Changes

It's essential to keep all changes made by IT administrators on a Windows Server under control. Knowing the details about who made what changes and which applications have been added, removed or changed is critical to mitigating problems such as service downtime or loss of sensitive data.

Netwrix Auditor tracks all software changes on each Windows Server and helps to answer the following questions:

- **Exactly what software changes were made on Windows Server?**
- **Who made each software change?**
- **From which computer was the change made?**
- **When did each change occur?**
- **How long was the duration of the user session during which the software change was made?**

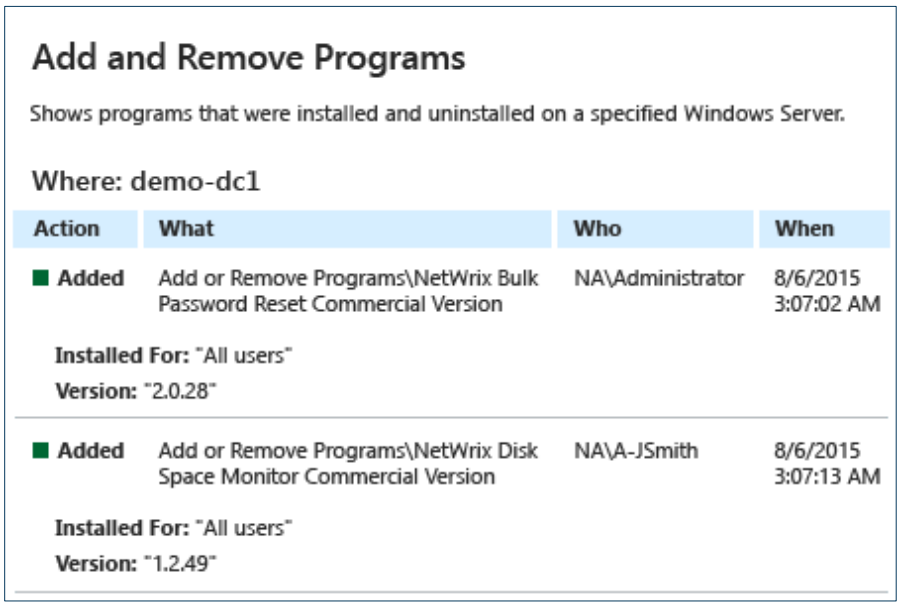


#2: Addition or Removal of Programs

Suspicious software on your Windows Server may be the result of an unauthorized installation by your own employee or may originate from a hacker's attack. Any suspicious software can potentially cause leakage of your most sensitive data, server performance problems or compliance failures.

Netwrix Auditor tracks all additions and removals of programs and helps to answer the following questions:

- Which programs were added or removed?
- Who added or removed each program?
- Which actions were performed using the program?
- Which server was the program added to or removed from?
- When was the program added or removed?



Add and Remove Programs

Shows programs that were installed and uninstalled on a specified Windows Server.

Where: demo-dc1

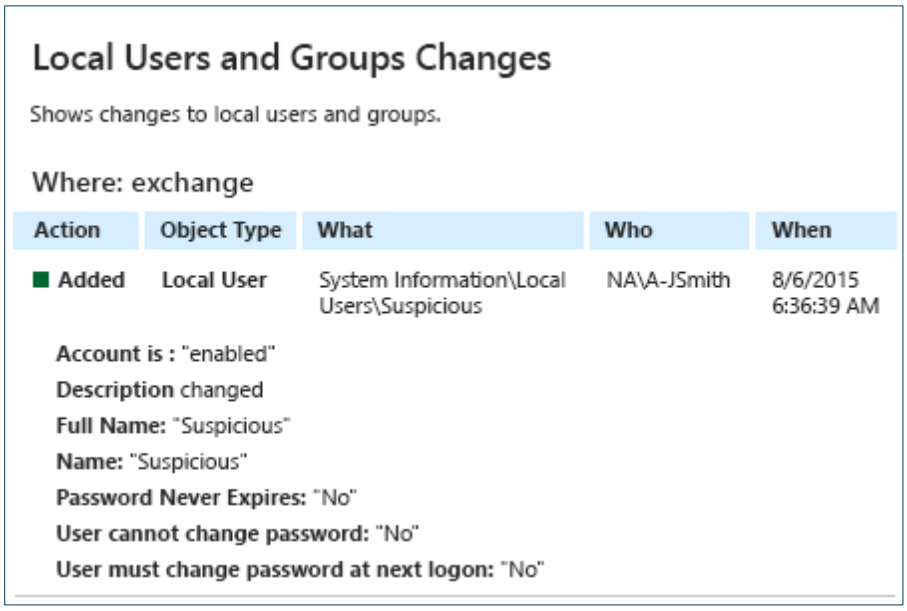
Action	What	Who	When
Added	Add or Remove Programs\NetWrix Bulk Password Reset Commercial Version	NA\Administrator	8/6/2015 3:07:02 AM
	Installed For: "All users"		
	Version: "2.0.28"		
Added	Add or Remove Programs\NetWrix Disk Space Monitor Commercial Version	NA\A-JSmith	8/6/2015 3:07:13 AM
	Installed For: "All users"		
	Version: "1.2.49"		

#3: Changes to Local Users and Groups

The unauthorized creation, modification or deletion of user accounts on Window Server might be a sign that internal or external attackers are trying to get into the system and make adverse changes. It's vitally important to monitor user account changes in order to reduce the possibility of system invasion.

Netwrix Auditor tracks all changes to local users and group and helps to answer the following questions:

- Which user accounts or groups were changed?
- What changes were made to the local user account or group?
- Who made each change?
- What type of object was changed?
- When was the change made?



Local Users and Groups Changes

Shows changes to local users and groups.

Where: exchange

Action	Object Type	What	Who	When
Added	Local User	System Information\Local Users\Suspicious	NA\A-JSmith	8/6/2015 6:36:39 AM

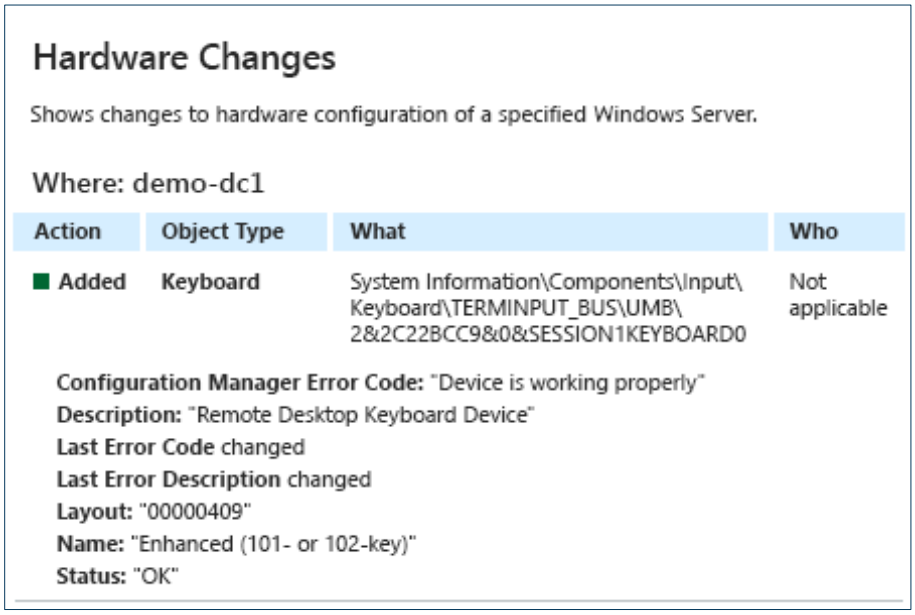
Account is : "enabled"
Description changed
Full Name: "Suspicious"
Name: "Suspicious"
Password Never Expires: "No"
User cannot change password: "No"
User must change password at next logon: "No"

#4: Hardware Changes

Intentional or accidental use of infected USB devices can slow a server's performance or even cause it to shut down. Hardware changes can also be a sign that a user has gotten access to the server and has keys to specific areas, such as RAM or HDD, which might result in a loss of sensitive data.

Netwrix Auditor tracks hardware changes and helps to answer the following questions:

- What hardware was added, deleted or modified?
- What type of hardware was changed in each case?
- Exactly what changes were made to the hardware?
- When was the change made?
- On which server was the hardware change made?



Hardware Changes

Shows changes to hardware configuration of a specified Windows Server.

Where: demo-dc1

Action	Object Type	What	Who
Added	Keyboard	System Information\Components\Input\Keyboard\TERMINPUT_BUS\UMB\2&2C22BCC9&0&SESSION1KEYBOARD0	Not applicable

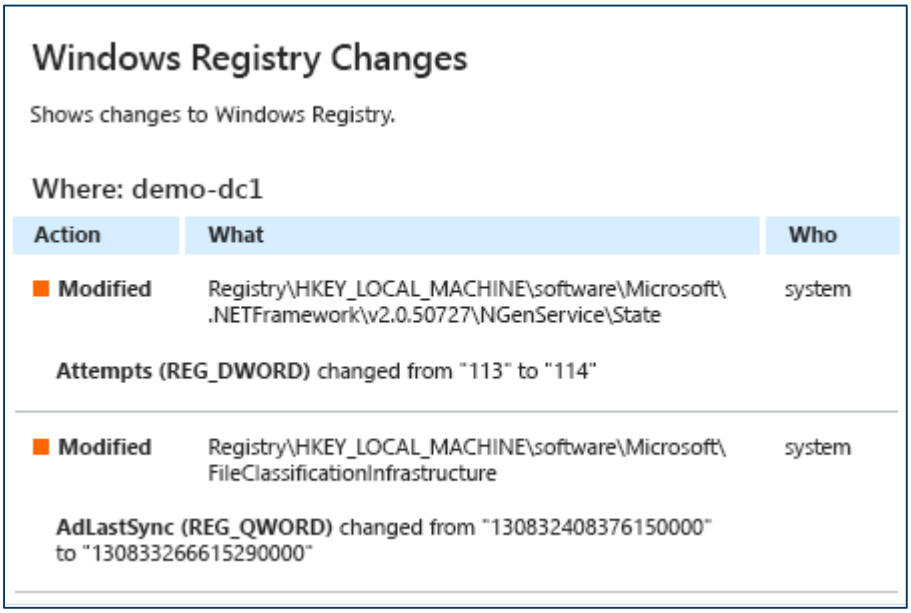
Configuration Manager Error Code: "Device is working properly"
Description: "Remote Desktop Keyboard Device"
Last Error Code changed
Last Error Description changed
Layout: "00000409"
Name: "Enhanced (101- or 102-key)"
Status: "OK"

#5: Registry Changes

Tracking changes to the Windows registry is critical to enhancing Windows security and preventing critical information from leaking out. A list of registry changes displays all configurations made on a Windows Server, which can be very helpful to investigations of security incidents caused by a virus or malicious admin activities.

Netwrix Auditor tracks registry changes and helps to answer the following questions:

- How exactly was the registry changed?
- Who made each registry change?
- On which server was the registry change made?
- Which registry keys were changed?



Windows Registry Changes

Shows changes to Windows Registry.

Where: demo-dc1

Action	What	Who
Modified	Registry\HKEY_LOCAL_MACHINE\software\Microsoft\.NETFramework\v2.0.50727\NGenService\State	system
Attempts (REG_DWORD) changed from "113" to "114"		
Modified	Registry\HKEY_LOCAL_MACHINE\software\Microsoft\FileClassificationInfrastructure	system
AdLastSync (REG_QWORD) changed from "130832408376150000" to "130833266615290000"		

About Netwrix Auditor

Netwrix Auditor delivers **complete visibility** into IT infrastructure changes and data access by providing actionable audit data about **who changed what**, **when and where each change was made**, and **who has access to what**. Netwrix Auditor helps organizations prevent security breaches caused by insider attacks, pass compliance audits with far less effort and expense, and keep tabs on what privileged users are doing in the environment.

Netwrix Auditor enables auditing of the broadest variety of IT systems, including Active Directory, Exchange, file servers, SharePoint, SQL Server, VMware and Windows Server. It also supports monitoring of privileged user activity in all other systems, even if they do not produce any logs, by enabling video recording of user screen activity and later search and replay.

More than 160,000 IT departments worldwide rely on Netwrix Auditor to secure IT infrastructure, prove compliance and increase operational efficiency. The product has earned over 70 awards from leading industry publications, including SC Magazine, Windows IT Pro, Redmond Magazine and WindowSecurity.com.

Download Free Trial: www.netwrix.com/auditor.html

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

netwrix.com/social

Toll-free: 888-638-9749 **Int'l:** +1 (949) 407-5125 **EMEA:** +44 (0) 203-318-0261