

Re: Auditing file deletion

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-04/msg01521.html>

- *From:* v-stezhu@xxxxxxxxxxxxxxxxxxxxxxxx (Steven Zhu [MSFT])
 - *Date:* Mon, 10 Apr 2006 08:53:40 GMT
-

Hi Nick,

Thanks for the new information.

Based on current information, I agree with Dana's suggestions. If you want to monitor files and folders deletions, you can use the filemon log file to find which files or folders have been deleted. To do so, please refer to the following steps:

1. Please visit the following link to download and save the Filemon version for your operating system from the following Web site:
<http://www.sysinternals.com/ntw2k/source/filemon.shtml>
– Download "Filemon (x86 – 76 KB) – you plan on using Filemon on WinNT/2K/XP/2K3" if you plan to use Filemon on Windows 2000, Windows XP, or Windows Server 2003.
2. Go to the folder where you saved the package and extract the package contents by using a compression utility such as Winzip. You can obtain the Winzip utility from <http://www.Winzip.com>.
3. After the files have been extracted, double-click "filemon.exe".
4. In the "Filemon Filter" window, make sure that the value in the "Include" box is "*".
5. Click "OK". A trace will start to run.
6. Please try to reproduce the issue (i.e. try to open a Word file). As soon as the issue occurs, switch to Filemon, and then click the microscope icon in the toolbar to stop the capture.
7. Click "File", click "Save", and then save the file as "FilemonLog" (without the quotation marks) on the desktop.

=====
Warning: This response contains a reference to a third party World Wide Web site. Microsoft is providing this information as a convenience to you. Microsoft does not control these sites and has not tested any software or

Re: Auditing file deletion

information found on these sites; therefore, Microsoft cannot make any representations regarding the quality, safety, or suitability of any software or information found there. There are inherent dangers in the use of any software found on the Internet, and Microsoft cautions you to make sure that you completely understand the risk before retrieving any software from the Internet.

=====
Note: The third-party product discussed is manufactured by a vendor independent of Microsoft; we make no warranty, implied or otherwise, regarding this product's performance or reliability.

If you want to know how to audit the permission on files and folders so that you can track who delete the files. Please double check you have the following correct steps:

Step 1: Enable audit policy

=====
Enable Audit object access policy under Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\

Since my test is on a domain controller, I enable the Domain Controller Security Policy from administrative tools.

Please refer to the following article for more details how to enable this policy. In addition, if your shares are not located on a domain controller, please enable the local policy on the server who holds the shares.

Audit object access

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/Serve rHelp/50fdb7bc-7dae-4dcd-8591-382aeff2ea79.mspx>

NOTE: You need to issue the command "gpupdate /force" in command-line to force the computer to apply the policy.

Step 2: Audit the user

=====
Right-click folder, click Properties, and then click the Security tab.

Click Advanced, and then click the Auditing tab.

Add TEST account, click Delete and Delete subfolders and Files.

Click OK to apply.

More details can be found from the article below:

Apply or modify auditing policy settings for a local file or folder

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/Serve rHelp/ecf63dcf-17e7-4279-91ff-beb11bd0d688.mspx>

Step 3: Verify the result

Re: Auditing file deletion

Re: Auditing file deletion

=====
Start win2k pro machine and use TEST to logon to the domain.
Visit the folder and delete one file.

On the DC, open the Event Viewer to see the security log; you can see the Event ID 560 is logged similar like this:

Object Name: C:\ public\edp\test.txt
Client User Name: test
Client Domain: WIN2K3DOM
Accesses: DELETE

Now, you can track who delete the files. You can add a group instead of one TEST account.

I hope the above information helps.

Have a nice day.

Best Regards,

Steven Zhu
MCSE
Microsoft Online Partner Support
Get Secure! – www.microsoft.com/security

=====
PLEASE NOTE the newsgroup SECURE CODE and PASSWORD were updated on February 14, 2006.? Please complete a re-registration process by entering the secure code mmpng06 when prompted. Once you have entered the secure code mmpng06, you will be able to update your profile and access the partner newsgroups.

=====
When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from this issue.

=====
This posting is provided "AS IS" with no warranties, and confers no rights.
=====