

Re: I need a Step-by-Step to set up file deletion Auditing on SBS...

Re: I need a Step-by-Step to set up file deletion Auditing on SBS...

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-11/msg02622.html>

- *From:* "Anna Clark" <anna.clark(remove this)@verizon.net>
 - *Date:* Wed, 15 Nov 2006 08:07:34 -0500
-

Hi David:

This is from a MS Support group, posted by one of the PSS specialists. Let us know if it helps

Regards:

—

Anna Clark

Please do reply/post the conclusion or solution to your issue so that others may benefit.

From your post, my understanding on this issue is: you configure auditing

for some file and directory deletions, but you cannot seem any log regarding this in the security event log. If I am off base, please feel free to let me know.

Based on my knowledge, if you want to configure auditing for file and directory deletions, please enable Audit Object Access success/failure in Default Domain Controllers Policy. To do so, please refer to the following steps:

1. Click Start, point to Programs, point to Administrative Tools, and then click Active Directory Users and Computers.
2. On the View menu, click Advanced Features.
3. Right-click Domain Controllers, click Properties.
4. Click the Group Policy tab, click Default Domain Controller Policy, and then click Edit.
5. Click Computer Configuration, double-click Windows Settings, double-click Security Settings, and double-click Local Policies, and then double-click Audit Policy.
6. In the right pane, right-click Audit Object Access, click Properties.
7. Click Define These Policy Settings, and then click to select one or both of the following check boxes:
 - Success: Click to select this check box to audit successful attempts for

Re: I need a Step-by-Step to set up file deletion Auditing on SBS...

Re: I need a Step-by-Step to set up file deletion Auditing on SBS...

the event category.

– Failure: Click to select this check box to audit failed attempts for the event category.

8. Click OK.

Note: Because the changes that you make to your computer's audit policy setting take effect only when the policy setting is propagated or applied to your computer, complete either of the following steps to initiate policy propagation:

– Type `gpupdate /Target:computer` at the command prompt, and then press ENTER.

– Wait for automatic policy propagation that occurs at regular intervals that you can configure. By default, policy propagation occurs every five minutes.

Also, please enable specify the files and folders that you want audited. To do so:

1. In Windows Explorer, locate the file or folder you want to audit. Right-click the file and folder you want to audit, and then click Properties.

2. Click the Security tab, and then click Advanced.

3. Click the Auditing tab, and then click Add.

4. In the Enter the object name to select box, type the name of the user or group whose access you want to audit. You can browse the computer for names by clicking Advanced, and then clicking Find Now in the Select User or Group dialog box.

5. Click OK.

6. Select the Successful or Failed check boxes for the actions you want to audit, and then click OK.

7. Click OK twice.

Finally, you can open the Security log to view logged events. Additionally, if you are either a domain or an enterprise administrator, you can enable security auditing for workstations, member servers, and domain controllers remotely.

I hope the above information helps.

Have a nice day.

Best Regards,

Steven Zhu
MCSE

Re: I need a Step-by-Step to set up file deletion Auditing on SBS...

Re: I need a Step-by-Step to set up file deletion Auditing on SBS...

Microsoft Online Partner Support

"dsatchell" <support@xxxxxxxxxxxxxxxxxxxxxx> wrote in message

news:A3E68496-ECB1-4796-AAB0-03E2BE923BF9@xxxxxxxxxxxxxxxxxx

I have a client that has had files suddenly disappear or get deleted

several

times over the last 3 months so I'm trying to set up Auditing so that if someone deletes a files or directory then that actions will get logged.

I know that SBS has this capability but I can't find anything on it. I

know

I'm just missing it but I would really appreciate a Step-By-Step if anyone has it.

Thankx, David.