

RE: Security Log Full

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-02/msg01590.html>

- *From:* George Beckwith <GeorgeBeckwith@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sun, 11 Feb 2007 14:59:00 -0800
-

Terrence,

I tried expanding the size of the log file, and clearing the log file, but this did not solve the problem. What is happening is that something is changing the security log setting back to their default. I changed the size to 1536 KB, but shortly thereafter it was back to 512 KB. Where are the settings stored – in the registry or some other place. Could Group Policy be changing the settings back to default or is something associated with Small Business Server changing them?

Thanks,

George

"Terrence Liu [MSFT]" wrote:

Hello George,

Thank you for posting here.

According to your description, I understand that you often receive error message "The security log on the system is full" when you log on SBS. If I have misunderstood the problem, please don't hesitate to let me know.

First, you go to Event Viewer, right click the Security Log and click Properties, uncheck Success Audit under the Filter tab, and apply these changes. When you go back to event viewer, the success audit is still ticked.

The filter is only filter the exist logs for view. The success audit will still write into the log files. When you go back to event viewer, the success audit is still display in the log list. This is correct.

But your event log is full very often is an issue. I suggest we try the following steps to see if we can resolve this issue:

Step 1:

Clear security log first: right click security in Event viewer, select

RE: Security Log Full

clear all events

Enlarge maximum log size: right click security in Event viewer, select properties, input larger size in the box Maximum log size.

Step 2:

Based on my research, in SBS 2003, the full security audit is enabled by default so that you are able to monitor the server and network access events if needed. It's normal that many logon/logoff events are logged because one logon/logoff procedure can generate several events. The logon/logoff procedures are always performed by service startup/shutdown, shared file accessing, network accessing, users' logon/logoff etc. So the event log will full very soon. You may safely ignore these events.

If you do want to stop these events, you can turn off Success logon auditing, although it is not recommended. To do so:

1. Click Start, click Run, type "gpmmc.msc" and click OK.
2. Expand Domains -> your domain -> Domain Controllers.
3. Right-click Small Business Server Auditing Policy and click Edit.
4. Expand Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy.
5. In the right pane, double-click Audit logon events and clear the Success check box. Click OK.
6. Run "gpupdate /force" on SBS

More information:

Securing Your Windows Small Business Server 2003 Network

<http://www.microsoft.com/downloads/details.aspx?familyid=f62b2722-267c-4642-b287-c31115ef10a4&displaylang=en>

Account Passwords and Policies

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/bpactlck.msp>

Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP

<http://www.microsoft.com/downloads/details.aspx?FamilyId=1B6ACF93-147A-4481-9346-F93A4081EEA8&displaylang=en>

Meanwhile, for the gpedit.msc grey out issue, this is a separate issue. Please understand that our newsgroup is an issue based service, meaning we usually respond to one question/issue per post. This will lessen the confusion for both of us, as well as ensure that our results are accurate and not a result of a test for a different question. Therefore, I suggest you create a new post for getting more quick assistance.

I hope the above information helps. If you have any questions or concerns, please do not hesitate to let me know.

Save the security event log as evt file on the problematic machines and

RE: Security Log Full

send to my mailbox: v-terliu@xxxxxxxxxxxxxx

Have a nice day!

Best regards,

Terence Liu(MSFT)

Microsoft CSS Online Newsgroup Support

Get Secure! – www.microsoft.com/security

=====
This newsgroup only focuses on SBS technical issues. If you have issues regarding other Microsoft products, you'd better post in the corresponding newsgroups so that they can be resolved in an efficient and timely manner. You can locate the newsgroup here:

<http://www.microsoft.com/communities/newsgroups/en-us/default.aspx>

When opening a new thread via the web interface, we recommend you check the "Notify me of replies" box to receive e-mail notifications when there are any updates in your thread. When responding to posts via your newsreader, please "Reply to Group" so that others may learn and benefit from your issue.

Microsoft engineers can only focus on one issue per thread. Although we provide other information for your reference, we recommend you post different incidents in different threads to keep the thread clean. In doing so, it will ensure your issues are resolved in a timely manner.

For urgent issues, you may want to contact Microsoft CSS directly. Please check <http://support.microsoft.com> for regional support phone numbers.

Any input or comments in this thread are highly appreciated.

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

| Thread-Topic: Security Log Full
| thread-index: AcdLzHtRhThc7kEgRdqJssYMK2xqyQ==
| X-WBNR-Posting-Host: 76.172.54.192
| From: =?Utf-8?B?R2VvcmdlIEJlY2t3aXRo?=
<GeorgeBeckwith@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
| Subject: Security Log Full
| Date: Thu, 8 Feb 2007 14:00:01 -0800
| Lines: 14
| Message-ID: <B5339078-F818-4C55-AB77-DD2B51D06929@xxxxxxxxxxxxxx>
| MIME-Version: 1.0
| Content-Type: text/plain;
| charset="Utf-8"

RE: Security Log Full

| Content-Transfer-Encoding: 7bit
| X-Newsreader: Microsoft CDO for Windows 2000
| Content-Class: urn:content-classes:message
| Importance: normal
| Priority: normal
| X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.2757
| Newsgroups: microsoft.public.windows.server.sbs
| Path: TK2MSFTNGHUB02.phx.gbl
| Xref: TK2MSFTNGHUB02.phx.gbl microsoft.public.windows.server.sbs:15880
| NNTP-Posting-Host: tk2msftibfm01.phx.gbl 10.40.244.149
| X-Tomcat-NG: microsoft.public.windows.server.sbs

|
| I am running SBS 2003 which I upgraded from SBS 2000. This problem
happened
| just after the upgrade.
| When I log on to the server I am getting Logon Message, "The security log
on
| the system is full". I go to Event Viewer, right click the Security Log
and
| click Properties. I then change the option to Overwrite as Needed, clear
the
| log, and also uncheck Success Audit in the Filter tab, and Apply these
| changes. If I go back a few minutes later these setting are still in
place,
| however a few hours later they have been mysteriously changed back to the
| default of Overwrite Events Older than 30 Days, and I get the Logon
Message
| again.
| Also when I Run gpedit.msc all of the options are greyed out.
| Any help you can provide will be greatly appreciated.

|
| Thanks, George Beckwith
|