

RE: Event ID 538 540 and 576

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-07/msg02729.html>

- *From:* ACPDON <ACPDON@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 19 Jul 2007 07:46:03 -0700
-

Thanks for taking the time to help me. There are about 28 users on the domain. The updates that I applied right before I started getting hit with these events were:

Security Update for Windows Server 2003 KB935840
Cumulative Security Update for Outlook Express for Windows Server 2003 KB929123
Cumulative Security Update for Internet Explorer for Windows Server 2003 KB933566
Critical Update for Windows Small Business Server 2003: Vista and Outlook 2007 KB926505
Update for Windows Server 2003 KB927891
Windows Malicious Software Removal Tool – June 2007 KB890830
Security Update for Windows Server 2003 KB935840

I changed the audit policy as you suggested and forced the update but I am still getting the 538/540/576 events for the server in the security log.

"Robert Li [MSFT]" wrote:

Hello,

Thanks for posting in our newsgroup.

First, I would like to introduce these events to you.

538 – The logoff process was completed for a user

540 – A user successfully logged on to a network.

576 – Specified privileges were added to a user's access token. Note: This event is generated when the user logs on

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

RE: Event ID 538 540 and 576

accessing, users' logon/logoff etc. Event 540 indicates a successful logon; event 538 indicates a successful logoff and event 576 indicates a successful special privilege assign. In most cases, it's a normal behavior and we can ignore the events.

To find the root cause of this issue, please help me collect the following information for further research:

1. Please export the Application Event log file and email it to me. To export the application event log:

Note: If the log is big file, you can select a export the log for only one day.

- 1) Click Start -> Run, type EVENTVWR.MSC and click OK.
- 2) Right click the Application Event, select Save Log File as, save it to .evt file.
- 3) Email me the file to v-robelt@xxxxxxxxxxxxxx with subject: 39927173-Event ID 538 540 and 576.

2. How many users are in your domain?

3. Do you remember which update you applied when the issue first occurred?

You may also consider disabling some security audit policies:

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".

I am looking forward to hear from you.

If you need further assistance, please don't hesitate to let me know.

Best regards,

Robert Li(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

RE: Event ID 538 540 and 576

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: Event ID 538 540 and 576
<thread-index: AcfJb8v6U6OUtH2uQ0GCe1zFK0mFZg==
<X-WBNR-Posting-Host: 207.46.193.207
<From: =?Utf-8?B?QUNQRE9O?=<ACPDON@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
<Subject: Event ID 538 540 and 576
<Date: Wed, 18 Jul 2007 12:14:00 -0700
<Lines: 94
<Message-ID: <4205F67A-105E-470F-9BF6-BD0F42C9DA41@xxxxxxxxxxxx>
<MIME-Version: 1.0
<Content-Type: text/plain;
< charset="Utf-8"
<Content-Transfer-Encoding: 8bit
<X-Newsreader: Microsoft CDO for Windows 2000
<Content-Class: urn:content-classes:message
<Importance: normal
<Priority: normal
<X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.2826
<Newsgroups: microsoft.public.windows.server.sbs
<Path: TK2MSFTNGHUB02.phx.gbl
<Xref: TK2MSFTNGHUB02.phx.gbl microsoft.public.windows.server.sbs:51182
<NNTP-Posting-Host: tk2msftsbfm01.phx.gbl 10.40.244.148
<X-Tomcat-NG: microsoft.public.windows.server.sbs
<
<I have been getting the events posted below in the security log. I have read
<some articles saying that having 1000's of 538,540,and 576 events is

RE: Event ID 538 540 and 576

normal

<and not to worry about it. My question is, if its normal, how come these
<events didn't start appearing in the log until recently? I haven't
changed

<any of the audit policies in over a year. They started after I installed
<some Patch Tuesday patches on June 19th.

< To make matters worse, I am required to keep at least 3 months of
security

<log data. The current log size is 348mb and it only goes back 3 days. To
<keep 3 months of data will require at least 10GB of space. That seems
<somewhat excessive for a Small Business server.

<How can I get the security event log back to the way it was before without
<turning off auditing entirely?

<

<Thanks

<

<

<Event Type: Success Audit

<Event Source: Security

<Event Category: Logon/Logoff

<Event ID: 538

<Date: 7/18/2007

<Time: 2:46:50 PM

<User: NT AUTHORITY\SYSTEM

<Computer: %ServerName%

<Description:

<User Logoff:

< User Name: %ServerName% \$

< Domain: %DomainName%

< Logon ID: (0x0,0x47DCEDAE)

< Logon Type: 3

<

<

<For more information, see Help and Support Center at

<<http://go.microsoft.com/fwlink/events.asp>.

<

<Event Type: Success Audit

<Event Source: Security

<Event Category: Logon/Logoff

<Event ID: 540

<Date: 7/18/2007

<Time: 2:46:50 PM

<User: NT AUTHORITY\SYSTEM

<Computer: %ServerName%

<Description:

<Successful Network Logon:

< User Name: %ServerName%

< Domain: %DomainName%

< Logon ID: (0x0,0x47DCEDAE)

< Logon Type: 3

< Logon Process: Kerberos

RE: Event ID 538 540 and 576

< Authentication Package: Kerberos
< Workstation Name:
< Logon GUID: {90a38bcb-997e-a552-2022-5b88cc8522b4}
< Caller User Name: -
< Caller Domain: -
< Caller Logon ID: -
< Caller Process ID: -
< Transited Services: -
< Source Network Address: 192.168.0.4
< Source Port: 29723
<
<
<For more information, see Help and Support Center at
<<http://go.microsoft.com/fwlink/events.asp>.
<
<Event Type: Success Audit
<Event Source: Security
<Event Category: Logon/Logoff
<Event ID: 576
<Date: 7/18/2007
<Time: 2:46:50 PM
<User: NT AUTHORITY\SYSTEM
<Computer: 'ServerName'
<Description:
<Special privileges assigned to new logon:
< User Name: 'ServerName' \$
< Domain: 'DomainName'
< Logon ID: (0x0,0x47DCEDAE)
< Privileges: SeSecurityPrivilege
< SeBackupPrivilege
< SeRestorePrivilege
< SeTakeOwnershipPrivilege
< SeDebugPrivilege
< SeSystemEnvironmentPrivilege
< SeLoadDriverPrivilege
< SeImpersonatePrivilege
< SeEnableDelegationPrivilege
<
<For more information, see Help and Support Center at
<<http://go.microsoft.com/fwlink/events.asp>.
<
<I changed the server and domain names in the events, but they are the name
<of the SBS server and my domain.
<
<