

Re: Security Logon/Logoff Events

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-01/msg01557.html>

- *From:* "Jon Lewis" <jon.lewis<nospam>@btinternet.com>
 - *Date:* Thu, 11 Jan 2007 10:22:40 -0000
-

Thank you Terence

I haven't yet set password policy or configured account lockout policy so I will do that in due course to fully secure the server. The majority of the security events that are being recorded are generated from the server itself, mainly logon, logoff and privilege assignment events 540, 538, 576

The client computer is not an issue here. I meant that only one client computer was logged on the system at the time of my post i.e. there was very little network activity. So my query refers to the server itself.

This is our brand new installation of SBS 2003 R2 Premium which includes ISA which I set up with the relevant wizards so I doubt whether it would be necessary to alter any of the default ISA settings.

I have sent the event logs (of the server) to you (zipped). Please let me know whether you think the frequency of the security events is normal. Our network is server and five client computers (all XP SP2 fully up to date).

Many thanks for your help.

Jon Lewis

"Terence Liu [MSFT]" <v-terliu@xxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:kf04deVNHHA.2080@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Hello Jon,

Thank you for your post.

According to your description, I understand that you get many logon/logoff event logs on SBS. If I have misunderstood the problem, please don't hesitate to let me know.

Generally, there really have many logon and logoff actions on SBS, for example, there is a GPO "Small Business Server Auditing Policy" on the SBS Server to audit logon events.

Re: Security Logon/Logoff Events

Just for your reference, the following are some common suggestions for securing the server.

1. Enable complicated password policy.

Note: The Password Policy need to be configured in Default Domain policy.

We can configure the settings under:

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy

2. Configure account lockout policy.

Generally, it is a best practices suggestion to set the Threshold value to 10 or higher. This is high enough to rule out user error and low enough to deter hackers, especially when the password complexity policy is enabled.

For medium security requirement, the recommended configurations are:

Reset account lockout counter after: 30

Account lockout duration: 30

Account Lockout Threshold: 10

For high security requirement, the recommendations are:

Reset account lockout counter after: 30

Account lockout duration: 0

Account Lockout Threshold: 10

For more information, please refer to:

Account Passwords and Policies

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

3. Check your firewall to ensure that only the necessary ports are opened.

Important: I strongly suggest you to close port 425.

4. Ensure the above settings have been successfully applied.

1) On the problematic SBS server, please run the following command to refresh the group policy changes:

GPUPDAGE /FORCE

2) Run SECPOL.MSC and check the above changed password, Account lockout and auditing policies to see their effective settings, and ensure that the policies have been applied successfully.

Re: Security Logon/Logoff Events

5. Please install latest service patch and apply all update on this problematic client.

6. Please install Antivirus software on this client, and do a full scan.

If the issue persists, please kindly help me collect some information for further investigation:

Save the application event log, security log and system event log as evt files on the problematic machine and send to my mailbox:
v-terliu@xxxxxxxxxxxxxx

Thank you for your time and cooperation!

Hope these steps will give you some help.

Thanks and 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.

Re: Security Logon/Logoff Events

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

| From: "Jon Lewis" <jon.lewis<nospam>@btinternet.com>
| Subject: Security Logon/Logoff Events
| Date: Wed, 10 Jan 2007 19:19:35 -0000
| Lines: 10
| X-Priority: 3
| X-MSMail-Priority: Normal
| X-Newsreader: Microsoft Outlook Express 6.00.2900.2869
| X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2962
| X-RFC2646: Format=Flowed; Original
| Message-ID: <uzHCCxONHHA.4992@xxxxxxxxxxxxxxxxxxxxxxxx>
| Newsgroups: microsoft.public.windows.server.sbs
| NNTP-Posting-Host: host81-130-202-78.in-addr.btopenworld.com
81.130.202.78
| Path: TK2MSFTNGHUB02.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTNGP04.phx.gbl
| Xref: TK2MSFTNGHUB02.phx.gbl microsoft.public.windows.server.sbs:9414
| X-Tomcat-NG: microsoft.public.windows.server.sbs
|
| I have one client (the one I'm sending this message from) currently
logged
| onto our new SBS2003R2 server. The EventLog is constantly recording
| thousands of System LogOn/LogOff events sometimes 80 per second. They
are
| all successfull and I can see from Googling that Logon/Logoffs happen
all
| the time but 80 per second!!!???? I know I can disable recording these
| events but am concerned that so many are being generated. Should I be?
|
| TIA
|
|
|