

Re: Security event id 537

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-09/msg00496.html>

- *From:* SteveC <scashman@xxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 8 Sep 2008 05:08:29 -0700 (PDT)
-

On Sep 7, 10:22 pm, v-mil...@xxxxxxxxxxxxxxxxxxxxxx (Miles Li [MSFT]) wrote:

Hello,

Thank you for posting here.

According to your description, I understand that:

You notice that there are thousands of the Event Id 537 that indicates the Logon Failure.

If I have misunderstood the problem, please don't hesitate to let me know..

Explanations:

=====

From the detail in the event log, the error code 0x80090308 can translated to SEC_E_INVALID_TOKEN indicating that an invalid token has been received.. As that is a invalid token, other fields are not recognized properly. This should be the reason why other fields are blank.

1. Because we cannot identify the source computer(s) which send the invalid request, we may have to perform a network traffic trace to narrow down the source. You can get the network monitor from the following link and install it on the SBS server.

Download the NetMon3.1 from the following link:
<http://www.microsoft.com/downloads/details.aspx?FamilyID=18b1d59d-f4d...8d17-2f6dde7d7aac&DisplayLang=en>

a) Start the capture and wait on until new Event log 537 is logged.

b) Stop the capture and save the network trace file.

2. From my experience, it may result from the third-party applications that try to communicate with network resource using unavailable protocols. Do you recently install any applications on the clients/server? To narrow down the source, you also can power down the suspect computer to have a try.

Re: Security event id 537

On the suspect computer we can perform a Clean Boot that will allow us to isolate any programs that are loading at startup that may be causing a conflict with other device drivers or programs that are installed in your computer.

- 1) Run MSCONFIG.EXE. (MSCONFIG is a built-in tool for Windows XP\2003 systems.)
- 2) In the Services tab, click "Hide All Microsoft Services" and click "Disable All". Please note that the Exchange services could be marked as non-Microsoft. Please do not disable those services.
- 3) In the Startup tab, click "Disable All". Click OK. (This will temporarily prevent third-party programs from running automatically during start-up.)
- 4) Restart the computer. Does the problem still persist?

If the problem does not occur, it indicates that the problem is related to one application or service we have disabled. You can use the MSCONFIG tool again to re-enable the disabled item one by one to find out the culprit.

To further troubleshoot this issue, please answer the following questions:

=====

1. Is the Event log 537 recorded regularly with a specific interval?
2. Have you deployed any applications/updates in the domain recently?
3. Try to enable debug logging for the Net Logon service according to the Microsoft knowledge Base article 109626 and collect the log file.

109626 Enabling debug logging for the Net Logon service <http://support.microsoft.com/kb/109626>

4. Please send me v-mil...@xxxxxxxxxxxxx the network trace and the log file.

If you have any questions or concerns, please do not hesitate to let me know.

Best regards,
Miles Li

Microsoft Online Partner Support
Microsoft Global Technical Support Center

Get Secure! - www.microsoft.com/security

=====

When responding to posts, please "Reply to Group" via your newsreader so

Re: Security event id 537

that others may learn and benefit from your issue.

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

Thank you Miles. I'll give those steps a try. I didn't install any software recently. I read another thread where someone mentioned that it might have been related to Trend Micros Worry Free Security. That was installed when the operating system was installed.

.