

Re: Event ID 537 and Kerberos

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-03/msg02939.html>

- *From:* v-robeli@xxxxxxxxxxxxxxxxxxxxxxxx (Robert Li [MSFT])
 - *Date:* Wed, 21 Mar 2007 10:24:48 GMT
-

Hi Dan,

Thanks for updating.

Since event 537 appears after you applied ISA 2004 SP2, the problem may be related to ISA, not virus or hacks.

Please take your time collect the following information for further research, thanks for your time and cooperation.

1. Collect the ISA firewall logs so that we can identify the cause from the log:

Enable the full firewall logging option:

- a. Open ISA 2004 management console.
- b. Expand the server node and highlight 'Monitoring'.
- c. In the right pane, switch to the 'Logging' tab, make sure the 'Task Pane' is showed there.
- d. In the 'Task Pane', click 'Configure firewall Logging' under 'Logging Tasks', and then switch the 'log storage format' from 'MSDE database' (default) to 'File'.
- e. Switch to the 'Fields' tab, and then click 'Select All'.
- f. Click OK, and then click 'Apply' to save changes and update the configuration.

Prepare to take the trace:

- a. Temporarily stop the Firewall service to clear the current existing W3C logs: Monitoring->Services tab, and then right click 'Microsoft Firewall' to choose 'Stop'.
- b. Go to the log saving directory and clean any existing .W3C logs. By default, the logs will be saved to 'C:\Program Files\Microsoft ISA Server\ISALogs'. (Some MDF may not be able to deleted, that's normal.)
- c. Go back to the ISA 2004 management console, and then Start the stopped 'Microsoft Firewall' service.

Reproduce the problem:

- a. Enable the 'Block IP Fragments' settings. Apply the change. Reboot the ISA server.

Re: Event ID 537 and Kerberos

- b. Stop the 'Microsoft Firewall' service. Open Windows Explorer, navigate to the ISA log file folder. Collect the recent w3c files. Save them to a zip package as 'isalogs.zip'. Start the 'Microsoft Firewall' Service.
- c. Send the zip packages to me.

2. MPS Report

- 1) Please download the MPSRPT_SETUPPerf.EXE from the following link and then run this tool to gather some information from the problematic computer:
<http://www.microsoft.com/downloads/details.aspx?familyid=cebf3c7c-7ca5-408f-88b7-f9c79b7306c0&displaylang=en>
- 2) Double-click on the MPSRPT_SETUPPerf.EXE file.
[Note] This process may take some time; however, it will not have a negative effect on the performance.
- c. A CAB file will be generated in the
%systemroot%\MPSReports\Setup\Reports\Cab directory called
%COMPUTERNAME%_MPSReports.CAB. The CAB file will contain the reports generated by the MPS Reporting Tool.

Please send the log files to my mailbox: v-robeli@xxxxxxxxxxxxx with subject: 38384907- Event ID 537 and Kerberos.

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 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

Re: Event ID 537 and Kerberos

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.

<From: "DanDanDan" <DanDanDan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
<References: <#Qy7OcgHHA.4808@xxxxxxxxxxxxxxxxxxxxxxxx>
<dGcY8esaHHA.1176@xxxxxxxxxxxxxxxxxxxxxxxx>
<Subject: Re: Event ID 537 and Kerberos
<Date: Tue, 20 Mar 2007 16:13:20 +0200
<Lines: 217
<X-Priority: 3
<X-MSMail-Priority: Normal
<X-Newsreader: Microsoft Outlook Express 6.00.2900.3028
<X-RFC2646: Format=Flowed; Original
<X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3028
<Message-ID: <OPBOBnvaHHA.4180@xxxxxxxxxxxxxxxxxxxxxxxx>
<Newsgroups: microsoft.public.windows.server.sbs
<NNTP-Posting-Host: 82.79.10.62
<Path: TK2MSFTNGHUB02.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTNGP05.phx.gbl
<Xref: TK2MSFTNGHUB02.phx.gbl microsoft.public.windows.server.sbs:24023
<X-Tomcat-NG: microsoft.public.windows.server.sbs

- <
<I installed again the server in this order:
<1. First phase (OS setup)
<2. Hardware drivers
<3. "Continue Setup" Step
<4. "To Do List -> Connect to the internet" Step
<5. "To Do List -> Configure Remote Access" Step
<6. SQL Server 2005
<7. SQL Server 2005 SP2
<8. ISA Server 2004
<9. ISA Server 2004 SP2
<10. ISA Server 2004 - KB916106
<11. Exchange Server 2003 - SP2
<12. SharePoint Services - SP2
<13. SBS 2003 R2
<14. Windows Server 2003 - SP2
<15. Activate Windows
<16. Microsoft Update
<18. WSUS Sync
<
<After each step I searched security log for 537 event.

Re: Event ID 537 and Kerberos

<Event ID 537 was logged after installing ISA Server 2004 SP2, after reboot.

<

<Regards,

<Dan

<

<

<

<"Robert Li [MSFT]" <v-robali@xxxxxxxxxxxxxxxxxxxxxx> wrote in message

<news:dGcY8esaHHA.1176@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

> Hi Dan,

>

> Thanks for posting in our newsgroup.

>

> From your description, I know that you get Event ID 537 every time you

> boot

> server. If I am off-base, please don't hesitate to let me know.

>

> Based on my research, a logon type of 3 translates to Network. Error

> 0xC00000DC means "STATUS_INVALID_SERVER_STATE" and you can try a reboot
> of

> the server.

>

> Please take the following steps to see if the problem can be resolved:

>

> Step 1: Please make a clean boot. The problem occurs when third-party

> software installed which need to communicate with the network, but it
> does

> not support Kerberos authentication. It is known that "hp laser jet tool

> box" and some other third-party software will have this issue.

>

> 1. Click Start->Run...->type msconfig and press Enter.

> 2. Click Services tab and select Hide All Microsoft Services and Disable

> All third party Services.

> 3. Click Startup tab and Disable All startup items.

> 4. Click OK and choose Restart.

> 5. After reboot, check whether the problem still occurs.

> 6. If there are no more problems, please use the above steps to enable

> services and startup items one by one in order to figure out the root

> cause

> of this issue.

>

> Step 2: Use an Enterprise anti-virus with updated signatures and scan you

> machine. The problem may be caused by some virus.

>

> Step3: Implement Strong password policies. To do this:

>

> Open "Server Management console", navigate to Users snap-in. In the

> right

> panel, click "Configure Password Policies". Enable the password

> policies.

>

Re: Event ID 537 and Kerberos

Re: Event ID 537 and Kerberos

◇ For more information, please refer to:

◇

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

◇ security/bpactlck.msp

◇

◇ Step 4: Configure account lockout policy.

◇

◇ 1) Click Start, click Settings, click Control Panel, double-click

◇ Administrative Tools, and then double-click Active Directory Users and

◇ Computers.

◇ 2) In the console tree, right-click the domain on which you want to set a

◇ Group Policy object.

◇ 3) Click Properties, and then click the Group Policy tab.

◇ 4) In Group Policy Object Links, click Default Domain Policy or create
and

◇ name your Group Policy object, and then click Edit.

◇ 5) In the console tree, double-click Computer Configuration, double-click

◇ Windows Settings, double-click Security Settings, double-click Account

◇ Policies, and then click Account Lockout Policy.

◇ 6) In the details pane, right-click the policy setting that you want, and

◇ then click Properties.

◇ 7) If you are defining this policy setting for the first time, click

◇ Define

◇ this policy setting.

◇ 8) Click the options that you want, and then click OK.

◇

◇ 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.msp

◇ If the problem still exists, please kindly collect the following

◇ information for further research:

◇

◇ MPS Report

◇

◇ 1) Download MPS report tool from:

◇

<http://download.microsoft.com/download/b/b/1/bb139fcb-4aac-4fe5-a579-30b0bd9>

◇ 15706/MPSRPT_SETUPPerf.EXE

Re: Event ID 537 and Kerberos

- <> 2)? Run the MPSRPT_SETUPPerf.exe on the server box.
- <> 3) Wait for 10~15 minutes.
- <> 4)? Open Windows explorer, navigate to
- <> %SYSTEMROOT%\MPSReports\Setup\Reports\cab\
- <> 5) Send the .cab file to us.
- <>
- <> Please send to information to v-robelt@xxxxxxxxxxxxxx with subject:
- <> 38384907-Event ID 537 and Kerberos.
- <>
- <> 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
- <> 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: Event ID 537 and Kerberos

◇ This posting is provided "AS IS" with no warranties, and confers no
◇ rights.
◇
◇ -----
◇ <From: "DanDanDan" <DanDanDan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
◇ <Subject: Event ID 537 and Kerberos
◇ <Date: Mon, 19 Mar 2007 11:14:52 +0200
◇ <Lines: 28
◇ <X-Priority: 3
◇ <X-MSMail-Priority: Normal
◇ <X-Newsreader: Microsoft Outlook Express 6.00.3790.3959
◇ <X-RFC2646: Format=Flowed; Original
◇ <X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.3959
◇ <Message-ID: <#Qy7OcgHHA.4808@xxxxxxxxxxxxxxxxxxxxxxxx>
◇ <Newsgroups: microsoft.public.windows.server.sbs
◇ <NNTP-Posting-Host: 82.79.10.62
◇ <Path: TK2MSFTNGHUB02.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTNGP04.phx.gbl
◇ <Xref: TK2MSFTNGHUB02.phx.gbl microsoft.public.windows.server.sbs:23722
◇ <X-Tomcat-NG: microsoft.public.windows.server.sbs
◇ <
◇ <Hello !
◇ <
◇ <At every server boot I found Event ID 537 in Security log.
◇ <What can I do to solve this ?
◇ <
◇ <Logon Failure:
◇ <Reason: An error occurred during logon
◇ <User Name: SBS1\$ <--(this is the server name)
◇ <Domain: DomainName.LOCAL
◇ <Logon Type: 3
◇ <Logon Process: Kerberos
◇ <Authentication Package: Kerberos
◇ <Workstation Name: -
◇ <Status code: 0xC00000DC
◇ <Substatus code: 0x0
◇ <Caller User Name: -
◇ <Caller Domain: -
◇ <Caller Logon ID: -
◇ <Caller Process ID: -
◇ <Transited Services: -
◇ <Source Network Address: 127.0.0.1
◇ <Source Port: 0
◇ <
◇ <Thank you !
◇ <Dan
◇ <
◇ <
◇ <
◇ <
◇ <
◇ <
◇ <

Re: Event ID 537 and Kerberos

<
<
.