

RE: Help .. Small Business Server Error may be DNS ?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-12/msg03893.html>

- *From:* "Iain Marshall" <IainMarshall@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 21 Dec 2005 00:37:02 -0800
-

Thank you so much for your reply...

I will follow the steps today you have outlined. (UK – GMT)

I Installed Symantec Anti-Virus Corporate Edition inc Exchange and I am sure the events occurred after said installation. (I will remove this today and re-boot)
this will be my first step.

I have already excluded remote Attacks as the domain server was isolated from the network & internet during the weekend and the Cisco router was set to Deny all Nettraffic and monitor packets. The same 3 errors occurred.

There is no 534 event.

Again the only event was as posted reference " server1\$ ".

I will keep this link active over the next day or so and would be grateful if you could monitor any postings.

Many Many thanks

Iain Marshall.

""Crina Li"" wrote:

- > Hi Iain,
- >
- > Thank you for posting in SBS newsgroup.
- >
- > From the description, I understand the issue to be: you have received event
- > 529 and LSASRV 40960 and 40961 on your SBS. If I have misunderstood your
- > concerns, please do not hesitate to let me know.
- >
- > {Note: the reply may be too long and I am appreciated your time to follow
- > it}

RE: Help .. Small Business Server Error may be DNS ?

- >
- > Regarding the event LSASRV 40960 and 40961 appear on SBS, as I know, this
- > issue can occur when you restart the SBS 2003 server. A service, for
- > example, the Windows Time service (W32Time), tries to authenticate before
- > Directory Services has started. You can just safely ignore the event as it
- > will not cause any adverse effects to the server. For more information, see:
- >
- > 823712 Event IDs 40960 and 40961 in the System Event Log When You Restart
- > <http://support.microsoft.com/?id=823712>
- >
- > 824217 LSASRV Event IDs 40960 and 40961 When You Promote a Server to a
- > Domain
- > <http://support.microsoft.com/?id=824217>
- >
- > I would suggest you reboot the server again and see if the event does not
- > appear. type the following commands:
- >
- > 1. Net Stop NETLOGON
- > 2. IPCONFIG /FLUSHDNS
- > 3. IPCONFIG /REGISTERDNS
- > 4. Net Start Netlogon
- >
- > The issue could also be a similar to the problem described in the following
- > KB article:
- >
- > 826819 The Server Stops Responding and an Access Violation Occurs in
- > Lsass.exe
- > <http://support.microsoft.com/?id=826819>
- >
- > Regarding event 529, based on my experience, it can occur if you enabled
- > the "Audit logon event" policy on the SBS server and a failure logon
- > attempt is performed from the internal or external computers. A type 3
- > logon type means this was generated from the user trying to access a
- > resource from the network with a bad password or an account that was locked
- > out.
- >
- > We may try the following to see if the problem can be solved:
- >
- > 1. Go to Active Directory Users and Computers and expand server name and
- > then click users.
- > 2. Double click IUSR and then on Account tab make sure the password never
- > expires and user cannot change password is selected and the account is not
- > disabled.
- > 3. Open IIS ADMIN and go to the Default web site and get properties.
- > 4. Go to directory security\Edit.
- > 5. In the Password Field type in a strong password and write it down and
- > hit apply\ok.
- >
- > If you get inheritance override click Select all.....only do this if the
- > IUSR account is the account chosen for these web sites... (this is the
- > default setting).

RE: Help .. Small Business Server Error may be DNS ?

- >
- > 6. Then go to Active Directory Users and Computers and reset the password
- > for the IUSR account (or delete the account).
- > 7. Then run iisreset from the command prompt. It will restart IIS.
- >
- > If it does not work, we can try to reset the anonymous account password as
- > following:
- >
- > 1. Click "Start", point to "Programs", point to "Administrative Tools", and
- > then click "Active Directory Users and Computers".
- > 2. Under the full domain name click "Users".
- > 3. Right-click "IUSR_ComputerName", and then click "Reset Password".
- > 4. Type the password in the "New password" box and in the "Confirm
- > password" box, and then click "OK".
- > 5. Right-click "IWAM_ComputerName", and then click "Reset Password".
- > 6. Type the password in the "New password" box and in the "Confirm
- > password" box, and then click "OK".
- > 7. Quit Active Directory Users and Computers console.
- > 8. Click "Start", and then click "Run".
- > 9. In the "Open" box, type "cmd" (without the quotation marks) and then
- > click "OK".
- > 10. Type the following command and press ENTER:
- >
- > cd \inetpub\adminscripts
- >
- > 11. To reset the password for the IUSR_ComputerName account, type the
- > following command (where <password> is the password that you set in step
- > 4), and then press ENTER:
- >
- > cscript.exe adsutil.vbs set w3svc/anonymoususerpass <password>
- >
- > 12. To reset the password for the IWAM_<omputerName account, type the
- > following command (where <password> is the password that you set in step
- > 6), and then press ENTER:
- >
- > cscript.exe adsutil.vbs set w3svc/wamuserpass <password>
- >
- > 13. After this, type iisreset and press ENTER.
- >
- > If the problem still persists, this may also be an automated dictionary
- > attack on weak passwords. The hacker is trying variable username/password
- > combinations to access the network. The attack can be initiated from
- > internal network or external network. As the event is missing much
- > information such as "Caller User Name" and "Caller Process ID", it is most
- > likely caused by spyware resides on your LAN workstations.
- >
- > Personally, I think if the SBS computer is connected to the internet, many
- > hacker activities may cause Event ID 529 etc. I recommend you to read the
- > following white paper and make sure your server is secure.
- >
- > Threats and Countermeasures: Security Settings in Windows Server 2003 and

RE: Help .. Small Business Server Error may be DNS ?

- > Windows XP
- > <http://www.microsoft.com/downloads/details.aspx?FamilyId=1B6ACF93-147A-4481-9346-F93A4081EEA8&displaylang=en>
- >
- > Sometimes, third party application/services and virus/Spyware may also
- > cause such issue; however, it will be difficult to isolate the root cause
- > if this is the point.
- >
- > Technically speaking, if 529 and 534 appears at the same time, it may
- > indicate that an attacker tries and fails to guess a username and password
- > combination for a local account. However, since there's only 529 event
- > logged (please confirm whether there's any 534 events), it may also occur
- > when a user forgets their password, or starts browsing the network through
- > My Network Places.
- >
- > In a large scale environment it can be difficult to interpret these events
- > effectively. As a rule, you should investigate these patterns if they occur
- > repeatedly or coincide with other unusual factors. For example, a number of
- > 529 events followed by a 528 event in the middle of the night could
- > indicate a successful password attack. You should also monitor your client
- > computers to make sure they do not use any unknown software. Up-to-date
- > Anti-virus software should be a must for all the clients.
- >
- > In addition, you may also want to restrict downloads of certain kind of
- > files from the Internet on the client computers (If you have ISA installed):
- >
- > 1. Create protocol rule and only apply to HTTP, HTTPS. (Maybe too restrict
- > if the users want to use some software such as IM)
- > 2. Create a Site and Content Rules to Allow All Content.
- > 3. Create a Site and Content Rule to Deny the following HTTP Content:
- >
- > - Application
- > - Compressed Files
- > - Macro Documents
- >
- > In addition, I provided some more Info for your reference:
- >
- > 1. I suggest you change the "nolmhash" value to "0" in the following
- > registry key on the SBS 2003 server:
- >
- > HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA
- >
- > Reboot the server for this change to take effect and check if the event
- > does not appear.
- >
- > If the event still appears, go to
- > HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanserver\Parameters
- >
- >
- > and set "enablesecuritysignature" and "requiresecuritysignature" to "0".
- > Reboot the server and check if everything is OK.

RE: Help .. Small Business Server Error may be DNS ?

- >
- > This occurs because the user accounts in the domain no longer had
- > LanManager (LM) hashes stored because of the NoLMHash security setting.
- > This is why existing users worked fine, but new users and users for whom we
- > changed the password, failed to logon. By removing this security setting
- > and resetting the password of the user accounts (to recreate a new LMHash
- > value for their password), the issue may be resolved.
- >
- > 2. This behavior may also happen when the machine password is not properly
- > sync. In order to reset the machine account password of a domain controller
- > use:
- >
- > NETDOM RESETPWD /Server:ServerName /UsedD:Administrator /PasswordD:*
- >
- > The syntax of this command is:
- >
- > NETDOM RESETPWD /Server:domain-controller /UserD:user /PasswordD:[password
- > | *]
- >
- > NETDOM RESETPWD Resets the machine account password for the domain
- > controller on which this command is run. Currently there is no support for
- > resetting the machine password of a remote machine or a member server. All
- > parameters must be specified.
- >
- > /Server Name of a specific domain controller that should have its
- > machine account password reset.
- >
- > /UserD User account used to make the connection with the domain
- > controller specified by the /Server argument.
- >
- > /PasswordD Password of the user account specified with /UserD. A * means
- > to prompt for the password
- >
- > After completing the command, reboot the server.
- >
- > 3. Scan virus on the workstations. Please use the anti-virus software to
- > perform full scan on the internal workstations. There is an online virus
- > scan link below:
- > <http://housecall.trendmicro.com>
- >
- > 4. Implement Strong password policies. Open 'Server Management console',
- > navigate to Users snap-in. In the right panel, click 'Configure Password
- > Policies'. Enable the password policies.
- >
- > For more information:
- >
- > [http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/bpactlck.mspx)
- > [security/bpactlck.mspx](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/bpactlck.mspx)
- >
- > 5. Monitor the internal users to see if anyone is testing the admin
- > accounts.

RE: Help .. Small Business Server Error may be DNS ?

- > 6. Scan and remove all spyware and adware on the server and workstations.
- > For more information and removal tools, see:
- >
- > <http://www.microsoft.com/athome/security/spyware/default.mspx>
- >
- > More information:
- >
- > Securing Your Windows Small Business Server 2003 Network
- > <http://download.microsoft.com/download/1/f/1/f15a874-f696-4992-b5ad-b1e7b258de1c/SecuringSBSnetwork.doc>
- >
- > Auditing User Authentication
- > <http://support.microsoft.com/default.aspx?scid=kb:en-us:174073>
- >
- > Security Event Descriptions
- > <http://support.microsoft.com/default.aspx?scid=kb:en-us:174074>
- >
- > Logoff event messages are not logged in the security log when you use the
- > Audit Logon Events feature in Windows 2000
- > <http://support.microsoft.com/default.aspx?scid=kb:en-us:318253>
- >
- > NOTE: This response contains a reference to a third party World Wide Web
- > site. Microsoft is providing this information as a convenience to you.
- > Microsoft does not control these sites and has not tested any software or
- > information found on these sites; therefore, Microsoft cannot make any
- > representations regarding the quality, safety, or suitability of any
- > software or information found there. There are inherent dangers in the use
- > of any software found on the Internet, and Microsoft cautions you to make
- > sure that you completely understand the risk before retrieving any software
- > from the Internet.
- >
- > I am appreciated your time and look forward to hearing from you.
- >
- > Best regards,
- >
- > Crina 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,

RE: Help .. Small Business Server Error may be DNS ?

> 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: Help .. Small Business Server Error may be DNS ?
> | | From: "=?Utf-8?B?b3BoZWxhaXN5cw==?="

> | <ophelaisys@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
> | Subject: Help .. Small Business Server Error may be DNS ?
> | Date: Tue, 20 Dec 2005 02:18:03 -0800
> | | Newsgroups: microsoft.public.windows.server.sbs
> | |
> | Hi Everyone & Merry Christmas..
> |
> | Can anyone help me put this problem to bed before
> | I start the holiday season.
> |
> | I have a 2k3 SBS standard server (server1) and 10 clients.
> | DHCP . DNS . AD. Exchange. all seem cool.... BUt
> |
> | In the error logs the domain server is failing kerberos authentication..
> |
> | here is a copy of the security error
> |
> | .

• **Follow-Ups:**

- ◆ **RE: Help .. Small Business Server Error may be DNS ?**
 ◇ From: "Crina Li"

• **References:**

- ◆ **Help .. Small Business Server Error may be DNS ?**
 ◇ From: ophelaisys
- ◆ **RE: Help .. Small Business Server Error may be DNS ?**
 ◇ From: "Crina Li"

- Prev by Date: **Re: Cannot browse Internet from ISA 2004 server in Remote Desktop session**
- Next by Date: **RE: Firewall Configuration for SMTP**

RE: Help .. Small Business Server Error may be DNS ?

- Previous by thread: ***RE: Help .. Small Business Server Error may be DNS ?***
- Next by thread: ***RE: Help .. Small Business Server Error may be DNS ?***
- Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***