

# Re: Problems with 529 Events

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-02/msg01773.html>

---

- *From:* [luv2chill@xxxxxxxxxx](mailto:luv2chill@xxxxxxxxxx)
  - *Date:* 12 Feb 2007 16:08:08 -0800
- 

On Feb 5, 1:05 am, v-rob...@xxxxxxxxxxxxxxxxxxxxxxxx (Robert Li [MSFT]) wrote:

Hi Dan,

Thanks for posting in our newsgroup.

I am sorry for the delay response due to the weekend.

From your description, I know that you receive the Event ID: 529 in the security event log. If I am off-base, please don't hesitate to let me know.

Based on my research, the problem may be caused by hackers who is attempting to logon on some services on the SBS server. Please do the following steps on the SBS 2003 server to see if the problem can be resolved:

Step1: 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.

For more information, please refer to:<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/techno...security/bpactlck.mspx>

Step 2: 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

## Re: Problems with 529 Events

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/techno...security/bpactlck.mspx>

Step 3: Use an Enterprise anti-virus with updated signatures and scan you machine.

Step 5: The issue may occur if the remote SBS server sends broadcast packets to the network. I suggest you change the "nolmhash" value to "0" in the following registry key on the SBS 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.

Step 6: Reset the domain controller computer account password. The behavior can happen when the password is not properly Sync.

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.

## Re: Problems with 529 Events

/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.

For more information, please refer to:

How to use Netdom.exe to reset machine account passwords of a Windows Server 2003 domain controller <http://support.microsoft.com/kb/325850>

One the problematic Windows XP clients, please do the following.

Step 1: Make a clean boot. The problem may caused by the some third party software.

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 anti-virus with updated signatures and scan you machine.

You mentioned in previous your post that you keep the port 80 opened, maybe that is not the cause the issue. Please don't close that port.

In addition, the command ;°NETDOM RESETPWD;± is used to reset machine account passwords of a SBS 2003 domain controller and you should use administrate account.

If the problem still exists, please help me collect the MPS Report on the SBS Server and problematic client computer.

1. Download MPS report tool  
from:[http://download.microsoft.com/download/b/b/1/bb139fcb-4aac-4fe5-a579-...15706/MPSRPT\\_SETUPPerf.EXE](http://download.microsoft.com/download/b/b/1/bb139fcb-4aac-4fe5-a579-...15706/MPSRPT_SETUPPerf.EXE)
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 v-rob...@xxxxxxxxxxxxxx with subject: 37724563-  
Problems with 529 Events

Re: Problems with 529 Events

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](http://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.

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

-----  
<From: luv2ch...@xxxxxxxxxx  
<Newsgroups: microsoft.public.windows.server.sbs  
<Subject: Problems with 529 Events  
<Date: 4 Feb 2007 16:22:35 -0800  
<Organization:<http://groups.google.com>  
<Lines: 130  
<Message-ID: <1170634955.293049.311...@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
<NNTP-Posting-Host: 24.124.21.196  
<Mime-Version: 1.0  
<Content-Type: text/plain; charset="iso-8859-1"  
<X-Trace: posting.google.com 1170634974 28191 127.0.0.1 (5 Feb 2007

Re: Problems with 529 Events

00:22:54 GMT)

<X-Complaints-To: groups-ab...@xxxxxxxxxxx

<NNTP-Posting-Date: Mon, 5 Feb 2007 00:22:54 +0000 (UTC)

<User-Agent: G2/1.0

<X-HTTP-UserAgent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727),gzip(gfe),gzip(gfe)

<Complaints-To: groups-ab...@xxxxxxxxxxx

<Injection-Info: v45g2000cwv.googlegroups.com; posting-host=24.124.21.196;

< posting-account=U4KEAQ0AAAA32P\_neBdR2zKw5bXs1WxB

<Path:

TK2MSFTNGHUB02.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTFEEDS01.phx.gbl!newsfeed-0

0.sul.t-online.de!t-online.de!border2.nntp.dca.giganews.com!border1.nntp.dc-a

.giganews.com!nntp.giganews.com!postnews.google.com!v45g2000cwv.googlegroup-s

.com!not-for-mail

<Xref: TK2MSFTNGHUB02.phx.gbl microsoft.public.windows.server.sbs:14901

<X-Tomcat-NG: microsoft.public.windows.server.sbs

<

<Hello all SBS Gurus,

<

<I've got a couple of different issues with 529 events stacking up in

<my security event log on my SBS 2003 SP1 box. I am hoping to get these

<both resolved because I know they're serious and I hate seeing them in

<the server report I get every morning.

<

<1. I think this is the easier of the two (but also the more

<dangerous). I am seeing 529s apparently coming from over the internet.

<Here's a sample:

<

<Date: 2/1/2007 Source: Security

<Time: 2:19:53 PM Category: Logon/Logoff

<Type: Failure Aud Event ID: 529

<User: NT AUTHORITY\SYSTEM

<Computer: SBSSVR

<

<Description:

<Logon Failure:

<

< Reason: Unknown user name or bad password

< User Name: MAILSERVER\$

< Domain: ADLDDOMAIN

< Logon Type: 3

< Logon Process: NtLmSsp

< Authentication Package: NTLM

< Workstation Name: MAILSERVER

< Caller User Name: -

< Caller Domain: -

< Caller Logon ID: -

< Caller Process ID: -

< Transited Services: -

< Source Network Address: -

< Source Port: -

Re: Problems with 529 Events

<  
<The user name, domain and workstation name are different each time and  
<are not any of mine. I have no wireless network and my physical  
<ethernet ports are secure so I assume these are coming in from over  
<the internet.  
<  
<>From the research I have done in this group and elsewhere, it seems  
<that I may be getting these because I have http (port 80) open on the  
<firewall and forwarded to the SBS server (by the way my SBS server has  
<only one network card and is not using ISA. I do all of my port  
<security on the NAT firewall).  
<  
<I do not host any public web sites on my SBS server, but I have kept  
<port 80 open to utilize the built-in http->https redirection built  
<into SBS so that my users don't have to remember to type https when  
<they connect to OWA. If I block port 80, that redirection can no  
<longer happen and typing https: is required.  
<  
<So I guess I am asking is there any way to have the best of both ...

read more »

Thank you for your reply Robert. I did some of the things you asked, but none of those were successful in fixing the two workstations constantly giving 529 errors on the SBS server. I ended up looking at the event viewer on those client machines and came up with some eventids that led me to the solution (1006 - "Windows cannot bind to x domain"). The problem involved old cached credentials on the machine. I had to go into the Users control panel, then click on "Manage Passwords" and delete the entry in there. That stopped the 529 errors from those two workstations. I think the cause for that was that these two users often stay logged in all the time, so when their passwords expired I think their cached credentials didn't get updated. If anyone can shed some light on why that happens, that would be great. For now I've just been trying to remind them to log off each day, but old habits are hard to break.

However, unfortunately I just noticed more 529s coming in from over the internet. I really thought that blocking port 80 would stop them but apparently it didn't. As of right now the only ports open to my SBS server from the net are:

TCP 4125 (Remote Web Workplace)  
TCP 1723 (PPTP)  
TCP 25 (SMTP)  
TCP 443 (HTTPS)

Here is one of the events:

529 2/11/2007 10:10 PM

Re: Problems with 529 Events

Re: Problems with 529 Events

Logon Failure:

Reason: Unknown user name or bad password

User Name: EXCHANGES

Domain: CLINICALSC

Logon Type: 3

Logon Process: NtLmSsp

Authentication Package: NTLM

Workstation Name: EXCHANGE

Caller User Name: –

Caller Domain: –

Caller Logon ID: –

Caller Process ID: –

Transited Services: –

Source Network Address: –

Source Port: –

Again, there is no workstation or domain on my network anywhere with those names. There were three of these in my SBS Security log yesterday. If it is normal to see a few of these then I won't worry about it, but I just want to make sure I don't have some problem that needs to be fixed. Can anyone experienced with SBS let me know if there's anything I can (or shoul) do about this?

Many thanks.

.