

Re: Event ID 539 & 529 in large numbers – from what?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-05/msg02701.html>

- *From:* "Cliff Galiher" <cgaliher@xxxxxxxxxx>
 - *Date:* Tue, 20 May 2008 12:57:49 -0600
-

In the logs you posted, is <username> the name of a user or a machine? And is <workstation> a machine on your network, or does it appear as though it is coming in from an external source?

–Cliff

"Ruth Cheesley suffolkcomputerservices co (dot) uk" <newsgroup<atdot> wrote in message news:eoKo6fquIHA.2188@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hello all,

Wondered if anyone can point me in the right direction for identifying what may be causing the following, which started appearing in the event logs today (SBS 2003). The only thing unique about this particular workstation is that it's running Sage Payroll with data on the SBS as a share. The company only has two other laptops alongside this workstation and the small business server, and 1 printer. Therefore this large number of failures was somewhat alarming when reading through the reports today! All computers and laptops are running legitimate copies of XP, with AVG Small Business Internet Security edition on server & all computers. All are up to date with windows critical & security updates bar SP3.

Source Event ID Last Occurrence Total Occurrences

Security 539 20/05/2008 14:35 12,232 *

Logon Failure:

Reason: Account locked out

User Name: <username>

Domain: <domain name>

Logon Type: 3

Logon Process: NtLmSsp

Authentication Package: NTLM

Workstation Name: <workstation name>

Caller User Name: –

Caller Domain: –

Caller Logon ID: –

Caller Process ID: –

Transited Services: –

Source Network Address: 10.0.0.53

Source Port: 0

Re: Event ID 539 & 529 in large numbers – from what?

Source Event ID Last Occurrence Total Occurrences

Security 529 20/05/2008 14:31 117 *

Logon Failure:

Reason: Unknown user name or bad password

User Name: <username>

Domain: <domain name>

Logon Type: 3

Logon Process: NtLmSsp

Authentication Package: NTLM

Workstation Name: <workstation name>

Caller User Name: –

Caller Domain: –

Caller Logon ID: –

Caller Process ID: –

Transited Services: –

Source Network Address: 10.0.0.53

Source Port: 0

Many thanks,

Ruth