

Exchange won't start, problems with the event viewer

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-08/msg05604.html>

- *From:* "Ambroise Nève" <noreply@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 30 Aug 2006 00:23:55 +0200
-

Hi Everybody,

New problem of the day :-)

One of my customers server was hacked (I presume because we forgot to setup SP4 for SQL Server — the port was open to the outside world for business purposes!). Anyways, the threat has been stoped (kind of trojan that setup a SERV-U FTP server on port 21 which was also open!). Everything was cleaned up one week ago and the server seemed to live again... but, today: new problems!

Problem 1: Event Viewer going crazy! (since the trojan)

One of the problems, the oldest, is that the Event Viewer does not seem to be updated with some events (e. g. when I get an error message on the console which usually leads to an error event, there is none in the Event Viewer) and also sends us regularly two alerts (from the Monitoring and Reporting stuff of SBS) that have nothing realistic (backup error and account lockout error when no backup is running and no account has been locked!)

Problem 2: Exchange services not starting (getting critical... — since today!)

Suddenly, since today, the Exchange Services are not starting anymore. I get the following error warning messages:

"Could not start the Microsoft Exchange System Attendant service on Local Computer. Error 1075: The dependency service does not exist or has been marked for deletion."

"Could not start the Microsoft Exchange Information Store service on Local Computer. Error 1068: The dependency service or group failed to start."

(all services use "Local System Account" to Log On)

Problem 3: Dependencies are disabled! (severely embarassed! — since today!)

The warning messages above are fine... but when I try to get to the service's properties > dependencies, both the "This service depends on the following system components" and "The following system components depend on this service" boxes are disabled and contain an information ballon "<No dependencies>" (also disabled).

Exchange won't start, problems with the event viewer

There I am: Event Viewer going crazy, Exchange not starting and Dependencies disabled. Is anyone having an idea of something to try before calling PSS?
If anybody has experience with PSS: can the solve this kind of case?

Thanks for your help folks,

Ambroise Nève — Small Business Specialist (doh!)

Note: I've might have excellent belgian chocolate reward for usefull help
:-)))))))))

.