

# Re: Error Event Logs after SP1 install

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-05/msg07307.html>

---

- *From:* "Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP]" <[sbradcpa@xxxxxxxxxxxx](mailto:sbradcpa@xxxxxxxxxxxx)>
  - *Date:* Mon, 30 May 2005 22:15:05 –0700
- 

www.eventid.net is a better resource.

What error codes?

jaredea wrote:

i have a few error logs i can't make heads or tails of after an install...first off, i tried to research it by clicking on the link at the bottom of most of the messages that says:

"see Help and Support Center at  
<http://go.microsoft.com/fwlink/events.asp>

and the first one i clicked on took me to a description of the error and some info...then i clicked on another one and got the following message:

" Cannot display the page The page you are trying to view cannot be displayed because the server it resides on does not respond. Please try again later."

This happened no matter what i clicked on and even when i clicked on the first like that had worked a few seconds previously...

here are the event errors and the logs they come from...i've replaced identifying information with things like xxx or (server\_name\_removed) just so it isn't "out there":

Re: Error Event Logs after SP1 install

=====

SYSTEM:

Event Type: Warning  
Event Source: DhcpServer  
Event Category: None  
Event ID: 1056  
Date: 5/30/2005  
Time: 10:07:18 PM  
User: N/A  
Computer: (SERVER\_NAME\_REMOVED)  
Description:  
The DHCP service has detected that it is running on a DC and has no credentials configured for use with Dynamic DNS registrations initiated by the DHCP service. This is not a recommended security configuration. Credentials for Dynamic DNS registrations may be configured using the command line "netsh dhcp server set dnscredentials" or via the DHCP Administrative tool.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Data:  
0000: 00 00 00 00 ....

=====

SECURITY:

Event Type: Failure Audit  
Event Source: Security  
Event Category: Logon/Logoff Event ID: 537  
Date: 5/30/2005  
Time: 10:02:48 PM  
User: NT AUTHORITY\SYSTEM  
Computer: (SERVER\_NAME\_REMOVED)  
Description:  
Logon Failure:  
Reason: An error occurred during logon  
User Name: (SERVER\_NAME\_REMOVED)\$  
Domain: xxxx.LOCAL  
Logon Type: 3

Re: Error Event Logs after SP1 install

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: 192.168.16.2  
Source Port: 1637

For more information, see Help and Support Center at  
<http://go.microsoft.com/fwlink/events.asp>.

=====  
APPLICATION:

Event Type: Warning  
Event Source: WinMgmt  
Event Category: None  
Event ID: 5603  
Date: 5/30/2005  
Time: 10:07:50 PM  
User: NT AUTHORITY\SYSTEM  
Computer: (SERVER\_NAME\_REMOVED)  
Description:  
A provider, PerfProv, has been registered in the WMI namespace, ROOT\CIMV2\MicrosoftHealthMonitor\PerfMon, but did not specify the HostingModel property. This provider will be run using the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests. Ensure that provider has been reviewed for security behavior and update the HostingModel property of the provider registration to an account with the least privileges possible for the required functionality.

For more information, see Help and Support Center at  
<http://go.microsoft.com/fwlink/events.asp>.

Re: Error Event Logs after SP1 install

=====  
APPLICATION:

Event Type: Warning  
Event Source: WinMgmt  
Event Category: None  
Event ID: 5603  
Date: 5/30/2005  
Time: 10:07:50 PM  
User: NT AUTHORITY\SYSTEM  
Computer: (SERVER\_NAME\_REMOVED)  
Description:  
A provider, PerfProv, has been registered in the WMI namespace, ROOT\CIMV2\MicrosoftHealthMonitor\PerfMon, but did not specify the HostingModel property. This provider will be run using the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests. Ensure that provider has been reviewed for security behavior and update the HostingModel property of the provider registration to an account with the least privileges possible for the required functionality.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

=====  
APPLICATION:

Event Type: Error  
Event Source: Windows SharePoint Services 2.0  
Event Category: None  
Event ID: 1000  
Date: 5/30/2005  
Time: 10:07:11 PM  
User: N/A  
Computer: (SERVER\_NAME\_REMOVED)  
Description:  
#50070: Unable to connect to the database STS\_Config on (SERVER\_NAME\_REMOVED)\SharePoint. Check the database connection

## Re: Error Event Logs after SP1 install

information and make sure that the database server is running.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

=====  
APPLICATION:

Event Type: Error  
Event Source: dsrestor  
Event Category: None  
Event ID: 1005  
Date: 5/30/2005  
Time: 10:06:20 PM  
User: N/A  
Computer: (SERVER\_NAME\_REMOVED)  
Description:  
The DSRestore Filter failed to connect to local SAM server. Error returned is <id:997>.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

=====  
APPLICATION:

Event Type: Warning  
Event Source: Userenv  
Event Category: None  
Event ID: 1524  
Date: 5/30/2005  
Time: 10:02:38 PM  
User: xxxx\Administrator  
Computer: (SERVER\_NAME\_REMOVED)  
Description:  
Windows cannot unload your classes registry file - it is still in use by other applications or services. The file will be unloaded when it is no longer in use.

## Re: Error Event Logs after SP1 install

For more information, see Help and Support Center at  
<http://go.microsoft.com/fwlink/events.asp>.

--

An open letter to the Security Community::  
<http://msmvps.com/bradley/archive/2004/12/12/23540.aspx>

.