

Re: New Event Log Errors!

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-09/msg01804.html>

- *From:* "Adam Butler" <adambutler100@xxxxxxxxxxxxx>
 - *Date:* Tue, 12 Sep 2006 06:46:06 -0500
-

Hi Chase,

I spent several hours last evening tracking down this issue.
I finally fixed everything relating to your post.

The problem originated when I installed the Internet Authentication Service (IAS) to be used as a Radius authentication for wireless authorization. Somehow along those lines I'd also installed the Certificate Authority thinking it was needed.

That is how the wrong certificate was installed.
Once I ran the certutil -deleteBad command, all was fixed and I no longer see any KDC errors.

Thanks!

"chace zhang" <v-chacez@xxxxxxxxxxxxx> wrote in message
news:5YB7Wlj1GHA.400@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi,

Thank you for posting here.

From your description, I understand you noticed Event ID 7022, 20, 4104 and 1005 on your SBS Server.

Please understand that our newsgroup is an issue based service, meaning we usually respond to one question/issue per post. This will lessen the confusion for both of us, as well as ensure that our results are accurate and not a result of a test for a different question. Therefore, I will work with you on the first question in this post. Regarding the additional question, please open a new post so that the dedicated MS engineer can help you on it in a more efficient manner.

Re: New Event Log Errors!

For Event 20 and 7022

First of all, in order to better assistance, please let me know the following questions:

Did you apply the last Server Pack for SBS Server?

Did you issue a new CA on SBS Server?

Did you notice any symptoms on your SBS Server?

I would like to double confirm "Kerberos Key Distribution Center" service has successfully started?

Per my research, Event ID 20 and 7022 could occur due to the current win2k3 SP1 machine cannot contact a valid CA (certificate authority), CA can issue many different types certificate and smart card is a one among them. For example, you installed CA on one DC and removed CA from it; however, the win2k3 SP1 machine still wants to contact the original CA. In this case, Event ID 20 is logged.

Once the CA has been taken down, the certificates that have been issued to all the domain controllers need to be removed. This can be done quite easily using DSSTORE.EXE from the Resource Kit.

To remove old domain controller certificates, please use the following article below.

NOTE: Please install Windows Support Tools on the win2k3 sp1 problematic machine.

Step 1:

=====

At the command prompt on a domain controller, type

certutil -dcinfo deleteBad

To do so:

1. Install the Windows Support Tools from the Support\Tools folder in the Windows Server 2003 DC.
2. Go to command prompt, type "certutil - dcinfo deleteBad" (without the quotation marks)
3. Cleaned out KDC 20 warnings in the System Event Log.
4. Restart the DC and then check if the issue is fixed.

Step 2:

=====

I suspect that the issue may be related to the DCOM protocol. Windows

Re: New Event Log Errors!

Server 2003 SP1 introduces enhanced default security settings for the DCOM protocol. Specifically, SP1 introduces more precise rights that give an administrator independent control over local and remote permissions for launching, activating, and accessing COM servers.

Windows Server 2003 SP1 introduces enhanced default security settings for the DCOM protocol. Specifically, SP1 introduces more precise rights that give an administrator independent control over local and remote permissions for launching, activating, and accessing COM servers.

As the Windows Server 2003 Certificate Services provides enrollment and administration services by using the DCOM protocol, I suspect that it may be the cause of the problem.

1. Please check to ensure that a new security group, CERTSVC_DCOM_ACCESS, has been created after applied the SP1.
2. Please add the "Domain Users", "Domain Computers", "Domain Controllers" groups to the new CERTSVC_DCOM_ACCESS security group.
3. If possible, please backup the other Windows Server 2003 DC (without SP1), and then apply Service Pack 1 on it as well.
4. Then, we can have Certificate Services update the DCOM security settings by running the following commands:

```
certutil -setreg SetupStatus -SETUP_DCOM_SECURITY_UPDATED_FLAG  
net stop certsvc  
net start certsvc
```

Please check if the problem has been fixed.

Step 3:

=====

Reissue a domain controller certificate:

1. Click "Start" -> "Run" -> Input "mmc" (without the quotation marks) and press Enter.
2. Click "File" -> "Add/Remove Snap-in". Click "Add" button and select "Certificate" snap-in. Select "Computer account".
3. In the certificate console, navigate to "Personal" \ "Certificates". Right-click the folder and choose "Request new certificate".
4. Follow the wizard to request a Domain Controller certificate.
5. Reboot the computer to see if the problem will be resolved.

Re: New Event Log Errors!

In addition, some other causes will also raise Event ID 20. If Event ID 20 occurs with other Events, please take a look at the following link, which has a brief summary about Event ID 20:

<http://www.eventid.net/display.asp?eventid=20&eventno=3396&source=KDC&phase=1>

This response contains a reference to a third party World Wide Web site. Microsoft can make no representation concerning the content of these sites.

Microsoft is providing this information only as a convenience to you: this is to inform you that Microsoft has not tested any software or information found on these sites and therefore 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 on the Internet.

For your convenience, I listed the following info on the other Event ID:
Regarding SBS monitoring error 4104

Based on my research, this error indicated a missing SBS Monitoring database (Monitoring did not install or the Monitoring MSDE has been uninstalled using Add/Remove Programs).

Please check if the MSDE instance for monitoring is running:

- 1) Bring up the Services by key in "services.msc" in run box.
- 2) Check if MSSQL\$SBSMONITORING is running.
- 3) Switch to Log On tab and check if Local system account is the startup account.

If the service is not running, most possibly, some third-party application caused monitoring corrupted, such as Veritas. Please uninstall the Monitoring component along with the Intranet component using the following steps:

Note: If you have any AV Filtering software installed that is installed as a Web site in IIS check to see what port it is using. If it is set to 8081 this is in conflict with the SharePoint Central Administration site which by default uses Port 8081. Uninstall the AV Software before proceeding.

Uninstall the intranet component

1. Click Start, click Control Panel, and then click Add or Remove Programs.

Re: New Event Log Errors!

2. Select Windows Small Business Server 2003 and then click Change/Remove. The Setup Wizard appears.
3. Click Next to start the wizard.
4. On the Windows Configuration page, click Next.
5. On the Component Selection page, in the Action column, change Server Tools to Maintenance, change Intranet component to Remove, and then click Next.
6. On the Component Summary page, click Next.
7. Click Finish.

Uninstall Microsoft SQL Server Desktop Engine (SHAREPOINT) In Add or Remove

Programs, select Microsoft SQL Server Desktop Engine (SHAREPOINT) and then click Remove. A dialog box appears. To confirm that you want to remove, click Yes.

Delete Registry Keys

1. Delete
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SmallBusinessServer\Intranet
2. Delete HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\SHAREPOINT
3. Delete HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions\Ports\Port /LM/W3SVC/4: (Do not delete "Port /LM/W3SVC/1:" because it is for the FrontPage Server Extension 2002 which is installed on the Default WebSite. If you see additional "Port /LM/W3SVC/X:", back them up and then remove them)

Delete IIS Virtual Directory

1. Delete SharePoint Central Administration (Do Not Delete Microsoft SharePoint Administration. It belongs to FrontPage Server Extensions)
2. Delete Companyweb Delete Application Pool.

There should be only 4 application pools (DefaultAppPool, ExchangeApplicationPool, ExchangeMobileBrowseApplicationPool, and MSSharePointAppPool). Besides those 4, delete any additional application pools.

Rename Folders

Rename C:\Program Files\Microsoft SQL Server\MSSQL\$SHAREPOINT
Rename C:\Inetpub\companyweb

Install the intranet component NOTE: If the monitoring component has been uninstalled, reinstall it at this time.

1. In Add or Remove Programs, select Windows Small Business Server 2003 and then click Change/Remove. The Setup Wizard appears.
2. Click Next.
3. On the Windows Configuration page, click Next.

Re: New Event Log Errors!

4. On the Component Selection page, in the Action column, change Server Tools to Maintenance, change Intranet component to Install, and then click Next.
5. On the Logon Information page, click Next.
6. On the Component Summary page, click Next.
7. Click Finish.

The Intranet component will install with no further error messages. NOTE: If they do not have the updated 3rd CD, then the Intranet install will fail, however applying the SharePoint hotfix will repair the Intranet install.

Regarding 1005 error

For the Event error "EventCode=1005 Source=dsrestor". This is a known bug with SBS 2k3 which has already been filed. Since it will not cause any problem, there is no hotfix released for it and can be safely ignored.

Additionally, The 1005 error indicates that dsrestore was unable to connect to the sam and verify the passwords are in synch when the server boots. The dsrestore process is to synch the domain admin password with the dsrm password. The dsrestor process will run every 30 mins to verify that the passwords are in synch. If the process fails it does not run again until the server is rebooted. As a workaround you can manually reset the DSRM password to match the domain admin password by using ntdsutil. For more information about resetting the password, see:

322672 How To Reset the Directory Services Restore Mode Administrator Account
<http://support.microsoft.com/?id=322672>

Hope this helps, if you have any other concerns on this issue, please feel free to let me know.

Have a nice day!

Best Regards,

Chace Zhang (MSFT)

Microsoft CSS Online Newsgroup Support

Get Secure! – www.microsoft.com/security

=====
This newsgroup only focuses on SBS technical issues. If you have issues

Re: New Event Log Errors!

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: "Adam Butler" <adambutler100@xxxxxxxxxxxx>
| Subject: New Event Log Errors!
| Date: Mon, 11 Sep 2006 12:17:27 -0500
| Lines: 104
| X-Priority: 3
| X-MSMail-Priority: Normal
| X-Newsreader: Microsoft Outlook Express 6.00.2900.2869
| X-RFC2646: Format=Flowed; Original
| X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2962
| Message-ID: <exwGpYc1GHA.2176@xxxxxxxxxxxxxxxxxxxxxx>
| Newsgroups: microsoft.public.windows.server.sbs
| NNTP-Posting-Host: adsl-66-140-203-41.dsl.stlsmo.swbell.net
66.140.203.41
| Path: TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTNGP04.phx.gbl
| Xref: TK2MSFTNGXA01.phx.gbl microsoft.public.windows.server.sbs:296724
| X-Tomcat-NG: microsoft.public.windows.server.sbs
|
| Hi,
|
| I'm seeing four new Application and System Event Log errors.
| I'll paste them below.

Re: New Event Log Errors!

|
| They all appeared in just the last couple of days.
| The first with an event id of 20 appears to repeat every 10 hours.
| I tried following the fwlink but I'm confused as ever as I don't recall
ever
| doing anything with KDC certificates before!
| The second event id 7022 also deals with KDC but this error is only
| generated once at boot.
|
| The third and fourth errors are both new and are only generated at boot.
| They have event id's of 4104 and 1005. The 4104 is about SBS Monitoring
and
| the 1005 has to do with DSRestore filter not connecting to the local SAM
| server.
|
| Can anyone help me out with these? Especially the ones involving KDC or
| Kerberos!
|
| Below this line is the text from all four event log errors.
| Thank Very Much!
|
| Begin paste:
|
| System
|
| Event Type: Warning
| Event Source: KDC
| Event Category: None
| Event ID: 20
| Date: 9/10/2006
| Time: 22:02:26
| User: N/A
| Computer: WX98
| Description:
| The currently selected KDC certificate was once valid, but now is
invalid
| and no suitable replacement was found. Smartcard logon may not function
| correctly if this problem is not remedied. Have the system
administrator
| check on the state of the domain's public key infrastructure. The chain
| status is in the error data.
|
| For more information, see Help and Support Center at
| <http://go.microsoft.com/fwlink/events.asp>.
| Data:
| 0000: 00 00 00 00 00 00 00 00
| 0008: 00 00 00 00 00 00 00 00
|
| System
|
| Event Type: Error

Re: New Event Log Errors!

| Event Source: Service Control Manager
| Event Category: None
| Event ID: 7022
| Date: 9/10/2006
| Time: 22:04:21
| User: N/A
| Computer: WX98
| Description:
| The Kerberos Key Distribution Center service hung on starting.
|
| For more information, see Help and Support Center at
| <http://go.microsoft.com/fwlink/events.asp>.

| Application

| Event Type: Error
| Event Source: SmallBusinessServer
| Event Category: SBS Monitoring
| Event ID: 4104
| Date: 9/10/2006
| Time: 23:46:48
| User: N/A
| Computer: WX98
| Description:
| Could not connect to the monitoring database. This can occur when there
are
| multiple connections to the database. Wait a short period of time, and
then
| try again. If this error persists, run the Monitoring Configuration
Wizard,
| and select Reinstall monitoring features.
|
| For more information, see Help and Support Center at
| <http://go.microsoft.com/fwlink/events.asp>.

| Data:
| 0000: 05 40 00 80 .@.?

| Application

| Event Type: Error
| Event Source: dsrestor
| Event Category: None
| Event ID: 1005
| Date: 9/10/2006
| Time: 23:43:16
| User: N/A
| Computer: WX98
| Description:
| The DSRestore Filter failed to connect to local SAM server. Error
returned
| is <id:997>.

Re: New Event Log Errors!

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