

Re: SBS2000 server generating DCOM errors and multiple security events.

Source:

<http://www.tech-archive.net/Archive/BackOffice/microsoft.public.backoffice.smallbiz2000/2004-12/0530.html>

From: Marina Roos [SBS-MVP] (marina_at_roos.nodontwantspam.nl.com)

Date: 12/16/04

Date: Thu, 16 Dec 2004 02:19:04 +0100

Hi Rabram,

Can you post the ipconfig/all from the server and one from a client?

--

Regards,

Marina

Microsoft SBS-MVP

"RDA" <rda@here.net> schreef in bericht

news:ek7c05u4EHA.1300@TK2MSFTNGP14.phx.gbl...

> Hello all,

>

> I have a SBS2000 sever that has been acting very strange as of late. The
> first problems began 2 weeks ago when no computers could authenticate to
> the server and this was in the system log:

>

> Event Type: Warning

> Event Source: MRxSmb

> Event Category: None

> Event ID: 3034

> Date: 12/8/2004

> Time: 6:13:39 AM

> User: N/A

> Computer: DC01

> Description:

> The redirector was unable to initialize security context or query
> context attributes.

> Data:

> 0000: 00 00 08 00 02 00 56 00V.

> 0008: 00 00 00 00 da 0b 00 80ú..€

> 0010: 00 00 00 00 5e 00 00 c0^..Ä

> 0018: 00 00 00 00 00 00 00 00

> 0020: 00 00 00 00 00 00 00 00

> 0028: 7d 04 00 00 5e 00 00 c0 }...^..Ä

>

> I thought maybe it was a problem with AD, so I ran through the steps in
> this JSI FAQ:

> <http://www.jsiinc.com/SUBO/tip8300/rh8320.htm>

>

> All tests indicated there was no problem. Then it happened again two
> days later. If I reboot the DC, the problem is corrected, but to do that
> in the middle of the day makes the VP cranky.

> I checked DNS, DHCP, Sntp, group policies, permissions to log on

Re: SBS2000 server generating DCOM errors and multiple security events.

microsoft.public.backoffice.smallbiz2000: Re: SBS2000 server generating DCOM errors and multiple security events

```
> locally, NTFS permissions to shares and drives on the DC, NetDIAG,  
> DCDiag, all with out finding any errors in configuration or operation.  
>  
> I fear the worst in that the AD is corrupted and last night I went  
> through the steps in the following KB articles:  
>  
> http://support.microsoft.com/kb/258062  
> I backup the system state, perform the Integrity check and the semantic  
> analysis, both complete without errors.  
>  
> http://support.microsoft.com/kb/232122  
> I perform the offline defragmentation successfully and reboot the server.  
>  
> Now I get the following errors:  
>  
> System Log...  
>  
> Event Type: Error  
> Event Source: DCOM  
> Event Category: None  
> Event ID: 10002  
> Date: 12/14/2004  
> Time: 11:55:43 PM  
> User: NT AUTHORITY\SYSTEM  
> Computer: DC  
> Description:  
> Access denied attempting to launch a DCOM Server. The server is:  
> {9DA0E106-86CE-11D1-8699-00C04FB98036}  
> The user is SYSTEM/NT AUTHORITY, SID=S-1-5-18.  
>  
> I find {9DA0E106-86CE-11D1-8699-00C04FB98036} is the MS Exchange  
> Property Mapping Interface by searching the registry, but there is no  
> info in the net about it at all!  
>  
> In the security log I have these 3 messages repeating every 30 - 45  
> seconds...  
>  
> Event Type: Failure Audit  
> Event Source: Security  
> Event Category: Account Logon  
> Event ID: 675  
> Date: 12/15/2004  
> Time: 2:14:30 PM  
> User: NT AUTHORITY\SYSTEM  
> Computer: DC  
> Description:  
> Pre-authentication failed:  
>   User Name: DC$  
>   User ID: MYDEV\DC$  
>   Service Name: krbtgt/HOLDINGS.LOCAL  
>   Pre-Authentication Type: 0x2  
>   Failure Code: 0x18  
>   Client Address: 127.0.0.1  
>  
>  
> Event Type: Failure Audit  
> Event Source: Security  
> Event Category: Account Logon  
> Event ID: 681  
> Date: 12/15/2004  
> Time: 2:14:30 PM  
> User: NT AUTHORITY\SYSTEM
```

```
> Computer: DC
> Description:
> The logon to account: DC$
> by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
> from workstation: DC
> failed. The error code was: 3221225578
>
>
> Event Type: Failure Audit
> Event Source: Security
> Event Category: Logon/Logoff
> Event ID: 529
> Date: 12/15/2004
> Time: 2:14:30 PM
> User: NT AUTHORITY\SYSTEM
> Computer: DC
> Description:
> Logon Failure:
> Reason: Unknown user name or bad password
> User Name: DC$
> Domain: MYDEV
> Logon Type: 3
> Logon Process: NtLmSsp
> Authentication Package: NTLM
> Workstation Name: DC
>
> What I interpret these to mean is this:
>
> 1. The machine account DC$ is locked out, has an incorrect password, or
> does not exist.
> 2. The user SYSTEM/NT AUTHORITY, SID=S-1-5-18 is locked out, has
> incorrect password, or does not exist.
>
> I have found the following info about resetting the machine account
> password.
> http://support.microsoft.com/default.aspx?scid=kb;EN-US;q260575
> It mentions the need for another DC, but I only have the one DC.
>
> I have not found any info about modifying NT AUTHORITY\SYSTEM account.
>
> Also, now if I run a DCdiag, DC fails test systemlog, but passes every
> other test.
>
> I have exhausted all resources I can think of to find the source of
> this. Please, if anyone has seen this before post your suggestions. I
> apologize for the length of this post, but I want to present all info I
> have and outline what I have tried to fix it.
>
> TIA
>
> RDA MCSE, CNE
> rabram AT gmail DOT com
```