

## Re: 1st DC in Small Domain Failed, \_msdcs still points to 1st DC

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2008-06/msg00177](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2008-06/msg00177)

---

- *From:* Darius Sanders <[DariusSanders@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:DariusSanders@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 4 Jun 2008 15:31:01 -0700
- 

Thanks for the input. I followed the directions in the KB articles and the problem is now fixed. Thanks again.

--

Darius Sanders

"chriss3 [MVP]" wrote:

How old is the backup you restored of the DC? (Hopefully not older than 60 days) (or tombstone lifetime)

If so. Shutdown the restored DC and remove it using

<http://support.microsoft.com/kb/216498>.

If not. You have to reset the secure channel.

How to use Netdom.exe to reset machine account passwords of a Windows 2000 Domain Controller

<http://support.microsoft.com/default...:EN-US;q260575>

How to use Netdom.exe to reset machine account passwords of a Windows Server 2003 Domain Controller

<http://support.microsoft.com/default...b:en-us;325850>

--

Regards

Christoffer Andersson

TrueSec – Executive Consultant

Microsoft MVP – Directory Services

No email replies please – reply in the newsgroup

---

<http://www.truesec.com>

"Darius Sanders" <[DariusSanders@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:DariusSanders@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message <news:5ADDDB099-9653-42A5-8B86-87B7026DE378@xxxxxxxxxxxxxxxxxxxxx>

Re: 1st DC in Small Domain Failed, \_msdcs still points to 1st DC

Thanks for the info. Since the last post I was able to bring the old DC backup and I have a new server on its way. I am less than confident in the current servers ability to handle the task. With the old DC up I am getting EventID 4 from Kerberos

"The kerberos client received a KRB\_AP\_ERR\_MODIFIED error from the server host/dc01.mycompany..com. The target name used was . This indicates that the password used to encrypt the kerberos service ticket is different than that on the target server. Commonly, this is due to identically named machine accounts in the target realm (MYCOMPANY.COM), and the client realm. Please contact your system administrator."

on my second domain controller. I am not sure what this means and what I need to do to clear it up so that I can proceed with moving the DC to a newer server. Any insight would be much appreciated. Thanks.

—  
Darius Sanders

"chriss3 [MVP]" wrote:

Hello.

1. Make sure that you remove the Domain Controller that failed from Active Directory using metadata cleanup (If there is no possibility to use DCPROMO to demote it)  
FYI: <http://support.microsoft.com/kb/216498>
2. Seize the FSMO roles to an other DC.  
FYI: <http://support.microsoft.com/kb/255504>
3. Install Windows Server Support Tools (Found on your Windows Server CD) and run the command nltest /dsregdns on your remaining DC. Review the \_msdcs zone and see of the record of the remaining DC is created.. Clean up records in your DNS zones from the failed DC. Make sure that the

Re: 1st DC in Small Domain Failed, \_msdcs still points to 1st DC

remaining DC is  
made a name server for the zones.

--

Regards  
Christoffer Andersson  
TrueSec – Executive Consultant  
Microsoft MVP – Directory Services

No email replies please – reply in the newsgroup

---

<http://www.truesec.com>

"Darius Sanders"

<DariusSanders@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in  
message

[news:940EEB33-1285-4A83-8ED9-87DF8671429A@xxxxxxxxxxxxxxxxxxxx](mailto:news:940EEB33-1285-4A83-8ED9-87DF8671429A@xxxxxxxxxxxxxxxxxxxx)

I have a situations were the first domain  
controller in our small,  
single  
site domain, has suffered a substantial  
hardware problem and is not  
operational. We have a second domain  
controller that is running DNS and  
is  
operating as a Global Catalog. Active  
directory seems to be operating  
normally for now even though the fsmo roles  
wer on the failed machine.

When I

go into the forward look up zone for the still  
operating DC and look

under

the \_msdcs folder I see one entry for the  
server that has failed.

Should

that

be modified to refer to the second DC that is  
still operational? If so,

how

is that accomplished. Any insight on this  
would be very much

appreciated.

Thanks in advance.

--

Darius Sanders

--

Re: 1st DC in Small Domain Failed, \_msdcs still points to 1st DC

Darius Sanders