

Re: How to decide on which network interface domain controller is available

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2006-06/msg00271.html

- *From:* Enkidu <enkidu.com@xxxxxxxxxxxxxxxx>
 - *Date:* Sun, 18 Jun 2006 16:00:25 +1200
-

Fair enough. I still think it is the wrong decision – you *will* as you have found have problems with multi-homed DCs as you have found – since you expose your DC even if only a little bit. I hope that someone can answer the original question for you.

Cheers,

Cliff

RAP wrote:

Hi Cliff,

I am aware that our setup is not optimal from a security point of view, but we are a private network with limited resources, from hardware to software everything is 2nd hand.

We are having two servers (normal PCs) and I decided that for us it is more important to have fault-tolerance (since I am away often and a hardware failure could mean a downtime of several weeks) then to increase security. Therefore we dedicated both machines to both jobs (DC and Internet Gateway/Servers).

Regards, Robert

Enkidu wrote:

RAP wrote:

Hi,

I have two domain controllers, both are connected to an internal (LAN with clients) and an external (a DMZ) network.

Re: How to decide on which network interface domain controller is available

How can I configure the servers in a way that the domain controller functionality is only available on the internal network?

My current problem is that the DNS server has both IP addresses for each server under one name. I cannot remove the external one, Windows automatically re-creates the entry. Now, when I resolve the name of server2 on server1 with nslookup it results in both IP addresses. For some reason the external address is chosen and any communication (e.g. ping or mount network drive) goes via the external network. This is not what I want, it should go via the internal (much faster) network.

I was hoping that when I deactivate the domain controller functionality on the external interface it will not re-create the entry in the DNS, however I'd be happy about any other solution for my problem as well.

Multi-homed DCs are always a bad idea, unless you cannot think of any other way of doing it. The way that you are doing it is essentially nullifying the security of having a DMZ, since if the DC on the DMZ (which is not absolutely trusted) is compromised, the attacker has a machine on your LAN!

Of course you may have reasons for doing it that way that I know nothing about, in which case my comments may help others. Just please disregard them.