

Re: Question for Ace – Why to not Multi-home a DC

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2005-10/msg00261.html

- *From:* "Cary Shultz" <cwshultz@xxxxxxxxx>
 - *Date:* Wed, 12 Oct 2005 00:19:09 -0400
-

Ace,

Thank you for the steps on the multi-homed Domain Controllers. I think that I will play with it in a lab to 'get good'. This is good information. It seems like a lot of people do this. Not sure why???? But lots seem to do this and, as a result, have problems. These steps should alleviate these problems. Hopefully your initial comments will scare the weary away from doing this.

And Thank you for the comment on my web sites. The contents pretty much stink at the moment. Well, better said, the content of the activedirectory web site pretty much stinks. The grouppolicy web site is simply a 'we are working on this' site. Anyway, now I am in a better position time-wise to do something. What you currently see was thrown together in about one hour. Boy, does it look like it!

I might just run a couple of ideas by you....since you offered. No worries, though. It is not going to start out as a drip and eventually become a busted dam! And feel free to comment. I am a big boy. You will not hurt my feelings!

Took a spin over to your site (never knew!!!). Interesting. Using Frames. Never thought of that. But, like I said, I threw my site up in about one hour! Going to change the content and then – eventually – going to change the format (using CSS and whatever I can learn!).

Anyway, time to go to bed.

--

Cary W. Shultz
Roanoke, VA 24012

<http://www.activedirectory-win2000.com>

(soon to be updated!!!)

<http://www.grouppolicy-win2000.com>

(soon to be updated!!!)

Re: Question for Ace – Why to not Multi-home a DC

"Ace Fekay [MVP]"

<PleaseSubstituteMyActualFirstName&LastNameHere@xxxxxxxxxxx> wrote in message news:OwujMltzFHA.2792@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

>

> "Cary Shultz" <cwshultz@xxxxxxxx> wrote in message

> news:Od1MkdszFHA.1028@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

>> Ace,

>>

>> In one of your posts, you offered to share with us your steps for
>> 'dealing' with a DC that is multi-homed. I can not find the post. So, I
>> am letting you know that I would be very interested in your steps – as I
>> am sure that all of us are.

>>

>> Thank you,

>>

>> --

>> Cary W. Shultz

>> Roanoke, VA 24012

>>

>> <http://www.activedirectory-win2000.com>

>> (soon to be updated!!!)

>> <http://www.grouppolicy-win2000.com>

>> (soon to be updated!!!)

>>

>>

>>

>>

>>

>

> My pleasure, Cary. I like your website names too. If there's anything I
> can help out with at your websites, let me know. I started a site years
> ago, but never finished it. It is very time consuming. I may complete it
> one of these days. I've closed much of it down lately.

> www.bandwidthpros.com.

>

>

> Here you go...but first my views on multi-homed DCs... (ouch!)

> =====

> Multi-homed DCs, What a Mess... It cuts into your drinking time...

> :-(

>

> Honestly, multi-homed DCs are not recommended because of the associated
> issues that can occur, as you've encountered. We usually recommend
> purchasing an inexpensive Linksys, DLink, etc, Cable/DSL router to perform
> NAT for you, take out the extra NIC off the DC, but still let the DC
> handle DHCP (and not the router).

>

> Since this DC is multi-homed, it requires additional configuration to
> prevent the public interface addresses from being registered in DNS. This
> creates a problem for internal clients locating AD to authenticate and

Re: Question for Ace – Why to not Multi-home a DC

- > find other services and resources such as the Global Catalog, file sharing
- > and the SYSVOL DFS share and can cause GPO errors with Userenv 1000 events
- > to be logged, authenticating to shares and printers, logging on takes
- > forever, among numerous other issues.
- >
- > But if you like, there are some registry changes to eliminate the
- > registration of the external NIC. Here's the whole list of manual steps to
- > follow (this includes some of the stuff I already gave you):
- >
- > But believe me, it's much easier to just get a separate NAT device or
- > multihomed a non-DC then having to alter the DC. – Good luck!
- >
- > =====
- > 1. In the DNS management console, in the properties of the DNS server,
- > Interfaces tab, set DNS to only listen on the private IP you want in DNS
- > for
- > the server. This is for your private network that your clients use.
- >
- >
- > 2. Add this registry entry with regedt32 to stop the (same as parent
- > folder)
- > records and the GC record, also called the LdapIpAddress and GcIpAddress.
- >
- > HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
- > On the Edit menu, point to New, and then click REG_MULTI_SZ as the data
- > type:
- >
- > Registry value: DnsAvoidRegisterRecords
- > Data type: REG_MULTI_SZ
- >
- > (and in the box, you would type in the following to stop their
- > registration):
- >
- > LdapIpAddress
- > GcIpAddress
- >
- >
- > 3. Then you will need to manually create the LdapIpAddress and GcIpAddress
- > records in DNS.
- > The LdapIpAddress resolves to the domain controllers in the domain. The
- > GcIpAddress resolves
- > to the Global Catalogs in the forest as gc._msdcs.forestroot.com.
- >
- > To manually create the LdapIpAddress, create a new host but leave the name
- > field blank,
- > give it the IP of the internal interface. Windows 2k barks at you saying
- > (same as parent folder) is not a valid host name,click OK to create the
- > record anyway.
- > Windows 2003 won't bark. It's house-broken out of the box.
- >
- > To manually create the GcIpAddress, navigate to the _msdcs folder, under

Re: Question for Ace – Why to not Multi-home a DC

- > it click the gc
- > folder, then rt-click, create new host, leave the name field blank, give
- > it the IP of the
- > internal interface. Windows 2k barks at you saying (same as parent folder)
- > is not a valid
- > host name,click OK to create the record anyway. Windows 2003 won't bark.
- >
- >
- > 4. To stop registration of both NICs, add (if it exists) or alter this reg
- > entry:
- >
- > HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
- >
- > On the Edit menu, point to New, and then click DWORD Value to add the
- > following registry value:
- > Value name: RegisterDnsARecords
- > Data type: REG_DWORD
- > Value data: 0
- >
- > Then manually create a new host record for the server name in DNS and give
- > it the IP of the internal interface
- >
- >
- > 5. Right click on Network places, choose properties, in the Advanced menu
- > item
- > select Advanced settings. Make sure the internal interface is at the top
- > of
- > the connections pane and File sharing is enabled on the internal
- > interface.
- >
- >
- > 6. On the outer NIC, disable File and Print Services, Microsoft Client
- > Service,
- > then go into IP properties, click on Advanced, choose the WINS tab and
- > disable NetBIOS.
- >
- >
- > 7. On the outer NIC, only put in the internal IP address of the DNS server
- > (this machine).
- >
- >
- > 8. If you haven't done so, configure a forwarder. You can use 4.2.2.2 if
- > not sure which
- > DNS to forward to until you've got the DNS address of your ISP. How to set
- > a forwarder?
- > Depending on your operating system,choose one of the following articles:
- >
- > 300202 – HOW TO: Configure DNS for Internet Access in Windows 2000
- > <http://support.microsoft.com/?id=300202&FR=1>
- >
- > 323380 – HOW TO: Configure DNS for Internet Access in Windows Server 2003

Re: Question for Ace – Why to not Multi-home a DC

- > (How to configure a forwarder):
- > <http://support.microsoft.com/d/id?=323380>
- >
- >
- >
- > *** Some additional reading:
- >
- > 246804 – How to enable or disable DNS updates in Windows 2000 and in
- > Windows Server 2003
- > <http://support.microsoft.com/?id=246804>
- >
- > 295328 – Private Network Interfaces on a Domain Controller Are Registered
- > in DNS
- > [also shows DnsAvoidRegisterRecords LdapIpAddress to avoid reg
- > sameasparent private IP]:
- > <http://support.microsoft.com/?id=295328>
- >
- > 306602 – How to Optimize the Location of a DC or GC That Resides Outside
- > of a Client's
- > Site [Includes info LdapIpAddress and GcIpAddress information and the SRV
- > mnemonic values]:
- > <http://support.microsoft.com/?id=306602>
- >
- > 825036 – Best practices for DNS client settings in Windows 2000 Server and
- > in Windows Server 2003 (including how-to configure a forwarder):
- > <http://support.microsoft.com/default.aspx?scid=kb:en-us:825036>
- >
- > 291382 – Frequently asked questions about Windows 2000 DNS and Windows
- > Server 2003 DNS
- > <http://support.microsoft.com/default.aspx?scid=kb:en-us:291382>
- >
- > 296379 – How to Disable NetBIOS on an Incoming Remote Access Interface
- > [Registry Entry]:
- > <http://support.microsoft.com/?id=296379>
- >
- > 292822 – Name Resolution and Connectivity Issues on Windows 2000 Domain
- > Controller with Routing and Remote Access and DNS Insta {DNS and RRAS and
- > unwanted IPs registering]:
- > <http://support.microsoft.com/?id=292822>
- > _____
- >
- >
- >
- > Ace
- >

• *Follow-Ups:*

Re: Question for Ace – Why to not Multi-home a DC

◆ **Re: Question for Ace – Why to not Multi-home a DC**

◇ From: Ace Fekay [MVP]

- Prev by Date: **Re: NT4.0 to AD 2003 Users and groups info**
- Next by Date: **Re: Connecting 2 networks with different Domain names together**
- Previous by thread: **Re: NT4.0 to AD 2003 Users and groups info**
- Next by thread: **Re: Question for Ace – Why to not Multi-home a DC**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**