

Re: Multihomed DC's

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2007-01/msg00090.html>

- *From:* "Bill Grant" <not.available@online>
 - *Date:* Mon, 8 Jan 2007 17:11:36 +1100
-

Hi Ace,

I agree with that! The original post is a bit confusing. I read it to mean that the multihomed server is the member server.

"Ace Fekay [MVP]" <PleaseAskMe@xxxxxxxxxxxxxxxx> wrote in message news:ulutG2sMHHA.1240@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

In news:2420BFE5-CD6E-459D-A79F-4948D0BADD29@xxxxxxxxxxxxxxxx, hedon <hedon@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> stated, which I commented on below:

We have a test lab with 2 DC's (1 AD Server/1Member server). Member Server. W2K3, with dual NICs that responds to domain traffic Vlan, 192.160.1.0/27 and Internet Vlan, 192.168.1.32/27. Internet traffic is outbound only for purposes of updating WSUS, AV pattern updates. The server is protected by Cisco CBAC Firewall.

How can I force all update traffic (http) to use the 192.168.1.32 vlan? Is their a better way I can design network flow, with the priority on server protection.

Thanks in advance for help

Along with Bill's suggestions, it is really not recommended to mutlihome a DC. It is hugely problematic due to the multiple interefaces and DNS registration.

However, if you insist, here is a step by step to alter default DC behavior to make it work for you:

=====
(Use this one):

Multihomed DCs, DNS, RRAS servers.

++++
++++

Below are the manual steps in more detail, which I had outlined in the

Re: Multihomed DC's

above paragraph:

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).

Little background on AD and DNS:

First, just to get this out of the way, if you have your ISP's DNS addresses in your IP configuration (DCs and clients), they need to be REMOVED.

If the ISP's DNS is in there, this will cause additional problems.

Also, AD registers certain records in DNS in the form of SRV records that signify AD's resource and service locations. When there are multiple NICs, each NIC registers. IF a client, or another DC queries DNS for this DC, it may get the wrong record. One factor controlling this is Round Robin. If a DC or client on another subnet that the DC is not configured on queries for it, Round Robin will kick in offering one or the other. If the wrong one gets offered, it may not have a route to it. On the other hand, Subnetmask Prioritization will ensure a querying client will get an IP that corresponds to the subnet it's on, which will work. To insure everything works, stick with one NIC.

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 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.

But believe me, it's much easier to just get a separate NAT device or multihome a non-DC then having to alter the DC. – Good luck!

1. Insure that all the NICS only point to your internal DNS server(s) only and none others, such as your ISP's DNS servers' IP addresses.
2. In Network & Dialup properties, Advanced Menu item, Advanced Settings, move the internal NIC (the network that AD is on) to the top of the binding order (top of the list).
3. Disable the ability for the outer NIC to register. The procedure, as mentioned, involves identifying the outer NIC's GUID number. This link will show you how:

Re: Multihomed DC's

246804 – How to Enable–Disable Windows 2000 Dynamic DNS Registrations (per NIC too):

<http://support.microsoft.com/?id=246804>

4. Disable NetBIOS on the outside NIC. That is performed by choosing to disable NetBIOS in IP Properties, Advanced, and you will find that under the "WINS" tab. You may want to look at step #3 in the article to show you how to disable NetBIOS on the RRAS interfaces if this is a RRAS server.
296379 – How to Disable NetBIOS on an Incoming Remote Access Interface [Registry Entry]:

<http://support.microsoft.com/?id=296379>

Note: A standard Windows service, called the "Browser service", provides the list of machines, workgroup and domain names that you see in "My Network Places" (or the legacy term "Network Neighborhood"). The Browser service relies on the NetBIOS service. One major requirement of NetBIOS service is a machine can only have one name to one IP address. It's sort of a fingerprint. You can't have two brothers named Darrell. A multihomed machine will cause duplicate name errors on itself because Windows sees itself with the same name in the Browse List (My Network Places), but with different IPs. You can only have one, hence the error generated.

5. Disable the "File and Print Service" and disable the "MS Client Service" on the outer NIC. That is done in NIC properties by unchecking the respective service under the general properties page. If you need these services on the outside NIC (which is unlikely), which allow other machines to connect to your machine for accessing resource on your machine (shared folders, printers, etc.), then you will probably need to keep them enabled.

6. Uncheck "Register this connection" under IP properties, Advanced settings, "DNS" tab.

7. Delete the outer NIC IP address, disable Netlogon registration, and manually create the required records

a. In DNS under the zone name, (your DNS domain name), delete the outer NIC's IP references for the "LdapIpAddress". If this is a GC, you will need to delete the GC IP record as well (the "GcIpAddress"). To do that, in the DNS console, under the zone name, you will see the _msdcs folder. Under that, you will see the _gc folder. To the right, you will see the IP address referencing the GC address. That is called the GcIpAddress. Delete the IP addresses referencing the outer NIC.

i. To stop these two records from registering that information, use the steps provided in the links below:

Private Network Interfaces on a Domain Controller Are Registered in DNS <http://support.microsoft.com/?id=295328>

ii. The one section of the article that disables these records is done with this registry entry:

Re: Multihomed DC's

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters

(Create this Multi-String Value under it):

Registry value: DnsAvoidRegisterRecords

Data type: REG_MULTI_SZ

Values: LdapIpAddress

GcIpAddress

iii. Here is more information on these and other Netlogon Service records:

Restrict the DNS SRV resource records updated by the Netlogon service

[including GC]:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddoc>

b. Then you will need to manually create these two records in DNS with the IP addresses that you need for the DC. To create the LdapIpAddress, create a new host under the domain, but leave the "hostname" field blank, and provide the internal IP of the DC, which results in a record that looks like:

(same as parent) A 192.168.5.200 (192.168.5.200 is used for illustrative purposes)

i. You need to also manually create the GcIpAddress as well, if this is a GC. That would be under the _msdcs._gc SRV record under the zone. It is created in the same fashion as the LdapIpAddress mentioned above.

8. In the DNS console, right click the server name, choose properties, then under the "Interfaces" tab, force it only to listen to the internal NIC's IP address, and not the IP address of the outer NIC.

9. Since this is also a DNS server, the IPs from all NICs will register, even if you tell it not to in the NIC properties. See this to show you how to stop that behavior (this procedure is for Windows 2000, but will also work for Windows 2003):

275554 – The Host's A Record Is Registered in DNS After You Choose Not to Register the Connection's Address:

<http://support.microsoft.com/?id=275554>

10. 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

(How to configure a forwarder):

<http://support.microsoft.com/d/id?=323380>

Active Directory communication fails on multihomed domain controllers

Re: Multihomed DC's

<http://support.microsoft.com/kb/272294>

<==*** Some additional reading ***==>

More links to read up and understand what is going on:

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>

Active Directory communication fails on multihomed domain controllers

<http://support.microsoft.com/kb/272294>

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>

Rid Pool Errors and other multihomed DC errors, and how to configure a multihomed DC, Ace Fekay, 24 Feb 2006

<http://www.ureader.com/message/3244572.aspx>

+++++

Re: Multihomed DC's

—

Ace
Innovative IT Concepts, Inc (IITCI)
Willow Grove, PA

This posting is provided "AS-IS" with no warranties or guarantees and confers no rights.

Ace Fekay, MCSE 2003 & 2000, MCSA 2003 & 2000, MCSE+I, MCT, MVP
Microsoft MVP – Directory Services
Microsoft Certified Trainer

Having difficulty reading or finding responses to your post?
Instead of the website you're using, I suggest to use OEx (Outlook Express or any other newsreader), and configure a news account, pointing to news.microsoft.com. This is a direct link to the Microsoft Public Newsgroups. It is FREE and requires NO ISP's Usenet account. OEx allows you to easily find, track threads, cross-post, sort by date, poster's name, watched threads or subject.

It's easy:

How to Configure OEx for Internet News
<http://support.microsoft.com/?id=171164>

Infinite Diversities in Infinite Combinations
Assimilation Imminent. Resistance is Futile
"Very funny Scotty. Now, beam down my clothes."

The only constant in life is change...