

Re: resolve incorrect IP from RRA server.

Re: resolve incorrect IP from RRA server.

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2009-05/msg00252.html>

- *From:* "Ace Fekay [Microsoft Certified Trainer]" <aceman@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 27 May 2009 20:25:08 -0400
-

"Calvin C." <yihsinchang@xxxxxxxxxxxxx> wrote in message
<news:8A0AC6C9-78C4-4212-ABC0-92F51A831AC1@xxxxxxxxxxxxxxxxxxxxx>

Hi All,

I have a DC with Routing and Remote Access installed. The server has been assigned a static IP, 10.5.100.100 and the internal interface of RRA got a dynamic address, 10.5.101.123 from DHCP server.

When I PING this server, it resolved to the dynamic IP instead of the static one. Flushing IP on server would not resolve the issue permanently.

Please advise.

Thanks
Calvin

This is by default. Multihomed DCs and multihomed DCs with RRAS (not RRA), unless it is SBS, are problematic. This is because the additional DNS records that get registered cause major problems with AD functionality, especially the additional IPs registered by RRAS. This is why you are seeing this issue. What is recommended is to move RRAS services off the DC to a member server (non-DC).

However, if you choose to keep RRAS on the DC, then you have to force DNS to only register the internal static interface, and no others. However because it is a DNS server, it will register itself to identify itself, as well as being a DC because the Netlogon service will register records to identify it as a DC, you can't simply uncheck the box in the NIC's properties to "not register this connection in DNS." This will require registry modifications.

Posted below are the steps that will need to be taken to modify a domain controller's default functionality. This will take care of this issue, and many other issues that come about because of multihoming a DC. Of course the other course of action, which I highly recommend instead of altering the DC, is to move RRAS to a member server, and disable one of the NICs on the DC.

Good luck, and let me know how you make out and what you decide to do.

** Please read the following before implementing so you fully understand the steps and what is involved before making the actual changes.

Re: resolve incorrect IP from RRA server.

** Please perform a System State backup, as well as backing up the registry before making any changes.

=====
=====
Multihomed DCs, DNS, RRAS servers.

By Ace Fekay
=====

Multihomed DCs WILL cause numerous issues. It's highly recommended to single home all DCs and use a non-DC for the multihoming purposes. If it is the internet gateway, it is recommended to purchase an inexpensive, or cable/DLS router, or even better, a Cisco or similar firewall to perform the task, which if it is compromised by an internet attacker remotely, can further compromise the rest of the internal network.

Also if attempting to use ICS on a DC, this further complicates matters with DC functionality, and cannot be fixed with the following steps outlined in this article.

To explain why will require a 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. I usually see errors (GPOs not working, can't find the domain, RPC issues, etc), when the ISP's DNS servers are listed on a client, DCs and/or member servers, or with multihomed DCs. If you have an ISP's (or some other outside DNS server or even using your router as a DNS server) DNS addresses in your IP configuration (all DCs, member servers and clients), they need to be REMOVED and ONLY use the internal DNS server(s). This can be very problematic.

Basically, AD requires DNS. DNS stores AD's resource and service locations in the form of SRV records, hence how everything that is part of the domain will find resources in the domain. If the ISP's DNS is configured in the any of the internal AD member machines' IP properties, (including all client machines and DCs), the machines will be asking the ISP's DNS 'where is the domain controller for my domain?', whenever it needs to perform a function, (such as a logon request, replication request, querying and applying GPOs, etc). Unfortunately, the ISP's DNS does not have that info and they reply with an "I dunno know", and things just fail. Unfortunately, the ISP's (or your router as a DNS server) DNS doesn't have information or records about your internal private AD domain, and they shouldn't have that sort of information.

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 Priortization 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 or simply use

Re: resolve incorrect IP from RRA server.

Re: resolve incorrect IP from RRA server.

the internal networking routing to allow access. Here's the whole list of manual steps to follow.

Another problem is the DC now becomes part of two Sites. This is another issue that can be problematic.

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. If the both NICs are internal, I would suggest to pick a subnet, team the NICs and allow your internal routers handle the traffic between subnets – 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:
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

Re: resolve incorrect IP from RRA server.

Re: resolve incorrect IP from RRA server.

<http://support.microsoft.com/?id=295328>

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

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/proddocs/standa>

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? Good question. 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

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

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

Re: resolve incorrect IP from RRA server.

Re: resolve incorrect IP from RRA server.

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/?id=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>

257623 257623 Domain Controller's Domain Name System Suffix Does Not Match Domain Name

<http://support.microsoft.com/?id=257623>

=====
=====

--
Ace

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

Ace Fekay, MCSE 2003 & 2000, MCSA 2003 & 2000, MCSA Messaging, MCT
Microsoft Certified Trainer

aceman@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

For urgent issues, you may want to contact Microsoft PSS directly. Please check <http://support.microsoft.com> for regional support phone numbers.

Re: resolve incorrect IP from RRA server.

Re: resolve incorrect IP from RRA server.

"Efficiency is doing things right; effectiveness is doing the right things." – Peter F. Drucker
<http://twitter.com/acefekay>