

# Re: sys vol check

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-08/msg03156](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-08/msg03156)

---

- *From:* "Jorge Silva" <jorgesilva\_pt@xxxxxxxxxxxx>
  - *Date:* Wed, 30 Aug 2006 12:33:37 +0100
- 

Inline

DNS zones are AD integrated. Not sure about the read/write local copy. How can I verify that?

– If DNS zones are AD Integrated are writable. (Secondary zones are read only—but it's not your case).

They do as well as the ISP DNS servers for right now. Once I get the DNS fixed I will try your suggestion again to add the public internet to DNS.

- Are you telling me that your servers have in their NIC Preferred DNS server
  - \*DC1 – IpAddress → 10.0.0.1
  - \*DC1 – Preferred DNS → 10.0.0.1
  - \*DC1 – Secondary DNS → 68.2.16.30 (ISP DNS)
  - \*DC1 – Third DNS → 68.1.208.30 (ISP DNS)

If yes, this is wrong.... You see your servers aren't using the ISP DNS Servers to resolve public names, your servers are using their root hints TO RESOLVE PUBLIC NAMES or any name that they're not authoritative for. DCs, member servers, clients, etc only TRY TO USE their secondary THIRD, etc... Other configured DNS servers on their NIC properties if the Primary Configured Server FAILS TO RESPOND. FOR EXAMPLE If the primary configured DNS server doesn't know anything about some Public or internal domain or name that the client is trying to resolve it will return a NEG ANSWER, and the clients WON'T TRY TO USE the secondary(s) configured DNS servers, They only try their secondary or other configured servers, IF THE PRIMARY FAILS TO RESPOND (example: is disconnected from network).

So the behavior and configuration is something like this: Clients should have configured in their NIC properties ONLY their LOCAL DNS server (You can if you want, configure secondary DNS servers for full tolerance, but use ONLY INTERNAL DNS Servers, because these servers are the only ones that knows where your Internal Resources are, Remember ISP DNS Servers Don't Know anything about your internal Domain, so they won't be able to "respond"

Re: sys vol check

correctly to your internal clients, member servers, besides that is bad from security perspective having clients, DCs whatever using the public DNS servers to resolve names.).

So if the DNS server isn't using the configured ISP DNS servers, how do they resolve public names? Simple they use the root hints to try to resolve any name which they're not authoritative for.

So why do I need to configure FORWARDING? If you configure forwarding your internal DNS servers will attempt to use their configured Forwarders to resolve names which they're not authoritative for, if these DNS servers FAIL, and only IF FAIL to respond, the servers will try to use the root hints (unless you configure the option "don't use recursion for this domain"). You can test this easelly, for example remove the ISP DNS Servers from secondaries, then CLEAR the DNS cache (dnscmd /cleardnscache) and local cache (ipconfig /flushdns) then try to resolve the Internal DNS names and Public Names... Result should be OK (assuming that the server is pointing to itself). However if you configure the ISP DNS servers as primary and the server Ip Address as secondary, then clear DNS cache and Local cache, then try to resolve internal names or srv records, what happens? IT will fail because the ISP DNS servers don't know anything about your internal domain srv records etc.... They only can resolve public names nothing more, and because of the default DNS behavior, the server won't try to use the secondary DNS server, because it received a NEG Answer from the ISP DNS server.

Note: Forwarding is different from conditional Forwarding.

Read carefully those links:

Deploying Domain Name System (DNS)

<http://technet2.microsoft.com/WindowsServer/en/library/7f6df44c-06c3-4b92-ba32-63d895a7924b1033.msp?mfr=>

Best practices for DNS client settings in Windows 2000 Server and in Windows Server 2003

<http://support.microsoft.com/default.aspx?scid=kb:en-us:825036&sd=RMVP>

How to configure DNS for Internet access in Windows Server 2003 (Forwarding)

<http://support.microsoft.com/kb/323380/>

Conditional Forwarding in Windows Server 2003

<http://support.microsoft.com/default.aspx?scid=kb:en-us:304491>

How Domain Controllers Are Located in Windows

Re: sys vol check

Re: sys vol check

<http://support.microsoft.com/kb/247811/>

How Domain Controllers Are Located in Windows XP

<http://support.microsoft.com/kb/314861>

They are getting the DHCP/DNS information from a firewall/security appliance. I have each local appliance to set the 1st DNS server as the local DNS server of that office and the next two are the ISP DNS servers. Again, I will fix that once I fix the DNS issues.

Wrong. Wrong.

If you're using DNS Integrated Zones, you probably have the zones allowing only secure updates; you should use MS DHCP to register the Clients records on behalf of the clients, because your FW/Router won't be able to do that. AGAIN the clients should no use ISP DNS servers in their NIC Properties

Using DNS servers with DHCP

<http://technet2.microsoft.com/WindowsServer/en/library/d0e19b57-c368-46c2-b017-caf25ae150ec1033.mspx?mfr=>

Well I don't want to get far way from the original problem which is replication problems.... Be aware that for replication work correctly you DNS infrastructure must be CORRECTLY configured, and I suggest you to read some technical articles about DNS configurations and default behavior. Another thing is related to Replication traffic itself, make sure that your FW isn't bloking need ports, you can use Portqry.exe

Portqry.exe

<http://support.microsoft.com/default.aspx?scid=kb:en-us:310099>

For FW needed ports check:

Active Directory Replication over Firewalls

<http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/deploy/confeat/adrepfin>

Service overview and network port requirements for the Windows Server system

<http://support.microsoft.com/default.aspx?scid=kb:en-us:832017>

Active Directory in Networks Segmented by Firewalls

<http://www.microsoft.com/downloads/details.aspx?FamilyID=c2ef3846-43f0-4caf-9767-a9166368434e&DisplayLa>

--

I hope that the information above helps you

Re: sys vol check

Re: sys vol check

Good Luck  
Jorge Silva  
MCSA  
Systems Administrator

"Scott Sendelbach" <ScottSendelbach@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:BFC0478A-B4E0-4418-BE13-0655E58DBB4B@xxxxxxxxxxxxxxxxxxxx

Please see below:

"Jorge Silva" wrote:

ahh.. Ok

Let's recap, if something is wrong please let me know...

You've 3 DC DNS servers one in each Site with different subnets.  
Yes (PHOENIX (168)) (IRVINE(184)) (LASVEGAS(200))

You've A forward lookup Zone named CORP.DLECINC.COM and a reverse lookup > zone.

Yes. 1 forward lookup zone and three reverse lookup zones. 1 for each subnet listed above.

All DNS zones are AD Integrated and each DC has one read/writte copy in their DNS console?

DNS zones are AD integrated. Not sure about the read/write local copy. How can I verify that?

You've only one domain?

Yes. CORP

You have the DCs in their correct Site with the correct subnet assigned.

Yes, Please see above for site name and IP subnet.

Is this all OK?

Yes

Next step is:

Each server should point to itself under NIC Preferred DNS.

They do as well as the ISP DNS servers for right now. Once I get the DNS fixed I will try your suggestion again to add the public internet to DNS.

Each client should have under NIC Preferred DNS the LOCAL SITE DNS DC server.

They are getting the DHCP/DNS information from a firewall/security

Re: sys vol check

Re: sys vol check

appliance. I have each local appliance to set the 1st DNS server as the local DNS server of that office and the next two are the ISP DNS servers. Again, I will fix that once I fix the DNS issues.

Forwarding in this case is ONLY TO Resolve public (Internet) Names. You can check the link that I provided you.

Another thing that I reviewed was your tests, that are given RPC server errors. Check if you have any FW between them not allowing RPC traffic. I don't believe there are any rules or policies blocking RPC. What can I do to check where the traffic is being blocked? It is possible the firewall/security appliance may be blocking the traffic.

Thank you for all your help so far on this

Scott

--

I hope that the information above helps you

Good Luck  
Jorge Silva  
MCSA  
Systems Administrator

"Scott Sendelbach" <ScottSendelbach@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote in  
message  
[news:1B3DBC70-F32C-48CD-B47A-0C176E6215A9@xxxxxxxxxxxxxxxxxxxx](mailto:news:1B3DBC70-F32C-48CD-B47A-0C176E6215A9@xxxxxxxxxxxxxxxxxxxx)

Yes there is only one folder under the forward list  
(corp.dlecinc.com)  
or  
domain name is CORP.

"Jorge Silva" wrote:

Only 1 folder???

Ok couple of options:  
-You can check DNS:  
How to Verify the Creation of SRV Records  
for a Domain Controller

Re: sys vol check

<http://support.microsoft.com/kb/241515/EN-US/>

How to verify that SRV DNS records have been created for a domain controller

<http://support.microsoft.com/kb/816587/en-us>

– You can run Dcdiag and netdiag and check if configurations are Ok.

Or you can rebuild DNS follow these steps carefully:

Assuming AD Integrated Zones. Point all existent DCs to the Main DC (Windows 2003), Point the Main DC to itself, then:

\*Also make sure that you have sites and related subnets properly configured, and that the Correct servers are in the correct site, this is important because allows windows clients and servers to reach and authenticate with the correct DC and for GC contact, DFS, etc.  
\*Now it's time to reconfigure the DNS:  
Point all existent servers in their NIC TCP/IP configuration – Preferred DNS – Pointing to the server where you are going to recreate the DNS Forward and Reverse Zones.

For example: Assuming DC1,DC2 and DC3, DC1 is where we're going to recreate the zones.

DC1 – IPAddress -> 10.0.0.1

DC1 – Preferred DNS -> 10.0.0.1

Re: sys vol check

DC2 – IPAddress -> 10.0.0.2

DC2 – Preferred DNS -> 10.0.0.1

DC3 – IPAddress -> 10.0.0.3

DC3 – Preferred DNS -> 10.0.0.1

\*Delete the forward zone and the reverse lookup zone on DC1.

\*Wait for replication and make sure that the zones are automatically removed from the other servers.

\*You can also force replication using Active Directory Sites and Services

or  
any other Tool.

\*Clear the DNS cache

– rightclick the DNS server and clear the cache.

– run from cmd: ipconfig /flushdns

\*Go to the %systemroot%\system32\dns – delete any old zone that you might have there.

\*delete the files netlogon.dnb and netlogon.dns from %systemroot%\system32\config

\*create the forward lookup zone and the reverse lookup zone on DC1 and make them AD integrated, for security purposes make sure that the zones only accept secure only – updates.

\*run ipconfig /registerdns

\*restart the netlogon service, confirm the creation of the files

netlogon.dnb and netlogon.dns on %systemroot%\system32\config

\*run netdiag /fix

\*Run REPADMIN /SYNCALL and wait a little bit (some times this can take awhile), You can also force replication using

Re: sys vol check

Active Directory Sites  
and  
Services or any other Tool. Then go to the  
others servers and if the  
zone  
was already transferred, then point these  
servers to itself again.

The Configuration after the Zone(s) have  
been transferred should be:

DC1 – IPAddress -> 10.0.0.1

DC1 – Preferred DNS -> 10.0.0.1

DC2 – IPAddress -> 10.0.0.2

DC2 – Preferred DNS -> 10.0.0.2

DC3 – IPAddress -> 10.0.0.3

DC3 – Preferred DNS -> 10.0.0.3

\*run dcdiag and netdiag and make sure that  
everything is ok.

Make sure that each client uses the correct  
DNS server in their  
Preferred  
DNS settings in their local site.

--

I hope that the information above helps you

Good Luck  
Jorge Silva  
MCSA  
Systems Administrator

"Scott Sendelbach"

<ScottSendelbach@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote

in

message

[news:C169CF88-CEE5-43CB-A680-C29E9465C88F@xxxxxxxxxxxxxxxxxxxxx](mailto:news:C169CF88-CEE5-43CB-A680-C29E9465C88F@xxxxxxxxxxxxxxxxxxxxx)

Each SITE has its own IP  
address and DNS server.  
There is only one

Re: sys vol check

folder  
under the DNS forward  
lookup zones. There are  
three folders under  
the  
reverse  
look up zone, 1 for each  
site/subnet. All three DNS  
servers has the  
same  
setup.

"Jorge Silva" wrote:

How sites  
and subnets  
are  
configured?

--

I hope that  
the  
information  
above helps  
you

Good Luck  
Jorge Silva  
MCSA  
Systems  
Administrator

"Scott  
Sendelbach"  
<ScottSendelbach@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote  
in  
message  
[news:0049D664-5C8F-457F-B725-34FDB068C7B9@xxxxxxxxxxx](mailto:news:0049D664-5C8F-457F-B725-34FDB068C7B9@xxxxxxxxxxx)

Yes  
the  
servers  
have  
the  
local  
DNS  
server  
listed  
as

Re: sys vol check

the  
first(primary  
DNS  
server)  
under  
the  
NIC  
properties.  
Then  
I  
removed  
the  
ISP  
DNS  
and  
added  
the  
other  
two  
DNS  
server  
addresses.

Yes,  
the  
DNS  
is  
AD  
integrated.

The  
DNS  
server  
addresses  
is  
being  
populated  
by  
a  
network  
appliance/firewall  
that  
is  
handing  
out  
DHCP  
address.  
I  
made  
the  
Phoenix

Re: sys vol check

DNS  
server  
primary,  
Las  
vegas  
second  
and  
California  
last.

I  
think  
there  
is  
a  
DNS  
issue  
and  
I  
believe  
that  
replication  
is  
working.  
How  
can  
I  
test  
both  
to  
see  
if  
they  
are  
setup  
correctly?

"Jorge  
Silva"  
wrote:

Are  
the  
users  
NIC  
DNS  
configuration  
pointing  
only  
to

Re: sys vol check

their  
local  
DNS  
servers?  
You  
have  
DNS  
AD  
Integrated  
right?  
Are  
the  
servers  
pointing  
to  
itself  
under  
their  
NIC  
DNS  
Preferred  
server?

You  
must  
had  
something  
wrong,  
because  
if  
you  
follow  
those  
links  
the  
Logon  
must  
work.  
Check  
if  
replication  
is  
working.

Another  
thing,  
you  
said  
that  
you  
undo

Re: sys vol check

Re: sys vol check

everything,  
so  
how  
is  
it  
configured  
now?

--  
I  
hope  
that  
the  
information  
above  
helps  
you

Good  
Luck  
Jorge  
Silva  
MCSA  
Systems  
Administrator

"Scott  
Sendelbach"  
<ScottSendelbach@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote  
in  
message  
[news:14F5AE16-61C8-4E4B-BE08-39C9BFF104](mailto:news:14F5AE16-61C8-4E4B-BE08-39C9BFF104)

I  
modified  
the  
forwarders  
tab  
on  
the  
DNS  
AD  
list  
like  
the  
intructions  
listed,  
and  
then

Re: sys vol check

I  
changed  
the  
DNS  
servers  
list  
on  
all  
three  
DNS  
server  
to  
point  
to  
each  
other  
rather  
then  
the  
ISP  
DNS  
servers.

When  
I  
got  
in  
this  
morning,  
no  
one  
was  
able  
to  
log  
on  
and  
see  
the  
network.  
I  
had  
to  
undo  
everything  
I  
did  
yesterday  
afternoon  
and  
it

Re: sys vol check

Re: sys vol check

seems  
to  
be  
working  
fine  
now.

I  
am  
not  
sure  
what

I  
did  
wrong.

I  
followed  
the  
instructions  
listed  
in  
the  
microsoft  
link  
you  
sent  
me  
earlier.

"Jorge  
Silva"  
wrote:

how?

The  
DNS  
server  
should  
point  
to  
itself  
in  
NIC  
Preferred  
DNSserver.  
The  
clients  
should  
use

Re: sys vol check

Re: sys vol check

only  
their  
local  
DNSserver  
in  
ther  
NIC  
Preferred  
DNSserver.

How  
clients  
and  
servers  
are  
configured  
now?

--  
I  
hope  
that  
the  
information  
above  
helps  
you

Good  
Luck  
Jorge  
Silva  
MCSA  
Systems  
Administrator

"Scott  
Sendelbach"  
<ScottSendelbach@xxxxxxxxxxxxxxxxxxxx>  
wrote  
in  
message  
[news:2016BC8A-6A8F-4113-9D34-...](mailto:news:2016BC8A-6A8F-4113-9D34-...)

I  
have  
done  
as  
you  
instructed  
and

Re: sys vol check

it  
crashed  
our  
network.  
No  
one  
is  
able  
to  
log  
on  
this  
morning  
and  
see  
any  
local  
resources.

"Jorge  
Silva"  
wrote:

Inline

1.  
How  
do  
I  
know  
when  
it  
will  
be  
safe  
to  
remove  
them  
from  
the  
DHCP  
device  
that  
is  
handing  
out  
licenses?

–  
Remove

Re: sys vol check

Re: sys vol check

what?