

## Re: Event ID 7062 in DNS logs

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2006-01/msg00049.html>

---

- *From:* "Ace Fekay [MVP]" <PleaseSubstituteMyActualFirstName&LastNameHere@xxxxxxxxxxxx>
  - *Date:* Tue, 3 Jan 2006 19:06:52 -0500
- 

In [news:1136281390.967898.214700@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:1136281390.967898.214700@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx),  
ovidiu\_m\_gheorghita@xxxxxxxx <ovidiu\_m\_gheorghita@xxxxxxxx> stated, which  
I commented on below:

- > Thank you for your time.
- > If I good understand, you advice me to let the default Internet root  
> hints in place and to use forwarders from the child DNS (DNS server in  
> child domain hosting the AD-integrated zone child.forestroot.com) to  
> the root DNS (DNS server on the forest root domain hosting the  
> AD-integrated forestroot.com zone).

That is correct.

- > I did not deleted the \_msdcs.co.test.com zone.

That is good because this zone should never be deleted. It is the zone that  
lets all domains know of the forest root domain and the GCs.

- > My DNS server on the root domain is hosting two forward zones: the  
> root  
> domain AD-integrated zone (which is also containing the child DNS  
> domains delegations) and also the \_msdcs zone that is correctly  
> replicated on all child DNS.

Good.

- > A chils DNS is containing its own AD-integrated DNS zone and also the  
> forestwide AD replicated \_msdcs zone.

That is good too, but hosting the \_msdcs zone is not necessary because of  
the forwarder from the child DNS to the parent DNS in the forest root  
domain.

- >
- > Also, there's no forwarders configured on the DNS server on the root  
> domain or on the DNS servers on the child domains.

If you want Internet access, you can configure a forwarder on the forest

Re: Event ID 7062 in DNS logs

root DNS servers to the Internet. In a proper delegation, the child DNS should forward only to the forest root domain's DNS server(s).

- > The forest root domain is not connected on the Internet and every
- > child
- > domain is getting out on the internet via proxy.

I thought you were using a proxy. Keep in mind the proxy has nothing to do with Active Directory as long as the internal subnets are in the LAT. The delegations we spoke of are to allow full infrastructure resolution for Active Directory.

- >
- > When I configured the DNS I tried to apply the following:
- >
- > High-Level DNS Security Policy
- >
- > High-level DNS security uses the same configuration as mid-level
- > security and also uses the security features available when the DNS
- > Server service is running on a domain controller and DNS zones are
- > stored in Active Directory. Also, high-level security completely
- > eliminates DNS communication with the Internet. This is not a typical
- > configuration, but it is recommended whenever Internet connectivity is
- > not required. High-level security policy includes the following
- > characteristics:
- >
- > · The DNS infrastructure of your organization has no Internet
- > communication by means of internal DNS servers.
- >
- > · Your network uses an internal DNS root and namespace, where all
- > authority for DNS zones is internal.
- >
- > · DNS servers that are configured with forwarders use internal DNS
- > server IP addresses only.
- >
- > · All DNS servers limit zone transfers to specified IP addresses.
- >
- > · DNS servers are configured to listen on specified IP addresses.
- >
- > · Secure cache against pollution is enabled on all DNS servers.
- >
- > · Internal DNS servers are configured with root hints that point to
- > the internal DNS servers hosting the root zone for your internal
- > namespace.
- >
- > · Secure dynamic update is configured for all DNS zones except for
- > the top-level and root zones, which do not allow dynamic updates at
- > all.
- >
- > · All DNS servers are running on domain controllers. An access
- > control list (ACL) is configured on the DNS Server service to allow

Re: Event ID 7062 in DNS logs

- > only specific individuals to perform administrative tasks on DNS
- > servers.
- >
- > · All DNS zones are stored in Active Directory. An ACL is configured
- > to allow only specific individuals to create, delete, or modify DNS
- > zones.
- >
- > · ACLs are configured on DNS resource records to allow only specific
- > individuals to create, delete, or modify DNS data.
- >
- >
- > Note
- >
- > · Windows Server 2003 DNS does not support the use of DACLs on zones
- > to control which clients or users can send queries to the DNS server.
- >
- > (Microsoft TechNet: Windows 2003 Deployment Guide>Deploying Network
- > Services>Deploying DNS>Securing Your DNS Infrastructure
- >
- > <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/DepKit/2011e2a8-1a45-4a27-9ea7-f7f77>
- > )
- >
- > I did not modified the ACLs.
- >
- > Maybe I'm not very good understanding what exactly a 'root' zone
- > means.
- > Especially for the '.' zone.

A Root zone, specifically the "." zone, means that you are telling the DNS server that it's a Root server, like one of the 13 Root servers on the Internet that has a reference of DNS servers that host all of the TLDs on the Internet. The Internet Root servers are the ones normally shown under the Root Hints tab. Once you make your DNS server a Root server by creating a "." zone, then the Root Hints disappear because now it believe that it's one of these servers. If not sure what the Root servers on the internet do, a better way to understand it is to understand the DNS resolution process. When a DNS server receives a query for a zone that is not authoritative for or has no reference to, it will contact the Root servers querying if it knows anything about that zone one by one until one responds that it has a reference to another DNS server that has information about that zone. That's what a Root server is and that is what the "." zone does to a DNS server. It is only useful in a scenario such as yours when you are using ISA or proxy for Internet control and resolution.

Here's more info on the resolution process:

How DNS query works Domain Name System(DNS):

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/0bcd97e6-b75d-48ce-83ca-b>

- >There's no such zone on the Windows 2003
- > DNS...at least when promoting a DC and we let the dcpromo wizard to
- > install and configure local DNS server and the DNS zones. Let say that

Re: Event ID 7062 in DNS logs

- > my forest name is forestroot.com.
- > When I'm installing the forest root domain, with an Windows 2003 DNS
- > and AD-integrated zones, the dcpromo wizard creates on the DNS server
- > (also DC) two zones:
- > forestroot.com
- > \_msdcs.forestroot.com

That is correct and normal.

- >
- > The forestroot.com is what I'm considering the forest root zone. This
- > is AD-integrated and it's replication scope is on all DNS servers on
- > the forest root domain (in my configuration there are DC's in the
- > forest root domain, both also DNS servers.)

This zone is the start of your AD namespace and is the forest root zone, but not to be confused with a ROOT SERVER, as I mentioned above.

- > This zone is also containing delegations for the child domains.
- >
- > The \_msdcs.forestroot.com zone is by default a zone containing SRV
- > records for all DC's in the forest and it's replication scope is on
- > all
- > DNS servers in the forest (in my configuration all DC's are also DNS
- > servers.). I think this is part of the DNS application partition, the
- > ForestDNSZones.
- >
- > The two root DC's (so also DNS servers) are configured at the TCP/IP
- > level as following:
- > – Preferred DNS server is it's own IP address
- > – Alternate DNS server is the other's root domain DC (also DNS) IP
- > address.

That is good too.

- >
- > Also, in the Microsoft TechNet, Designing and Deploying Directory and
- > Security Services>Deploying the Windows Server 2003 Forest root
- > domain>Creating the Forest Root Domain>Deploy the First Forest Root
- > Domain Controller>Verify DNS server recursive name resolution on the
- > first forest root DC, at

>

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/DepKit/2011e2a8-1a45-4a27-9ea7-f7f77>

- > they are stating, in the Table 6.2 Information to Verify DNS Server
- > Recursive Name Resolution that the root hints are the preferred method
- > to use for recursive name resolution in Windows 2003.

Most would say using a forwarder to the ISP is the preferred method for internet name resolution, but this does NOT apply in your case because you are using a proxy.

Re: Event ID 7062 in DNS logs

- > Or, for me, what I'm trying to configure is a recursive name
- > resolution, meaning for me that, if in a child domain a client makes a
- > DNS query for a name in another child domain, the clien's DNS server
- > will look up first in it's own zone, then in its root hints in order
- > to
- > address the root server and to find the requested name's DNS server.
- >
- > I think it should work as fine as using forwarders.
- >
- > Am I wrong? Please help me to understand....

To make that work, follow the recommendations I previously made to delegate to the child, and forward from the child to the parent. You will be fine., believe me...

- >
- >
- > Thank you,
- > omg

You are welcome.

Ace

---

• **References:**

- ◆ **[Event ID 7062 in DNS logs](#)**
  - ◇ *From:* ovidiu\_m\_gheorghita
- ◆ **[Re: Event ID 7062 in DNS logs](#)**
  - ◇ *From:* Ace Fekay [MVP]
- ◆ **[Re: Event ID 7062 in DNS logs](#)**
  - ◇ *From:* ovidiu\_m\_gheorghita
- Prev by Date: **[Re: OT: The Philly Eagles Re: AD does not start](#)**
- Next by Date: **[Re: OT: The Philly Eagles Re: AD does not start](#)**
- Previous by thread: **[Re: Event ID 7062 in DNS logs](#)**
- Next by thread: **[Re: AD integrated DNS transfer](#)**
- Index(es):
  - ◆ **[Date](#)**
  - ◆ **[Thread](#)**