

## Re: Forest to Child -- Permissions

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2006-09/msg00350.html>

---

- *From:* "Herb Martin" <[news@xxxxxxxxxxxxxxxx](mailto:news@xxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 18 Sep 2006 21:01:17 -0500
- 

Hey Herb ---- thanks for taking care of me ... Again!! :)

Well, I don't see that I am helping all that much since I am close to stumped if everything you have reported is accurate.

I just did a copy from the default 'Administrators' group once I created the first DC in the root.  
What I don't understand is that my account works perfectly with all 9 of the DCs. No issues.  
However, the member servers (in both child and newtree domains) only authenticate me as a regular user.

Well, you should go check the domain's Administrators contains Enterprise Admins from the root domain (it should.)

Also note that by default an ordinary users should not be able to logon to a DC at all. (Only the 'powerful' groups like Admins, Server Ops, Print Ops, Account Ops, and Backup Ops can do this by default -- I believe that is the default even for ordinary member servers too.)

They have their primary and secondary dns pointers going to their DCs in their (child/newtree) domain, which should (as shown below) then point up to the root.

Sounds right.

I re-ran DCDIAG on all 9 DCs ---- and everything passes without exception.  
Ideas?

Re: Forest to Child -- Permissions

DCDiag pretty much confirms authentication AND that DNS is right.  
(It might not notice that one domain cannot reach another domain, but you seem to have that covered with conditional forwarding, stubs, and delegation anyway.)

Check the Administrators group though even though that should never happen unless some admin has been mucking about.

--  
Herb Martin, MCSE, MVP  
Accelerated MCSE  
<http://www.LearnQuick.Com>  
[phone number on web site]

"santa"'s helper" <santashelper@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message [news:489F28A5-A749-4FB7-8137-0C6A9AA439D8@xxxxxxxxxxxxxxxxxxxx](mailto:news:489F28A5-A749-4FB7-8137-0C6A9AA439D8@xxxxxxxxxxxxxxxxxxxx)

"Herb Martin" wrote:

"santa"'s helper" <santashelper@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message [news:CA980F9B-FA7D-4F5E-A7EE-8816E6EC175D@xxxxxxxxxxxxxxxxxxxx](mailto:news:CA980F9B-FA7D-4F5E-A7EE-8816E6EC175D@xxxxxxxxxxxxxxxxxxxx)

Here is my environment:  
There are 3 domains -- root.com, child.root.com,  
newtree.com - ea  
with 3  
DCs

Concerning DNS:  
Root domain  
has a delegated sub domain pointing to the child.root domain

Technically a "delegated zone" and "subdomain" are two different things -- the latter being merely an additional name tag in the parent zone -- but I assume you mean the parent DELEGATED to the child zone servers (if not you need to fix this by removing the true "subdomain" and actually delegating or using another method.)

has a stub domain pointing to the newtree domain  
Root.child domain  
has conditional forwarding, no recursion, back to the root  
has a stub pointing to the newtree domain

## Re: Forest to Child -- Permissions

You could use Conditional Forwarding for each stub, but there is nothing wrong with the current method. You could also use Forest-Wide AD Integration for EVERY ZONE instead of these conditional forwarders, stubs, and delegation even.

Just choices however so nothing wrong with what you have.

NewTree domain  
has conditional forwarding, no recursion, back to the root  
has a stub pointing to the child.root domain

Perfectly fine again, but technically the stub is technically unnecessary since the entire Parent-Child tree can be found from the parent.

DCDiag --- passes all test for all DCs

Good.

I have a root, domain admin account.  
I was able to create and can login to all DCs with my root account as  
an  
admin

So generally authentication and trusts are working as expected.

Any comments (or a better way) on the above are welcome; however, here is my issue at the moment:  
I can create member servers at the child and new tree levels, but after the reboot, when I login with my root account to the member servers I don't have administrator privileges -- only user privileges. Why? What am I missing?

I don't see it -- unless those member servers cannot authenticate properly OR your client DNS settings (even on servers) cannot find everything. You've covered this from the DNS SERVER point

Re: Forest to Child -- Permissions

of view, but perhaps the client settings are wrong...

All internal "client DNS" settings must reference ONLY "internal" DNS servers that can resolve all (both internal and external) names the clients will need.

When you said "root Domain Admin" did you in fact mean an ENTERPRISE ADMIN or "just" a domain admin?

--

Herb Martin, MCSE, MVP  
Accelerated MCSE  
<http://www.LearnQuick.Com>  
[phone number on web site]

Thanks in advance for your help. S

Hey Herb --- thanks for taking care of me ... Again!! :)

I don't see it -- unless those member servers cannot authenticate properly OR your client DNS settings (even on servers) cannot find everything. You've covered this from the DNS SERVER point of view, but perhaps the client settings are wrong...

All internal "client DNS" settings must reference ONLY "internal" DNS servers that can resolve all (both internal and external) names the clients will need.

When you said "root Domain Admin" did you in fact mean an ENTERPRISE ADMIN or "just" a domain admin?

Yeah -- I don't get it either.

My account, at the root level, is a member of:

Administrators

Domain Admins

Domain Users

Enterprise Admins

Group Policy Creator

Schema Admins

I just did a copy from the default 'Administrators' group once I created the

first DC in the root.

What I don't understand is that my account works perfectly with all 9 of

Re: Forest to Child -- Permissions

the

DCs. No issues.

However, the member servers (in both child and newtree domains) only authenticate me as a regular user. They have their primary and secondary dns

pointers going to their DCs in their (child/newtree) domain, which should

(as

shown below) then point up to the root.

I re-ran DCDIAG on all 9 DCs --- and everything passes without exception.

Ideas?

Thanks Again, S