

Re: Forest to Child -- Permissions

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2006-09/msg00348.html>

- *From:* "Herb Martin" <news@xxxxxxxxxxxxxxxx>
 - *Date:* Mon, 18 Sep 2006 17:16:35 -0500
-

"santa"'s helper" <santashelper@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:CA980F9B-FA7D-4F5E-A7EE-8816E6EC175D@xxxxxxxxxxxxxxxx

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

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

Re: Forest to Child -- Permissions

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 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

Re: Forest to Child -- Permissions