

# Re: dns administration delegation

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2007-06/msg00185.html>

---

- *From:* "Herb Martin" <[news@xxxxxxxxxxxxxxx](mailto:news@xxxxxxxxxxxxxxx)>
  - *Date:* Wed, 13 Jun 2007 19:01:55 -0500
- 

"doh" <[doh@xxxxxxxxxxx](mailto:doh@xxxxxxxxxxx)> wrote in message [news:f4ppt3\\$74c\\$1@xxxxxxxxxxx](mailto:news:f4ppt3$74c$1@xxxxxxxxxxx)

I'm not sure if I got my point across with what my ultimate goal is. As I do know there is a GPO key to allow specific users to start/stop a service, this is only half of the job. Does the same GP setting allow these users to fully manage DNS? Meaning add/delete/modify zones?

Yes, full control of the SERVICE will allow you read and write its data, or you can give limited permissions such as "read" to the Help Desk to allow those folks to VIEW but not change settings.

Aside from the fact that the main ADI replicated zone for the domain will be under their control, I'm more concerned about these admins to have the ability to add zones for their specific site.

How often do zones get added? This is usually a (nearly) static thing -- set once, early in the deployment of DNS servers and then seldom if every modified (the actual zones.)

Hope this is a bit more clear now.

"Herb Martin" <[news@xxxxxxxxxxxxxxx](mailto:news@xxxxxxxxxxxxxxx)> wrote in message [news:umCsOJfrHHA.3228@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:umCsOJfrHHA.3228@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

"doh" <[doh@xxxxxxxxxxx](mailto:doh@xxxxxxxxxxx)> wrote in message [news:f4pan0\\$db2\\$1@xxxxxxxxxxx](mailto:news:f4pan0$db2$1@xxxxxxxxxxx)

The method I initially described was in fact setting the permissions via

## Re: dns administration delegation

the security tab in dnsmgmt.msc. You are correct about the additional permissions that grant unnecessary rights. I wasn't aware of the GPO method where one can delegate rights to a specific dns server.

The usual way is to do this through a GPO -- to make someone a service admin for all servers of that type -- but you can still use a GPO for one or a few servers if you find a way to distinguish them by filter (permissions or WMI) or by Site as in your specific case.

You are also correct in that the "site admins" are not domain admins otherwise they would have full control anyway.

I presumed that, but people ask all sorts of strange things based on what they have tried without thinking it through, so it was important for you to confirm.

What is the setting(s) via GP that you're referring to that could grant these admins full access to their local dns servers (which are also domain controllers), but not access any other dns servers within the domain?

Computer->Windows Settings->Security->Services

I am aware of filtering out GPs based on groups, which would be my preferred method rather than adding child OUs.

Good, as I am really nervous about even child OUs for DCs. Although in your case I might well suggest Sites for this, then you would not need to modify it if you add another DC in either location -- it would just work.

You could even move a DC from one site and the control would switch with the location.

Re: dns administration delegation

At any rate, if this causes more trouble than its worth, then I might just opt to drop all the admins into the DNS Administrators group and state that they should not manage any other servers.

Curious: What is different about the two sets of services? Do they have different zones, or what else is different? We must presume you have at least some of the zones replicated for the Domain since they are all DCs.

Auditing would have to be put in place here just in case an admin from an alternate site does make a modification on a dns server not within their administrative boundary.

You can also use the GPO (Advanced) settings for the service to add not just permission but also Auditing, and also make certain services required or forbidden (this last is not what you were asking of course.)

--  
Herb Martin, MCSE, MVP  
<http://www.LearnQuick.Com>  
(phone on web site)

"Herb Martin" <news@xxxxxxxxxxxxxx> wrote in message [news:OVB9%238WrHHA.532@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OVB9%238WrHHA.532@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

"doh" <doh@xxxxxxxxxxxxxx> wrote in message [news:f4nglt\\$hn1\\$1@xxxxxxxxxxxxxx](mailto:news:f4nglt$hn1$1@xxxxxxxxxxxxxx)

4 total DNS servers runnin  
on domain controllers

2 domain controllers are in  
site A

2 domain controllers are in  
site B

I want admins from site A to  
be able to manage only the  
DNS servers at  
site A.

I want admins from site B to  
be able to manage only the  
DNS servers at

Re: dns administration delegation

site B.

I create a group named siteA\_dns and add this group to the two servers security tab in site A to read/write access.

Are you doing this in the DNS MMC properties on the Security tab?

Does this work?

I will look forward to other answers but I don't think this is the way to do this, and have always done it with a GPO to delegate control of the service.  
(There is a problem with this method in your case however which may be as bad as what you are seeing even though it is different.)

I am not even sure that permissions you are actually delegating there — if you look at the Standard Permissions permissions you see there is nothing in there for stopping and starting the service. If you further look in the Special Permission for any ACE you will also see this is missing but worse there seems to be all sorts of additional permissions that seem to be concerned with all sorts of unrelated (and in your case undesirable) areas.

Replication takes effect and I check the two dns server in site B.  
They both now have the

## Re: dns administration delegation

same security read/write  
access for the  
siteA\_dns group.

Anyone know of a way to  
work around this to be able  
to prevent admins  
from one site making mods  
at another site (besides  
blocking rpc via  
registry)?

The problem with doing it through a GPO is  
that you would normally want  
to  
do this by putting the servers in different  
OUs -- you must however NOT  
move your DCs outside of the Domain  
Controller OU.

Some claim you can put them in child OUs  
but my experience was NOT  
good when I tried that and I have never  
tested it again.

You could however (with no problem I can  
conceive) link to the existing  
DC OU but use permissions (on the DC  
computer accounts) to filter  
the GPO to only apply to one set of DC and  
then the other set of DCs  
for the other users.

Or you could link the GPOs to the respective  
SITES instead of using  
permission filtering.

Since these are all one DCs do you really  
have trouble with admins  
messing  
where they shouldn't?

Can't you just (reliably) make  
business/security rules where one set of  
Admins  
doesn't mess with the other set of DNS  
servers?

Re: dns administration delegation

Presumably these are NOT "domain admins"  
either -- but just something  
you  
are calling Site admins?

--

Herb Martin, MCSE, MVP  
<http://www.LearnQuick.Com>  
(phone on web site)