

Re: dns administration delegation

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2007-06/msg00219.html>

- *From:* "doh" <doh@xxxxxxxxxxxx>
 - *Date:* Fri, 15 Jun 2007 15:50:54 -0400
-

Let's not worry about why the zones need to be created. Let's just say that it's necessary. ;)

On the other issue, I still can't access the dnsmgmt.msc because of an Access Denied. Any ideas?

"Herb Martin" <news@xxxxxxxxxxxx> wrote in message <news:%23uUS3C4rHHA.5028@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

"doh" <doh@xxxxxxxxxxxx> wrote in message [news:f4ugp3\\$hh9\\$1@xxxxxxxxxxxx](news:f4ugp3$hh9$1@xxxxxxxxxxxx)

I just executed the following:

Created a group named site_DNSadmin.
Created a GP object.
Allow site_DNSadmin group to FULL control Computer Configuration\Windows Settings\Security Settings\System Services\DNS Server via the GP.
Apply the GP to the domain controllers in question.
Force replication.
Force GP update.
Verified with RSOP that the GP is in fact applied to the domain controllers.

Logged on to a workstation in the domain with an admin account which is a member of the site_DNSadmin group.

Executed dnsmgmt.msc and added one of the dns servers.
The console of course results with an Access Denied.

Did I miss a step in this process? Would I need to grant these admins the

Re: dns administration delegation

right to logon to the domain controller directly and then have them run dnsmgmt.msc from the server itself?

No, logon locally to the DC should NOT be needed.

Also, to answer your question about zones... some of the dns servers hosts services for different development groups. They have needs to add local zones to their servers that dont apply to other sites.

And do these zones get added and modified frequently? Even in such as case the zones shouldn't be changing that often.

You could just get a (real) admin to conditionally forward to a server used by the "development" groups -- it is not obvious why developers would be creating DNS zones in a production system.

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

"Herb Martin" <news@xxxxxxxxxxxxxx> wrote in message
news:OIVq5chrHHA.3356@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

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

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

Re: dns administration delegation

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@xxxxxxxxxxxxxx>
wrote in message
news:umCsOJfrHHA.3228@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

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

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

Re: dns administration delegation

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
waht
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

Re: dns administration delegation

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

Re: dns administration delegation

with the location.

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

Re: dns administration delegation

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@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

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

4
total
DNS
servers
runnin
on
domain
controllers

2
domain
controllers
are
in
site

Re: dns administration delegation

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
site
B.

I
create
a

Re: dns administration delegation

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
the
DNS
MMC
properties
on
the
Security
tab?

Does
this
work?

I
will
look
forward
to
other
answers
but
I
don't
think
this

Re: dns administration delegation

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

Re: dns administration delegation

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

Re: dns administration delegation

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
same
security
read/write
access
for
the
siteA_dns

Re: dns administration delegation

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

Re: dns administration delegation

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

Re: dns administration delegation

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

Re: dns administration delegation

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?

Presumably

Re: dns administration delegation

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)

Re: dns administration delegation