

Re: ad and dns setup

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-08/msg01050

- *From:* PDIDY <PDIDY@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 22 Aug 2007 14:04:03 -0700
-

Jorge,

Many Thanks for the info provided. I am almost done with this conversion and looks pretty good. However I have some observations I want to share to see if there are any issues, I perform netdiag /fix after registering dns and stop/restarting netlogon on the root dc's and no problem, but on the child domain It gave me 2 errors, no dns servers have dns records for this dc registered and trust relationship test came back as failed secure channel to the domain "xxxx" is broken. error no logon servers.. any clues???

"Jorge Silva" wrote:

Ok.

To fully rebuild DNS:

- For each domain all DCs should point to the same DC/DNS then you can perform the changes only in one DC and replicate the changes to the other DC.
- Each time you delete/create something in DNS you should replicate the changes immediately to all servers, this helps to speedup the process.
- Note that in the end EACH child domain should be able to solve each existing DNS domain, the same applies to the root domain. You can use conditional forwarding, forwarding, secondary zones, etc... choose what best suits for your scenario
- In the root domain you need extra cautions because you have the _msdcs zone that is used by servers and clients for many different things including replication. Make sure that the _msdcs zone exists and the scope is set to forest wide (don't need to be this way but in my opinion you should have it like that, of course this depends of your existing scenario).
- The root domain should have have delegations created for each child domain and for the _msdcs zone (this is not automatically created you must do it manually after deletion).

Basic steps:

Check Sites configuration make sure it's correct.

In the root domain (DC01):

Re: ad and dns setup

- Point each DC to Dc01, clear cache in both DCs, delete everything inside _msdcs, forward zone, reverse lookup zone.
- Replicate changes.
- Create the delegation for each child domain and _msdcs zone.
- Delete the files netlogon.dnb and netlogon.dns from %systemroot%\system32\config.
- Run From cmd ipconfig /registerdns (on both DCs)
- Restart the netlogon service and confirm the creation of the netlogon.dnb and netlogon.dns Files in System32.
- Run from cmd
- netdiag /fix (on both DCs)
- Replicate changes.

In the Child domain(s):
same thing except for _msdcs zone and zone delegation(s) (assuming that you don't have child domains for these child domains).

--

I hope that the information above helps you.
Have a Nice day.

Jorge Silva
MCSE, MVP Directory Services
"PDIDY" <PDIDY@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:565E325A-92C0-4A05-BBF7-DC1B5C15D9ED@xxxxxxxxxxxxxxxxxxxx

Parent Child config.

2 Dcs per domain for a total of 6 Dcs

"Jorge Silva" wrote:

Is this a parent child configuration or 2 tree root domains?
How many DCs for each domain?

--

I hope that the information above helps you.
Have a Nice day.

Jorge Silva
MCSE, MVP Directory Services
"PDIDY" <PDIDY@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote
in message
news:96DA105E-2A5B-49D7-907B-DADB70ABDDAE@xxxxxxxxxxxxxxxxxxxx

Re: ad and dns setup

before i start this just a couple of things:
I have 6 dcs and all have dns, so I do this on
each server or only 1 in
each
domain, since it is ad intergrated, and once i
create the sites in ad
sites
and services should i delete the old ones as it
might conflict with the
new
ones..and one more thing if i need to do this
on all the servers it it
better
to change the config on all servers first and
then reboot 1 at a time
or
do
the root first followed by the children

"Jorge Silva" wrote:

- Make sure that DNS service is installed.
- Make sure that the DC1 points to itself on Preferred DNS NIC properties.
- Make Sure that you've DNS Zone for your domain and the _msdcs zone created, and these zones should be ADI (Active Directory Integrated), and allow Secure updates (better from security prespective).
- Make sure that AD Sites and Services have the correct subnet(s) assigned.
- Mark Server as GCs in Active Directory Sites and Services.

- Delete everything INSIDE the _msdcs zone and forward lookupZone for your domain.
- Delete the files

Re: ad and dns setup

netlogon.dnb and
netlogon.dns from
%systemroot%\system32\config.

- Run From cmd
ipconfig /registerdns
- Restart the netlogon
service and confirm the
creation of the
netlogon.dnb
and netlogon.dns Files in
System32.
- Run from cmd
netdiag /fix
- Confirm the creation of
the records on DNS server.
- You can do a reboot check
evrything Ok (1 at the time).

-Run dcdiag and netdiag.

--

I hope that the information
above helps you.
Have a Nice day.

Jorge Silva
MCSE, MVP Directory
Services
"PDIDY"

<PDIDY@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in message

news:5F241E62-7A3C-4FBC-A7B9-93460F5BEF8A@xxxxxxxxxxxxxxxxxxxx

Jorge,

Sorry for
the little
information.
I took an
exsiting
functioning
AD
strcuture
from
VMware
and copied
it over. So
there was
no need to

Re: ad and dns setup

seize
any
of the
roles,even
though
server 1 in
a.com has
all the roles.
All I want
to do is
change
networks
and bring
the test env.
back up
with
new
IP
address..The
only things
killing me
is DNS..:(

Thanks,

Paul

"Jorge
Silva"
wrote:

Hi
(assuming
that
your
test
server
is
NOT
going
to
be
connected
again
to
the
production
environment)
Can
you

Re: ad and dns setup

explain
how
did
you
removed
the
setup
from
a
different
network?
Did
you
removed
references
to
existing
DCs
in
the
Real
environment?
Did
you
Seize
the
roles?
Did
you
run
dcdiag
and
netdiag
after
that?

--

I
hope
that
the
information
above
helps
you.
Have
a
Nice
day.

Re: ad and dns setup

Jorge
Silva
MCSE,
MVP
Directory
Services
"PDIDY"
<PDIDY@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote
in
message
news:13E0327D-A09A-4EEA-8530-07B9472417D4@xxx

okay
here
is
my
setup.....

I
have
a
test
env.
with
forest
a.com
and
2
domains
within,
b.a.com
and
c.a.com.(all
win2003)

I
have
pulled
this
setup
from
a
different
network
and
want
to
configure
it
on

Re: ad and dns setup

a
different
network.

I
have
three
ad
sites
and
all
the
ou's
and
gpo's
are
setup.

I
am
not
worried
about
names
conflicting

as
this
will
be
on
an
isolated
network
but
would
like
to
keep
all
the
ad
stuff
intact.

I
tried
to
change
the
ip
setup
on
all
these

Re: ad and dns setup

servers
and
restarted
dns
and
the
netlogon
service.
i
did
a
dnsflush
and
dns
register
and
i
am
still
not
able
to
have
dns
work
correctly.
all
the
dcs(6
in
all,
are
dns
servers
and
there
are
2
servers
per
site)...i
am
getting
alot
of
kdc
errors
and
frs
errors
as

Re: ad and dns setup

well
as
nslookup
doesn't
come
back
with
the
right
server.
my
question
besides
what
am
i
missing
is,
do
i
need
to
change
the
ns
in
dns
on
all
machines,
and
should
i
get
rid
of
all
old
ips
in
dns
and
replace
with
new
ones...also
i
created
new
ad
sites

Re: ad and dns setup

with
the
new
ip
addresses
and
assigned
servers
to
those
sites
and
deleted
the
old
ones..
i
rebooted
one
of
the
a.com
servers
and
now
i
can't
even
log
in...i
guess
my
question
is
when
changing
over
to
a
new
network
with
an
existing
ad
and
dns,
how
can
i
achive

Re: ad and dns setup

Re: ad and dns setup

no
pain
in
doing
this?