

# Re: Active Directory Restructure Question

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2008-10/msg00521](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2008-10/msg00521)

---

- *From:* "Paul Bergson [MVP-DS]" <[pbergson@xxxxxxxxxxxxxxxxxxxxx](mailto:pbergson@xxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Thu, 9 Oct 2008 08:23:05 -0500
- 

I would try and hold off on 2008 if you can, but if dollars are tight then go ahead. Problem with 2008 is third party vendor support is behind. So validate that your AV, patch management and backup support are compatible.

--  
Paul Bergson  
MVP – Directory Services  
MCTS, MCT, MCSE, MCSA, Security+, BS CSci  
2008, 2003, 2000 (Early Achiever), NT4

<http://www.pbbergs.com>

Please no e-mails, any questions should be posted in the NewsGroup  
This posting is provided "AS IS" with no warranties, and confers no rights.

"divins" <[divins@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:divins@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message  
[news:35116F18-777D-42A6-941F-44D3F2D567F6@xxxxxxxxxxxxxxxxxxxxx](mailto:news:35116F18-777D-42A6-941F-44D3F2D567F6@xxxxxxxxxxxxxxxxxxxxx)

One more thing. All of the servers are Windows 2003 SP2. Would there be any benefit to upgrading to Windows 2008, or having a mixed environment 2003/2008, and how difficult would it be to introduce 2008 into this? I assuming that maybe we would want to have 2008 in the beginning if possible.

"Paul Bergson [MVP-DS]" wrote:

Sure you can do that, that is pretty normal if I follow you correctly. I would work to limit the number of domains unless there is a specific business rule that requires separate domains.

Info on migrating below:

If you are building a new forest you can use the Active Directory Migration Toolkit, that is free from Microsoft. This requires you to build a trust

## Re: Active Directory Restructure Question

between the source and destination forest.

### ADMT

<http://support.microsoft.com/default.aspx?scid=kb:en-us:326480>

### Download

<http://www.microsoft.com/downloads/details.aspx?FamilyId=6F86937B-533A-466D-A8E8-AFF85>

### Webcast

<http://support.microsoft.com/?kbid=325393>

### Trusts

To start would have to establish dns connectivity both ways, usually the easiest thing to do would be to create secondary's of each others primary.

[http://expertanswercenter.techtarget.com/eac/knowledgebaseAnswer/0,295199,sid63\\_gci1104911,00,h](http://expertanswercenter.techtarget.com/eac/knowledgebaseAnswer/0,295199,sid63_gci1104911,00,h)

Once established you can then go and create your external trust, I wouldn't create a forest trust this established a two trust.

### Creating an External Trust

<http://technet2.microsoft.com/WindowsServer/en/library/b30ef067-746e-4453-b879-804259aafdd3>

You would then look at running exmerge if you are looking at moving mailboxes across

### Download ExMerge

<http://www.microsoft.com/downloads/details.aspx?FamilyID=429163ec-dcdf-47dc-96da-1c12d673>

### ExMerge Details

<http://support.microsoft.com/kb/174197>

--

Paul Bergson

MVP – Directory Services

MCTS, MCT, MCSE, MCSA, Security+, BS CSci

2008, 2003, 2000 (Early Achiever), NT4

<http://www.pbbergs.com>

Please no e-mails, any questions should be posted in the NewsGroup  
This posting is provided "AS IS" with no warranties, and confers no rights.

"divins" <divins@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
<news:E5A1FC1C-3A5C-466B-A730-C36BAF021D00@xxxxxxxxxxxxxxxxxxxx>

Re: Active Directory Restructure Question

OK. So If I want to create a new domain called test.com, and then create the other sub-domains, and then migrate us.test.com to a new sub-domain called na.test.com. Is that ok? If we should limit the amount of sub-domains, then what is the best path for me to take?

"Paul Bergson [MVP-DS]" wrote:

The standard for AD is now to try and have as few domain within a forest as needed. The empty root structure is know discouraged since security boundaries are now considered at the forest level. You can't have two domains within the same dns root, since the dc's would get confused (DNS service records over written, etc...) so no you can't migrate to the same name structure unless you have separate dns servers that don't know about one another.

--  
Paul Bergson  
MVP – Directory Services  
MCTS, MCT, MCSE, MCSA, Security+, BS  
CSci  
2008, 2003, 2000 (Early Achiever), NT4

<http://www.pbbergs.com>

Please no e-mails, any questions should be posted in the NewsGroup  
This posting is provided "AS IS" with no warranties, and confers no rights.

"divins"  
<divins@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Re: Active Directory Restructure Question

wrote in message

[news:730736A6-674B-4AEB-AD6E-87603888F443@xxxxxxxxxxxxxxxxxxxxx](mailto:news:730736A6-674B-4AEB-AD6E-87603888F443@xxxxxxxxxxxxxxxxxxxxx)

Mel-

We currently don't have a top level domain test.com. We just have us.test.com. We want to create test.com and then all of the additional domains, and then migrate us.test.com underneath test.com. Will this be a problem?

Dave

"Mel K" wrote:

You have a top level AD/DNS domain named test.com and a sub AD/DNS domain named us.test.com. That seems fine. And you want to create sub AD/DNS domains for your UNIX/LINUX servers, which also sounds fine. Just note that for every AD domain,

## Re: Active Directory Restructure Question

you'll need  
at least two  
domain  
controllers  
for  
redundancy.  
If you want  
all member  
servers to  
be  
UNIX/LINUX  
servers  
that's  
fine, as long  
as they have  
the  
appropriate  
software  
that allows  
them  
to  
be  
AD domain  
members.

IIRC, after  
you set up  
all these  
domains,  
there will be  
automatic  
transitive  
trust  
relationships  
between  
domains in  
the forest so  
that users in  
one  
domain can  
use  
resources in  
another  
domain  
without  
having to  
reauthenticate  
(assuming  
that the user  
has the  
appropriate

Re: Active Directory Restructure Question

permissions  
to the  
resource).

IMO, you're  
on the right  
track. The  
only issue is  
that having  
all  
these  
domains  
requires a  
lot of  
domain  
controllers  
and adds to  
the  
complexity  
of  
managing  
AD. If you  
understand  
that want to  
keep the  
separation  
of  
domains,  
then I don't  
see any  
other  
alternatives.

--

Regards,  
Mel K,  
MCSA: M

"divins"

<divins@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in  
message

[news:F32E2F22-CE4F-4CCD-BC53-A1CB99D00222@xxxxxxxxxx](mailto:news:F32E2F22-CE4F-4CCD-BC53-A1CB99D00222@xxxxxxxxxx)

My  
company  
is  
planning  
to  
do  
a

## Re: Active Directory Restructure Question

restructure  
of  
our  
Active  
Directory  
Domain.  
Currently,  
we  
have  
one  
domain,  
let's  
call  
it  
us.test.com.  
We  
also  
have  
multiple  
non-AD  
DNS  
Domains  
that  
we  
have  
non-member  
Windows  
Servers.  
These  
DNS  
domains  
are  
prod.test.com,  
dev.test.com,  
qa.test.com,  
staging.test.com,  
etc.  
These  
are  
seperated  
by  
different  
subnets,  
and  
seperate  
firewalls  
so  
that  
traffic  
does  
not

## Re: Active Directory Restructure Question

flow  
between  
them.  
Traffic  
is  
independent  
among  
them.  
We  
would  
like  
to  
create  
a  
new  
domain,  
let's  
call  
it  
test.com  
and  
then  
create  
sub-domains  
underneath.  
We  
would  
recreate  
the  
us.test.com,  
and  
then  
create  
prod.test.com,  
dev.test.com,  
etc.  
as  
AD  
domains.  
We  
will  
have  
administration  
at  
the  
top-level.  
We  
are  
looking  
to  
do

Re: Active Directory Restructure Question

this  
for  
better  
administration  
and  
also  
due  
to  
the  
fact  
of  
us  
have  
UNIX  
and  
LINUX  
servers  
in  
the  
environment  
to  
be  
able  
to  
use  
tools  
that  
allow  
the  
AD  
domain  
account  
to  
be  
able  
to  
login  
to  
the  
UNIX  
and  
LINUX  
servers.  
Is  
this  
the  
right  
way  
to  
do  
this,

Re: Active Directory Restructure Question

or  
is  
there  
a  
better  
way?  
Let  
me  
know  
if  
you  
have  
any  
additional  
questions.

Dave