

RE: New Forest – Old Domain – Plus DMZ – Help Please

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.migration/2006-05/msg00282.html>

- *From:* v-xuwen@xxxxxxxxxxxxxxxxxxxxxx (Vincent Xu [MSFT])
 - *Date:* Mon, 29 May 2006 03:29:55 GMT
-

Hi,

1. it depends upon what DNS address is configured in the clients.

However,

1) I'm not sure if it can coexist when the linux has the same name with AD domain name.

2) Make sure Windows XP client should use the AD DNS

2. It is for manager reason that create a new child domain. Since you only have 50 users, I don't think it is required.

3. No, so far there are no known issues in such scenario.

4. The Cert should match the name in Internet. In another word, www.acme.net. I think there should not be any problem.

5. Yes, it is supposed to be no problem.

Best regards,

Vincent Xu
Microsoft Online Partner Support

=====
Get Secure! – www.microsoft.com/security
=====

When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from this issue.

=====
This posting is provided "AS IS" with no warranties, and confers no rights.
=====

RE: New Forest – Old Domain – Plus DMZ – Help Please

From: "phatgeezer" <LDunham@xxxxxxxx>
Newsgroups: microsoft.public.windows.server.migration
Subject: New Forest – Old Domain – Plus DMZ – Help Please
Date: 27 May 2006 08:42:56 -0700
Organization: <http://groups.google.com>
Lines: 112
Message-ID:
<1148744576.105606.263400@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
NNTP-Posting-Host: 12.202.81.168
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
X-Trace: posting.google.com 1148744581 4825 127.0.0.1 (27 May 2006

15:43:01 GMT)

X-Complaints-To: groups-abuse@xxxxxxxx
NNTP-Posting-Date: Sat, 27 May 2006 15:43:01 +0000 (UTC)
User-Agent: G2/0.2
X-HTTP-UserAgent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
SV1;

..NET CLR 1.1.4322),gzip(gfe),gzip(gfe)

Complaints-To: groups-abuse@xxxxxxxx
Injection-Info: i39g2000cwa.googlegroups.com;
posting-host=12.202.81.168;
posting-account=OAMDXg0AAACTQiDCKuCXhZFtIPe6KxgD
Path:

TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTFEEDS01.phx.gbl!newsfeed.c
w.net!cw.net!news-FFM2.ecrc.de!news.glorb.com!postnews.google.com!i39g2000cw
a.googlegroups.com!not-for-mail

Xref: TK2MSFTNGXA01.phx.gbl

microsoft.public.windows.server.migration:23870

X-Tomcat-NG: microsoft.public.windows.server.migration

My situation is somewhat complex, so I apologize for the length of this, but I will be as succinct as possible.

I am the network admin for a company of about 50 users. I have been charged with moving us off our older Linux mail server to an Exchange 2003 server; that of course requires Active Directory, which we have never used here. Although I am new to AD, I have worked on the project full time for the last few weeks—I have learned a lot and feel as though I have fair grasp of the major concepts.

Environment: We do extensive data processing for our outside clients, and have about 50 servers total in addition to about 50 desktops. The

RE: New Forest – Old Domain – Plus DMZ – Help Please

vast majority of our inside production equipment is 2003 servers and XP desktops, but we do have one application that runs on several NT4 servers with some NT4 data entry workstations associated with that process. All internal production equipment (and about half of our users) are members of an NT4 domain. We also have a number of workgroups containing both servers and workstations, that I would like to bring under the AD umbrella. We also have a number of servers in the DMZ including public web servers, none of which belong to any domain currently, except for one Win2003 Small Business Server (which is its own single-box domain) whose only function now is running backups of the DMZ. No inbound connections are permitted from the DMZ to our internal LAN. All data is pulled into the inside LAN by internal servers.

One big challenge—the NT4 domain was created years ago when much less attention was paid to security, and the domain admin password is fairly easily guessed. I want to tighten security while I am implementing the AD/Exchange project, however I cannot change the domain admin password because of its being hard-coded in some of our legacy production applications....and of course the ancient code, which dates from the days when our company was basically a one man operation, is undocumented, so no one knows exactly how to change the code to allow me to reset the password, but I am assured by the development staff that the insecure reference is used numerous times throughout the old code. And the older operation is now a small enough portion of our business that there is a reluctance to devoting developer resources to rewriting the apps, and now we have SLA's that call for big penalties should processes break, as in losing communication if we move the newer processes to a new domain -- no pressure though 8–)

If that were not enough of a design challenge, our internal DNS is static, and is hosted by an older Linux server, manually maintained, although for redundancy we do zone transfers to secondary DNS hosted on 2 Win 2003 servers, one on our inside LAN and one in the DMZ..

My goals are to:

--bring all of our business process equipment into the Active Directory, including the DMZ

--tighten security so that a user who guesses the domain admin password for the existing domain cannot change their own access permissions (or worse)

--prepare the new AD structure to make Exchange implementation as seamless as possible

--zero or minimal downtime (my maintenance window is two hours)

This is what I am considering:

--create a new root domain in a pristine forest (let's call it

RE: New Forest – Old Domain – Plus DMZ – Help Please

acme.com)

--move the machines not currently in the NT4 domain into the new domain

--move all users into the new domain (I could be phatgeezer@xxxxxxx, which will minimize the users' confusion between their domain account and their email account, since it will be the same name)

--do an in-place upgrade of the existing NT4 domain (let's say it's called biz) and make it a child domain of the root-- biz.acme.com

--create a new domain for the DMZ machines, dmz.acme.com and use a secure method of AD replication like IPSec with machine certificates

Here (finally) are my questions:

1. Can I name our new root domain the same as our current internal namespace without causing DNS resolution problems during the installation? In other words if AD maintains the acme.com namespace and the acme.com namespace is also available statically from our existing Linux server, which DNS is authoritative? Or is it solely dependent upon what DNS address is configured in the clients?
2. Is there any value to creating a new child domain off the root to hold our user objects? Conversely is there any security risk to putting them in the root domain? (since it will be above the "biz" domain in the heirarchy as opposed to a sister domain)
3. Are there any installation, and later, authentication problems associated with making an in-place-upgraded NT domain a child of a pristine root, rather than making it the first domain in a new forest?
4. If our current web servers' certificates are issued to the acme.net domain, and I add the machines to our acme.com domain, will web users get the "certificate name doesn't match site" error on connecting? I think I know the answer to this but want to be sure -- we do not publish our internal DNS on the internet, instead we have our ISP publish a separate DNS list using our public address pool and then we NAT requests at the firewall to the proper internal address -- therefore having the machine known on the internet as www.acme.net (with a cert installed issued to www.acme.net) and known internally as www.dmz.acme.com in our AD namespace should not be a problem -- correct?

Whew -- that's a lot of stuff, and I'm sure I'll need to know more as the project goes along, but it's taken me two weeks of full time study and analyzing our operations in light of the new knowledge, just to know some of the questions I need to ask. Thanks everyone!

RE: New Forest – Old Domain – Plus DMZ – Help Please