

Re: AD domain structure – a bit concerned now!

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-03/msg00508

- *From:* "Matthew M \(\UK\) " <mattee76@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 8 Mar 2007 13:24:00 -0000
-

BTW, of course i cannot find that video !!

"Herb Martin" <news@xxxxxxxxxxxxxxxx> wrote in message
news:ule2pCYYHHA.1008@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

"Matthew M (UK)" <mattee76@xxxxxxxxxxxxxxxxxxxx> wrote in message
news:032040C1-4BB1-44B4-BB5D-228894437EE0@xxxxxxxxxxxxxxxxxxxx

Hi,

Im really just looking at getting an idea of what other people may have done when in our situation? Your ideas would be appreciated.

We currently have the following new windows 2003 domain structure (root with sub domains for each country), we also have another forest where the bulk of our UK users (1500 users) exist, the new forest has about 250 users (expanding quickly). We will be moving all the resources from the current forest to a subdomain in the new forest this year sometime.

ALL the information below relates to the new forest.

New forest looks like:

domain.local (root domain)
eucountry1.domain.local (EU Country 1 – currently 0 users, going to 1500)
eucountry2.domain.local (EU Country 2 – currently 50 users, going to 150)
eucountry3.domain.local (EU Country 3 – not deployed yet, start with 20 users, going to 250)
apacountry1.domain.local (APAC country 1 – currently 200 users – staying static)
qa.domain.local (Domain for QA environment)

The original idea was to have a subdomain for each country, the original reasons for this being:

1. Isolate replication – most of these sites have pretty limited bandwidth

Re: AD domain structure – a bit concerned now!

Not usually a big issue for these kinds of numbers due to Sites and AD replication efficiency.

2. Localised administration of domains – i know that we could do this via OUs, but we have far reaching sites with local admins, who by their nature want domain admin access.

This is then a political problem which YOUR Org much decide — no one can tell the decision makers if this is sufficient reason or not, just advise them that it isn't a "real" reason but a politic desire on the part of some admins.

We have some level of trust between the admins, so are not overly concerned with any elevation of privaleges or them doing things outside of their own domain.

Argues against the number of domains.

3. Individual account policies – to be honest this was possibly the main reason for multiple domains, and was a prereq put down by our security department. Hmm, how things change, now this is not a major concern, and we can have similar accout policies across the board.

If we are talking about Kerberos, Lockout, and Password such difference are TECHNICAL reasons for splitting to multiple domains IF the reasons for the differences are good ones.

Such are set on a PER DOMAIN basis.

My concern now is that it may have been over designed, with hindsight, i would have preferred to have a single subdomain for each continent, then we could have OUs for countries, etc etc.

Possibly better — Microsofts own domain designer ran into international legal issues which argued for both a separte German (DE) and French domain and so he described* how this led to ultimately separating most EU countries into separate domains.

* There is a paper and a video presentation on the MS web site somewhere about Microsoft's own decision process in a similar situation. The original plan was one domain for all of Europe but ended up being many domains.

Re: AD domain structure – a bit concerned now!

The problem we have now is how do we move forward? I would like to rename our local new subdomain and then move the other EU domain resources into this.

Not sure what you are asking here — you must first make a final decision to use the planned design. If that is the case then begin building the infrastructure and develop a plan for (eventually) migrating users.

I really dislike the idea of user migrations when it can be avoided but it appears that you may (now) be in one of the cases where it is justified.

Just be aware that even though the ACTUAL Migration is relatively easy with ADMT v3, the cleanup process can be a real bear to fully plan and execute: Resources, SID migration or change access, and especially EXISTING PROFILES are real problems — not insurmountable but significant to require real planning and practice.

We have the following already placed into the new forest....

eucountry1.domain.local (EU Country 1 – currently 0 users, going to 1500)
– Localised admins (this would be our team)
– Exchange 2003 installed – being used for IIFP and InterOrg replication.

eucountry2.domain.local (EU Country 2 – currently 50 users, going to 150)
– No local admins, delegated access to desktop guys
– No exchange, they are using the other forest exchange resources.
– Users and computer accounts have been created migrated.

eucountry3.domain.local (EU Country 3 – not deployed yet, start with 20 users, going to 250)
– Localised admins, full local management of all resources
– As mentioned this has not been created, but i am in two minds wether we continue with the agreed upon design, or change the design midway.

apacountry1.domain.local (APAC country 1 – currently 200 users – expecting rapid growth)
– Localised admins
– Local exchange/file etc etc – full local management

qa.domain.local (Domain for QA environment)

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

Re: AD domain structure – a bit concerned now!