

Re: AD over the Internet

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2005-10/msg00300.html

- *From:* "Cary Shultz" <cwshultz@xxxxxxxx>
 - *Date:* Wed, 12 Oct 2005 23:48:29 -0400
-

Jess,

Hey, sorry for the late reply. My wife would not let me play! ;-)

Anyway, with 5-10 people in each of the 'remote' Sites you have many options available to you.

There are some people who will contend that wherever there are fewer than 10 people that 'Site' does not get a Domain Controller. Some will contend that five is the magic number. For others the number is higher (25 comes to mind). So, your two remote locations are available to be (and I am going to make up a word in the English language in a second) Domain Controller-less. That, naturally, implies that the users in those two 'Sites' will be authenticating over the WAN. Your WAN link speed and reliability come into play here. Terminal Services might come into play here. This is a very valid solution – based on what you have stated so far. However, that might not end up being the case. Set up the TS in the HQ and have at it!

You could also place a Domain Controller in each 'Site'. However, it might behoove you to make sure to create subnets for each of those two locations, then create the Sites and then associate the appropriate subnet to the proper Site. You do this in the Active Directory Sites and Services MMC (ADSS MMC). This helps to make sure that your clients are authenticating against the local DC. Well, you also need to have DNS and GCs properly configured. Simply make each of the DCs in both of the Sites a DNS Server as well as a GC and you should be fine. What type of growth do they expect? Will the number of employees in each remote office grow to something like 20 employees?

Keep the Exchange Server in the HQ. The users in the two remote locations will simply have to use that one. There should not be any problem with this so long as you are not sending e-mails with big attachments to everyone in the company. Those on the other side of the WAN link will experience some slow going when that sort of thing happens.

I would also suggest – based on what you have provided so far – that you keep one domain. If you are going with the DC in each Site solution then

Re: AD over the Internet

you would simply have one Domain with three Sites (HQ, RL01 and RL02). This is one of the neat things about WIN2000 and WIN2003. There are two types of replication: intrasite and intersite. Intrasite would be the replication that happens between the Domain Controllers that are in the same Site (as defined in the ADSS). Obviously, this requires multiple Domain Controllers. Since you would have only one DC in each of the remote locations you would not have intrasite replication there. Intersite replication is what happens between Domain Controllers in the different Sites. This, again, is determined by the way that you have configured things in the ADSS MMC. Our little buddy, the Knowledge Consistency Checker – or KCC for short – takes care of all of this for you (or you can manually do it all yourself or you can do some and then let the KCC finish up). It uses its buddy, the ISTG.

There is a schedule and an interval. The intersite interval is 180 minutes (three hours) by default. This can be a bit frustrating at times. What this means is that you could create a user account object on a DC in one of the remote locations and you would not see it on the other Domain Controllers in the other Sites for another three hours. So, you might have to play with it a bit. Just be aware that as you decrease the time increment you potentially increase the amount of replication going over your WAN links). But, with WIN2000 only the attribute(s) whose value(s) you have changed replicate so it is not all that bad (in WINNT 4.0 the entire user account would replicate).

As to controlling access: shared folders and ntfs permissions. I like to assign permissions to groups (not to individual user account objects). So, if you create a shared folder on the DC in RL01 and you want only those people to be able to do anything then create a security group for RL01 and use that. This way, only those that are a member of that security group can access it.

--

Cary W. Shultz
Roanoke, VA 24012

<http://www.activedirectory-win2000.com>

(soon to be updated!!!)

<http://www.grouppolicy-win2000.com>

(soon to be updated!!!)

"Jess" <jess@xxxxxxxxxxxx> wrote in message
<news:O5Gdnc3C1O7ZBtHeRVnyuQ@xxxxxxxxxxxx>

> Hi Cary

>

> Thanks for the reply.

> There is roughly 5 – 10 staff in two offices with 75 in the main.

> There will be DNS, DHCP and a Global Catalogue PDC in each.

> How best to share network resources in particular exchange email is my

Re: AD over the Internet

Re: AD over the Internet

> concern. The firewall is a FreeBSD running ipfw. Am considering whether
> to
> VPN through the firewall or to buy software for this.
>
> Should the new domain be in the same forest or best to create new ones. I
> would like to have password changes replicated between each site. I am
> not
> sure on the best AD relationship between each office. Both for security
> and
> access to resources.
>
> Jess
>
> "Cary Shultz" <cwshultz@xxxxxxxx> wrote in message
> news:OUsZ2mrzFHA.2064@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
>> Jess,
>>
>> One way to do this – if the option is still available to you – is to set
> up
>> Active Directory Sites for each location. You could then set up a
>> Firewall-to-Firewall VPN between each location.
>>
>> I would suggest that you have at least one domain controller in each
> site.
>> Well, actually two would be a really good idea....you have not mentioned
> how
>> many users are in each site. And at least one of the DCs in each site
>> should be a GC. I would probably make both of them a GC, but we might
> need
>> some more details.
>>
>> Each site should also have a DNS server. As well as a DHCP
> server....well,
>> that one is debatable.
>>
>> This is a very common situation.
>>
>> --
>> Cary W. Shultz
>> Roanoke, VA 24012
>>
>> <http://www.activedirectory-win2000.com>
>> (soon to be updated!!!)
>> <http://www.grouppolicy-win2000.com>
>> (soon to be updated!!!)
>>
>>
>>
>> "Jess" <jess@xxxxxxxxxxxx> wrote in message
>> news:n82dnW12gaTDrdHenZ2dnUVZ8qCdnZ2d@xxxxxxxxxxxx
>>>

Re: AD over the Internet

>>> Hi,
>>>
>>> We have just upgraded to Active Directory 2000 from NT4.
>>> I have created a new domain in a new forest and everything is fine.
>>>
>>> We have another 2 offices in other cities and I am reading up on the
> best
> way to link them.
>>>
>>> All offices are connected via broadband with static ip addresses.
>>>
>>> Can someone please advise me what is the best way to link these. We
> will
>>> want to access the Exchange Server in the main office from each.
>>>
>>> At the moment, two offices are using OWA access only. There are
>>> network
>>> shares in each office all needing access to.
>>>
>>> I want an active directory domain controller in each office. Is it
> best
>>> to
>>> have only one as a global catalog server or each??
>>>
>>> I dont think child domains should be on other office networks, so is a
> new
>>> domain in an existing forest an option in Win 2000 AD?
>>>
>>> I was thinking of linking secondary DNS in each office first of all,
>>> setting
>>> up a VPN link and routing rules for both networks through this.
>>>
>>> Another option I was considering but unsure if possible was to create a
>>> subnet site in AD with an internal network range and specify the
> external
>>> static ip as the gateway for this network. Would this work and is it
>>> wise??
>>>
>>> We have three offices. I would love to hear what methods others may
> have
>>> used to implement active directory over multiple office scenarios
>>> linked
>>> via
>>> the Internet.
>>>
>>> Thanks for any assistance.
>>>
>>> Jess
>>>
>>>
>>>

>>
>
>

.

• **References:**

- ◆ **AD over the Internet**
 - ◇ *From: Jess*
 - ◆ **Re: AD over the Internet**
 - ◇ *From: Cary Shultz*
-
- Prev by Date: **Re: Computer SID question**
 - Next by Date: **Re: adprep problems**
 - Previous by thread: **Re: AD over the Internet**
 - Next by thread: **Re: ADUC offline and user accounts disabled**
 - Index(es):
 - ◆ **Date**
 - ◆ **Thread**