

Re: Satellite Branch Office Woes

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-01/msg01139

- *From:* Slandrum <Slandrum@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 16 Jan 2007 08:41:00 -0800
-

Thanks for the replies all.

A bit more info:

The client machine has a hard-coded IP address that includes the DNS entry for the central site. All AD DNS entries are correct and available, and both the client subnet and the central subnet have reverse lookup zones configured in the (AD-Integrated) DNS. All DNS is internal, in all subnets, with forwarders configured on the central DNS servers. Likewise, all SRV records are correct and available, including GC and DC entries, etc.

I am uncertain what you mean by a single label domain name, unless you mean the use of only a single character for the name. If so, this is not the case in my environment. The domain name is xxxxxxxx.com; with eight characters, all text.

Putting a DC in the remote client subnet is a non-starter, as the whole point of a satellite branch office is to provide Directory and all other services from the central site, eliminating the need for costly server hardware in the remote site. According to Microsoft, this is a perfectly viable solution, and one that I would imagine is in use in literally thousands of businesses.

The section on the PPPoE is of immense help though, as it gives me something to have the WAN guy check out. I'll do a bit more research on this issue and will then let him know what I've found when we hook up in Omaha this week. (Different install ;-)

In the interim, I encourage additional replies from you folks, and would be especially interested in hearing from anyone currently using a satellite branch office setup in their production environments.

Regards,

"Ace Fekay [MVP]" wrote:

Re: Satellite Branch Office Woes

In [news:EA7C3AAC-E839-41CF-BFFB-9151B5A5C546@xxxxxxxxxxxxxx](mailto:EA7C3AAC-E839-41CF-BFFB-9151B5A5C546@xxxxxxxxxxxxxx), Slandrum <Slandrum@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> stated, which I commented on below:

We are currently testing a traditional satellite branch office solution (no servers in the SBO) for several small locations that will be coming online this year. I've been through several different sources now, including the WSSRA, but either I've missed something completely, or I am stuck with an (unacknowledged) WAN configuration issue. Hopefully you folks can help me decide which.

To elaborate, we have the traditional setup where we have a WAN guy who handles all the telecom stuff, and then we have a Windows server guy (me) who handles all the Windows/AD stuff, etc. Although we work well together, the WAN guy is pretty anti-MS, which means that anytime I suspect something amiss on his end, I have to really jump through the hoops to get him to double-check configuration settings on his side of the fence. Otherwise his answer is always "Must be a Microsoft issue". And he may be right, this time, or at least a "Windows Admin issue". :-)

At any rate, he has setup a DSL connected VPN IPSEC tunnel that is entirely hardware based. At one end of the tunnel he has a Cisco router, and at the other end a Cisco VPN Concentrator. I'm not sure of the actual model numbers, but for the sake of this discussion it shouldn't really matter. There are a few other hardware devices in between, a VLAN, etc, but still pretty standard from what I've reviewed thus far. He is handling the IPSEC via an internal Cisco certificate solution, so right now I view this connection as being a straight through, clean pipe, just like it was one of our WAN circuits.

It passes pings just fine, and I have done some portqry testing to verify that LDAP, Kerberos, NTLM, SMB and various other TCP/UDP traffic types go through okay, so right now I don't think it's a port blocking issue. I tested in both directions, so all should be fine, but the behavior I am seeing makes me wonder if there is a port filtering issue, or a bounce issue, etc.

Since as I said I view the connection as operating just like one of our WAN links, the only AD side change I made was to create a subnet to match the SBO site and assigned it to the Central AD Site. Based on experience and subsequent re-checking, I see no other required AD changes at this time. However, I could be wrong in this.

We have a client PC in the SBO running WinXPsp2. At first "the WAN guy" was providing DHCP from the Cisco router endpoint on the SBO side, but just to make it cleaner I have since given the PC a manual IP address, with two DNS entries, a WINS entry and so on. I will eventually provide DHCP from the Central Site as well, but not until I can get past the current issue.

Re: Satellite Branch Office Woes

Also, due to SPNEGO errors in the Event Log of the client PC that match KB article numbers 891559 and 885887, I have applied the kereberos.dll sp2 hotfix as described in KB 885887 in an attempt to correct the below described problems. It didn't help any.

The PC itself does have a workstation account in the domain, and I have placed this account in its own OU and have checked on "Block Policy Inheritance" to ensure that it's not receiving any of our GPOs. And its Host entry does appear in the AD-integrated DNS Zone for the Domain. I have also configured a reverse lookup zone for the SBO subnet.

The primary problem that I am seeing is that the PC will not log into the domain. It accepts the domain user name and password, albeit rather slowly, then goes to the "Loading Your Personal settings" screen and stays there . forever. This occurs whether I am attaching via Remote Desktop, or if he is actually logging in at the console. We have left it at this stage for as much as 24 hours at one point, and it never completes the login.

I can attach to the PC with Remote Desktop (through the VPN IPSEC Tunnel) but I receive the standard "user domain/username is currently logged in ." message that requires me to do a forced Remote Logoff. This often will take several tries, but eventually the incomplete domain login session will end.

Once it does I can attach to the PC with Remote Desktop by logging onto the local machine Administrator account. I can then attach to domain resources on our file servers by providing a domain/username and password when prompted to do so. However, these operations are also very slow; much slower than the ping times would lead me to expect.

I'm sorry this is sooo long, but I've tried to paint as complete a picture as possible to eliminate the "did you check this and this" stuff, but will watch for and happily answer any additional configuration or environment questions you may have.

What do you think I've missed, or barring that, what should I have "the WAN guy" check?

To add to Danny's response, all machines must only use the internal DNS, and that means you cannot use the ISP's DNS in any AD machine otherwise it will be asking the ISP's DNS, "Where is a domain controller in my domain so I can logon?" Using anything other than the DNS servers that hold the AD DNS zone, *will* cause numerous issues. Internet resolution will still work by the use of the Roots, but you can make it more efficient, if you like, by configuring a forwarder to your ISP.

Re: Satellite Branch Office Woes

However, there are also other factors that can cause issues, such as the domain name. Is it a single label name? I hope not. Also, do the SRV records exist under the zone? Is there a GC record (under the `_gc._msdc` folder)? Can you ping the DC's FQDN from the remote workstation?

You only provided a 'scenario' and no specific configuration information. Since you didn't provide any configuration information (`ipconfig /all` would have been helpful from the branch workstation and from the main office domain controller for starters), it will be difficult to pinpoint the cause of your issues.

I would go along with Danny's suggestion to immediately put a DC in the branch office. The speed of the link is also helpful. Below 128k will be problematic. Also, ADSL PPPoE is notorious for messing with the MTU (1492 vs the required 1500), which the LDAP requires a minimum PDU size of 300kb, otherwise with an MTU of 1492, I believe the PDU drops down to 64kb. LDAP tests don't confirm this either but are evident when domain communication issues arise and an ADSL link is in use.

SPNEGO errors can be eliminated by creating a reverse zone for your subnet(s) and making sure all domain controllers have a PTR created in the zone.

--

Ace
Innovative IT Concepts, Inc (IITCI)
Willow Grove, PA

This posting is provided "AS-IS" with no warranties or guarantees and confers no rights.

Ace Fekay, MCSE 2003 & 2000, MCSA 2003 & 2000, MCSE+I, MCT, MVP
Microsoft MVP – Directory Services
Microsoft Certified Trainer

Having difficulty reading or finding responses to your post?
Instead of the website you're using, I suggest to use OEx (Outlook Express or any other newsreader), and configure a news account, pointing to news.microsoft.com. This is a direct link to the Microsoft Public Newsgroups. It is FREE and requires NO ISP's Usenet account. OEx allows you to easily find, track threads, cross-post, sort by date, poster's name, watched threads or subject.

It's easy:

How to Configure OEx for Internet News
<http://support.microsoft.com/?id=171164>

Infinite Diversities in Infinite Combinations
Assimilation Imminent. Resistance is Futile
"Very funny Scotty. Now, beam down my clothes."

Re: Satellite Branch Office Woes

The only constant in life is change...