

# Re: AD Login

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-09/msg01280](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-09/msg01280)

---

- *From:* "Herb Martin" <[news@xxxxxxxxxxxxxxx](mailto:news@xxxxxxxxxxxxxxx)>
  - *Date:* Tue, 19 Sep 2006 17:39:02 -0500
- 

<[open24hrs@xxxxxxxxxx](mailto:open24hrs@xxxxxxxxxx)> wrote in message  
[news:1158704168.040346.130750@xx](mailto:news:1158704168.040346.130750@xx)

We are using a web based application (plumtree software) hosted in the root domain that the users from our domain, (including our users physically in the root domain), logon to with their own AD credentials.

You may have to ask "plumtree" for application specific issues but we can certainly help you with AD Authentication and how all compatible applications SHOULD work.

When the vpn site to site goes down between our sites though, none of the users can logon to the web based program using their AD credentials, but when the site to site vpn is up theres no problem.

You have left it very unclear whether this is a separate domain or not. You mentioned a "root domain" as if there were a distinction but then never mentioned any other domains so we don't know if you have one or multiple domains.

Sites are totally unrelated to the domains within a Forest. Sites are best thought of as a Forest wide configuration (i.e., for all domains in that forest.)

Our dc in the root site is using the dns ip's of the root dc's and all servers are windows 2003 latest sp's an dupdates etc...

Do you have any DCs in the remote Sites? From which domains?

I can also access the website straight thru the internet hosted in at the root of the forest by logging in with my AD credentials to the

## Re: AD Login

platform no problem. If I disconnect the vpn site to site connection at work from our domain to the root domain I get an error logging in.

If this is a single domain it is almost certainly related to either DNS issues OR to firewall/routing issues.

If this is a cross domain access then maybe your DCs cannot route or perhaps the DNS servers for one domain cannot find the "other" domain(s).

How is it possible that I can log in right thru the internet but not when the vpn is down???

We don't know which DOMAIN you are logging onto, where it's DCs are located, nor what sort of firewall filters might be on those VPNS.

I think what may be a problem is that as I login with my AD credentials it tries to authenticate me across the vpn

If there is no local DC or if your Sites are misconfigured despite a local DC, or if your DNS is hosed up/misconfigured.

to in our domain then travels back thru the vpn to the root for authentication – this is defeating the whole purpose of why we physically put a DC in the root domain site connected to our domain.

The above sentence is unclear.

Which domain has the accounts? Which domain has the resources?

Which Sites have which DCs (from which domains)?

How can we make sure that users will be authenticated by the DC in the root domain not in our local domain?

They will ONLY be authenticated in the DOMAIN which holds their account.

They will be authenticated a DC (of their domain) in the LOCAL SITE if your sites are setup correctly and DNS is configured correctly.

Re: AD Login

Re: AD Login

Thanks so much in advance for your help!

Below are general recommendations on DNS for AD:

- 1) Dynamic for the zone supporting AD
- 2) All internal DNS clients NIC\IP properties must specify SOLELY that internal, dynamic DNS server (set.)
- 3) DCs and even DNS servers are DNS clients too -- see #2
- 4) If you have more than one Domain, every DNS server must be able to resolve ALL domains (either directly or indirectly)

netdiag /fix

....or maybe:

dcdiag /fix

(Win2003 can do this from Support tools):

nltest /dsregdns /server:DC-ServerNameGoesHere

<http://support.microsoft.com/kb/q260371/>

Ensure that DNS zones/domains are fully replicated to all DNS servers for that (internal) zone/domain.

Also useful may be running DCdiag on each DC, sending the output to a text file, and searching for FAIL, ERROR, WARN.

Single Label domain zone names are a problem Google:

[ "SINGLE LABEL" domain names DNS 2000 | 2003 microsoft: ]

--

Herb Martin, MCSE, MVP

Accelerated MCSE

<http://www.LearnQuick.Com>

[phone number on web site]

.

Re: AD Login