

## Re: Kerberos Issue

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-04/0106.html>

---

**From:** Steven L Umbach (*n9rou\_at\_nospam-comcast.net*)

**Date:** 04/07/05

Date: Thu, 7 Apr 2005 12:25:48 -0500

First make sure that this domain controller is in synch with the other domain controllers for time. Be sure to check day/date/month/AM&PM/year/time zone. Verify that it can ping the other domain controllers by at least their IP address and the others can ping it. Then verify that it is correctly configured for dns in that it points to the domain pdc fsmo and then itself as preferred dns servers and make sure that there are no ISP dns servers in the list. Temporarily configure your domain zone to accept dynamic updates but NOT secure updates if you have that configured. Use nslookup on your problem dc to make sure it can find the dns servers you have configured for it. If you get an error about it can not find the name of the dns servers that just means that you do not have a reverse lookup zone configured but it still should be able to find the dns servers and resolve names through them. Use nslookup and enter your domain name as in mydomain.com and you should get back IP addresses of your domain controllers [at least some of them] if your dns is working correctly and use it to verify it can find \_srv records for your domain as shown below. If that works then on the problem dns server, after you make any dns configuration changes, run the command netdiag /fix and then restart the netlogon service. After a few minutes run netdiag again to see if your dns errors have gone away. It may help to reboot the computer. You must get dns sorted out first. The links below may help. --- Steve

<http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B291382> ---- AD dns FAQ.

<http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B219289>

<http://support.microsoft.com/?kbid=260371>

<http://support.microsoft.com/?kbid=241515>

### Using Nslookup

1. From your DNS server, type nslookup at a command prompt.
2. Type set type=all, and then press ENTER.
3. Type \_ldap.\_tcp.dc.\_msdcs.domainname (where domainname is the name of your domain), and then press ENTER.

Nslookup returns one or more SRV service location records in the following format

hostname.domainname internet address = ipaddress

"Ralish" <Ralish@discussions.microsoft.com> wrote in message  
news:08F28FAA-BAEB-4EB6-A617-2DCFB4917F78@microsoft.com...

> Thank-you for all correspondence. It is greatly appreciated.  
> I have completed a netdiag and dcdiag as suggested and here is the output:  
>  
> NetDiag:  
> Computer Name: LFN-SVR-1  
> DNS Host Name: lfn-svr-1.LFN.net  
> System info : Windows 2000 Server (Build 3790) --- Surprised this  
> hasn't  
> been  
>  
> noticed and fixed ;)...  
> Processor : x86 Family 6 Model 8 Stepping 6, GenuineIntel  
> List of installed hotfixes :  
> Q147222  
> Netcard queries test . . . . . : Passed  
> Per interface results:  
> Adapter : LFN Network Connection  
> Netcard queries test . . . : Passed  
> Host Name. . . . . : lfn-svr-1  
> IP Address . . . . . : 192.168.0.2  
> Subnet Mask. . . . . : 255.255.255.0  
> Default Gateway. . . . . : 192.168.0.1  
> Primary WINS Server. . . . : 192.168.0.2  
> Dns Servers. . . . . : 192.168.0.2  
> 127.0.0.1  
> AutoConfiguration results. . . . . : Passed  
> Default gateway test . . . : Passed  
> NetBT name test. . . . . : Passed  
> No remote names have been found.  
> WINS service test. . . . . : Passed  
> Global results:  
> Domain membership test . . . . . : Passed  
> NetBT transports test. . . . . : Passed  
> List of NetBt transports currently configured:  
> NetBT\_Tcpip\_{889147D6-99FA-410E-A4F8-E95AD376DBCf}  
> 1 NetBt transport currently configured.  
> Autonet address test . . . . . : Passed  
> IP loopback ping test. . . . . : Passed  
> Default gateway test . . . . . : Passed  
> NetBT name test. . . . . : Passed  
> Winsock test . . . . . : Passed  
> DNS test . . . . . : Failed  
> [WARNING] Cannot find a primary authoritative DNS server for the  
> name  
> 'lfn-svr-1.LFN.net.'. [WSAEADDRNOTAVAIL ]  
> The name 'lfn-svr-1.LFN.net.' may not be registered in DNS.  
> [WARNING] Cannot find a primary authoritative DNS server for the  
> name  
> 'lfn-svr-1.LFN.net.'. [WSAEADDRNOTAVAIL ]

> The name 'lfn-svr-1.LFN.net.' may not be registered in DNS.  
> [WARNING] Cannot find a primary authoritative DNS server for the  
> name  
> 'lfn-svr-1.LFN.net.'. [ERROR\_TIMEOUT]  
> The name 'lfn-svr-1.LFN.net.' may not be registered in DNS.  
> [WARNING] The DNS entries for this DC are not registered correctly on  
> DNS server '0.0.0.0'. Please wait for 30 minutes for DNS server  
> replication.  
> [FATAL] No DNS servers have the DNS records for this DC registered.  
> Redir and Browser test . . . . . : Passed  
> List of NetBt transports currently bound to the Redir  
> NetBT\_Tcpip\_{889147D6-99FA-410E-A4F8-E95AD376DBCf}  
> The redir is bound to 1 NetBt transport.  
> List of NetBt transports currently bound to the browser  
> NetBT\_Tcpip\_{889147D6-99FA-410E-A4F8-E95AD376DBCf}  
> The browser is bound to 1 NetBt transport.  
> DC discovery test. . . . . : Passed  
> DC list test . . . . . : Passed  
> Trust relationship test. . . . . : Skipped  
> Kerberos test. . . . . : Failed  
> [FATAL] Kerberos does not have a ticket for host/lfn-svr-1.LFN.net.  
> LDAP test. . . . . : Passed  
> Bindings test. . . . . : Passed  
> WAN configuration test . . . . . : Skipped  
> No active remote access connections.  
> Modem diagnostics test . . . . . : Passed  
> IP Security test . . . . . : Skipped  
> Note: run "netsh ipsec dynamic show /?" for more detailed information  
> The command completed successfully  
>  
> NOTES:  
> 1. The DNS Server Test Failure is because AD is not starting up (error  
> loading the GC, as a result of Kerberos Auth Failure, and hence, DNS can  
> not  
> load zones (stored in the AD)).  
> 2. The Kerberos Failure seems to indicate that there is no key stored for  
> the DC (LFN-SVR-1). Interestingly, I ran netdiag twice (second time output  
> to  
> file to c/p here), and first time round, this line was also listed in  
> Kerberos Failure:  
> [FATAL] Kerberos does not have a ticket for krbtgt/LFN.net.'  
> This would mean the TGT key for the LFN.net realm is gone (from my VERY  
> basic knowledge of Kerberos inner workings). Wouldn't this account for the  
> Authentication issues, how would I go about regenerating the TGT for the  
> realm?  
>  
> DCDiag:  
> Domain Controller Diagnosis  
> Performing initial setup:  
> Done gathering initial info.  
> Doing initial required tests

- > *Testing server: LFN\LFN-SVR-1*
- > *Starting test: Connectivity*
- > *The host 6b610473-2182-402d-9273-67cea2ce7610.\_msdcs.LFN.net could*
- > *not be resolved to an*
- > *IP address. Check the DNS server, DHCP, server name, etc*
- > *Although the Guid DNS name*
- > *(6b610473-2182-402d-9273-67cea2ce7610.\_msdcs.LFN.net) couldn't be*
- > *resolved, the server name (lfn-svr-1.LFN.net) resolved to the IP*
- > *address (192.168.0.2) and was pingable. Check that the IP address*
- > *is*
- > *registered correctly with the DNS server.*
- > *..... LFN-SVR-1 failed test Connectivity*
- > *Doing primary tests*
- > *Testing server: LFN\LFN-SVR-1*
- > *Skipping all tests, because server LFN-SVR-1 is*
- > *not responding to directory service requests*
- > *Running partition tests on : ForestDnsZones*
- > *Starting test: CrossRefValidation*
- > *..... ForestDnsZones passed test*
- > *CrossRefValidation*
- > *Starting test: CheckSDRefDom*
- > *..... ForestDnsZones passed test CheckSDRefDom*
- > *Running partition tests on : DomainDnsZones*
- > *Starting test: CrossRefValidation*
- > *..... DomainDnsZones passed test*
- > *CrossRefValidation*
- > *Starting test: CheckSDRefDom*
- > *..... DomainDnsZones passed test CheckSDRefDom*
- > *Running partition tests on : Schema*
- > *Starting test: CrossRefValidation*
- > *..... Schema passed test CrossRefValidation*
- > *Starting test: CheckSDRefDom*
- > *..... Schema passed test CheckSDRefDom*
- > *Running partition tests on : Configuration*
- > *Starting test: CrossRefValidation*
- > *..... Configuration passed test*
- > *CrossRefValidation*
- > *Starting test: CheckSDRefDom*
- > *..... Configuration passed test CheckSDRefDom*
- > *Running partition tests on : LFN*
- > *Starting test: CrossRefValidation*
- > *..... LFN passed test CrossRefValidation*
- > *Starting test: CheckSDRefDom*
- > *..... LFN passed test CheckSDRefDom*
- > *Running enterprise tests on : LFN.net*
- > *Starting test: Intersite*
- > *..... LFN.net passed test Intersite*
- > *Starting test: FsmoCheck*
- > *Warning: DcGetDcName(TIME\_SERVER) call failed, error 1355*
- > *A Time Server could not be located.*
- > *The server holding the PDC role is down.*

microsoft.public.windows.server.security: Re: Kerberos Issue

> *Warning: DcGetDcName(GOOD\_TIME\_SERVER\_PREFERRED) call failed,*  
> *error*  
> *1355*  
> *A Good Time Server could not be located.*  
> *..... LFN.net failed test FsmoCheck*  
>  
> *Notes:*  
> *1. DNS Failure is due to DNS Zones not loading (see Note 1 from*  
> *'netdiag').*  
> *2. The FsmoCheck errors concerning W32Time appear to be due to the Time*  
> *Server being unable to communicate with AD.*  
>  
> *Once again, thank-you for your continued help. I hope this is useful. I*  
> *have*  
> *checked EventID.net as usual against errors as well as the MS*  
> *KnowledgeBase*  
> *and other sites.*  
>  
> *"Ralish" wrote:*  
>  
>> *I have been tearing my hair out over an issue with this Windows Server*  
>> *2003*  
>> *machine for days now. Thankfully, I have made some progress in diagnosing*  
>> *the*  
>> *problem, but I am unsure how to proceed.*  
>>  
>> *In short, the Active Directory service starts up, but is unable to load*  
>> *the*  
>> *global catalog – citing access denied.*  
>>  
>> *Furthermore, as a result, all services that depend on Active Directory,*  
>> *such*  
>> *as DNS, DHCP, Certificate Services, etc... are unable to establish*  
>> *communication and fail as well.*  
>>  
>> *I have tracked the issue down to an authentication issue with Kerberos.*  
>>  
>> *The system appears to be unable to authenticate as itself, with the*  
>> *Security*  
>> *Log flooded with Events from 'Security' with Event ID '675':*  
>>  
>> *Pre-authentication failed:*  
>> *User Name: LFN-SVR-1\$*  
>> *User ID: LFN\LFN-SVR-1\$*  
>> *Service Name: krbtgt/LFN.NET*  
>> *Pre-Authentication Type: 0x2*  
>> *Failure Code: 0x18*  
>> *Client Address: 127.0.0.1*  
>>  
>> *LFN-SVR-1 is the name of the machine and LFN is the short domain name.*  
>>

microsoft.public.windows.server.security: Re: Kerberos Issue

>> *I have also downloaded the MS Resource Tools Kit – and used klist.exe.*  
>>  
>> *klist tickets – Informs me that there are 0 cached tickets...*  
>> *klist tgt – 'Error calling function LsaCallAuthenticationPackage: 0*  
>> *The operation completed successfully.*  
>> *Substatus: 0x8009030e*  
>>  
>> *Any and all help would be greatly appreciated in solving this problem.*  
>>  
>> *Yours hopefully,*  
>>  
>> *Ralish*