

Re: Re-Post – "the trust relationship between this workstation and the

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-02/msg00897

- *From:* "Herb Martin" <news@xxxxxxxxxxxxxxxx>
 - *Date:* Fri, 9 Feb 2007 22:18:33 -0600
-

"Server Guy" <ServerGuy@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:85CBBBA3-6A67-4311-8F96-95924C80B26B@xxxxxxxxxxxxxxxx

Hi,

I have a big problem I sure could use some help with!
This was previously posted but the thread got really long. I tried to repost only the relative info.

When I try to add a new user account at a workstation joined to a domain, I get an error saying I can't add the user because

"the trust relationship between this workstation and the primary domain failed".

This is occurring on stations that are working fine otherwise. The only problem is adding a new user account on the station. Existing accounts on the stations are working fine.

Ok, let's straighten out the terminology before you spend another 20 messages just getting the details set: You don't add a DOMAIN account "on the station", that would be a local computer account. So if you are adding an account locally then you must be a LOCAL ADMINISTRATOR.

If this is really * the case then perhaps you are logged on with a domain account that is in the Domain Admins and thereby getting Administrator privileges on the local machine — but that authentication is failing? Otherwise the DOMAIN has nothing to do with adding an account LOCALLY to that machine.

You may add a domain account FROM a station IF you have installed the AD management tools, i.e., AdminPak.MSI there.

Re: Re-Post – "the trust relationship between this workstation and the

For adding DOMAIN accounts to work OR for using a domain account with local admin privileges a few things must be true:

- 1) Your User account must be authenticated with the domain, and that means you are authenticating the computer account there correctly as well.
- 2) Your user account must have sufficient privileges, e.g., be an Domain Admin, or have the Explicit RIGHT to add users (e.g., Account Operators), or have enough PERMISSIONS in some specific OU.
- 3) Name resolution must succeed so you can find the DC to which you connect
- 4) Your account on that DC must be fully replicated from the DC where you authenticated (OR your password/credentials might not be accepted.)
- 5) The tools must be the correct version for the workstation (XP needs 2003 AdminPak, 2000 needs 2000 AdminPak — the last I checked — and you might need to update these with current service pack versions.
- 6) RPCs must not be filtered by firewalls — either the built-in firewalls, or add-ons like ZoneAlarm, or intermediate firewalls on routers between the machines.
- 7) Other protocols (DNS, DS, etc) must not be filtered but #6 RPCs were mentioned separately since you indicate most things are working correctly.
- 8) Any trusts involved must work, but here I am generally assuming a single domain.
- 9) The computer account is hosed in AD, but you have already reset the computer account.
- 10) The DNS Zone for your AD Domain must be DYNAMIC, with the DC(s) properly registered on all DNS servers which hold the zone.
This would be on the DNS server 172.20.100.2

All of the above are things to check explicitly; some are elaborated below.

For #1, the computer & user accounts to authenticate the DCs must be findable

Re: Re-Post – "the trust relationship between this workstation and the

Re: Re-Post – "the trust relationship between this workstation and the

(fully) in DNS, this means it must be fully registered (DCDiag /c wiith no FAIL or WARN should do).

Client computer must use STRICTLY the INTERNAL DNS server which can resolve the DC. DC is a DNS client too, and this rule applies to it too.

The time on the local computer and DC must be WITHIN 5 minutes (by default) in Universal time. So check time AND make sure both DC and station TIMEZONE are correct set, otherwise the time may look right but be an hour or hours off.

If I add an existing account to a different station, same result.
Tried setting up a new account in AD. Same error when adding account to station.

* Why do you keep saying "at" a different station, or "to" a local machine?
Are you really adding LOCAL accounts?

If so, you should test that by trying to logon as the LOCAL ADMIN and see if it then works. If so, you have a problem (perhaps) with the domain authentication,
if not, you have a local problem and might need to do a REPAIR install or otherwise
correct the local machine — the domain is not then involve AT ALL.

I get the error when I go to Control panel/Users/Add User/Enter User Name and Domain, then get "the trust relationship between this workstation and the primary domain failed " message

I also a Kerberos failed message from the workstation NetDiag, is this a problem here as well?

Yes, check TIME and ESPECIALLY TIMEZONE. Say timezone is set 1 zone away; and DC and workstation LOOK correct, they are really out of sync by an ENTIRE hour.

What I have to do to add the user is leave the domain, login as administrator add the local user and make it a member of the local administrator group, join the domain.

Ok, you really are trying to add to the WORKSTATION — I doubt that

Re: Re-Post – "the trust relationship between this workstation and the

Re: Re-Post – "the trust relationship between this workstation and the
has ever been really clear in your posts.

While this does get the user in the system, I need to make this user a
local
administrator but they only have limited rights eventhough they show as
being
a member of the local administrator group. We have 3rd party software
requiring them to be local administrators.

That software should be replaced OR the reason tracked down and explicit
rights or permission to files or registry keys granted.

I'm not sure when the problem first occurred, but users already on the
workstations are working fine.
This is causing major issues of not being able to setup new accounts on
workstations. Big Problem!

--END OF COMMENTS--

Thanks in advance!!!

=====

I included:
IPConfig /all for DC/DNS & Workstation
NetDiag for DC/DNS & workstation
NSLookup from workstation
NLTest

=====

Lan configuration:
Single DC/DNS server Win2k SP4 server 172.20.100.2
Member Win2003 SP1 server 172.20.100.4
50-nodes: 2-W2k SP4 rest are XP-Pro SP2
USR Router used for Internet access 172.20.100.200
DNS Forwarder to 172.20.100.200
"." zone removed from Forwarder

=====

What I have tried:
Resetting computer object in AD

Removing the computer object from AD, renaming the workstation &
re-joining
but that didn't
help.

Re: Re-Post – "the trust relationship between this workstation and the

Re: Re-Post – "the trust relationship between this workstation and the

```
C:\>nltest /sc_reset:contoso.org
Flags: 30 HAS_IP HAS_TIMESERV
Trusted DC Name \\server1.ABC.org
Trusted DC Connection Status Status = 0 0x0 NERR_Success
The command completed successfully
```

```
C:\>nltest /sc_verify:contoso.org
Flags: b0 HAS_IP HAS_TIMESERV
Trusted DC Name \\server1.ABCC.org
Trusted DC Connection Status Status = 0 0x0 NERR_Success
Trust Verification Status = 0 0x0 NERR_Success
The command completed successfully
```

```
=====
NSLookup from Workstation
=====
```

```
C:\Program Files\Support Tools>nslookup server1 172.20.100.2
Server: server1.contoso.org
Address: 172.20.100.2
```

```
Name: server1.contoso.org
Address: 172.20.100.2
```

```
C:\Program Files\Support Tools>
C:\Program Files\Support Tools>nslookup www.google.com 172.20.100.2
Server: server1.contoso.org
Address: 172.20.100.2
```

```
Non-authoritative answer:
Name: www.l.google.com
Addresses: 216.239.37.99, 216.239.37.104
Aliases: www.google.com
```

```
C:\Program Files\Support Tools>
C:\Program Files\Support Tools>nslookup www.google.com 172.20.100.200
Server: usr8200.home
Address: 172.20.100.200
```

```
Non-authoritative answer:
Name: www.l.google.com
Addresses: 216.239.37.104, 216.239.37.99
Aliases: www.google.com
```

```
C:\Program Files\Support Tools>
```

Re: Re-Post – "the trust relationship between this workstation and the

C:\Program Files\Support Tools>nslookup www.google.com 209.143.0.10
Server: primary.dns.bright.net
Address: 209.143.0.10

Non-authoritative answer:
Name: www.l.google.com
Addresses: 216.239.37.99, 216.239.37.104
Aliases: www.google.com

=====
IPConfig – Workstation
=====

Windows IP Configuration
Host Name : RM-7-1
Primary Dns Suffix : contoso.org
Connection-specific DNS Suffix . :
IP Address. : 172.20.7.1
Subnet Mask : 255.255.0.0
Default Gateway : 172.20.100.200
DNS Servers : 172.20.100.2

=====
IPConfig – DC/DNS Server
=====

Host Name : server1
Primary DNS Suffix : contoso.org
Node Type : Broadcast
IP Routing Enabled. : No
WINS Proxy Enabled. : No
DNS Suffix Search List. : contoso.org

IP Address. : 172.20.100.2
Subnet Mask : 255.255.0.0
Default Gateway : 172.20.100.200
DNS Servers : 172.20.100.2

=====
NetDiag – Workstation
=====

Gathering the list of Domain Controllers for domain 'contoso'
Testing trust relationships... Passed

Re: Re-Post – "the trust relationship between this workstation and the

Testing Kerberos authentication... Failed
Testing LDAP servers in Domain contoso ...

Tests complete.
Default gateway test . . . : Passed
Pinging gateway 172.20.100.200 – reachable
At least one gateway reachable for this adapter.

Domain membership test : Passed
Machine is a : Member Workstation
Netbios Domain name. : contoso
Dns domain name. : contoso.org
Dns forest name. : contoso.org
Domain Guid. : {437C8357-82E5-44BB-87EC-FB3DE7E91058}
Domain Sid :
S-1-5-21-1838114092-1579624115-538272213
Logon User : Administrator
Logon Domain : contoso
Logon Server : \\server1

DNS test : Passed
Interface {7723A855-721E-4C55-B595-814BDDE90AE5}
DNS Domain:
DNS Servers: 172.20.100.2
IP Address: 172.20.7.1
Expected registration with PDN (primary DNS domain name):
Hostname: RM-7-1.contoso.org.
Authoritative zone: contoso.org.
Primary DNS server: server1.contoso.org 172.20.100.2
Authoritative NS:172.20.100.2
Verify DNS registration:
Name: RM-7-1.contoso.org
Expected IP: 172.20.7.1
Server 172.20.100.2: NO_ERROR
The DNS registration for RM-7-1.contoso.org is correct on all DNS servers

DC discovery test. : Passed

Find DC in domain 'contoso':
Found this DC in domain 'contoso':
DC. : \\server1.contoso.org
Address : \\172.20.100.2
Domain Guid : {437C8357-82E5-44BB-87EC-FB3DE7E91058}

Re: Re-Post – "the trust relationship between this workstation and the

Domain Name : contoso.org
Forest Name : contoso.org
DC Site Name. : Default-First-Site-Name
Our Site Name : Default-First-Site-Name
Flags : PDC emulator GC DS KDC TIMESERV WRITABLE
DNS_DC DNS_DOMAIN DNS_FOREST CLOSE_SITE 0x8

Find PDC emulator in domain 'contoso':
Found this PDC emulator in domain 'contoso':
DC. : \\server1.contoso.org
Address : \\172.20.100.2
Domain Guid : {437C8357-82E5-44BB-87EC-FB3DE7E91058}
Domain Name : contoso.org
Forest Name : contoso.org
DC Site Name. : Default-First-Site-Name
Our Site Name : Default-First-Site-Name
Flags : PDC emulator GC DS KDC TIMESERV WRITABLE
DNS_DC DNS_DOMAIN DNS_FOREST CLOSE_SITE 0x8

Find Windows 2000 DC in domain 'contoso':
Found this Windows 2000 DC in domain 'contoso':
DC. : \\server1.contoso.org
Address : \\172.20.100.2
Domain Guid : {437C8357-82E5-44BB-87EC-FB3DE7E91058}
Domain Name : contoso.org
Forest Name : contoso.org
DC Site Name. : Default-First-Site-Name
Our Site Name : Default-First-Site-Name
Flags : PDC emulator GC DS KDC TIMESERV WRITABLE
DNS_DC DNS_DOMAIN DNS_FOREST CLOSE_SITE 0x8

DC list test : Passed
List of DCs in Domain 'contoso':
server1.contoso.org

Trust relationship test. : Passed
Test to ensure DomainSid of domain 'contoso' is correct.
Secure channel for domain 'contoso' is to '\\server1.contoso.org'.
Secure channel for domain 'contoso' was successfully set to DC
'\\server1.contoso.org'.

Kerberos test. : Failed
Cached Tickets:
Server: krbtgt/contoso.org
End Time: 2/8/2007 4:29:12
Renew Time: 2/14/2007 18:29:12
Server: krbtgt/contoso.org
End Time: 2/8/2007 4:29:12

Re: Re-Post – "the trust relationship between this workstation and the

Renew Time: 2/14/2007 18:29:12
Server: cifs/server1.contoso.org
End Time: 2/8/2007 4:29:12
Renew Time: 2/14/2007 18:29:12
Server: ldap/server1.contoso.org/contoso.org
End Time: 2/8/2007 4:29:12
Renew Time: 2/14/2007 18:29:12
Server: LDAP/server1.contoso.org
End Time: 2/8/2007 4:29:12
Renew Time: 2/14/2007 18:29:12
Server: cifs/server1
End Time: 2/8/2007 4:29:12
Renew Time: 2/14/2007 18:29:12
[FATAL] Kerberos does not have a ticket for
host/RM-7-1.contoso.org.

Do Negotiate authenticated LDAP call to 'server1.contoso.org'.

Found 1 entries:

Attr: currentTime

Val: 17 20070207233554.0Z

Attr: subschemaSubentry

Val: 57

CN=Aggregate,CN=Schema,CN=Configuration,DC=contoso,DC=org

Attr: dsServiceName

Val: 109 CN=NTDS

Settings,CN=server1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=org

Attr: namingContexts

Val: 44 CN=Schema,CN=Configuration,DC=contoso,DC=org

Val: 34 CN=Configuration,DC=contoso,DC=org

Val: 17 DC=contoso,DC=org

Attr: defaultNamingContext

Val: 17 DC=contoso,DC=org

Attr: schemaNamingContext

Val: 44 CN=Schema,CN=Configuration,DC=contoso,DC=org

Attr: configurationNamingContext

Val: 34 CN=Configuration,DC=contoso,DC=org

Attr: rootDomainNamingContext

Val: 17 DC=contoso,DC=org

Attr: supportedControl

Val: 22 1.2.840.113556.1.4.319

Val: 22 1.2.840.113556.1.4.801

Val: 22 1.2.840.113556.1.4.473

Val: 22 1.2.840.113556.1.4.528

Val: 22 1.2.840.113556.1.4.417

Val: 22 1.2.840.113556.1.4.619

Val: 22 1.2.840.113556.1.4.841

Val: 22 1.2.840.113556.1.4.529

Val: 22 1.2.840.113556.1.4.805

Val: 22 1.2.840.113556.1.4.521

Re: Re-Post – "the trust relationship between this workstation and the

Val: 22 1.2.840.113556.1.4.970
Val: 23 1.2.840.113556.1.4.1338
Val: 22 1.2.840.113556.1.4.474
Val: 23 1.2.840.113556.1.4.1339
Val: 23 1.2.840.113556.1.4.1340
Val: 23 1.2.840.113556.1.4.1413
Attr: supportedLDAPVersion
Val: 1 3
Val: 1 2
Attr: supportedLDAPPolicies
Val: 14 MaxPoolThreads
Val: 15 MaxDatagramRecv
Val: 16 MaxReceiveBuffer
Val: 15 InitRecvTimeout
Val: 14 MaxConnections
Val: 15 MaxConnIdleTime
Val: 16 MaxActiveQueries
Val: 11 MaxPageSize
Val: 16 MaxQueryDuration
Val: 16 MaxTempTableSize
Val: 16 MaxResultSetSize
Val: 22 MaxNotificationPerConn
Attr: highestCommittedUSN
Val: 6 648273
Attr: supportedSASLMechanisms
Val: 6 GSSAPI
Val: 10 GSS-SPNEGO
Attr: dnsHostName
Val: 19 server1.contoso.org
Attr: ldapServiceName
Val: 32 contoso.org:server1\$@contoso.org
Attr: serverName
Val: 92
CN=server1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=org
Attr: supportedCapabilities
Val: 22 1.2.840.113556.1.4.800
Val: 23 1.2.840.113556.1.4.1791
Attr: isSynchronized
Val: 4 TRUE
Attr: isGlobalCatalogReady
Val: 4 TRUE
[WARNING] Failed to query SPN registration on DC 'server1.contoso.org'.

Routing table test : Passed
Active Routes :
Network Destination Netmask Gateway Interface
Metric
0.0.0.0 0.0.0.0 172.20.100.200 172.20.7.1
10
127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1

Re: Re-Post – "the trust relationship between this workstation and the

Re: Re-Post – "the trust relationship between this workstation and the

```
1
172.20.0.0 255.255.0.0 172.20.7.1 172.20.7.1
10
172.20.7.1 255.255.255.255 127.0.0.1 127.0.0.1
10
172.20.255.255 255.255.255.255 172.20.7.1 172.20.7.1
10
224.0.0.0 240.0.0.0 172.20.7.1 172.20.7.1
10
255.255.255.255 255.255.255.255 172.20.7.1 172.20.7.1
1
No persistent route entries.
```

Netstat information test : Passed

IP Security test : Passed
Service status is: Started
Service startup is: Automatic
IPSec service is available, but no policy is assigned or active
Note: run "ipseccmd /?" for more detailed information

The command completed successfully

=====