

RE: Failed to create a trust relationship between NT4 and 2003 AD

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.migration/2006-08/msg00011.html>

- *From:* ODBC <ODBC@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 21 Jul 2006 04:03:01 -0700
-

Hi Vincent,

One more question, right now both WINS are pointing to their own DC. Should I need to point the NT4 PDC's IP to the primary WINS and DNS of the W2K3 AD domain and vice versa? Thanks.

Regards,
ODBC

"Vincent Xu [MSFT]" wrote:

Hi,

Seems to be a duplicate post. Whatever, make the reply more detail:

1. Check that the LMHOSTS file is in the correct location and formatted properly
 - Location: %SystemRoot%\System32\Drivers\Etc
 - Formatting: Spacing is crucial with the 0x1b entry in the example. There needs to be 20 spaces (characters) inside the " " marks. The domain name is padded with spaces to use 15 characters. The 16th character is the backslash followed by the "0x1b" value.

314108 How to Write an LMHOSTS File for Domain Validation and Other Name Resolution Issues

<http://support.microsoft.com/default.aspx?scid=kb:EN-US:314108>

Once loaded into the cache correctly, test connectivity.

- PING each DC (e.g. "ping NT4PDCName" and "ping W2KPDCName")
- NET VIEW each DC (e.g. "net view \\NT4PDCName" and "net view \\W2KPDCName")

Let me know the results.

2. SECURITY SETTINGS

RE: Failed to create a trust relationship between NT4 and 2003 AD

Most commonly the Active Directory side is the "locked down" side of the trust that causes problems. However, both sides must be checked.

For Windows 2000 and 2003 these settings may be applied/configured via group policy or a local policy (or applied security template). When determining the current values of these settings it is imperative that the proper tools be used or inaccurate readings may occur.

- Enable Winlogon logging

How to Enable Logging for Security Configuration Client Processing in Windows 2000

<http://support.microsoft.com/?id=245422>

- Look at the local cache of the group policy applied security policies.

Event ID 1000 and event ID 1202 are logged to the event log every five minutes in Windows 2003 Server

<http://kb/article.asp?id=319352>

Ensure the following settings are configured as shown:

RestrictAnonymous and RestrictAnonymousSam

- Network access: Allow anonymous SID/Name translation **ENABLED**

- Network access: Do not allow anonymous enumeration of SAM accounts **DISABLED**

- Network access: Do not allow anonymous enumeration of SAM accounts and shares **DISABLED**

- Network access: Let Everyone permissions apply to anonymous users **ENABLED**

- Network access: Named pipes can be accessed anonymously **ENABLED**

- Network access: Restrict anonymous access to Named Pipes and shares **DISABLED**

LM Compatibility

- Network security: LAN Manager authentication level: "LM & NTLM responses" or

"Send LM & NTLM – use NTLMV2 session security if negotiated"

SMB Signing and/or Encrypting

- Microsoft network client: Digitally sign communications (always) **DISABLED**

- Microsoft network client: Digitally sign communications (if server agrees) **ENABLED**

- Microsoft network server: Digitally sign communications (always) **DISABLED**

- Microsoft network server: Digitally sign communications (if client agrees) **ENABLED**

- Domain member: Digitally encrypt or sign secure channel data (always) **DISABLED**

- Domain member: Digitally encrypt secure channel data (when possible) **ENABLED**

RE: Failed to create a trust relationship between NT4 and 2003 AD

- Domain member: Digitally sign secure channel data (when possible)
ENABLED
- Domain member: Require strong (Windows 2000 or later) session key
DISABLED

Once the settings are properly configured, reboot. After reboot ensure the values are still set as expected.

With NT4 the only way to verify the settings is with the Regedt32 tool.

Registry and Group Policy locations for the above values:

RestrictAnonymous

- Windows NT registry:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rdr\Parameters

LM Compatibility

- Windows NT/2000/2003 registry:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LsaLMCompatibilityLevel

RequireSecuritySignature (server)

- Windows NT registry:

HKey_Local_Machine\System\CurrentControlSet\Services\Rdr\Parameters\RequireSecuritySignature

RequireSignOrSeal

- Windows NT/2000/2003 registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters

SignSecureChannel

- Windows NT/2000/2003 registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters

RequireStrongKey

- Windows NT/2000/2003 registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters

3. USER RIGHTS

Ensure User Rights are set as the following:

- Access this computer from network Everyone
- Deny access to this computer from network Does not contain a principal that would affect the PDC (e.g. Everyone, Authenticated Users, etc)

4. GROUP MEMBERSHIP

This aspect only applies to 2003 domain controllers.

Ensure the following group memberships are in place.

Pre–Windows 2000 compatible access group contains:

RE: Failed to create a trust relationship between NT4 and 2003 AD

– Windows 2003: Everyone, Anonymous Logon

Note: "Anonymous Logon" must be added if the "Let Everyone permissions apply to anonymous users" policy setting is not enabled.

OK, let me know the results.

Best regards,

Vincent Xu
Microsoft Online Partner Support

=====
Get Secure! – www.microsoft.com/security

=====
When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from this issue.

=====
This posting is provided "AS IS" with no warranties, and confers no rights.
=====

From: qqharry@xxxxxxxxx
Newsgroups: microsoft.public.windows.server.migration
Subject: Failed to create a trust relationship between NT4 and 2003 AD
Date: 19 Jul 2006 09:09:25 -0700
Organization: <http://groups.google.com>
Lines: 41
Message-ID:
<1153325365.444994.27380@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
NNTP-Posting-Host: 202.175.191.37
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
X-Trace: posting.google.com 1153325370 26990 127.0.0.1
(19 Jul 2006

16:09:30 GMT)

X-Complaints-To: groups-abuse@xxxxxxxxx
NNTP-Posting-Date: Wed, 19 Jul 2006 16:09:30 +0000
(UTC)
User-Agent: G2/0.2
X-HTTP-UserAgent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;

SV1),gzip(gfe),gzip(gfe)

RE: Failed to create a trust relationship between NT4 and 2003 AD

RE: Failed to create a trust relationship between NT4 and 2003 AD

Complaints-To: groups-abuse@xxxxxxxxxx
Injection-Info: p79g2000cwp.googlegroups.com;
posting-host=202.175.191.37;
posting-account=CFJK8Q0AAABf04tXj5JHDrHBrD6k-4HR
Path:

TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTFEEDS02.phx.gbl!newsfeed00
.sul.t-online.de!t-online.de!border2.nntp.dca.giganews.com!border1.nntp.dca.
giganews.com!nntp.giganews.com!postnews.google.com!p79g2000cwp.googlegroups.
com!not-for-mail

Xref: TK2MSFTNGXA01.phx.gbl

microsoft.public.windows.server.migration:24493

X-Tomcat-NG: microsoft.public.windows.server.migration

Dear all,

I got a NT4 domain with "SP3" only, would like to migrate its user accounts (> 1000) to a new 2003 AD. Right now I have trouble on creating the trust relationship between them.

I did the entries for both DCs on LMHOSTS file. I did the WINS service and created the Static Mapping entries for the opposite DC.

My problem is:

I can't create the one-way or two-way trust relationship between NT and 2003 AD. On the NT4 PDC, I created a Trusting domain into Policy and entered the password. But I can't create a Trusted domain and the error said "Could not find domain controller for this domain". On the 2003 AD, I created a New Trust and the NT4 domain name can be recognized, but failed into the last step and got this error on the validation.

"Verification of the trust between the domains was unsuccessful because: Access is denied"

What my case is very similar with this link but even I disabled the "Require Strong (Windows 2000 or later)" session key, the

RE: Failed to create a trust relationship between NT4 and 2003 AD

problem is
still existed.

<http://www.eggheadcafe.com/ng/microsoft.public.windows.server.migration/po>

st643927.asp

I tried the below:

On the Network Neighbour I can browse into the NT4 domain with their related computers from 2003 AD server. I still can do browsing into 2003 domain from NT4 DC server and listing their related computers, but I can't access it regarding the trust relationship failure.

I even followed some case to find a "Restricted Anonymous" registry to make it 0, but I can't find this entry into my server. Can anyone help????!!!!!! I'm exhausted to find the solution for this problem. Please help!!!!!! Thanks a lot.

Regards,
ODBC