

# Re: two-way forest trust issue

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2007-03/msg00445](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-03/msg00445)

---

- *From:* John <[John@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:John@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 7 Mar 2007 19:46:16 -0800
- 

Sorry for the delay.

No errors in the event logs on either DC's.

I used portqryUI on DC's in both domains with similar results.

UDP 389 first lists as Listening or Filtered. After ldap query it lists as Listening  
UDP 88 lists as Listening or Filtered  
UDP 137 first lists as Listening or Filtered. After ldap query it lists as Listening  
UDP 138 lists as Listening or Filtered  
TCP 42 Not listening

NTFRSUTL tool returns "ERROR - Cannot RPC to computer, FQDN; 00001f47 (8007)". This error occurs when i run ntfrsutl from either domain.

I checked all dc's and they are not running any type of firewall or port filtering software. I also verified windows firewall is disabled and no port filtering via tcp/ip. I'm also not running any type of filtering or firewalling across the WAN. I have a DC from domain a physically located in domain b and i get the same results with the portqryui and ntfrsutl so i can rule out WAN issues.

Do you think this can have something to do with the default domain controller policy?

John

"Paul Bergson [MVP-DS]" wrote:

Any errors in the Event Log on either DC?

Re: two-way forest trust issue

If you would like to validate connectivity between the DC's use the tool PortQryUI

Download PortQryUI and run the tool

Select the destination DC

Select Domains and Trusts

Validate the ports that should be open in fact are via the output provided by the tool.

For additional info on this tool see PortQry features, this is the backend tool for PortQryUI

Here is a little trick to see if communications are on going

If you would like to test connectivity to validate FRS communication

NTFRSUTL version server\_name

If the two can communicate via FRS the response will provide the current version number

--

Paul Bergson  
MVP – Directory Services  
MCT, MCSE, MCSA, Security+, BS CSci  
2003, 2000 (Early Achiever), NT

<http://www.pbbergs.com>

Please no e-mails, any questions should be posted in the NewsGroup  
This posting is provided "AS IS" with no warranties, and confers no rights.

<lessard.john@xxxxxxxx> wrote in message  
[news:1173246751.722884.44630@xx](mailto:news:1173246751.722884.44630@xx)

Hi,

The issue is i cannot access a resource located on a DC in domain b from a DC in domain a. I CAN access a resource located on a DC in domain b from a member server or workstation in domain a. I can access a resource located on a DC/member server/workstaion in domain a from a DC/member server/workstation in domain b.

When i try to access the resource on a DC in domain b from a DC in domain a I am prompted for a logon. I've tried several accounts

## Re: two-way forest trust issue

(domain a and b accounts) with various ranges of rights from domain user to domain admin. the error message is "Logon unsuccessful: Windows is unable to log you on. Be sure that your user name and password are correct."

I have a Forest two-way trust, all DC's running w2k3 sp1 R2. DNS in both domains are configured with secondary zones of the other domains DNS.

I can validate outgoing trust in both domains but i cannot validate the incoming. It will not take the acct/password i supply (domain admin for the respective domain).

I disabled sid filtering on the trust using netdom and /quarantine option. i have deleted this trust and re-created it

I was going to use the PES service to migrate user passwords. I created the encryption key on the fsmo holder in domain a. Installed the PES service on fsmo holder of domain b and imported the key. (this is around the time frame i noticed the issue). I just checked and this is still installed.

I installed admt v3 on the fsmo holder of domain a but never launched admt. I have since uninstalled admt.

If more info is needed (i'm sure it is) let me know.

The reason for the trust was to use admt v3 to migrate objects from domain b to domain a and decommission domain b.

Thanks for any insight,

John