

## Re: Directory Service Event 1311

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-05/msg01325](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-05/msg01325)

---

- *From:* Manoj <[Manoj@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Manoj@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Thu, 18 May 2006 13:17:02 -0700
- 

Wow, I would have imagined this to be a routine problem, but guess not. In my case, it seemed to be a firewall problem too, but my Cisco router guy does not think so, saying all tcp traffic is going through the VPN tunnel. Was there any specific ports they had to open up in the firewall?

My problem is how to prove to the router guy that it is an access control list in the router config that is blocking the traffic. How can that be proved. Any debugging tools to help this sort out.

Thanks  
Manoj

"Net Admin" wrote:

I had to call MS Support and it took us 14 hours and 6 engineers to finally fix the problem. The main issue was DNS. I had to point all DNS servers, even the child domain DNS servers, to the PDC in the main site as their primary DNS server. I had to allow zone transfers to all DNS servers in the forest. There were issues with routers and our firewall appliance blocking certain ports. I also had to create a zone delegation for the child domain zone. Since The firewall admin and router admin are 2 other administrators we all had to get in on it to figure this thing out. I downloaded and ran the GUI port query tool to see what was being filtered. I am happy to say that everything works just fine now. It was well worth the money to call Microsoft. Sometimes you need an expert from the outside to come in and take a look. I hope you figure your issues out.  
Good Luck!

"Manoj" wrote:

I get a similar error from a new server that is at site 2 while sending portqry to a PDC at site 1.

I am trying to join this new server to domain and am not able to contact the PDC at site 1.

Re: Directory Service Event 1311

Does this mean a firewall is blocking it. I have windows firewall turned off on the PDC and on this new server. My routers at both sites, do not specifically block this TCP port. What else must be going on. How did you solve your problem .

Thanks  
Manoj

"Net Admin" wrote:

Ok our firewall admin says all traffic is allowed between child domain DCs and parent domain DCs. I ran the query command you gave me and this is what I got:

```
H:\>portqry -n childdc -e 135 -p tcp
Querying target system called:
childdc
Attempting to resolve name to IP address...
Name resolved to 10.0.17.2
TCP port 135 (epmap service): FILTERED
H:\>
Could this be filtered on the server itself?
```

"Paul Williams [MVP]" wrote:

Sorry for the delay!

That sounds fine. Run the following tests to be sure we've not missed anything re. DNS:

```
nltest /dsgetdc:domain-name.com
nltest /dsgetsite
```

Run that from a client and a DC. NLTEST is a support tool.

If you don't have NLTEST and can't install the support tools for whatever reason, use NSLOOKUP:

```
nslookup -type=srv
_ldap._tcp.dc._msdcs.domain-name.com
```

Re: Directory Service Event 1311

If that is yielding a positive result, the problem is elsewhere. Use REPLMON to monitor replication and see what is going on.

Are there any firewalls in between DCs and PCs? Check that you are able to query the end-point mapper (TCP135) and one of the DS ports returned by the end-point mapper using PORTQRY (support tool or download), like so:

```
portqry -n hostname -e 135 -p tcp
```

--

Paul Williams  
Microsoft MVP – Windows Server –  
Directory Services  
<http://www.msresource.net> |  
<http://forums.msresource.net>