Article ID: 306843 - Last Review: October 29, 2007 - Revision: 5.3

How to troubleshoot MS DTC firewall issues

This article was previously published under Q306843

SUMMARY

This article describes troubleshooting steps to help you enable Microsoft Distributed Transaction Coordinator (MS DTC) to communicate through a firewall with another MS DTC. The following list outlines some of the problems that you may experience when you use MS DTC through a firewall:

- Your application functions successfully when your MTS or COM+ components have their **Transaction Support** property set to **Not Supported** or **Supported**, but it does not function successfully when that property is set to **Requires** or **Requires New**.
- You receive the following error message:

  New transaction cannot enlist in specified transaction coordinator

- You receive the following error message:

  Error 8004d00a. Distributed Transaction error

Although several other Microsoft documents describe how to address this problem, this article summarizes most of them.

Note The troubleshooting steps that follow are designed for use with Microsoft Windows NT and Microsoft Windows 2000 operating systems only.

MORE INFORMATION

Troubleshooting steps

Important This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:

322756 (http://support.microsoft.com/kb/322756/) How to back up and restore the registry in Windows

1. Verify that the MS DTC service is started on both servers.
2. If your server is running Windows NT 4.0, you must reapply Windows NT 4.0 Service Pack 6 (SP6) after you install Windows NT 4.0 Option Pack (NTOP). Review the file versions that are listed in the following table to verify that

Windows NT 4.0 SP6 has been reapplied after the installation of the Windows NT 4.0 Option Pack:

File Name	Version After You Install NTOP	Version After You Reinstall SP6
Msdtcprx.dll	1997.11.532	1999.6.854.0
Msdtctm.dll	1997.11.532	1999.6.854.0
Xolehlp.dll	1997.11.532	1998.08.762

For more information about Windows NT 4.0 Option Pack installation, see the following Microsoft white paper:

IIS 4.0 Recommended Installation Procedure
http://support.microsoft.com/support/iis/install/install_iis4.asp
(http://support.microsoft.com/?scid=http%3a%2f%2fsupport.microsoft.com%2fsupport%2fiis%2finstall%2finstall_iis4.asp)

3. Configure both servers so that MS DTC communication flows between the firewall. Follow these steps to control RPC dynamic port allocation.

   Note You must follow these steps on both computers.

   Note The firewall must be open in both directions for the specified ports.

   a. To start Registry Editor, click **Start**, click **Run**, type **regedt32**, and then click **OK**.

      You must use the Regedt32.exe file instead of the Regedit.exe file. The Regedit.exe file does not support the REG_MULTI_SZ data type that is required for the Ports value.

   b. In Registry Editor, expand the following key:
      HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc

   c. Click the **RPC** folder, and then click **Add Key** on the **Edit** menu.
   d. In the **Add Key** dialog box, type **Internet** in the **Key Name** box, and then click **OK**.
   e. Click the **Internet** folder, and then click **Add Value** on the **Edit** menu.
   f. In the **Add Value** dialog box, type **Ports** in the **Value Name** box.
   g. In the **Data Type** box, select **REG_MULTI_SZ**, and then click **OK**.
   h. In the **Multi-String Editor** dialog box, specify the port or ports that you want RPC to use for dynamic port allocation in the **Data** box, and then click **OK**.

      Each string value that you type specifies either a single port or an inclusive range of ports. For example, to open port 5000, specify "5000". To open port 5000 to port 5020 inclusive, specify "5000-5020". You can specify multiple ports or ports ranges by specifying one port or port range per line. All ports must be in the range of 1024 to 65535. If any port is outside this range or if any string is invalid, RPC treats the whole configuration as invalid.

      We recommend that you open ports from 5000 and higher, and that you open a minimum of 15 to 20 ports.

   i. Follow step e through step h to add another key. Use the following values:
      - Value: PortsInternetAvailable

- Data type: REG_SZ
- Data: Y

This signifies that the ports that are listed under the Ports value are to be made Internet-available.

j. Configure your firewall to allow for incoming access to the specified dynamic ports and to port 135 (the RPC Endpoint Mapper port).

k. Restart the computer. After RPC restarts, it assigns incoming ports dynamically, based on the registry values that you have specified. For example, to open ports 5000 through 5020 inclusive, create the following named values:

- Ports : REG_MULTI-SZ : 5000-5020
- PortsInternetAvailable : REG_SZ : Y
- UseInternetPorts : REG_SZ : Y

DTC also requires that you can resolve computer names by using NetBIOS or DNS. You can test whether NetBIOS can resolve the names by using the PING protocol and the server name. The client computer must be able to resolve the name of the server. Additionally, the server must be able to resolve the name of the client. If NetBIOS cannot resolve the names, you can add entries to the Lmhosts files on the computers. For more information about how to configure TCP ports on Windows 2000, click the following article number to view the article in the Microsoft Knowledge Base:

300083 (http://support.microsoft.com/kb/300083/) How to restrict TCP/IP ports on Windows 2000 and Windows XP

4. If MS DTC still does not work through the firewall, download the DTCPing.exe tool, and install this tool on both servers involved.The following file is available for download from the Microsoft Download Center:

Download DTCPing.exe now
(http://download.microsoft.com/download/d/0/0/d00c8f6b-135d-4441-a97b-9de16a1935c1/dtcping.exe)

The DTCPing.exe file contains the following files:

```
Date         Time   Version  Size     Filename
-------------------------------------------------------
29-Oct-2003  22:56  1.8.0.1  274,490  Dtcping.exe
15-Dec-2003  22:05             1,618  Eula.txt
24-Nov-2003  20:59             1,560  Machinea_failure.log
24-Nov-2003  20:21             1,901  Machinea_success.log
24-Nov-2003  20:55               999  Machineb_failure.log
24-Nov-2003  20:31             1,750  Machineb_success.log
24-Nov-2003  20:15             2,325  Readme.txt
```

Release Date: November 24, 2003

For more information about how to download Microsoft support files, click the following article number to view the article in the Microsoft Knowledge Base:

119591 (http://support.microsoft.com/kb/119591/) How to obtain Microsoft support files from online services

Microsoft scanned this file for viruses. Microsoft used the most current virus-detection software that was available on the date that the file was posted.

The file is stored on security-enhanced servers that help prevent any unauthorized changes to the file.

5. Use the Readme.txt file that is included in the DTCPing.exe download to test Remote Procedure Call (RPC) and Distributed Transaction Coordinator (DTC) communication from Server1 to Server2. If this test is successful, run the test from Server2 to Server1.

   Note that if RPC cannot flow in either direction, MS DTC communication fails in both directions. If RPC communication fails, the DTCPing window (on either server) displays this failure, which is also saved in the associated dtcping.log file. See the Readme.txt file for more information. If the test fails in either direction and the log indicates the failure is in RPC communication, continue to the next step. If the test fails in either direction and the log indicates the failure is in DTC communication, continue to step 9 below.
6. If RPC has failed in at least one direction (for example, from Server1 to Server2), direct your firewall administrator to make sure that the Internet Control Message Protocol (ICMP) is open in both directions.

   Note You can typically determine if RPC has failed by reading the dtcping.log file.

   By default, ICMP is port1. You can verify this in your protocol file, which is located in the %windir%\WinNT\System32\Drivers\ folder. Ping Server2 by NetBios name from Server1. If the ping fails, continue to the next step. Otherwise, continue to step 8.
7. Ping Server2 by IP address from Server1 to make sure that the correct port is open for a ping on the firewall. A Network Monitor trace can verify this. If the IP address ping succeeds and the NetBios name ping fails, there is a name resolution problem.

   Note You can use the **ipconfig /all** command to retrieve the IP address or the IP addresses of a server.

   A quick way to test name resolution is to make an entry in the Hosts file of the client server. This is the server on which the NetBios name ping fails. You can model your entry after the sample entry that is included in the file.

   Note You must only make an entry in the Hosts file for troubleshooting purposes. If the new entry corrects the name resolution problem, remove the entry from the Hosts file, and make the entry you must in the DNS, the WINS server, or the LmHosts file.

   Other solutions to name resolution problems exist, but they are outside the scope of this article.
8. If pinging Server2 from Server1 by NetBios name fails, or if pinging Server2 from Server1 by NetBios name succeeds but the DTCPing test shows RPC communication still fails, it is possible that Port 135 (the End Point Mapper, or EPM) has not been opened bi-directionally on the firewall. Check the firewall to make sure that the EPM is open in both directions. At this point, a Network Monitor trace may help to pinpoint the problem.
9. You only reach this step if the DTCPing test indicates RPC communication works in both directions. If DTCPing indicates no errors in either direction, then RPC and MS DTC communication is flowing properly.
10. If DTCPing indicates that DTC communication has failed in at least one

direction (for example, from Server1 to Server2), direct firewall administrators to verify that the ports are open that the developer specified when the developer went through the MS DTC configuration article (see step 3). Additionally, some rules may be applied to the firewall that prohibits RPC callbacks for either (or both) servers. A Network Monitor trace may help to troubleshoot this particular scenario.

11. If DTCPing returns an error message similar to the following:

    Unexpected: My session guid is same as partner's guid

    check whether the current server has been duplicated or cloned from the other server. If so, locate the **HKEY_CLASSES_ROOT\CID** key in the registry. Under this key, you may notice more than one GUID. Locate the GUID whose underlying Description key is **MSDTC**. Note that this GUID is also listed in the DTCPing output window. If the other server has a GUID that is exactly the same for MS DTC in its registry, you must create a new GUID for MS DTC in one of the registries. You can use GuidGen to do this.

    After you add this new GUID, and also all of its underlying keys to **HKEY_CLASSES_ROOT\CID**, make sure to delete the old GUID that it is replacing.

    If this step resolves your problem, it is highly recommended that you read the following article to learn more about duplicating (or "ghosting") computers: For more information, click the following article number to view the article in the Microsoft Knowledge Base:

    162001 (http://support.microsoft.com/kb/162001/) Do not disk duplicate installed versions of Windows

APPLIES TO

- Microsoft COM+ 1.0
- Microsoft Transaction Services 2.0

Keywords: kbproductlink kbdownload kbdtc kbhowto KB306843

Retired KB Content Disclaimer

This article was written about products for which Microsoft no longer offers support. Therefore, this article is offered "as is" and will no longer be updated.