http://support.microsoft.com/kb/555017

HOWTO: Enable DTC Between Web Servers and SQL Servers Running Windows Server 2003

Article ID: 555017 - View products that this article applies to.

Author: Robert McLaws MVP

Community Solutions Content Disclaimer

System TipThis article applies to a different version of Windows than the one you are using. Content in this article may not be relevant to you. Visit the Windows 7 Solution Center

Expand all | Collapse all

MORE INFORMATION

Configuring Windows Server 2003 to handle DTC transactions across non-domain web environments is a several-step process that will require the modification of several critical systems, including the registry. It is highly recommended that a full system backup be performed before attempting these changes.

WARNING: DO NOT attempt to adjust the COM+ security settings to enable this service. If you change the COM+ user permissions to any account other than the one specified, you may permanently disable COM+ on that system, crippling several major Windows subsystems. If this happens, the only resolution is to wipe the machine's hard drive and reinstall Windows Server 2003.

Step One: Steps to Enable Network DTC Access (Run on all machines requiring DTC access)

1. Click Start, point to Control Panel, and then click Add or Remove Programs.
2. Click Add/Remove Windows Components.
3. Select Application Server, and then click Details.
4. Select Enable network DTC access, and then click OK.
5. Click Next.
6. Click Finish.
7. Stop and then restart the Distributed Transaction Coordinator service.
8. Stop and then restart any resource manager services that participates in the distributed transaction (such as Microsoft SQL Server or Microsoft Message Queue Server).

For more information on this step, see MSKB 817064

Step Two: Install the SQL Server 2000 Client Tools on all machines requiring DTC access.
The SQL Client Tools can be found on the SQL Server 2000 CD. During Setup, ensure that the MSDTC option is checked.

Step Three: Install Simple VPN (OPTIONAL)
If the computers involved are part of the same IP subnet and workgroup, then skip this step. Otherwise, you will have create a secondary network using a VPN to bring all servers into the same workgroup.

Part One: Setting Up The VPN Server

1. Click Start, point to Control Panel, and then click Network Connections.
2. Click Create New Connection.
3. Select Set up an advanced connection and then click Next.
4. Select Accept incoming connections and then click Next.
5. Do not select an incoming device and then click Next.
6. Select Allow virtual private connections and then click Next.
7. Select the user account(s) you wish to grant access and then click Next.
8. Configure the VPN server network settings, specifying your new network's IP range.
9. Ensure that Allow callers to access my local area network is checked, and then click Next.
10. Click Finish to create the VPN server.

Part Two: Setting Up The VPN Clients

1. Click Start, point to Control Panel, and then click Network Connections.
2. Click Create New Connection.
3. Select Connect to the network at my workplace and then click Next.
4. Select Virtual Private Network connection and then click Next.
5. Type in a name for your connection in the prompt and then click Next.
6. Select Do not dial an initial connection and then click Next.
7. Type in the VPN Server's IP address, and then click Next.
8. Select Anyone's use and then click Next.
9. Check the Create a shortcut to this connection on my desktop checkbox and then click Finish.

At this point, you can firewall off your internet connections on every server with the Internet Connection Firewall (ICF), because the machines will be communicating over a secure VPN connection.

Step Four: Enable NETBIOS Across All Machines

Alternatively, you can add entries in the HOSTS file (c:\windows\system32\drivers\etc) so that the machines can be pinged by server name. See the comments in the HOSTS file for more information on how to accomplish this.

Step Five: Disable RPC Security for MSDTC Service on SQL Server

This step requires accessing and modifying the registry. If you have not already done so, it is highly recommended that you back up the registry at this time.

1. Click Start, click Run, type in "Regedt32", and click OK.
2. Select HKEY_LOCAL_MACHINE, then SOFTWARE, then Microsoft.
3. Right-click on MSDTC, point to Add, then select DWORD Value.
4. Rename the key from the default New Value #1 to TurnOffRpcSecurity.
5. Double-click the new key and change the value to 1.
6. Close the Registry Editor and restart the SQL Server

For more information on this step, see MSKB 827805

Step Six: Set VPN Connection To Automatically At Startup, and Connect to VPN (OPTIONAL)

Complete the following steps on each VPN client machine:

1. Open the VPN connection and select Properties.
2. On the Options tab, uncheck the Prompt for name and password, certificate, etc. checkbox.
3. On the Security tab, select Internet Protocol (TCP/IP) option, then click Properties.
4. In the resulting TCP/IP Properties dialog, click Advanced, and uncheck the Use default gateway on remote network checkbox.

5. Close out each dialog box by clicking OK.
6. Input the desired username and password (from Step 3, Part 1, Item 7), and check the Remember me option.
7. Open Windows Explorer, and navigate to the C:\Documents And Settings\All Users\Start Menu\Programs\Startup folder.
8. Drag the VPN shortcut you created in Step Three, Part 2, Item 8 from the Desktop to the Startup folder in Windows Explorer.
9.Shut down and restart the machine.

The process is now complete. Your Web Server and SQL Server should now be able to participate in coordinated transactions.

Special Thanks to ORCSWeb for helping develop this article.