Tech Note 532
Troubleshooting Communication Issues Between Historian Server and Remote IDAS

Topic#: 002269
Created: March 2008
Updated: April 2009
Updated: February 2011
Updated: January 2012

Introduction

Wonderware Historian Data Acquisition (InSQL Data Acquisition Service or IDAS) is an application that accepts data values coming from one or more I/O Servers or DAServers via SuiteLink® or DDE and passes it on to the Historian Server for storage. You can configure Historian tags to use either the local IDAS installed on the server or a "Remote IDAS" installed separately on a remote computer in order to take advantage of store-and-forward or failover functionality.

If the Remote IDAS is unable to communicate with the Historian Server, all data currently being processed can be stored on the local hard drive. Note that the store-and-forward option is not available if you have specified a failover IDAS.

This *Tech Note* provides tips to help you troubleshoot and fix communications issues between the Historian Server and the Remote IDAS.

Application Versions

- Historian 10.x

Procedure

If you set up a remote IDAS, you must configure security settings that allow access permissions between the remote IDAS and the Historian Server, and the remote IDAS needs to access the Historian Server to send data.

These tasks require administrative permissions. Therefore, make sure that the user account you specified when installing the Historian Server is added to the Administrators group on the remote IDAS computer.

Note: A remote IDAS only requires the same administrative account to exist on the local computer and the Historian Server. It is not necessary to log in to the remote IDAS computer using this administrative account.

1. If the remote IDAS is running in a workgroup environment, create the same administrative user account (same user name and password) on the Historian Server and each of the computers running the remote IDAS component.
2. Make sure the OS Configuration Utility has been run on both the Historian Server and the Remote IDAS computers. This utility is required for Windows 2003 SP1 or higher, and Windows XP SP2 or higher. You can find this utility on Wonderware's Technical Support website, or **download** the Utility.

3. Where applicable, make sure the User Account Control (UAC) is disabled on BOTH computers. See **Tech Note 733 Disabling UAC for Wonderware® Product Support** for instructions.

4. Click **Start/Programs/Wonderware/Common**, then select **Change Network Account** to configure the network account settings. The User Name and Password can be anything, but be sure to use the same User Name and Password on both the Historian Server and the Remote IDAS machine.

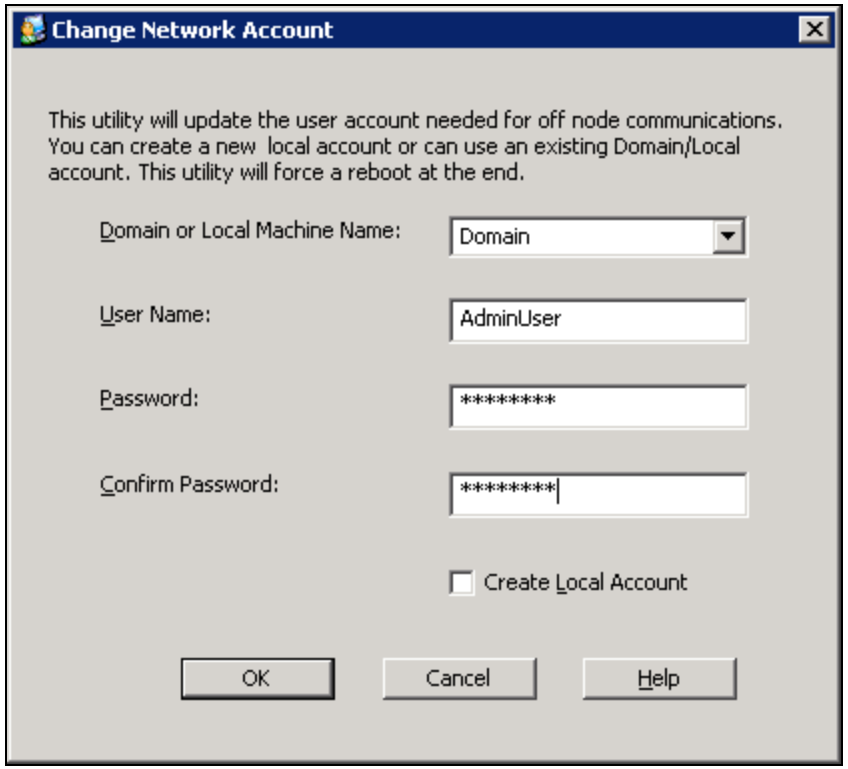

FIGURE 1: CHANGE NETWORK ACCOUNT

5. Verify that the remote IDAS has been installed on the remote machine, and the version and patch or service pack level of the Historian Server and the remote IDAS are the same. You can use the **Control Panel/Add or Remove Programs** to check the version number of Wonderware IndustrialSQL Server.

6. Verify that you can ping back and forth between the Historian Server and the remote IDAS machine.

7. Verify that the remote IDAS computer name (or NetBIOS name) is configured with an IP address that matches with that returned by the Command Prompt IPCONFIG on the remote IDAS machine and identical to the IP address returned by the ping.

   If the computers belong to a workgroup and you cannot ping them by computer names, you can populate the HOSTS file on each of the machines with IP addresses and machine names for both of the Historian Server and Remote IDAS computers. The HOSTS file is normally found in: **C:\WINDOWS\system32\drivers\etc**.

   In the following example, the IP address returned by the IPConfig command is 10.2.81.95 matches with the IP address returned from the ping test. In addition, a valid ping test also returns 3 or 4 replies:

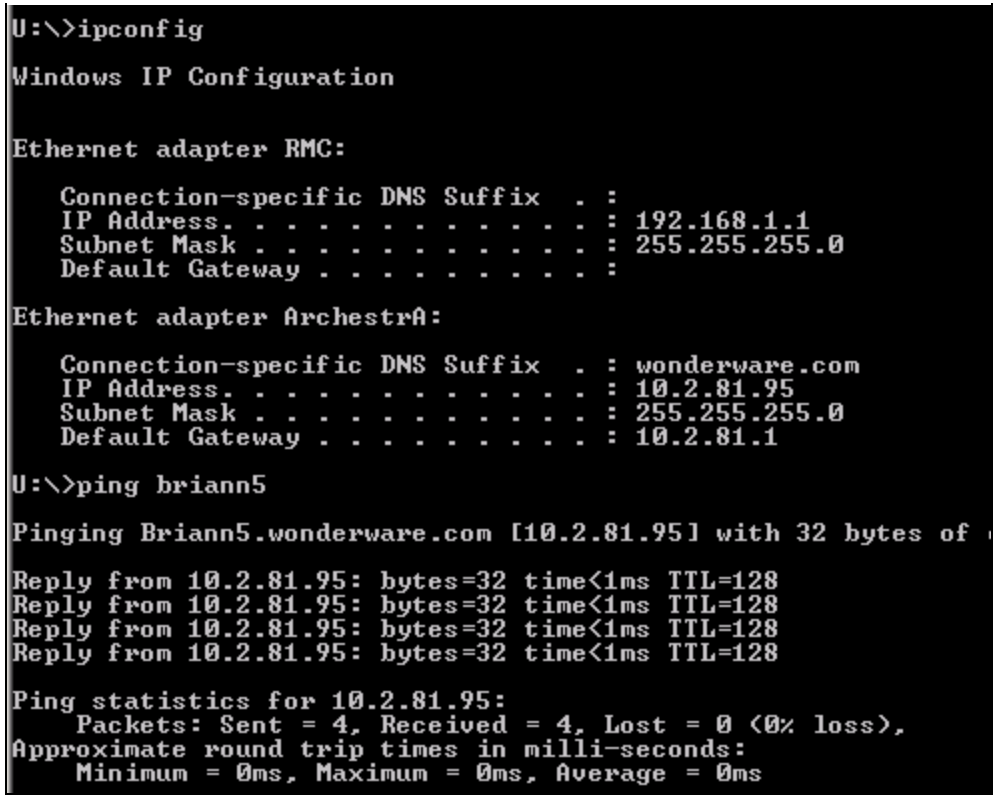

FIGURE 2: VERIFYING VALID IP ADDRESS USING IPCONFIG AND PING COMMANDS

8. It is recommended that DCOM on each computer has been enabled even though the remote IDAS communicates with the Historian Server via named pipes.

   If a firewall exists between a remote IDAS and the historian computer, the firewall must allow communication using ports from 135 through 139 (TCP/UDP) and port 445 (TCP/UDP).

9. To enable DCOM, click **Start/Settings/Control Panel/Administrative Tools/Component Services**.

10. Expand **Component Services/Computers**, then right-click **My Compute**r and click **Properties**.

11. Click the **Default Properties** tab and select **Enable Distributed COM on this computer** (Figure 3 below).

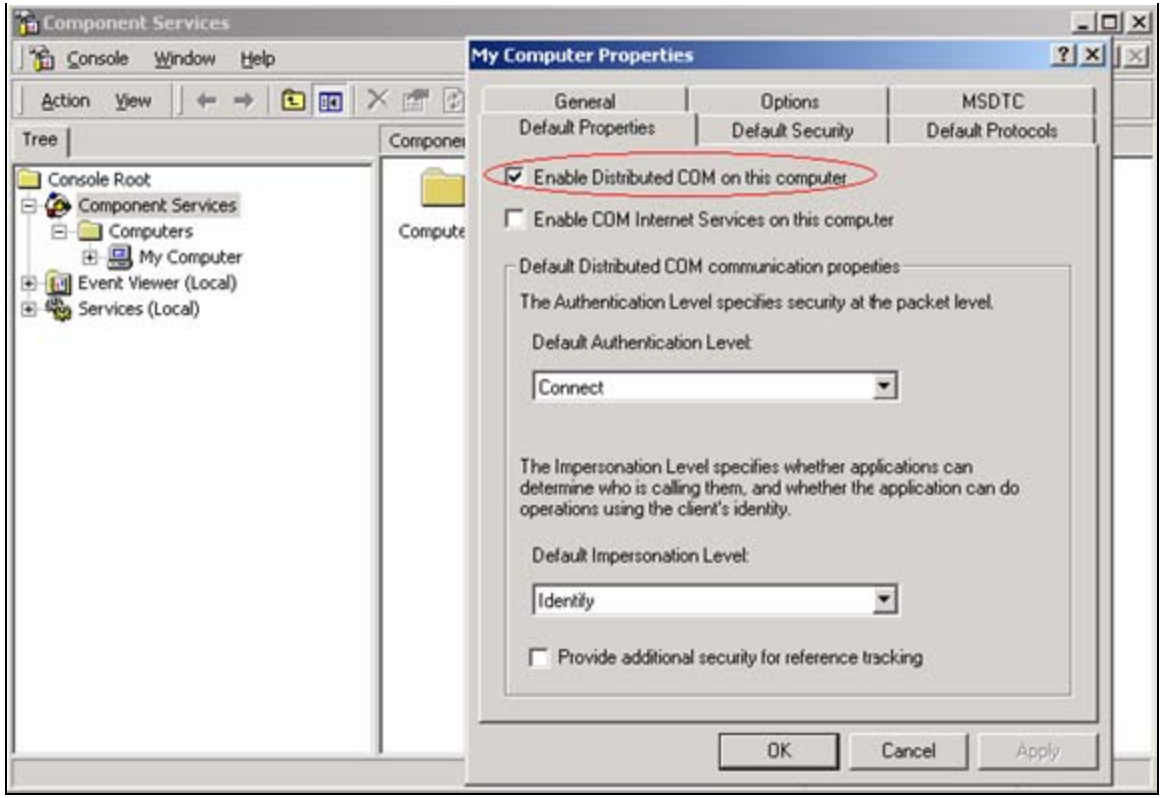

FIGURE 3: ENABLE DISTRIBUTED COM

12. After enabling the DCOM, reboot the computer for the change to take effect.

13. Verify that the **File and Printer Sharing for Microsoft Networks** is enabled as shown in Figure 4 (below). This is a requirement for using Remote IDAS on the Windows XP Operating System:

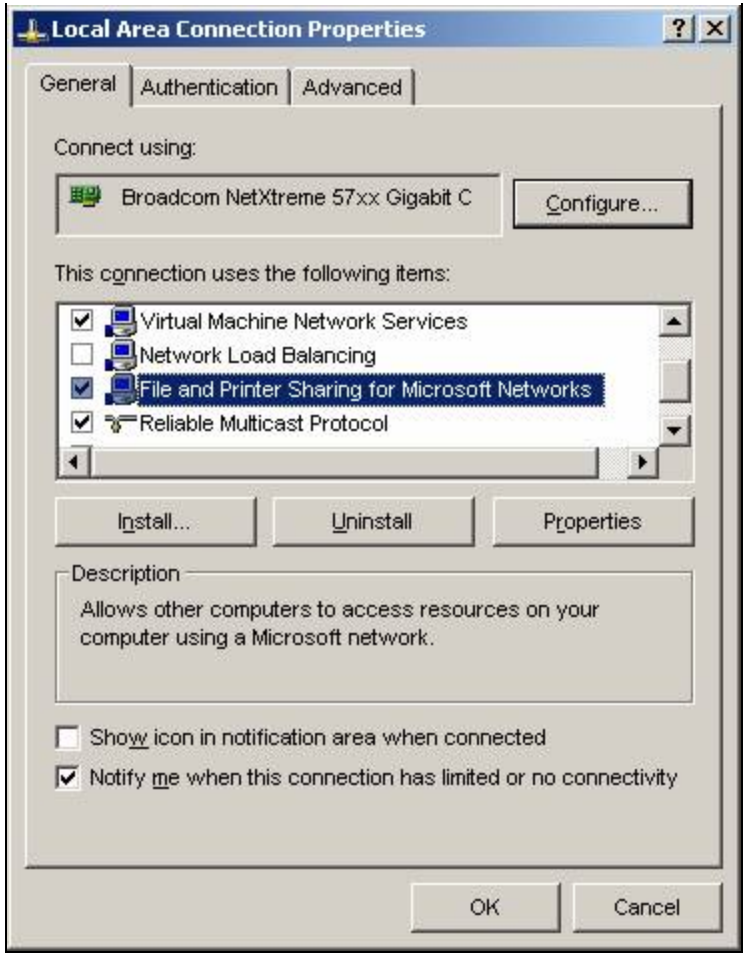

FIGURE 4: FILE AND PRINTER SHARING REQUIRED FOR XP

14. On the remote IDAS computer, verify that you can start / stop the **InSQLDataAcquisition** service when logged in as the user you specified in the **Change Network Account** utility shown in Figure 1 (above).

15. From the Historian Server machine, make sure you can query, start, and stop the remote IDAS service (InSQLDataAcquisition) using the **SC.EXE** utility.

    This utility is a command line program used for communicating with the computer system's Service Control Manager and Services.

    The following examples provide the supported syntax to use the Command Prompt program SC on the Historian PC to query, start, and stop the InSQLDataAcquisition service:

- To **query** the status of the InSQLDataAcquisition service on the remote IDAS type the following:

```
SC  \\<RemoteIDAS PC name> QUERY InSQLDataAcquisition
```

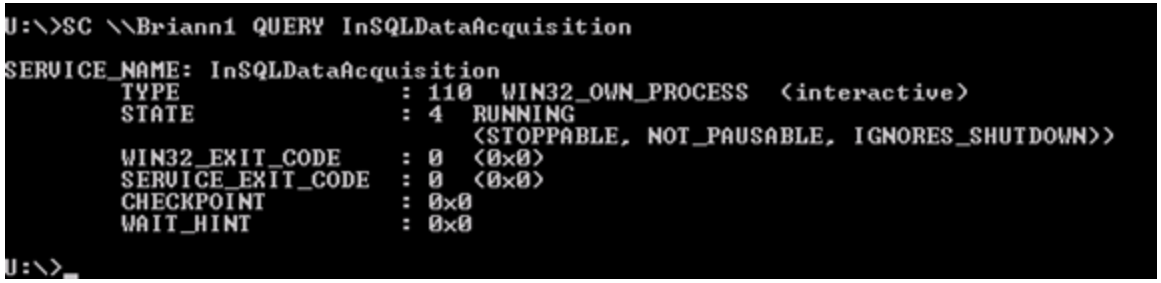

Figure 5: Command Line Syntax to Query the Remote DataAcquisition Service

- To **start** the InSQLDataAcquisition service on the remote IDAS from the Historian Server:

  ```
  SC  \\RemoteIDAS PC name START InSQLDataAcquisition
  ```

- To **stop** the InSQLDataAcquisition service on the remote IDAS from the Historian Server:

  ```
  SC  \\RemoteIDAS PC name START InSQLDataAcquisition
  ```

B. Nguyen, C. Boutcher

Tech Notes are published occasionally by Wonderware Technical Support. Publisher: Invensys Systems, Inc., 26561 Rancho Parkway South, Lake Forest, CA 92630. There is also technical information on our software products at **www.wonderware.com/support/mmi**

For technical support questions, send an e-mail to **support@wonderware.com**.

Back to top