Tech Note 861
Wonderware System Platform FAQs for IT Professionals

All Tech Notes, Tech Alerts and KBCD documents and software are provided "as is" without warranty of any kind. See the **Terms of Use** for more information.

Topic#: 002659
Created: May 2012

Introduction

This *Tech Note* includes frequently asked questions regarding Wonderware System Platform by IT Professionals. The topics that are covered in this tech note are:

- **Compatibility and System Requirements**

- **Firewall and DCOM Settings**

- **Antivirus**

- **Computer Name Resolution**

- **Time Synchronization**

- **Network Service Account**

Application Versions

- Wonderware Application Server 3.1 and later

- InTouch 10.1 and later

Compatibility and System Requirements

Q: What are the OS, Software, and Hardware requirements for installing Wonderware products?

A: You select the Operating System based on the requirements defined by the system architecture. The OS requirements for Development Node, Application Node, and GR Node are different. Some Operating Systems might be compatible with your Development Node and incompatible with the other nodes (and vice-versa).

Similarly, SQL Server requirements for each product are different. To get a list of compatible OS and SQL Server version, refer to the ReadMe file of the specific Wonderware product you are installing. The document also provides the Minimum Hardware, Software, and Compatibility requirements for successful installation and operation of the system. The ReadMe file is located in the Wonderware installation CD and on the Wonderware Developer Network (WDN).

Firewall and DCOM Settings

Q: Can firewalls be enabled on the system?

A: It is best practice to turn off the firewall.

Q: If firewall cannot be turned off, what precautions can I take?

A: If a firewall needs to be on, ensure that the firewall allows required ports to communicate. In other words, make sure the firewall does not block the required ports.

The DCOM Ports used by the Bootstrap are:

- Port **135**

- Port **139**

- Port **445**

- Ports **1024** to **65535**

For details, refer to **Tech Note 461 – Troubleshooting Industrial Application Server Bootstrap Communications**.

Antivirus

Q: Is antivirus recommended for use with Wonderware products?

A: A strong antivirus package should be used to protect your SCADA system. The antivirus software should be updated on a regular basis to ensure that your system is free of virus attacks.

Q: What are the exclusions required for proper functioning of Wonderware products?

A: The following folders should be excluded by the antivirus software:

32-bit Operating System

- C:\Program Files\ArchestrA*.*

- C:\Program Files\Common files\ArchestrA*.*

- C:\Program Files\FactorySuite*.* (may not exist in newer installations)

- C:\Program Files\Wonderware*.*

- C:\InSQL\Data*.*

- C:\Historian\Data*.*

- C:\Documents and Settings\All Users\Application Data\ArchestrA*.*

64-bit Operating System

- C:\Program Files (x86)\ArchestrA*.*

- C:\Program Files (x86)\Common files\ArchestrA*.*

- C:\Program Files (x86)\FactorySuite*.* (may not exist in newer installations)

- C:\Program Files (x86)\Wonderware*.*

- C:\InSQL\Data*.*

- C:\Historian\Data*.*

- C:\ProgramData\Archestra *.*

If you choose different drives/folders for the program files and data files, be sure that you configure the Antivirus software accordingly.

Computer Name Resolution

Q: What is recommended for ensuring proper name resolution?

A: The Archestra system requires strong name resolution to ensure that node to node communication and deployment is successful. Normally a DNS server is sufficient.

Q: What can I use if a DNS Server is not available, or if there are problems with the DNS Server?

A: In the absence of a DNS server you must use a set of **hosts** files. The hosts file is normally located under C:\Windows\system32\drivers\etc.

Every server in the system should be listed with its correct IP address in the hosts file. You can copy the file to all the machines in the system.

Using the hosts files guarantees that the name resolution is correct (provided that the files are correctly set up).

Note: If the hosts files are not all identical on all machines, it will cause communication problems on a network.

Time Synchronization

Q: Why is time synchronization important?

A: ArchestrA platforms have difficulty communicating to each other when they are not synchronized to the same time.

Functions such as scripting, alarming, and historizing depend on all nodes in the Galaxy being synchronized to the same time.

Q: Which nodes need to be time synchronized?

A: All machines in the system (InTouch, Application Server, Information Server, Wonderware Historian etc.) must be synchronized.

Q: How does time synchronization affect ArchestrA and Wonderware Historian performance?

A: Due to the fact that both Archestra and Wonderware Historian are real-time systems, time synchronization is critical. Wonderware Historian does not accept data that is more than 30 seconds old (according to the Historian servers' local time) or more than 5 seconds early.

Q: Is it possible to initiate time synchronization from InTouch?

A: Time synchronization should be at the OS level. InTouch does not have a time synchronization function.

Q: What are the recommendations for ensuring that all machines are time synched?

A: The typical recommendation is to use the following:

- Run the **NET TIME** function from the DOS/Command prompt.

- Configure a Galaxy time master which requires Application Server. Refer to the Application Server user guide – **Synchronizing Time across a Galaxy**.

Network Service Account

Q: Why is the Network Service Account required?

A: All Wonderware nodes use the Network Service Account for node-to-node communications between Archestra components. During the initial installation of an Archestra component, you must create a new user account or use an existing account. The same user account should be used on each computer that requires communication with other computers in an Archestra environment.

Q: What features are required for the Network Service Account user?

A: The network account User must have the following properties:

- Local administrative rights

- Log on as Service rights

- Never expire

- User cannot change the password

Q: How do I modify the Network Service Account?

A: The Network Service Account is managed by the **Change Network Account** Utility.

To run the Change Network Account,

1. Click **Start -> Programs -> Common -> Change Network Account**.

2. Type the user name and password for the network account. If the account is local and does not exist, ensure that **Create Local Account** is checked.

A prompt will appear.

3. Reboot the machine for the changes to take effect.

Q: Can domain accounts be configured for the Network Service Account?

A: In a domain environment, it will be beneficial to have a domain account. This is because a domain account provides better security and a single password to manage.

Q: What precautions do I take with the local Network Service Account?

A: In a local account, there are always possibilities for someone to change the password of the local network account user. If this occurs, all machines in the ArchestrA environment will be affected. In that case, all machines need to be updated with the same password in order for the system to work properly.

P. Karthikeyan

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

 Back to top