Tech Note 508
Troubleshooting Wonderware Application Server Processes

Topic#: 002234
Created: November 2007
Updated: September 2009

Introduction

A Wonderware Application Server process or file can appear to stop responding. The most common causes are:

- **Locked System Files**
- **Security Restrictions**
- **Lack of System Resources**

Software conflicts caused by third party applications can also be a contributor.

If any of the above factors are present, they can cause unpredictable and adverse behaviors.

This *Tech Note* provides general guidelines for troubleshooting non-responsive Application Server processes, and providing an optimal environment for a Wonderware Application Server implementation.

Application Versions

- Industrial Application Server 2.1 and later (includes Wonderware Application Server)

Identifying the Processes

The processes most likely to be affected are listed below:

Process	Description
aaEngine.exe	Engine Module
aaPlatformInfoSvr.exe	PlatformInfoServer Module
aaBootstrap.exe	Bootstrap Module
aaGlobalDataCacheMonitorSvr.exe	GlobalDataCacheMonitorServer Module
aaGR.exe	Galaxy Repository service that processes requests to the ArchestA configuration subsystem.
aahSCM.exe	ArchestrA Historian SCM
aaLogger.exe	aaLogger Module
aaUserValidator.exe	UserValidator Module
NmxSvc.exe	NmxSvc Module
slssvc.exe	SuiteLink Inbound Connection Service

While there is no specific error message in the SMC logger that explicitly indicates a frozen or locked process, unpredictable system behavior can be sufficient reason to check these processes.

You can determine non-responsive processes using:

- SMC Error Logger message, which includes component name and description.
- Windows Task Manager and sorting by process name (aaEngine aaBootstrap, etc.).
- Microsoft Event Viewer application and the System Logs for additional information, where applicable.

The following sections explain how to eliminate or minimize the factors.

File Locking

File Locking is typically caused by such popular application types as:

- Anti-Virus software
- Back-up software or Microsoft Volume Shadowing Copy Service
- Windows Indexing Service
- Defragmenting Software
- Other disk intensive applications/ scripts

Symptoms of File Locking

The following conditions can occur as a result of locked files:

- Setup hangs when installing and registering the **LMX.DLL** file.
- Checkpoint errors appear in the Logger. For example

  INVARIANT FAILED LINE 489 FILE U:\MagellanDev\src\EngineServices\Checkpointer\CheckpointFileServer
- **Moved file failed** error in the logger.
- The redundant App Engine uses all available RAM, and the system does not respond.
- The status of the Standby Engine is **resyncing with partner**, and uses up to 100% CPU.

Avoiding Locked Files

Exclude key IAS files and directories from being scanned, as listed in the FSA2 Deployment Guide and the **Read Me** file on the Application Server Installation CD.

Perform maintenance, backups or other disk-intensive operations during a planned maintenance window with scheduled downtime (where applicable). Files are often locked during the back or copying process. In a running App Server environment, this can cause issues with

the checkpoint files and can result in system instability.

Security Restrictions

Typical Security Restriction conditions include the following items:

- Security Controls that prohibit DCOM, Shared Network Folders, or other file level security constraints imposed either by local or remote group policies. A common example is a Group Policy Object pushed from an Active Directory implementation on the domain.
- Operating System-, Hardware-, and Software-level firewalls.
- Local User-based permissions (i.e., **User**, **Power**, **Administrator**). Ensure the user being invoked has the matching permissions that the application requires.

  Ensure that "background" users are correctly verified for appropriate security levels. For example, users with **NT AUTHORITY\Network Service** and **ArchestrA Network User Account** permissions.

  When working with any kind of Web Services, check the IUSR and IWAM accounts.

Symptoms of Security Restrictions

The following conditions can occur as a result of incorrect Security Restrictions:

- DCOM errors in the Window Event Viewer.
- Deploying Platforms Engines, Areas and Objects fails and generates the following errors:
  - `Failed to deploy Platform <PlatformName>: remote node's UserID/password don't match the GR Node.`
  - `Error: The Server is unavailable HRESULT=80070005 after failed deploy.`
  - `Error: Failed to deploy Platform <PlatformName>. Cannot communicate with remote node version information from bootstrap.`
  - `Error: Failed to deploy code modules to target when deploying objects to another node.`
- User error messages in the Wonderware Logger:
  - `ImpersonateUser failed(0x8000401a). ArchestrA Admin user has not been setup or machine is shutting down.`

Avoiding Security Issues

For Windows 2003 and Windows XP, run the Wonderware O/S Configuration Utility.

> **Note:** If your system is part of a Window 2000 or Windows 2003 Active Directory Domain, your network administrator may need to manually change the settings. Contact wonderware technical support for further information.

- Ensure that any corporate level Group Policy Object's are permanently configured and aligned with the required application permissions.
- Configure any network hardware to allow proper network traffic
- Use an administrator level account for any application installations

Lack of System Resources

Lack of System Resources is broadly defined as:

- Low Memory
- High CPU Usage
- Intensive Disk Usage
- Intensive Network Traffic combined with and/or causing Low Bandwidth

Mitigating or Avoiding System Performance Issues

- Monitor your system's Memory, CPU, Disk Usage, and Network Bandwidth on a regular basis to ensure the proper resources are available relative to system load.
- Use diagnostic tools or information such as Microsoft Performance Monitor to trend resource utilization over time. See **Tech Note 329** for details.
- Refer to IAS Engine Statistics that are provided by default when an IAS engine is deployed. For example, check for Scan Overruns or the **Scheduler.CheckpointPeriodAvg** attribute, viewable from Object Viewer.
- When analyzing an IAS Redundant partner, ensure that it is capable of supporting two nodes in the event of a failover. A "good rule-of-thumb" is that the CPU should average 30-40 % or less per processor on *both* nodes in the redundant pair.
- Follow best-practices for Architecture and Plant modeling as described in the FSA2 Deployment Guide.
- Leverage the Wonderware Historian by historizing Platform and Engine performance metrics for trend analysis.
- Distribute intensive databases across multiple nodes.
- As architecture requirements increase, it is more effective to have a highly-distributed network of entry level Automation Object Servers (AOS) rather than a small number of powerful and centralized Automation Object Servers.
- Keep all software running at its latest major version, patch, or service pack level.

File Scan Exclusion List for Anti-Virus Software

If your Anti-Virus software is configured to scan all system files, Application Server system performance is negatively affected.

After installing Application Server, configure your antivirus software to prevent archive files from being scanned. Also, antivirus software should not scan files in the following ArchestrA folders (ensure subfolders of the listed directories are also excluded):

- 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:\Documents and Settings\All Users\Application Data\ArchestrA

From Application Server Platform Objects

- History Store Forward directory, if not the default.

From Application Server Engine Objects

- Checkpoint directory location, if not the default.
- <InTouch Application folder path> including:
  - C:\Documents and Settings\All Users\Application Data\ArchestrA\<SMCLoggerStoragefilepath>.

    The default is: C:\Documents and Settings\All Users\Application Data\ArchestrA\LogFiles\
- SQL Server database files of type **.mdf** and **.ldf**.

Other Information

For related information, refer to the following *Tech Note(s)*:

- **Tech Note 478 Industrial Application Server Platform Deployment Checklist**

S. Kermani, K. Lovejoy

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