DAServer Does Not Appear in the DAServer Manager of the System Management Console (SMC)

Legacy Tech Note

576

SUMMARY

Sometimes, after successfully installing a Wonderware DAServer, the DAServer is not available in the DAServer Manager in the System Management Console. This *Tech Note* discusses reasons why this may occur and how to correct issues that are causing this problem.

This problem can occur due to one or more of the following reasons.

- Integral DCOM Components have problems with their DCOM Identity credentials.
- The account used during the DAServer installation does not have local administrator privileges.
- Part of the hierarchy in the DAServer Manager is missing.
- Data Execution Prevention is enabled on the computer. This setting can prevent the System Management Console (SMC) from working properly.
  - For XP, Server 2003, and earlier OS.
  - For Vista, Windows 7, Server 2008 and later OS.
- There is a problem with the information entered for the ArchestrA network account.

SITUATION

Tasks

This information lists a series of tasks you can complete to diagnose and fix the problems.

Verify the Identity Credentials for Integral DCOM Components

1. Open Component Services (**Start > Run > DCOMCNFG**)
2. Navigate to **Component Services > Computers > My Computer > DCOM Config**
3. Locate **DAS_Agent** component, right-click and choose **Properties** and go to the **Identity** tab
4. It should be set to '**This User**' and the user name and password should match the account that is used in the Change Network Account Utility (Start > Programs > Wonderware > Common > Change Network Account)
5. Re-enter the password to confirm that it is correct, press OK to save.
6. Repeat steps 3 through 5 for the **IOSrvCfgPersist** DCOM component
7. Reboot and see if the problem is resolved.
8. If the problems remains, continue with the steps in the remainder of this Tech Note

Verify the Login Account Used During the DAServer Installation is a Local Administrator

To determine if a user is a local administrator

1. Open **Control Panel**, then **Administrative Tools > Computer Management**.
2. In the Computer Management console, expand **Local Users and Groups**, then **Groups**.
3. Double-click **Administrators** to view the Administrators list. The account used to install your DAServer should be a member of this group.

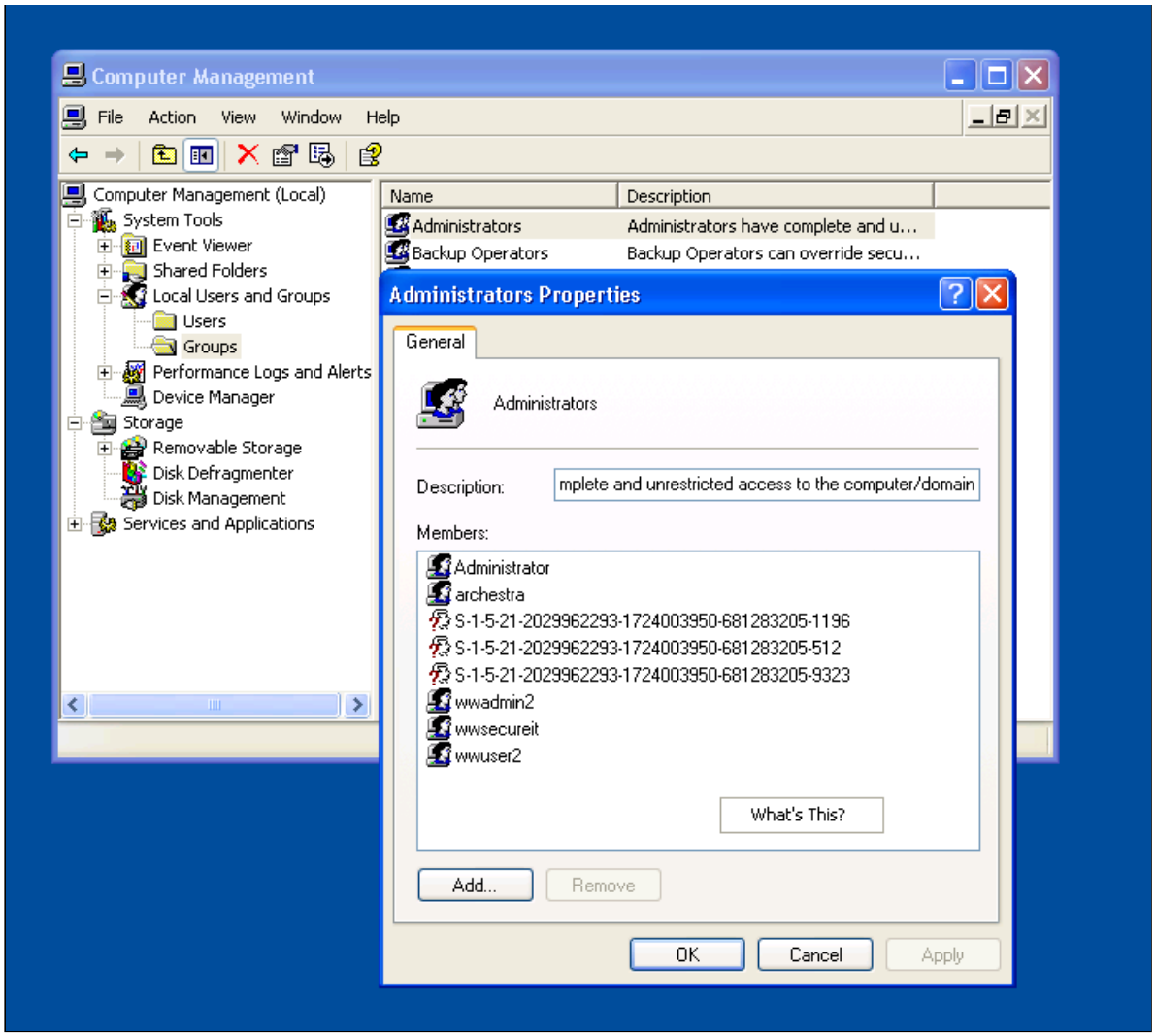

Figure 1: Verify the Administrator Account Used to Install Your DAServer

If this user is not an Administrator, the DAServer was not installed properly.

4. Log into an account with Local Administrator privileges, and *uninstall* the DAServer.

Note: You may want to go through the rest of the tech note before re-installing the DAServer to make sure there are no other issues that will prevent the DAServer from appearing in the SMC.

Verify that No Part of the Hierarchy is Missing from the DAServer Manager

1. Expand the **DAServer Manager** root in the SMC.
2. Under the DAServer Manager root you should see a group called **Default Group** (Figure 2 below).

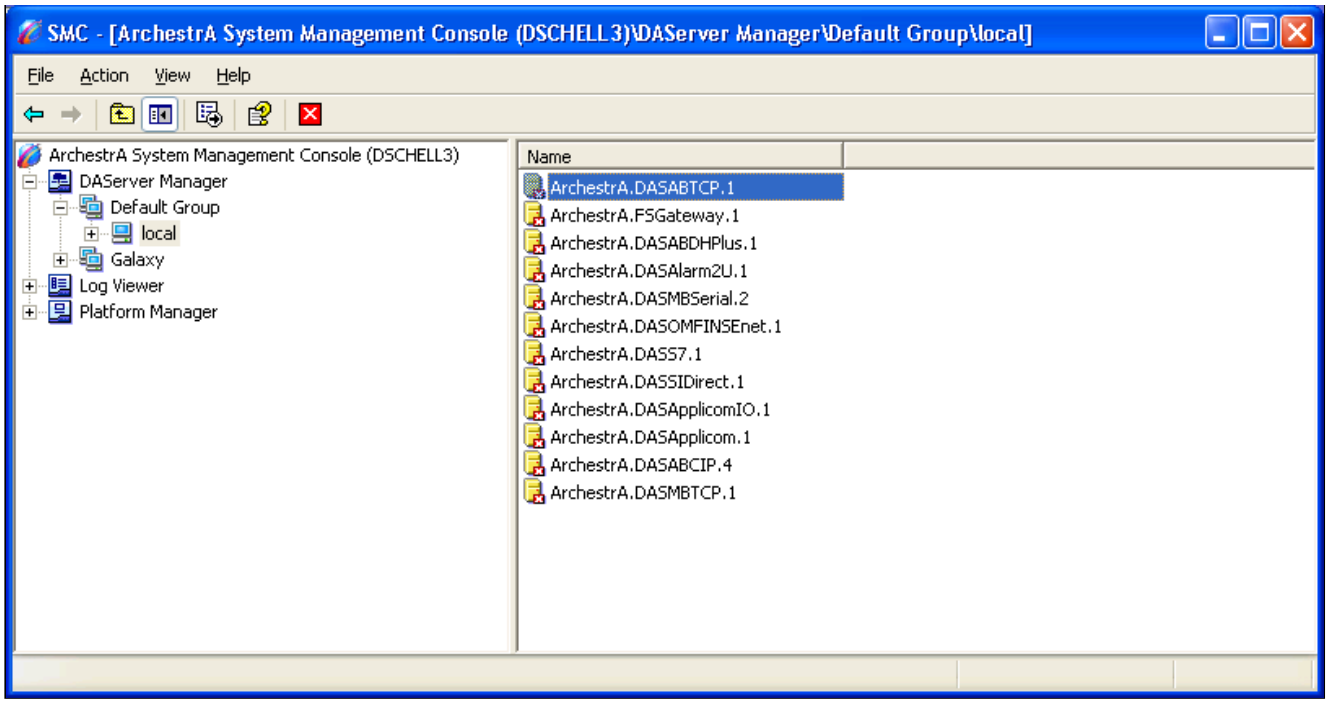

Figure 2: DAServer Manager Default Group

3. If the **Default Group** is missing, highlight **DAServer Manager** and then right-click.
4. Click **New** > **Node Group**.

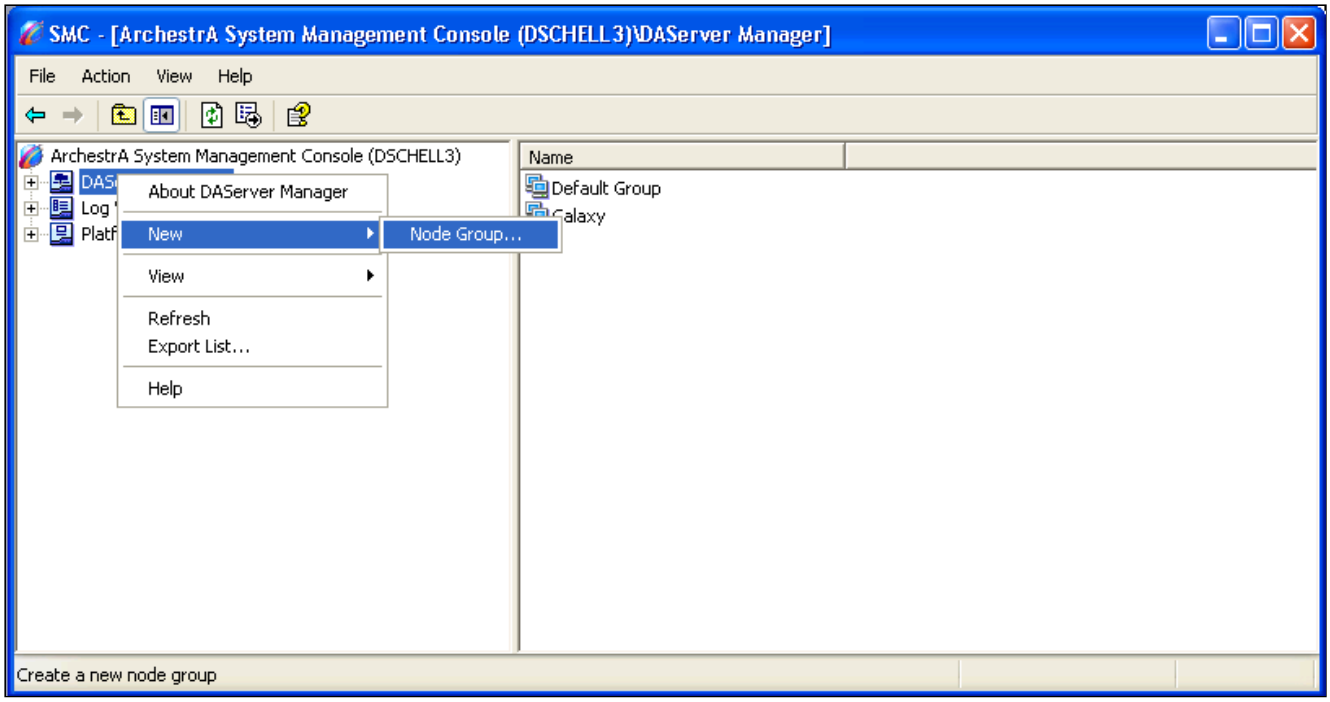

Figure 3: Create New Node Group

5. Type **Default Group** when prompted for a name.
6. Expand **Default Group**. A node called **Local** should appear under the **Default Group** root.

   If the **Local** node is missing, highlight **Default Group**.
7. Right click and select **New > Node**.

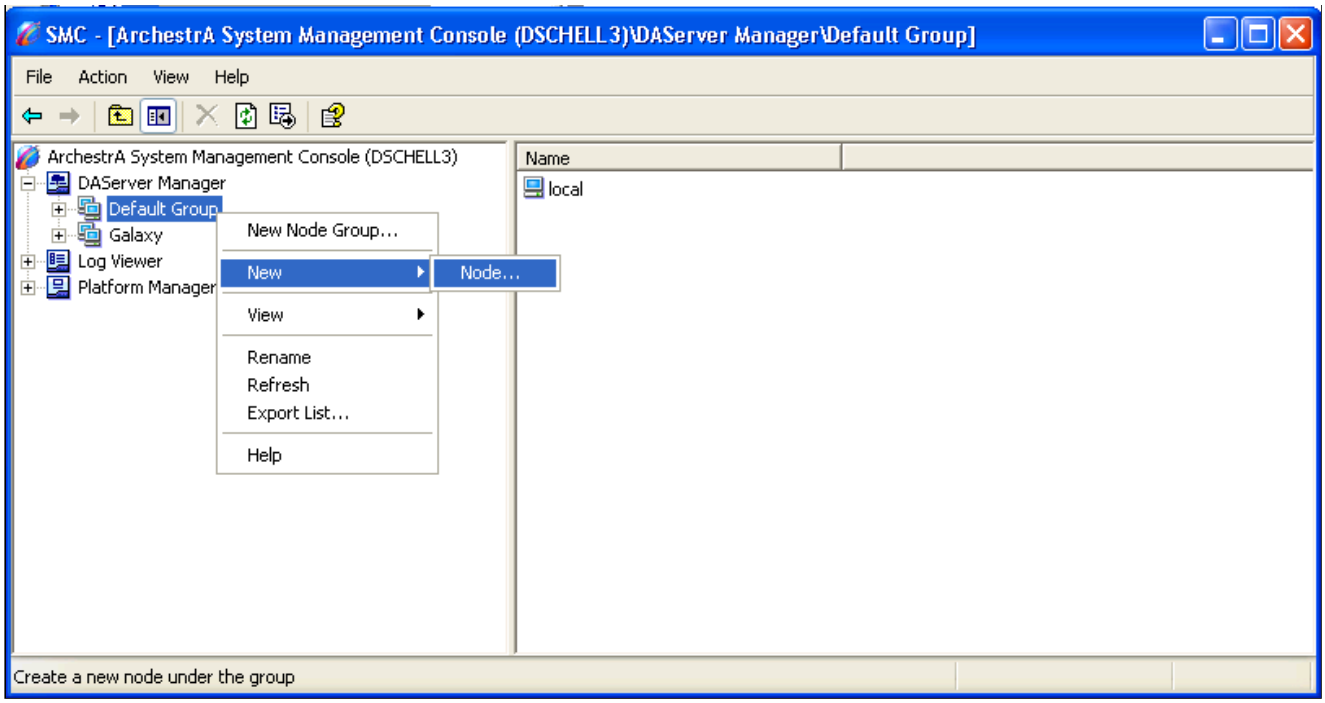

Figure 4: New Node

8. When prompted for a name, type **Local**.
9. Expand the new node. If there are no other problems, the newly-installed DAServer should now appear in the list. If the DAServer is now working correctly, your work is complete and you do not need to read the rest of this *Tech Note*.

Verify that Data Execution Prevention is Disabled - Windows XP, Server 2003 and Earlier Operating Systems

Note: For more information on Data Execution Prevention, see Technote 437: Unable to Open Logger under Windows XP SP2 and Windows 2003 SP1.

To disable Data Execution Prevention, you must modify the **boot.ini** file. This is an operating system file that is usually hidden and read-only. You can configure Windows Explorer to see the file location and to modify this file.

1. Open Windows Explorer and navigate to the **C:** drive. The **boot.ini** file should appear in the root directory of the **C:** drive.
2. If this file does not appear click the **Tools** menu and click **Folder Options**. Click the **View** tab.
3. Select **Show hidden files and folders**.
4. Uncheck **Hide protected operating system files**.

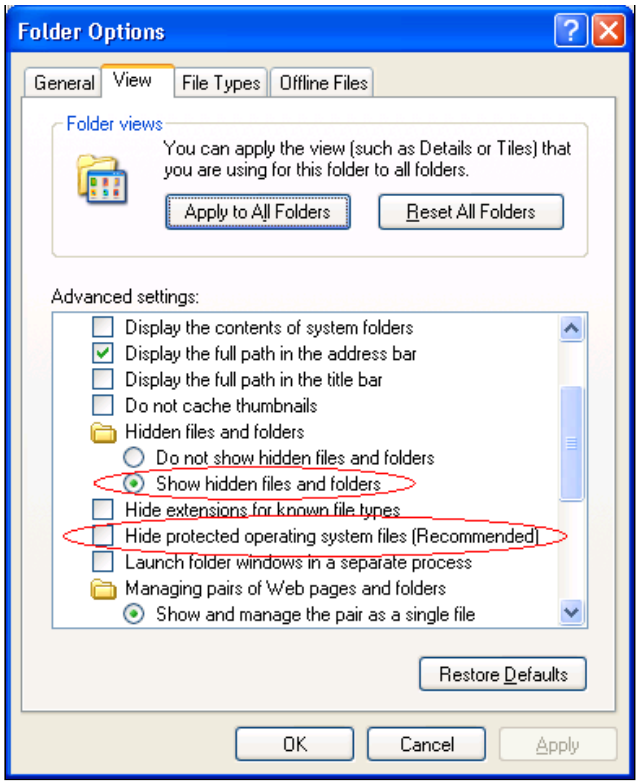

Figure 5: Configure Windows Explorer

5. Click **OK**. You should now be able to locate the **boot.ini** file.
6. Right-click **boot.ini** and click **Properties**.
7. On the **General** tab make sure that **Read-only** is unchecked.

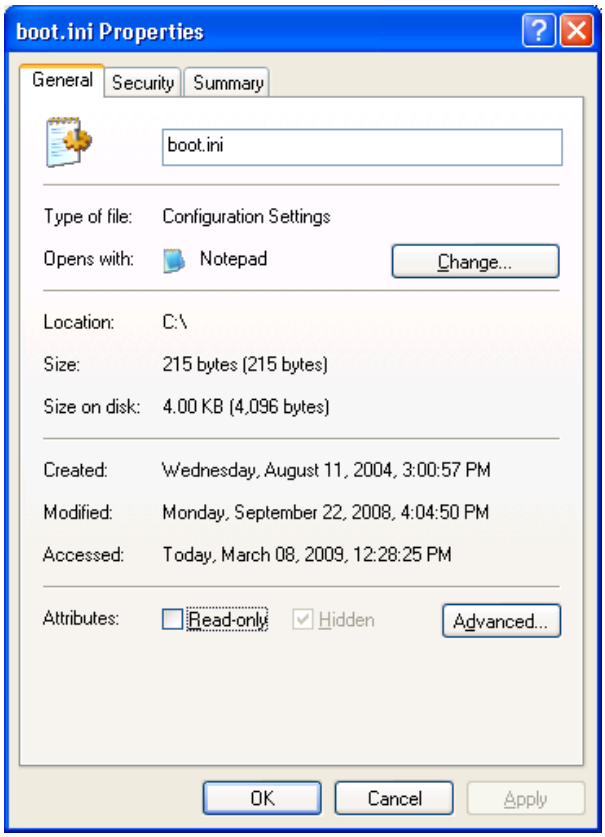

Figure 6: Configure Read-only

8. On the **Security** Tab make sure that the user you are logged in as has privileges to modify the file.
9. If you have made changes to the properties apply them.
10. Open the file using WordPad or Notepad. Look at the **noexecute** parameter in the last line in the file.
11. If this parameter is set to **OptIn**, **OptOut** or **AlwaysOn**, change it to **AlwaysOff** as shown in Figure 7 (below).

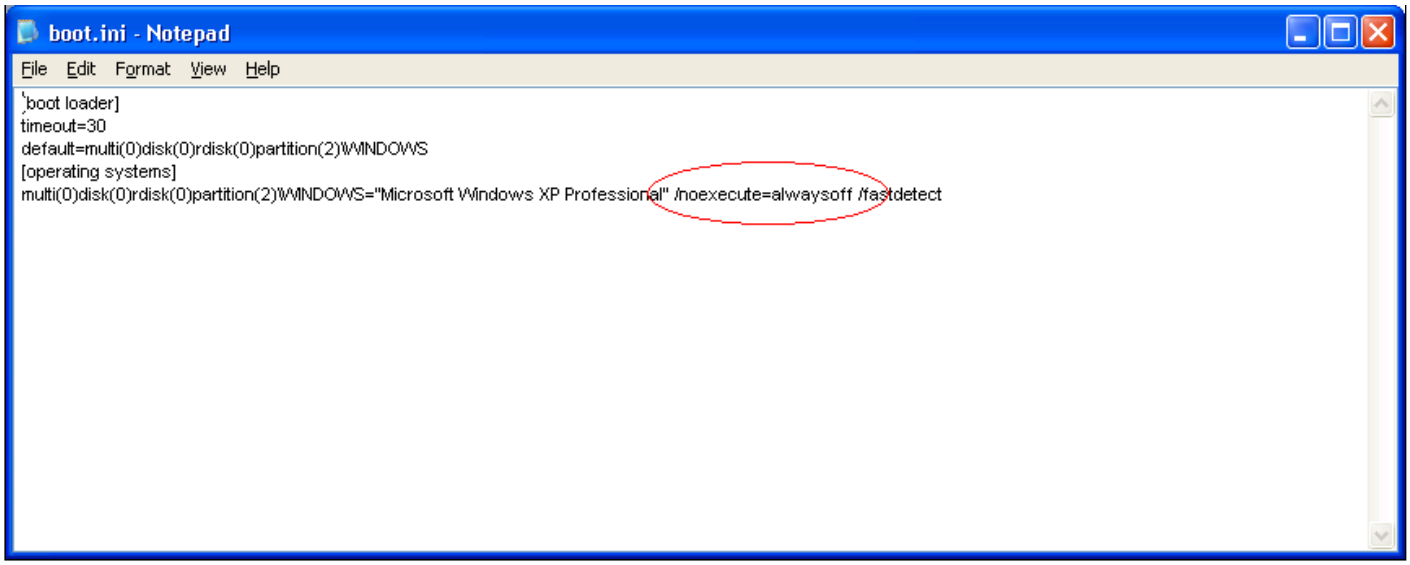

Figure 7: /noexecute=alwaysoff

12. Save the file, and restore the file attributes to their previous settings using Windows Explorer.
13. Restore the Folder Options to their previous settings.

These changes take effect when you restart the computer. However, the following task in the next section also requires a reboot. Complete those steps before restarting the computer.

Verify that Data Execution Prevention is Disabled - Windows Vista, Windows 7, Windows Server 2008 and Later Operating Systems

Beginning with Windows Vista, the **boot.ini** file no longer exists, so the procedure to configure DEP is different.

If DEP is enabled, you can manage the settings by doing the following:

1. On your desktop, right-click **Computer** and click **Properties**.
2. Click Advanced System Settings.
3. Click the **Performance Settings** button.
4. Click the **Data Execution** tab

To completely disable DEP as we need to do in this case, the boot parameters must be edited using Microsoft's BCDEdit command line utility.

1. Open a command prompt by clicking **Start > Run**, then type **CMD** and press enter.
2. To disable DEP (Always Off), type this command:

   bcdedit.exe /set {CURRENT} nx AlwaysOff
3. If for some reason you need to re-enable DEP (Always On), type this command:

   bcdedit.exe /set {CURRENT} nx AlwaysOn
4. These changes take effect when you restart the computer. However, the following task in the next section also requires a reboot. Complete those steps before restarting the computer.

Note: If you disable DEP and you are not able to start Windows, run Windows in safe mode and enable DEP again, using the command above. Start Windows in safe mode by pressing **F8** during bootup.

Verify the Information for the ArchestrA Network Account is Correct

All computers that have ArchestrA-enabled software installed must be able to communicate with each other. Communication is enabled through an ArchestrA-specific user account set up during the installation of an ArchestrA component on each computer.

You must use the same account on each computer that requires communication with other computers in an ArchestrA environment. The account must be a part of the Local Administrators group *on each computer* and the password should not expire. It is not necessary to log in as this account or to use this account to install Wonderware software.

To determine which account is used as the ArchestrA network account, use the Change Network Account Utility.

1. Click **Start > All Programs > Wonderware > Common > Change Network Account**.

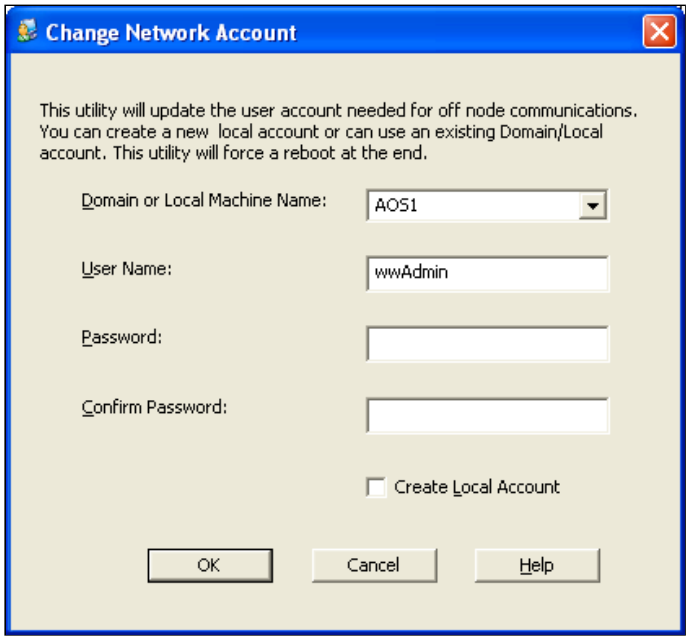

Figure 8: Change Network Account

If the password you typed in the Change Network account utility for this account is incorrect or too short, the DAServer Manager or Log Viewer may not work properly.

Wonderware does not require the password to be a certain length; however, on some computers a password shorter than 8 characters can cause problems. You may need to make the password at least 8 characters if you are otherwise unsuccessful at getting the DAServer to appear in the DAServer Manager.

2. If you have not uninstalled the DAServer by this point, uninstall it.
3. Re-type the password for the ArchestrA network account. This will cause the computer to reboot.

Re-install the DAServer

If you have made changes to the boot.ini file or to the ArchestrA network account, you should have uninstalled the DAServer and restarted the computer by this point in the *Tech Note*. If you have uninstalled the DAServer, reinstall it at this time.

The DAServer should now appear in the DAServer Manager under the **Local** node.

If it still does not appear, add another node to the **Default Group** in the DAServer Manager.

1. Highlight the **Default Group**.
2. Right-click it and click **New** > **Node**.
3. When you are prompted for a name, type the computer's network name instead of **Local**.

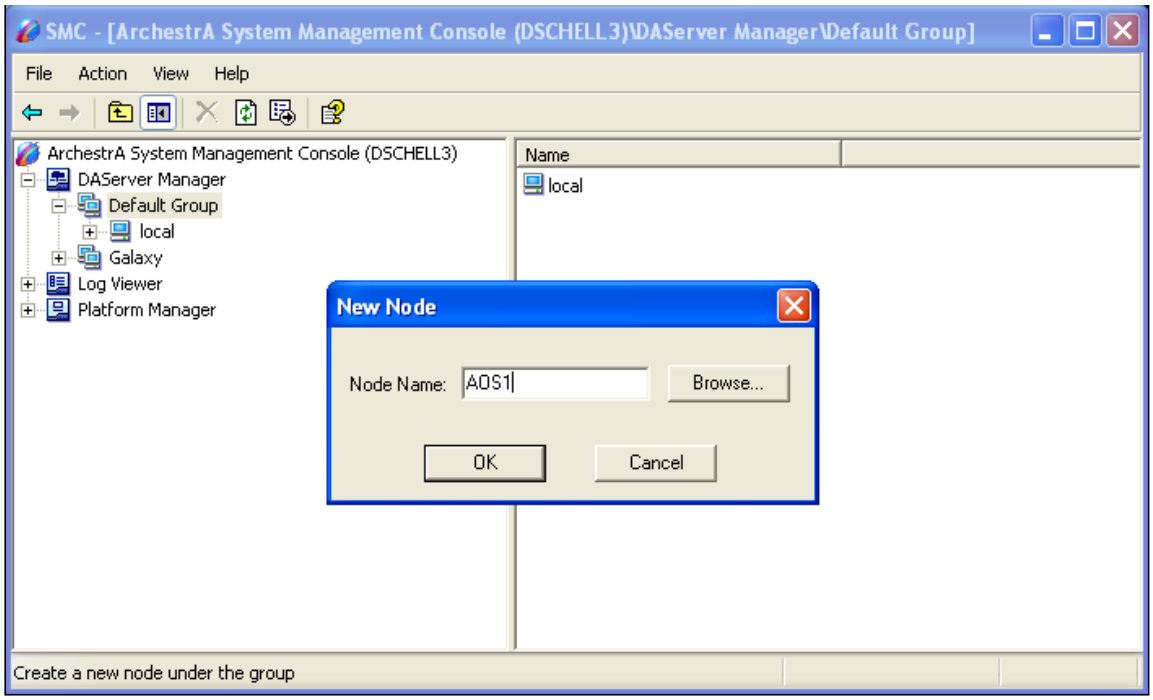

Figure 9: Create a New Node Using its Computer Name

4. Expand the node with the same name as the computer; the DAServer should appear in the list. Once it appears under the node with the computer name, it should also appear under **local**.

   If the DAServer does not appear in the DAServer Manager after following this procedure, contact Wonderware Technical Support for assistance.

MORE INFORMATION

Revised 01Apr2015 by D. Scott