Folder Virtualization concepts in Windows Vista

Vijay Raj

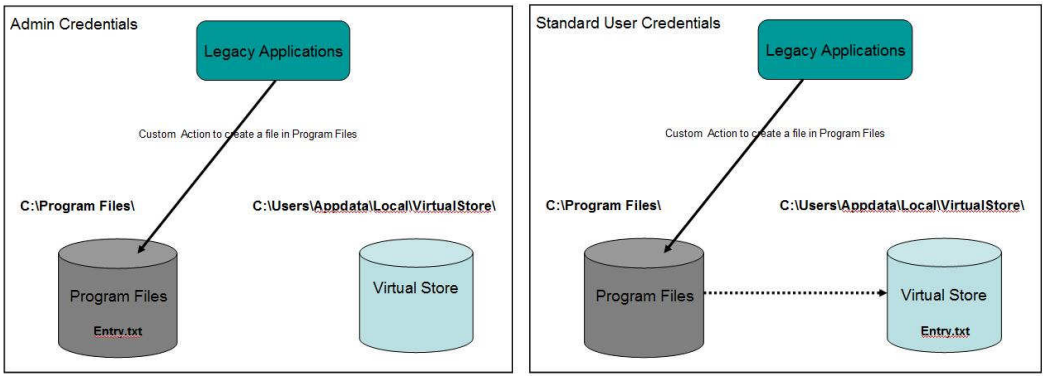
Introduction to Virtualization

Under User Account Control, Windows Vista restricts portions of the Windows file system and registry. UAC also restricts write operations during normal operation (i.e., standard user mode). For example, applications no longer have unlimited access to C:\Program Files and C:\Windows, which has considerable ramifications because most software created for Windows today expects unfettered access to all directories. The system-wide file system and Registry writes are automatically and silently redirected to per-user locations that won't harm the wider system.

To accommodate existing software for Windows that writes to protected file directories, Microsoft provides a backward compatibility technology known as Virtualization. While virtualization enables older applications to run without programmer intervention, it does not guarantee correct behaviour, and many applications will need to be updated to comply with UAC restrictions. Virtualization is often referred to as data redirection because it functions by funnelling attempted access to protected locations to new locations stored under user profiles. For example, if a legacy application attempts to write to the Program Files directory, UAC silently redirects that operation to an unprotected user-specific folder.

Virtualization Process

When an application installer attempts to write a file called Entry.txt in C:\Program Files, it is silently redirected to a Virtual Store directory located inside the current user's account. To the application, things proceed as normal, and it has no idea that it is being redirected. To the user, the application, too, still appears to be located at the old, expected location. But because the application is not access system-wide file locations, it cannot be used to harm the system. And on multi-user systems, each user will have isolated, local copies of redirected files. When this action is being invoked by a admin user, the file entry is done in Program Files itself. This is depicted in the figure below.



Registry virtualization works similarly. In this case, the HKEY_LOCAL_MACHINE\SOFTWARE hive is virtualized so that applications which attempt to store configuration information in system-wide portions of the Registry are re-directed to a new introduced structure under HKEY_CLASSES_ROOT\VirtualStore\MACHINE\SOFTWARE. As with file virtualization, each user on a system will have their own copy of configuration information that was previously issued once on a global basis.

Limitations of Virtualization

Virtualization is a stop-gap measure aimed at making legacy software work better in Vista. Microsoft expects Vista compliant applications to respect the new Windows application guidelines. And future Windows versions will do away with file system and Registry virtualization after more applications are moved to the new development style. This is short-term solution only.

Although most legacy applications created for previous versions of Windows will run because of virtualization, it is not an ideal solution and only intended to serve as a short-term workaround. Because virtualization isolates files in per-user locations, it can lead to undesirable and seemingly bizarre behaviour, especially on computers shared by multiple users.

Consider, for example, a test application created for Windows XP that performs quality assurance on products at the end of a manufacturing line. Like many existing applications, this software writes test data to a location in the Program Files directory. "C:\Program Files\QA".

Under Windows Vista, virtualization could affect the behaviour of the application. If you run the application on this machine using your standard user profile, Windows Vista automatically detects that you don't have permission to access that location and redirects the data to the following location:

C:\Users\<username>\AppDataLocal\VirtualStore\ProgramFiles\QA

Subsequent write and read operations performed under this user profile will always use the copy located in the Virtual Store. But, the application will continue to believe that it's accessing the Program Files directory. If a second operator logs into this computer under his or her profile, he or she won't have access to the previously saved data because it's not shared across user profiles.

While an administrator can forcibly disable virtualization in Windows Vista, Microsoft has vowed to remove it in a subsequent version of Windows. To ensure that software behaves as expected under all use cases in Windows Vista and beyond, you must update test systems so that writable files no longer appear in virtualized directories. In many cases, software rewrites may be minimal, but compliance with UAC restrictions could entail major architectural changes, depending on the application.

Steps to follow when virtualization is not needed

If the developer needs to install the application into C:\Program Files\ProductName\... and write into HKEY_LOCAL_MACHINE\Software\ProductName registry key then he can do these two things:

1) Provide a manifest file with the application where the credential level should be set to "asInvoker"

2) Provide a manifest file with your installer (or a separate helper EXE) where you mention level="asInvoker". Then give your installer (or a separate helper EXE) the ability to grant the 'Users' group write access into the C:\Program Files\ProductName\ and into the HKEY_LOCAL_MACHINE\Software\ProductName registry key so that, normal users have access.