Software Deployment Using Group Policy I

Software Deployment - Then and Now:

In the early days of computer networks, installing, supporting and maintaining software applications on a user's workstation typically *often required a personal visit* by a network technician.

New technology from Microsoft and Novell is now available to enable desktop software applications to be deployed and maintained remotely. Novell's technology is embodied in a product called ZenWorks for Desktops; in Windows 2008, Microsoft has provided Windows Installer to replace "Setup" and has incorporated remote software installation technology into Group Policy.

Windows Installer:

Microsoft actually purchased the "WinINSTALL" product from Veritas and included it in Windows 2008 as *Windows Installer*. This introduces the Windows Installer *package* or *.msi file* to replace the traditional Setup.exe file for installing new applications. All new Microsoft applications use .msi packages and many third party software vendors also use this format. The .msi format is required if you wish to take full advantage of the automated remote software installation technology in Windows 2008 Group Policy. It is possible to "repackage" older non .msi software using the WinINSTALL program.

Essentially WinINSTALL works by taking a “snapshot” of the Windows 2008 system *before* and *afte*r the installation of the software using it’s “setup” program or other installation method. WinINSTALL produces *the .msi file which documents the differences.*

The benefits of using Windows Installer technology are:

- *Custom installations* - optional features of an application can be visible without actually being installed. The feature will only be installed when the user first accesses the command for the optional feature. This helps reduce required hard disk space by only installing the parts of an application that the user actually uses.

- *Resilient applications* - if a critical file gets deleted or corrupted, the application will automatically return to the installation source and acquire a new copy of the file.

- *Clean removal* - applications can be uninstalled without leaving orphan files behind or inadvertently breaking another application by deleting a shared file.

- *Users only need READ access to installation folders* - deployed applications install using the elevated permissions of Windows Installer itself. Hence users do not need administrative permissions to their computers or the installation folders to install applications.

Group Policy Software Installation Technology:

If an organization has obtained a Windows Installer package file for an application it wishes to deploy, Group Policy may be used to automate the deployment process. This is done by *associating the .msi package with a Group Policy object* and specifying the desired deployment options. All the features of Group Policy (e.g. inheritance, etc.) will apply to the software deployment.

Besides initially installing a new application, Group Policy may be used to automatically perform a *mandatory or optional upgrade* to a new version and perform a *mandatory or optional removal* of an application.

A **mandatory upgrade** forces the new version to be installed to replace the old version the next time the user logs on. If a user had not previously installed the old version, only the new version will be available to install now.

An **optional upgrade** permits a user to continue using the previous version. If the user wishes, the new version may be installed and used as well as keeping the old version. If a user had not previously installed the old version, both the old version and the new version will be available to install now.

A **mandatory removal** forces the software to be uninstalled at the next user logon. The user has no choice in this matter.

An **optional removal** will permit users who had previously installed the software to continue using it. However no new installations of that software will be permitted.

The Software Life Cycle:

The software life cycle can be divided into four phases as follows:

1. **Preparation Phase** - the administrator must acquire the Windows Installer package file from the software vendor or in cases where this is not available, create the package file using WinINSTALL. Not all applications can be “packaged”; in this case you can create a .zap file (this is a text file) which can be used to “publish” an application (does not have all the features of a packaged application). You can also use package modifications which have a *.mst* file extension. These may be used to modify the base installation (e.g. install a different language).

2. **Deployment Phase** - the software is actually installed on computers. There are two main options for software deployment:

> **Assigning Applications**: the application is “advertised” on the Programs menu. Clicking the icon on the Programs menu or double clicking a document associated with the application (document invocation) will automatically install it. The application may also be installed through *Add/Remove Programs* in the Control Panel.
>
> **Publishing Applications**: the application is *not* “advertised” on the Programs menu. Users can install the application through *Add/Remove Programs* in the Control Panel or *optionally* via document invocation.

3. **Maintenance Phase** - software is upgraded or redeployed. A service pack is applied to currently deployed software or a new version is installed to replace a previous version. The upgrade or redeployment can be mandatory or optional as explained earlier.

4. **Removal Phase** - software can be removed using group policy. The removal can be mandatory or optional as explained earlier. Note that for software to be automatically removed, it must have been previously installed using Group Policy.

Deploying a New Application:

There are four main steps to deploying a new application:

1. Acquire or create a Windows Installer package file.

2. Place the package file and any related installation files in a shared folder on the network.

3. Create or modify an existing GPO to add the package to the *Software Installation* settings of the User or Computer Configuration section.

4. Select the required deployment options.

It is recommended that you test software deployment with a small selected “Testers” group prior to implementing an organization-wide rollout. This can be accomplished by creating a *Testers* security group, removing the Apply Group Policy permission from Authenticated Users and adding it to the Testers group only, until you are satisfied everything is OK.

Assigning Software Packages:

Software is usually assigned when an application is required by a user to do his/her job. Software may be *assigned to a user or to a computer.*

Assigned applications are resilient. If the application or any of its components are deleted or become corrupted for any reason, the *application will be reinstalled* the next time the user logs on or the computer restarts.

When you assign an application to the users in an OU, the program will be advertised in the Programs menu when the user logs on. The program will also be shown as available in the Add/Remove Programs of the Control Panel. The program will actually be installed when one of these events occurs:

1. The user clicks the icon on the Programs menu.

2. The user double clicks a file type associated with the application (document invocation).

3. The user adds the program using Add/Remove Programs in the Control Panel.

When you assign an application to a computer, no advertising takes place. However, the next time the computer is restarted, the application will be installed automatically. This ensures the application is available to *all users* of the computer.

When in doubt about assigning to a user or a computer, assign the application to a user. No hard disk space will be wasted.

Publishing Software Packages:

When an application is published, it is not installed or advertised. It is available to the user however in one of two ways: 1. Add/Remove Programs and 2. document invocation.

Using Add/Remove Programs:

Prior to Windows 2008, many organizations placed the Setup files for new applications in shared folders on the network and then allowed users to connect to these shares and install the applications themselves. For power users this was satisfactory, but for the average user, the process was somewhat unfriendly and error-prone. The Publishing process and Add/Remove Programs provided in Windows 2008 provides the following improvements to this process:

- Friendly names are provided for the installations (e.g. Microsoft Office 2010 versus \\Server4\Apps\msofc10\Setup)
- Centralized distribution - all applications are installed through Add/Remove Programs; it is not necessary for users to know the network location of the install files.
- Use of Windows Installer packages for simplified installation with minimal user intervention.
- Control over which software is available to groups of users. Only the published software for a given user is shown in Add/Remove Programs.

Using Document Invocation:

When an application is published, the administrator has the option to enable *Auto-install this application by file extension activation* (document invocation). In this case, the following happens when a user doble-clicks an unknown file type:

1. The computer sends a query to Active Directory to check if it knows of any applications associated with this file extension.

2. If Active Directory knows of such an application, it checks to see if the application has been assigned or published to the user.

3. If the application is assigned, it is automatically installed.

4. If the application has been published, the system checks if the Auto-Install option was selected and if so the application is installed.

5. If neither 3 or 4 above is true, Windows will ask the user what is to be done (i.e. open this file with what application).

Assigning Versus Publishing Applications:

- Assigned applications are *advertised* on the Programs menu; document invocation is *not* optional.

- Assigned applications are resilient, published are not.

- Assigned applications can be assigned to computers as well as users.