

## Building Your Virtual Desktop

### **P2V or Clean Build?**

You can create your original virtual desktop image in a number of ways, but essentially they break down into either performing a physical-to-virtual (P2V) migration on a target physical desktop or starting with a clean build. In most cases, a clean build is preferred, but there are always a few exceptions to this rule. For example, it may make sense to do a P2V migration to create a virtual desktop for a small proof of concept (PoC) environment. If you are considering this method, there are several issues to keep in mind, such as ensuring that after everything is converted, any services or configurations that are not applicable or detrimental to a virtual environment are updated. One of the common services is the power policy. On a physical desktop, it makes sense to have certain features power off if they are idle, such as dimming the display or putting the computer to sleep.

Often, cleaning an image that has been migrated from physical to virtual can be more problematic than building one from scratch. For any production implementation, using a clean imaging process is necessary. There are also a number of tweaks that you will want in place as part of the image. As mentioned in Chapter 3, “VMware View 5 Implementation,” you may also want to customize the local computer policy to ensure any configurations are incorporated into the image.

One point to keep in mind when you are optimizing a virtual desktop is that there are lots of recommendations to drive the ultimate performance. There is a fine line between great performance and the end-user experience, because the more you optimize, the more you impact the end-user experience. You do not want to drive performance at the risk of disabling useful end-user features. This is again the point at which user profiling adds value, but also knowing what effect you are having is key. Even when the optimization

seems benign, you have to be careful because it may lead to problems or issues down the road. My rule of thumb is to optimize and test and be wary of turning off useful features to drive every bit of performance out of the desktop.

One other issue that comes up quite often is whether you should standardize on the x86 or x64 version if you are deploying Windows 7. In general, if your virtual desktop is going to be deployed with less than 4 GB of memory, running Windows 7 x32-bit is ideal. If you plan to deploy desktops with memory requirements larger than 4 GB, 64-bit versions are better.

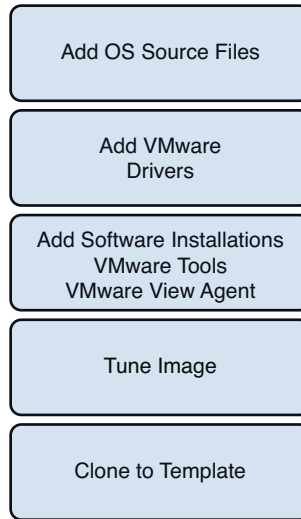
When we talk about imaging, we generally refer to source desktops and target desktops. *Source* generally refers to the image source desktop or VMDK or OVF file, and *target* describes the desktop on which the image or process is being applied.

If you are going to build the image from scratch, you can choose from three available methods: manually installing and configuring, using a desktop build process such as the Microsoft Deployment Toolkit (MDT),<sup>1</sup> or using a VM through vCenter to create an image build. VMware provides a straightforward process to perform an image build directly in vSphere/vCenter to ensure that the recommended optimizations for Windows 7 are incorporated into the automated build process.

We go through both the manual and automated build process. In the automated build process, we show how to extend the process to include ThinApp packages and also to manage the integration of Terminal Services, or Windows 2008 Remote Desktop Services as it is now called. The automated process starts with the OS installation files, necessary VMware drivers and tools, and View agents. The manual process requires installing the OS files, VMware drivers, and View agents; tuning; and then cloning the image, as shown in Figure 5.1.

---

<sup>1</sup>These procedures are based on the VMware View Optimization Guide for Windows 7 white paper from VMware.



**Figure 5.1** Building the desktop image.

Using MDT, you can create a Windows image file that can be applied to any desktop (virtual or physical), and you can build on the OS deployment with applications and custom tasks. Is the flexibility worth the additional time and effort? You have to look at the overall situation to make that determination.

If you are creating a master image that will be applied to a percentage of physical and virtual machines that may have many different application loads based on business unit, the additional effort spent on MDT makes sense. If you are running only virtual machines, you should use vSphere. If you have only one or two images with a fairly generic application load, the cloning and sysprep available within the virtualization tools are probably sufficient. In this book we go through the vSphere method of creating the Windows 7 image and some of the optimizations that should be applied to the image.

## Manually Installing Windows 7

When manually installing Windows 7, you should understand the following:

- System Requirements: The recommended minimum specs for Windows 7 are
  - 1 GHz 32-bit or 64-bit processor
  - 1 GB of system memory
  - 16 GB of available disk space

- Support for DirectX 9 graphics with 128 MB memory (to enable the Aero theme)
- DVD-R/W drive
- Internet access (to activate and get updates)
  
- The size of the virtual hard drive needed

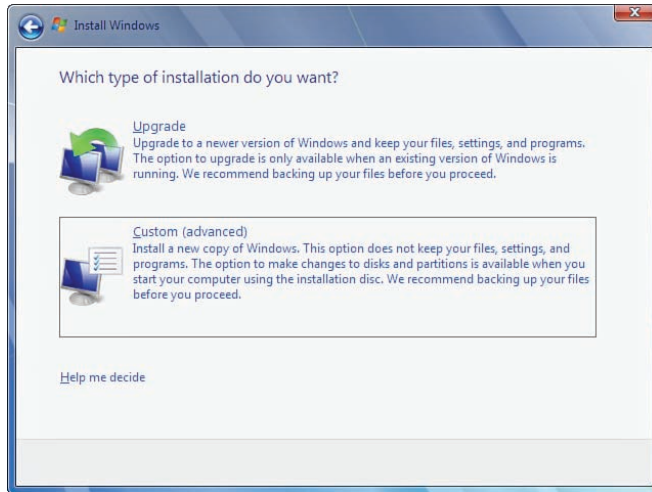
You need to decide whether to install the 32-bit or 64-bit version of Windows 7. The Windows 7 installation media includes both 32-bit and 64-bit versions of Windows 7. If you plan on using Windows 7 on a virtual machine with more than 3 GB of RAM, you should use the 64-bit version; otherwise, use 32-bit. Most programs designed for the 32-bit version of Windows work on the 64-bit version of Windows, so application compatibility is not typically a problem.

In creating the master image, you do a custom, or clean, installation. This installation formats the hard drive and installs a new copy of the operating system.

When installing on a virtual machine, simply map the virtual CD/DVD to the source ISO file and reboot the VM.

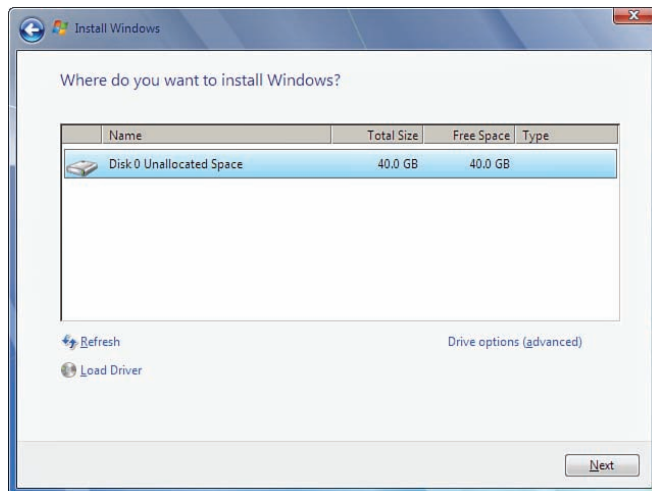
Like in Windows Server 2008, Windows 7 boots directly into the graphical user interface (GUI) mode.

1. After a few moments, you see the first prompt. Set whatever regional options are appropriate and click **Next**.
2. Click the **Install Now** button.
3. Accept the license terms and click **Next**.
4. Click the **Custom (Advanced)** installation type button, as shown in Figure 5.2.



**Figure 5.2** Select the custom installation.

Because this computer has a new virtual hard disk that hasn't been formatted previously, you have only the option to create a new partition on it. Click **Next** to begin the installation (see Figure 5.3).



**Figure 5.3** Format the unallocated space.

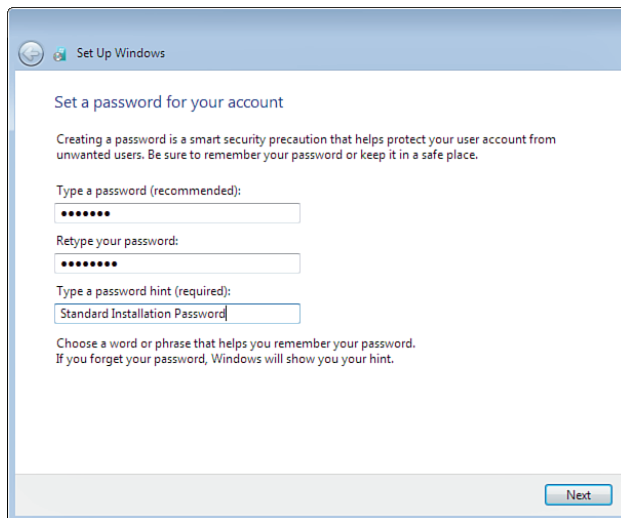
The setup process now begins to copy files from the installation DVD media virtually mapped to the virtual hard disk. This process might take awhile to complete.

After the setup is complete, the computer reboots. By default, the computer's name is *username-PC*, where *username* is the username you entered.

**NOTE**

The user you're creating is the only user currently available on the system.

5. Click **Next**.
6. Enter the user's password; this is the only user on the system initially. You must also enter a password hint (see Figure 5.4). Click **Next**.

The image shows a screenshot of the Windows Setup window titled "Set Up Windows". The main heading is "Set a password for your account". Below this, there is a paragraph of text: "Creating a password is a smart security precaution that helps protect your user account from unwanted users. Be sure to remember your password or keep it in a safe place." There are three input fields: "Type a password (recommended):" with a masked password of seven dots, "Retype your password:" with a masked password of seven dots, and "Type a password hint (required):" with the text "Standard Installation Password" entered. Below the hint field, there is another paragraph: "Choose a word or phrase that helps you remember your password. If you forget your password, Windows will show you your hint." At the bottom right of the window, there is a "Next" button.

**Figure 5.4** Provide a password.

7. Type in your product key. To avoid any problems, you should use the Multiple Activation Key (MAK).
8. Choose the type of protection for the computer: Use Recommended Settings, Install Important Updates Only, or Ask Me Later. In most cases, Use Recommended is fine. Make the selection.
9. Set the time zone, date, and time and click Next.

10. Select your computer's current location: Home Network, Work Network, or Public Network. On an internal corporate network, Work Network is the typical choice.
11. When the welcome screen opens, log in and check your installation.

## Manually Installing the VMware View Agent

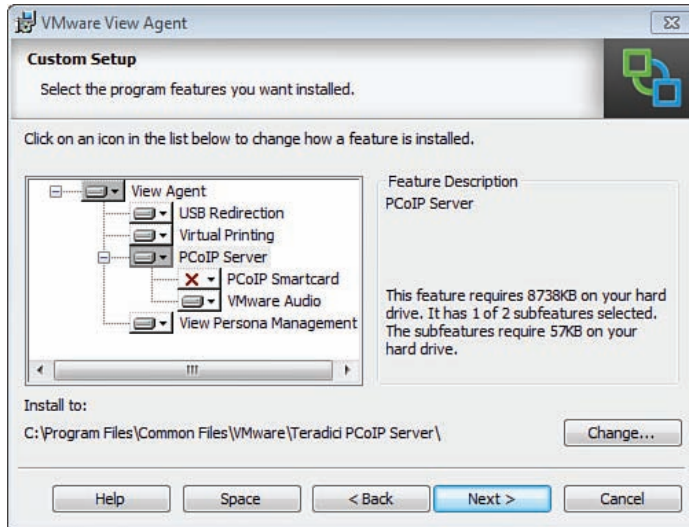
You are able to manually install the VMware View Agent. It is required on any desktop OSes or Windows Terminal Servers that you plan to offer through the View Connection Server. Separate install packages are available for the x86 and x64 operating systems, but the same package is used for both desktop and server operating systems. The components that get installed on a desktop versus a Terminal Server are different, however, as shown in Table 5.1. Features such as PCoIP and Persona Management are not supported on a Terminal Server. The platform is dedicated during the installation, and the unsupported components are not available for installation based on the OS.

**Table 5.1** Components Supported on a Desktop Versus Terminal Server

Guest Operating System	Version	Edition	Service Pack
Windows 7	64-bit and 32-bit	Enterprise and Professional	None and SP1
Windows Vista	32-bit	Business and Enterprise	SP1 and SP2
Windows XP	32-bit	Professional	SP3
Windows 2008 R2 Terminal Server	64-bit	Standard	None and SP1
Windows Terminal Server	64-bit	Standard	SP2
Windows 2003 R2 Terminal Server	32-bit	Standard	SP2
Windows 2003 Terminal Server	32-bit	Standard	SP2

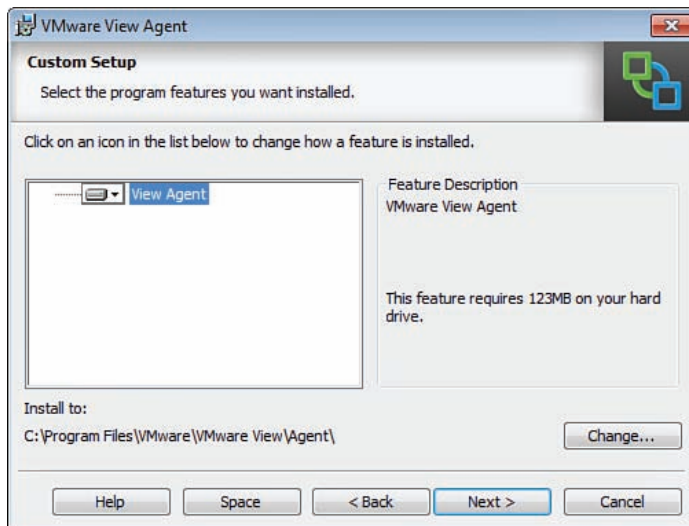
To install the VMware View Agent manually, follow these steps:

1. Ensure you use the appropriate installer depending on whether you are installing on the x86 or x64 platform. Launch the installer and click **Next**.
2. Click **Next** on the patent agreements.
3. Accept the license agreement and click **Next**.
4. If this is a Windows 7 virtual desktop, all the components are eligible for installation. Accept the defaults (see Figure 5.5) and click **Next**.



**Figure 5.5** Installing the View Agent.

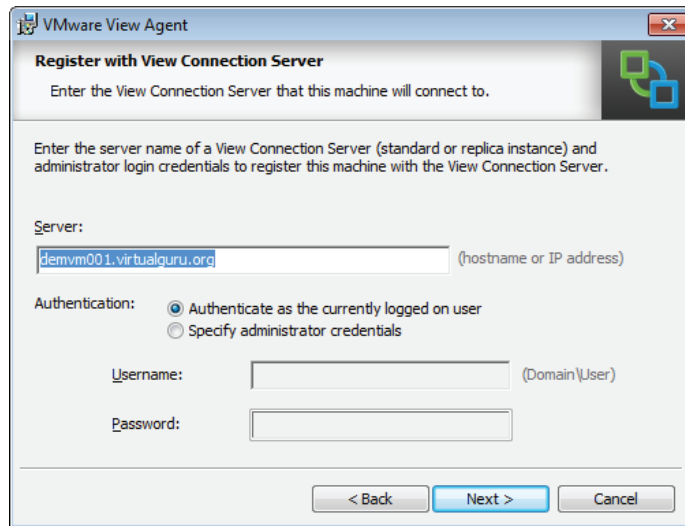
Figure 5.6 shows what the same screen looks like when installed on a Windows 2008 R2 RDS server. Note that many of the features are available for installation on the server platform.



**Figure 5.6** View Agent installation on a Terminal Server.



5. Specify your View Connection Server information and an account that can authenticate to the server. If you are the administrator on the View Server, you can select **Authenticate as the Currently Logged On User**. Click **Next** (see Figure 5.7).



**Figure 5.7** Specify the View Connection Server information.

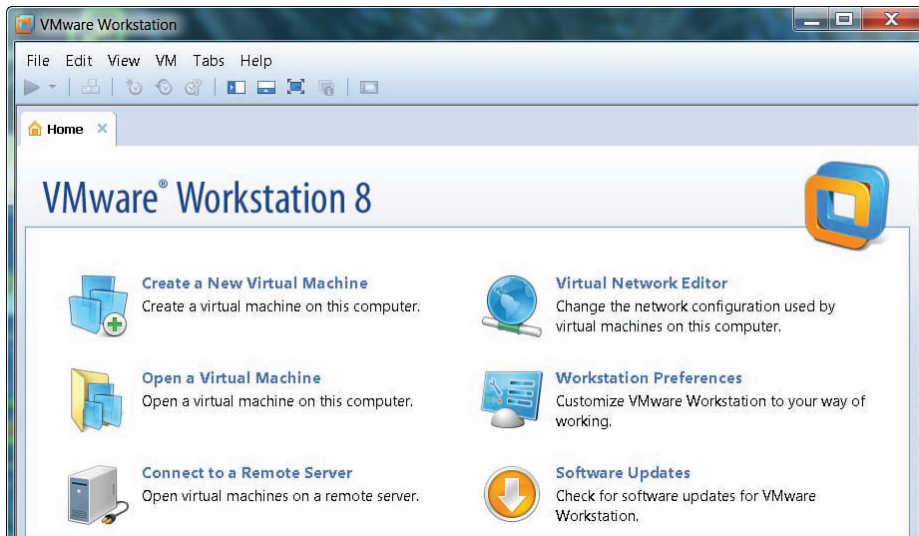
6. Click **Install** and watch the install process on the progress bar.

When everything is installed, you will notice a new service running called the VMware View Agent.

## Installing Windows 7 Through VMware Workstation

In an environment where vSphere is deployed, very often you will find an IT administrator with VMware Workstation installed to do common tasks such as image building. With version 8 of VMware Workstation, you can directly connect to a vCenter or vSphere environment. If you combine the automated image build process Workstation 8 with the direct connection to vCenter, you have a very efficient and simple way of building desktop golden images for your environment.

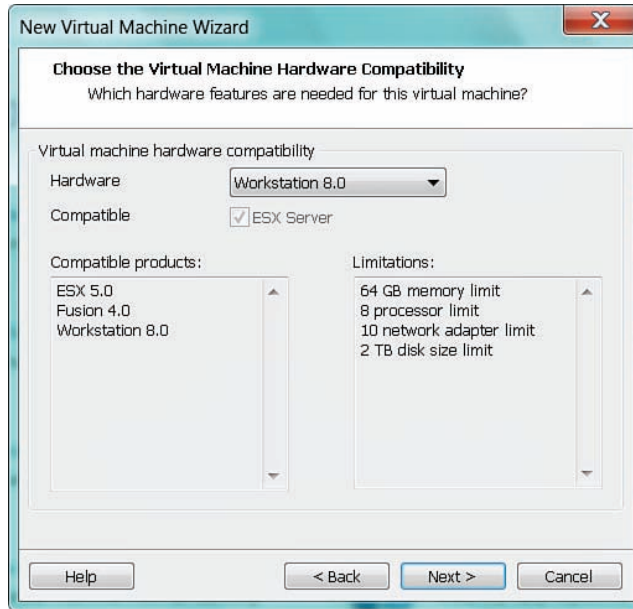
We explain here how easy it is to build and deploy an image to the vCenter from VMware Workstation 8, as shown in Figure 5.8.



**Figure 5.8** VMware Workstation 8.

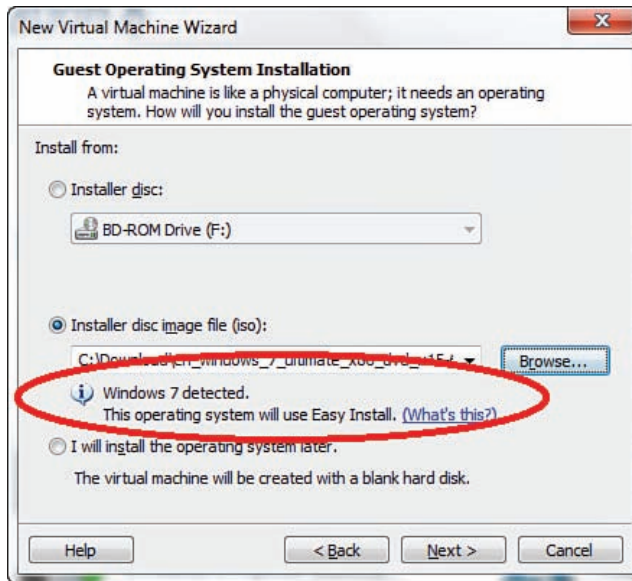
You start by choosing the **Create a New Virtual Machine** option in the main screen of Workstation. You then choose the **Custom (Advanced)** installation. Be aware, however, that there are a few parameters you need to adjust for preparation of a gold image for View.

Make sure you choose **Workstation 8.0** for hardware compatibility (see Figure 5.9); this is a requirement for ESXi 5.x, which we suggest you use for the deployment of a View 5.x environment.



**Figure 5.9** Hardware compatibility choices.

The next few steps are familiar and most IT administrators will recognize them. In the Guest Operating System Installation screen, browse to your installation media, which should be either a Windows 7 x32-bit or 64-bit ISO file. Because you are using Workstation 8, if the software properly detects the ISO, it tells you that it can use the Easy Install process, which basically installs the new OS automatically without user interaction, as shown in Figure 5.10.

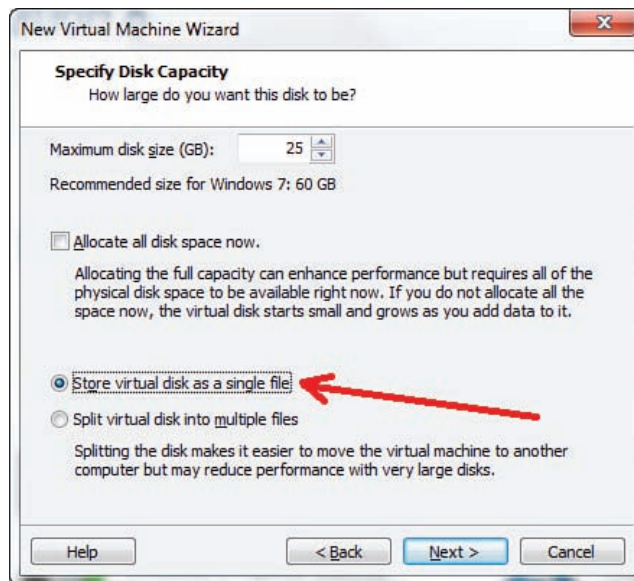


**Figure 5.10** Easy Install process selection.

You should configure the next few screens as follows:

1. Enter the product key (remember to use an MAK key or KMS Server).
2. Specify a local administrator account with a complex password. (It is important to note that because you're using the Easy Install process, you should not use Administrator as the username. VMware Workstation is already using that name. Just choose something different.)
3. Put in the virtual machine name. This is the name used locally in VMware Workstation because you are not linked to vCenter yet.
4. Choose the number of processors and number of cores per processor. To make the right choice, you have to go back to your requirements and make sure that the choice you make here will meet your specifications. If uncertain, choose one core and one processor. Windows 7 is peculiar when you are removing a vCPU; it supports moving from single to multiple, but not the other way around.
5. Choose the memory for this virtual machine. It should match your requirements. For a Windows 7 image, it generally should be between 1 and 4 GB, although you may have specific memory requirements.

6. Select the network type. The type is important because it enables you to make any additional changes to the virtual image after the install. You can leave the default setting using Network Address Translation (NAT).
7. Change the controller type to LSI Logic. As an optional step, you can even update the driver from the manufacturer website after the Easy Install is complete. Look for LSI\_U320\_W2003\_IT\_MID1011438.zip from www.lsi.com.
8. Create a new virtual hard disk according to your application installation requirements with some additional space for growth. The Windows 7 base image is anywhere from 8 to 10 GB, so make sure you choose a disk size big enough for your users to be able to use applications and their documents, but not too big to overprovision. The default is 60 GB, which might be a little too big. Even though we're talking about linked clones, resizing closer to 30–40 GB is more reasonable. One important point to note: Because you are migrating this virtual machine to a vCenter environment, it is recommended you keep all information from the VM in one file (see Figure 5.11).



**Figure 5.11** Virtual machine disk size.

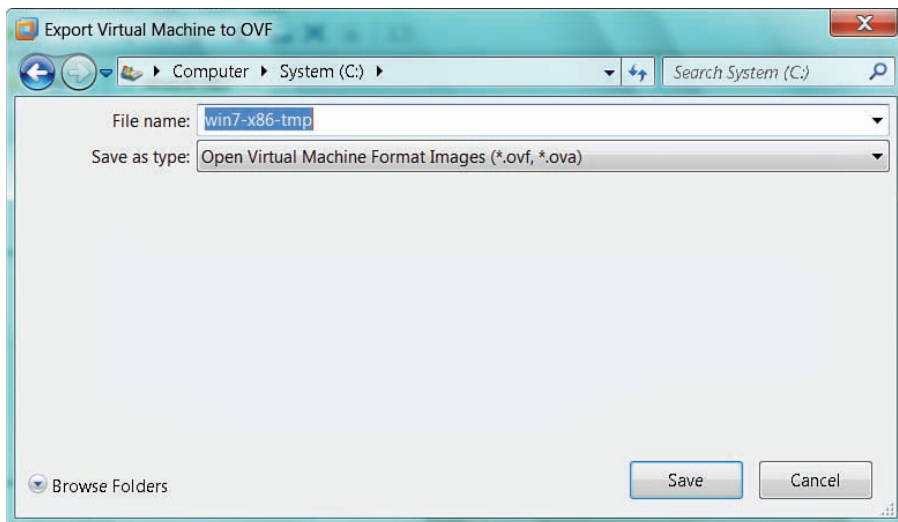
9. Specify the virtual machine location in this last step before the automated process starts. Use the local drive for now; you upload to vCenter later in this chapter.
10. If all the information was installed properly, you see VMware Workstation install the OS, reboot the VM, and install the VMware tools. If, for any reason, a step does not

work according to plan, you can always pick up where the automated install stopped and complete the installation. This process is straightforward and fast and it works!

When the Easy Install process is complete, you can log in to the virtual machine to check that everything is installed properly and that no outstanding messages need action. When you are satisfied with the results, shut down the virtual machine.

You have two choices regarding how to move this virtual machine to the vCenter. The traditional way is to open the vSphere client, create a new virtual machine, and point the VDMK to the new VM you created.

The second option, now available in VMware Workstation 8, is to export the VM you created in an OVF format. After you choose your virtual machine from the File menu, choose **Export to OVF** (see Figure 5.12).



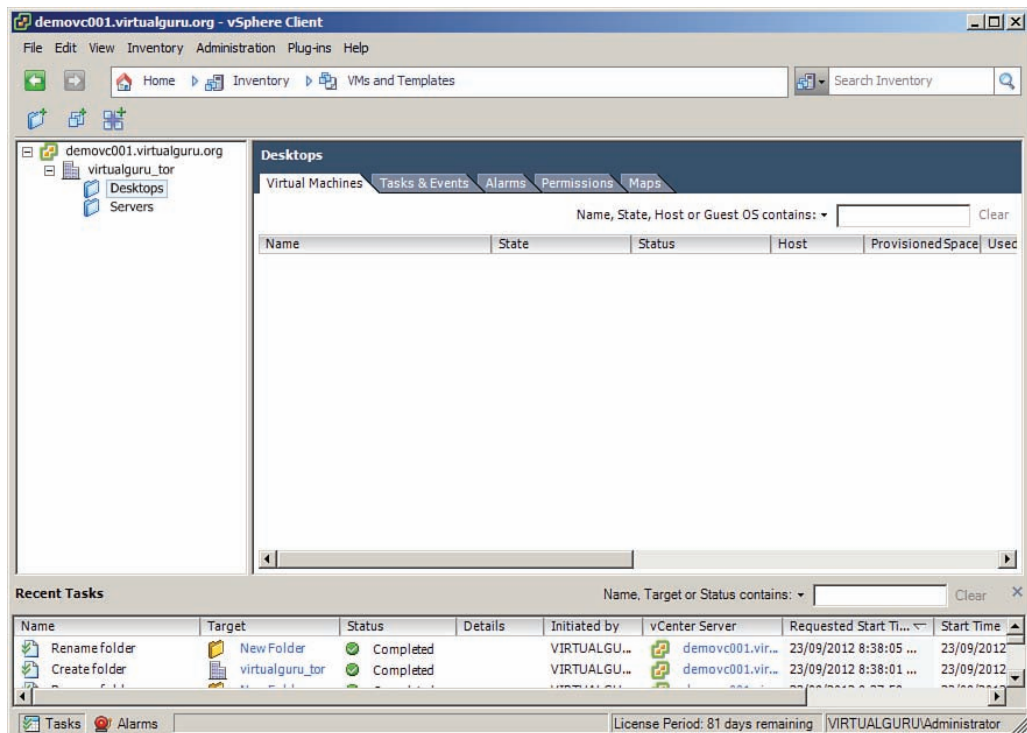
**Figure 5.12** OVF export for vCenter.

Then all you need to do is to go into your vSphere client and choose **Deploy OVF Template** from the File menu.

## Installing an Image Through vCenter

When you're ready to install an image through vCenter, it's a best practice to have a repository for your gold master images, a place where you keep all your references and corporately approved templates from which all your desktop images are spun off.

1. Start the vSphere client and connect to the vCenter.
2. In Home, Inventory, choose **VMs and Templates**.
3. Create a folder called **Templates**.
4. Create two subfolders underneath Templates and name them **Servers** and **Desktops**, as shown in Figure 5.13.



**Figure 5.13** VMs and Templates view.

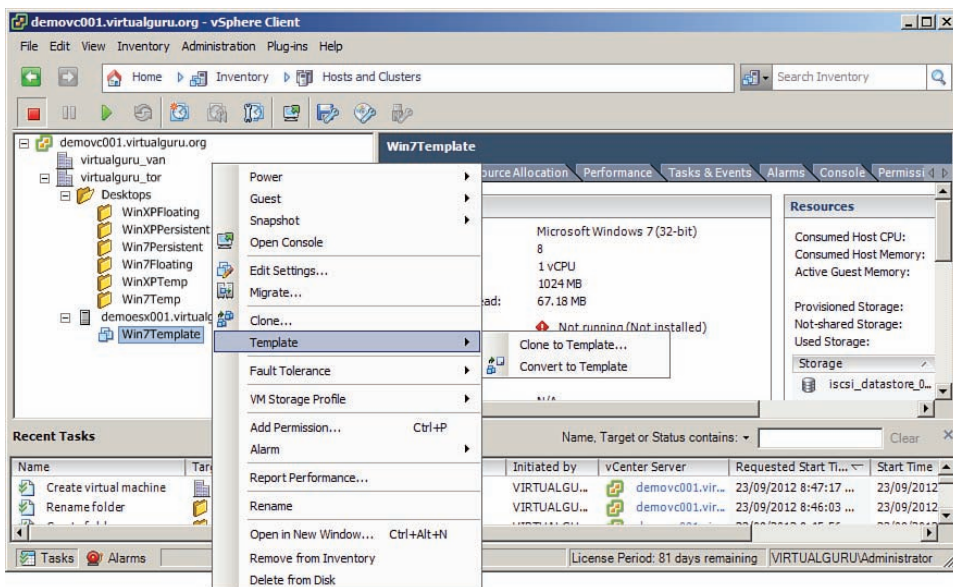
You need to complete a couple more preparation steps before you start the automated build process. You should create a hidden network share from which you will retrieve the ThinApp packages during or after the build process. It is also possible to combine ThinApp applications into your build if you have packaged them as MSIs. Keep in mind that if you do this, the applications will be deployed into the image versus “streamed.”

You should upload the master ISO files to your vCenter environment, into the datastore of your choice, one that will be accessible during the build process.

The steps to create your first Windows image are similar for the automated and manual processes. Rather than repeat the steps here, refer to the previous section “Manually Installing Windows 7” or “Installing Windows 7 Through VMware Workstation” for the steps for the initial image creation.

When the image is built, put it in the Templates\Desktops folder.

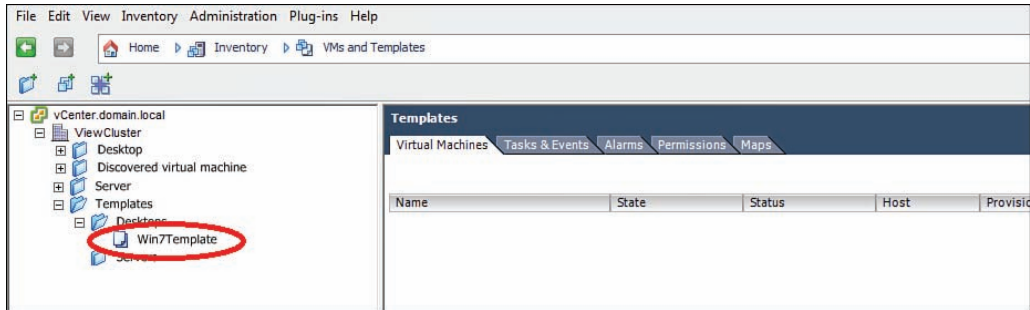
The goal of creating that initial image is to be able to convert it to a template. In the vCenter client, choose the image you just created and right-click it. Then choose **Template** and **Convert to Template** (see Figure 5.14).



**Figure 5.14** Template conversion.

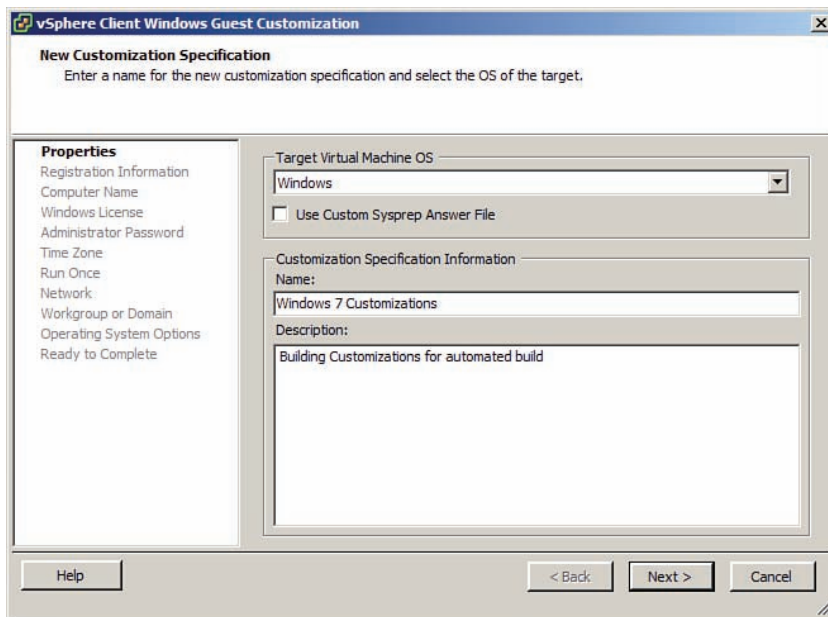
Choosing this option launches the conversion process. This step is actually pretty fast, and the final result is that the Virtual Image icon changes to a Template icon and is ready for you to use for the automated image deployment (see Figure 5.15).





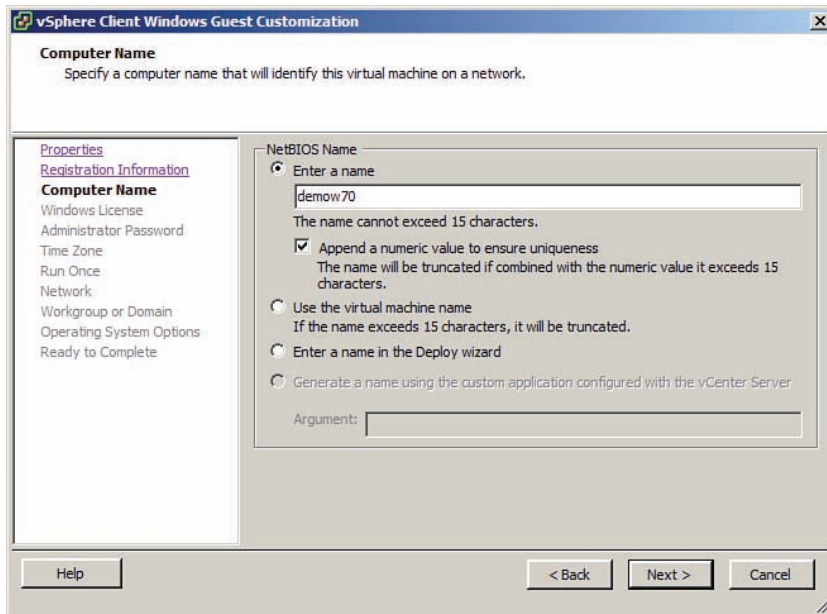
**Figure 5.15** Template icon change.

Put this image aside for now. The other part of this process is to create a new customization specs in vCenter. From the Management section of the home screen, choose **Customizations Specification Manager**. Then choose **New** to start the wizard you use to build an answer file for your image and specify any customization for the image, as shown in Figure 5.16.



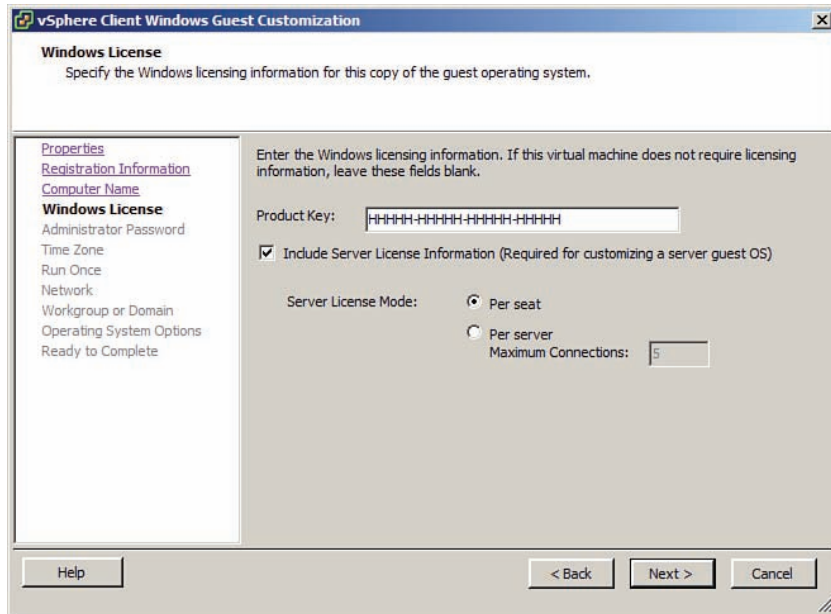
**Figure 5.16** Registration information.

The next screen asks you to enter your name and organization name. Then the following screen, shown in Figure 5.17, asks you to enter the computer name; this is a different name from what is used for the linked clones in VMware View. It is a good idea to enter a name that has meaning in the View build process; the OS and pool names are usually good choices.



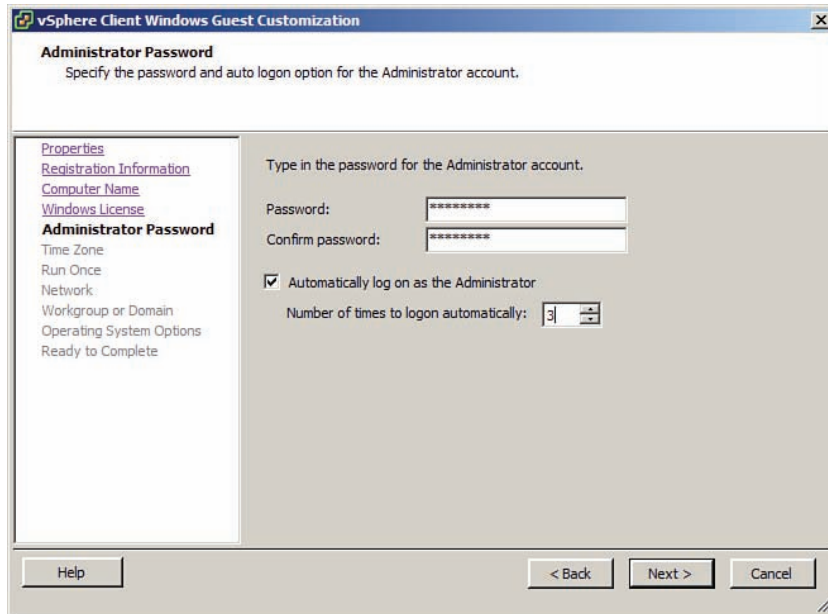
**Figure 5.17** Computer name.

The next screen, shown in Figure 5.18, asks you to enter a valid license key. Similar to the build process used earlier, it's a good practice to enter a Multiple Activation Key. This MAK can be the same one used in the earlier process, but it does not have to be.



**Figure 5.18** Windows product key.

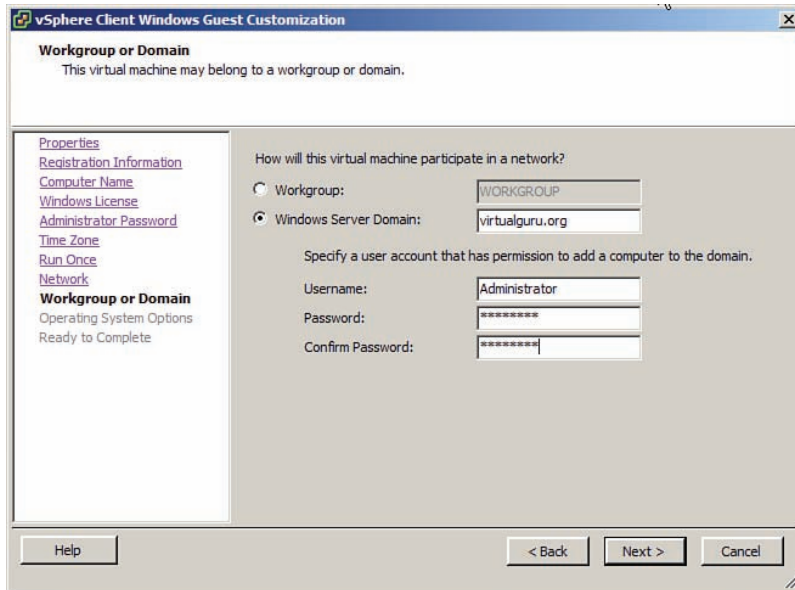
The next screen, shown in Figure 5.19, asks you to enter the credentials for the local administrator account that will be used during the automated image build. Because you will join this machine to the domain when it's being created, it's a good practice to enable the automated logon so that Windows is able to complete its build process and reboot a few times to make sure all steps are completed.



**Figure 5.19** Local administrator password.

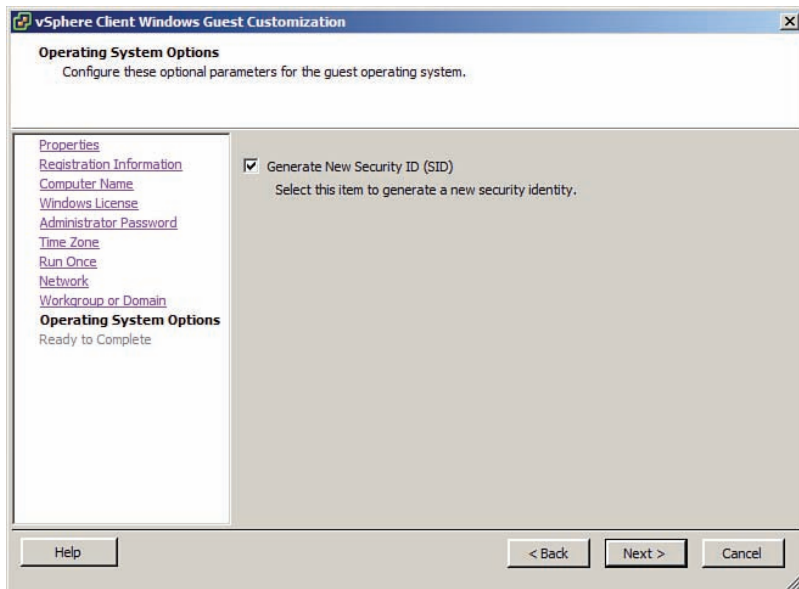
You are then asked for your time zone. You also can choose the Run Once option (for now, leave these settings at the defaults). On the following screen, enter the right network information. Choose a valid network and make sure to leave DHCP as your choice for IP address.

The following screen, shown in Figure 5.20, asks you to place the virtual image in the domain or leave it in a workgroup. This choice is totally up to you, but the important point to remember, in VMware View version 5 and forward, is that the gold master image does not have to be joined to the domain to be used as the reference image; you can leave it in a workgroup if you prefer. Remember that if you have Group Policy Objects (GPOs) applied to your image, it might be a better idea to place that image into a domain when it's being built.



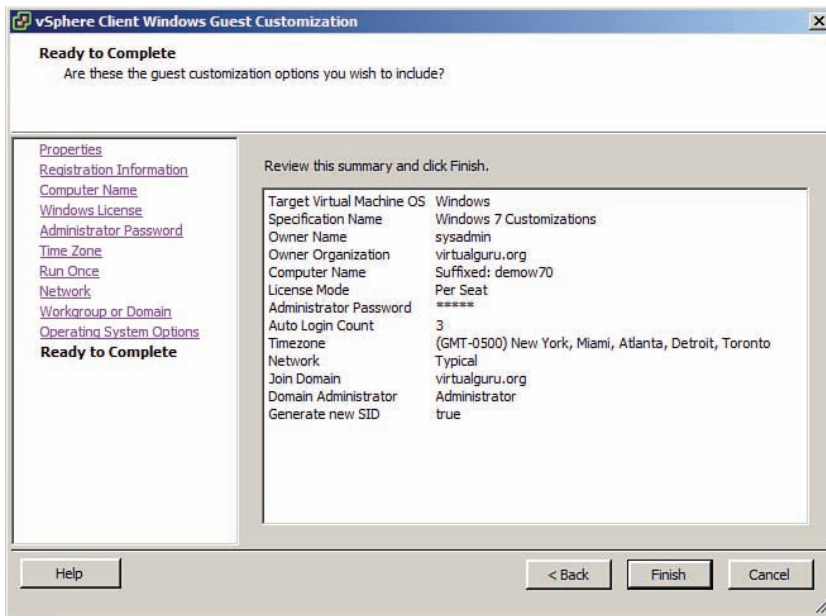
**Figure 5.20** Domain join.

Make sure you leave the **Generate New Security ID (SID)** option checked, as shown in Figure 5.21.



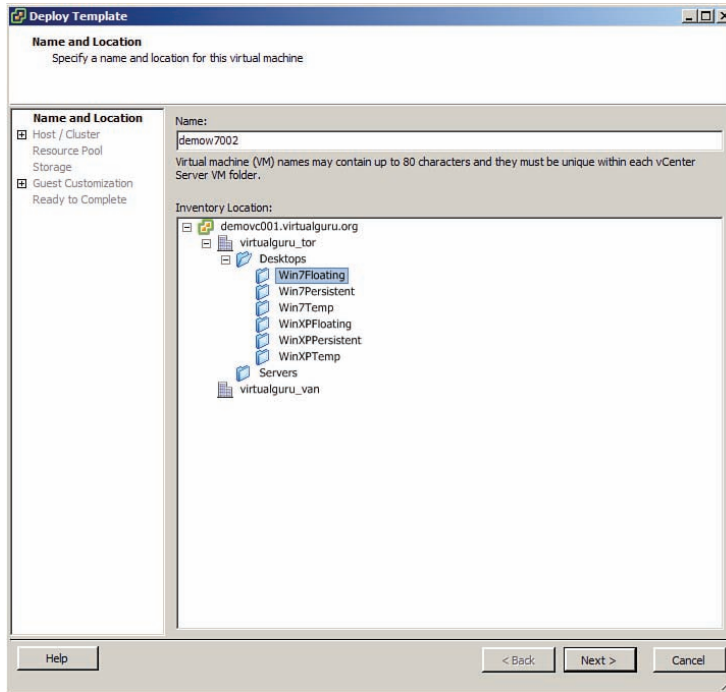
**Figure 5.21** SID generation.

Finally, you can review the choices you just made, and if everything is acceptable, click **Finish**, as shown in Figure 5.22.



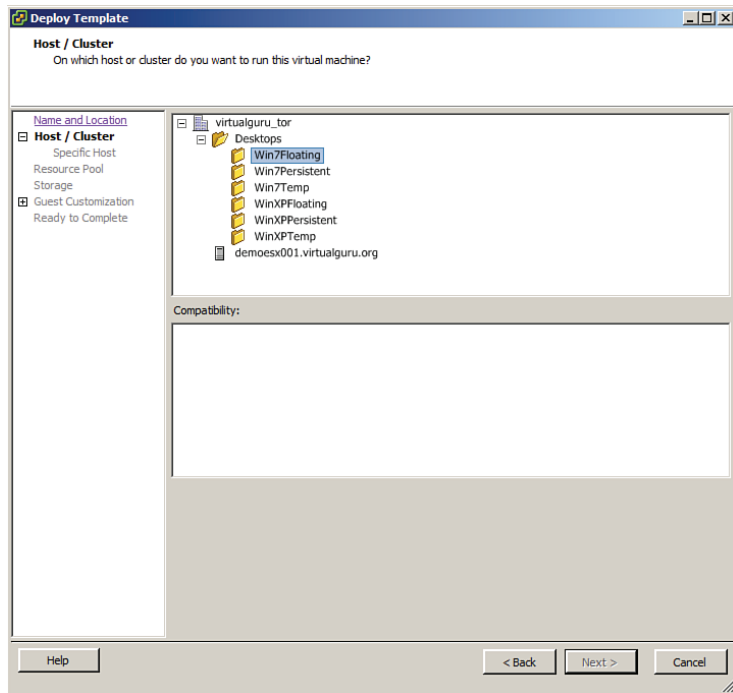
**Figure 5.22** Windows guest customization summary.

Now that you have completed your guest customization, you can apply this to your template created earlier. In the VMs and Templates view in vCenter, right-click your template and choose **Deploy VM** from this template (see Figure 5.23) to launch the Deployment Wizard.



**Figure 5.23** Deploy Virtual Machine from this Template.

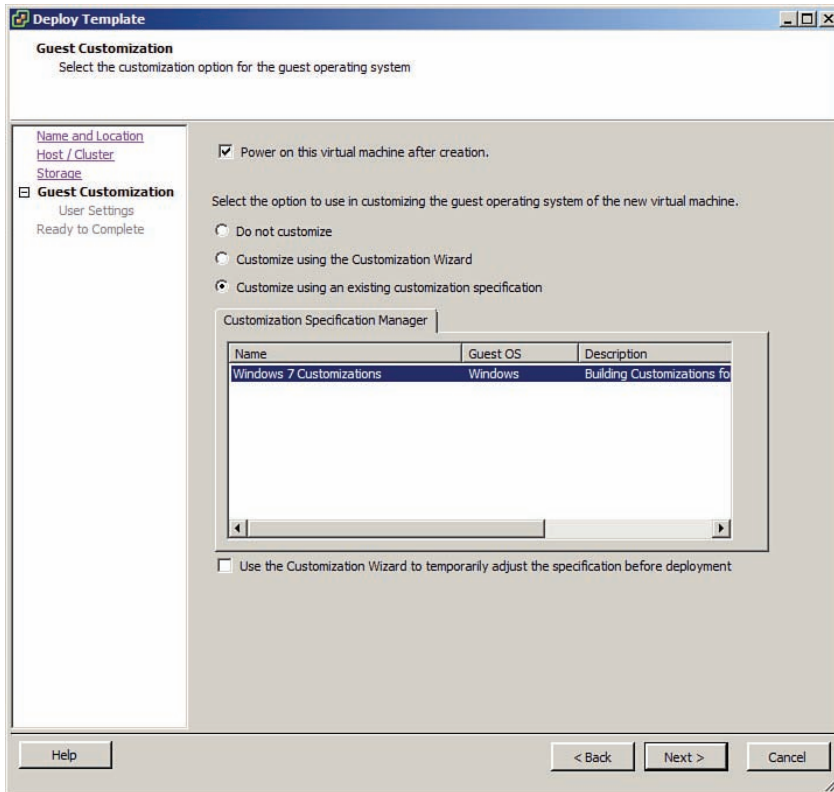
After the wizard starts, give the virtual machine a name (see Figure 5.24). Again, make sure you use something that will be significant in preparation for your VMware View environment. Then you configure the usual information (host/cluster, resource pool, storage).



**Figure 5.24** Provide Virtual Machine name.

The important part is when you reach the Guest Customization screen, shown in Figure 5.25. Here, you choose one of the many guest customizations you have created and link it back to this virtual machine.





**Figure 5.25** Guest Customization screen.

In the final screen, you are able to see all the options you chose, and if these choices are okay, click **Finish**. vCenter launches the creation process and uses the parameters you chose in the Guest Customization script. Repeat the process as many times as needed to prepare your gold master images for your VMware View environment.

## General Optimizations

To optimize your virtual machine, you can tweak a number of areas from the virtual machine hardware configuration, the operating system, and general networking and application considerations and settings. For the virtual machine hardware optimizations, make sure the following are completed:

- Install VMware Tools.
- Disable any hardware not required in the virtual machine, such as floppy devices.

- Ensure media devices are all set to Disconnected so that you do not have devices connected and autodiscovered in the Windows 7 OS.
- Turn off logging of the virtual machine. Under the Settings\Options and General option, deselect the Enable Logging option.

## Operating System Optimizations

Within the Windows 7 image, you should make the following changes to reduce the number of unnecessary processes running in the virtual machine:

- Disable System Sounds (set the Sound scheme to None).
- Disable serial and parallel ports in Device Manager (if they exist).
- Install Windows Patches; then turn off automatic updates.
- Set Screensaver to None or Blank.
- (Windows 7) Uninstall Tablet PC components.
- Disable Windows Error Reporting.
- Remove unnecessary boot applications (QuickTime, Real, Adobe Acrobat Updater, and so on).
- Remove unneeded Windows components (Outlook Express, Messenger, Games, and so on).
- Disable unnecessary services.

As with any OS image, you should install all common applications but make sure that you have turned off automatic updates and autostarting applications that are not required.

Following are some of the more common applications:

- Install Adobe Flash Player (turning off automatic updates).
- Install Adobe Reader and set to Do Not Download or Install Updates Automatically.
- Turn off Java Updater.
- Remove the MS OneNote tray service (if installed).

You should also look at the default network settings for network optimizations. For example, you should disable, configure, and verify the following settings:

- Disable NetBIOS over TCP/IP.
- Disable IPv6.

- Join Master Image to Domain (if using View Composer).
- Add any necessary DNS suffixes.
- Add any necessary HOSTS entries for “custom” applications.

You can also find a number of additional options in the attached commands file in the VMware View Optimization Guide for Windows 7 whitepaper.<sup>2</sup>

These commands can be applied through a single batch file to further tune the operating system.

## Manually Installing Windows 2008 RDS Server

To install a Windows 2008 RDS Server within Server Manager, follow these steps:

1. Open Server Manager from the Windows 2008 R2 Server.
2. In the left pane, highlight **Roles**; then on the right under Role Services, select **Add Role Services**.
3. Check **Remote Desktop Connection Broker** and then click **Next**.
4. Click **Install** at the confirmation and then click **Close** after the install is complete.
5. To make the Windows 2008 RDS Server look like a Windows 7 desktop, see the following section.

## Making a Terminal Server Look Like a Desktop

The Desktop Experience feature turns on themes on the Windows 2008 R2 operating system. After you install it, you see a new service that supports the themes feature. Using it, you can customize the look and feel of the server desktop.

Of course, you can go further and merge the Windows 7 themes included in the Windows 2008 operating system so that the look is seamless. You need a clean Windows 7 x64-bit operating system and a target Windows 2008 R2 Server operating system. Turning on the desktop experience creates the same folders on the Windows 2008 R2 Server that are included by default on the Windows 7 x64 operating system.

Background images are stored in the following directories on both Windows 7 x64 and Windows 2008 R2:

```
%SystemRoot%\Web\Wallpaper\  
%SystemRoot%\Resources\Themes\  

```

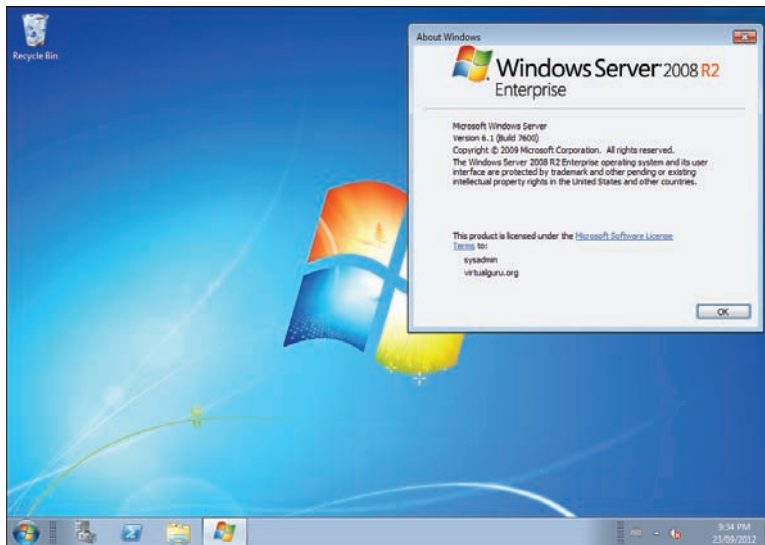
---

<sup>2</sup><http://www.vmware.com/files/pdf/VMware-View-OptimizationGuideWindows7-EN.pdf>

Because the default permissions deny access to administrators, you must reset the permissions on the default IMG file. You can do this from the command line using the following commands:

```
takeown /f "%SystemRoot%\Web\Wallpaper\Windows\img0.jpg">nul
icaccls "%SystemRoot%\Web\Wallpaper\Windows\img0.jpg" /grant
administrators:F>nul
rename "%SystemRoot%\Web\Wallpaper\Windows\img0.jpg" "img1.jpg">nul
```

You can then copy the `img0.jpg` file from the Windows 7 x64 desktop's `%SystemRoot%\Web\Wallpaper\Windows` folder to the same folder on the Windows 2008 R2 Server. You also need to copy the `%SystemRoot%\Resources\Themes` folder to the same location on the Windows 2008 R2 Server. Copying these folders produces the effect shown in Figure 5.26 on your Terminal Server.

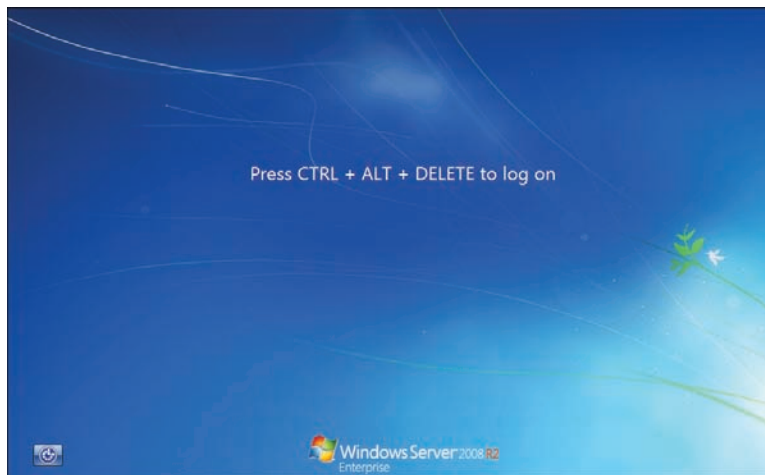


**Figure 5.26** Your server now looks like a desktop.

In addition to making the default background, you also can update the login screen to make everything look and feel like a desktop operating system. Of course, in reality, you will most likely brand this “themes and defaults” with corporate logos, but you can easily do this by turning on the OEM background feature and using the default login background from a Windows 7 x64 desktop. To turn on the OEM background feature, you need to enable it in the registry of the Windows 2008 R2 Server. The keys are identical to a Windows 7 desktop. You can complete this part of the process as follows:

1. Click the **Windows** button and type **regedit.exe** in the search field.
2. Browse to HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\Background.
3. Change the OEMBackground DWORD value to a Hex value of 1 to enable the feature.
4. Create a subdirectory called **info** in c:\windows\system32\oobe.
5. Under the info subdirectory, create an additional subdirectory called **backgrounds**.
6. From your Windows 7 x64 desktop, browse to c:\windows\system32\oobe.
7. Open the background.bmp file with Microsoft Paint.
8. Save the file as **backgrounddefault** in JPEG format and save it somewhere you can easily copy it to your Windows 2008 R2 Server.
9. Copy backgrounddefault.jpg to c:\windows\system32\oobe\info\backgrounds on the Windows 2008 R2 Server.
10. Reboot the server.

The changes produce the Windows 7 color scheme on the Windows 2008 R2 Server, as shown in Figure 5.27.



**Figure 5.27** Windows 7 color scheme on Windows Server 2008 R2.

## View Persona Management

View Persona is an enhancement to using traditional Windows roaming profiles, designed to reduce login times. Unlike a traditional roaming profile that copies the entire profile down during the login, View Persona downloads only what is required for the login. Additional files are downloaded when a user or application requests them. During the user session, synchronization occurs at periodic intervals (10 minutes is the default) to ensure the amount of data required to synchronize at logoff is minimal. During logoff, only the deltas are synced back to the central repository. View Persona is fully compatible with ThinApp and allows sandbox data to be stored in the user persona. This allows application configuration data to roam with the user without a performance penalty. View Persona is not dependent on Windows profiles and can be used instead or in combination with an existing Windows profile management strategy. You can use both by selectively identifying which files or folders should be managed by Windows profiles versus Persona in the synchronize folder policy of View Persona.

View Persona can be used in combination with persistent disks so that a persistent local cache of the user data or persona is available and also that a persona is stored centrally. This capability ensures the user configurations are available locally and can be recovered centrally if a problem occurs with the virtual desktop. View Persona is installed when the VMware View Agent is installed, provided the platform is supported. View Persona is supported only on virtual desktops not using local mode. It is not supported on Terminal Servers, but is supported on physical desktops with VMware View 5.1. It is added to the virtual desktop when you install the VMware View Agent. It is fairly easy to set up but requires some tuning of the default settings to get working properly. At a high level, the steps to implement View Persona are as follows:

1. Set up the file share or remote repository.
2. Install View Agent and ensure the View Persona Management is selected.
3. Add the View Persona Management Administrative Template to the organizational unit (OU) in which the virtual desktops will be deployed.
4. Configure the group policy settings for Persona Management.
5. Deploy virtual desktops with the persona management service running.
6. Verify that the user directories are created on the remote file share.

The exact steps to enable persona management are as follows. You need to create a centralized file share with the same permissions required to set up Windows profiles. If the environment will span multiple sites, you need to have some mechanism to replicate the file repository to ensure it is readily available. You can choose from many methods to do this depending on what you are using for file services. The supported Microsoft method is

to use Distributed File Services (DFS). In Chapter 11, “High Availability Considerations,” we go through the steps to set up DFS to ensure you have a site-to-site high availability solution. If you do not require this level of availability, simply create a file share with the appropriate permissions applied. The steps to do this follow.

Create a Windows file share and ensure the permissions on the parent folder are as shown in Table 5.2.

**Table 5.2** Parent Folder

User Account	Permissions Required
Administrator	Full
Security group permissions	List Folder/Read Data, Create Folders/Append Data (This Folder Only)
Everyone	No Permissions
Local System	Full Control, This Folder, Subfolders and files

Referenced from the Microsoft Technet library at <http://technet.microsoft.com/en-us/library/>.

On the Share for the View Persona, ensure the permissions are as shown in Table 5.3.

**Table 5.3** Share Level (SMB) Permissions for VMware View Persona Share

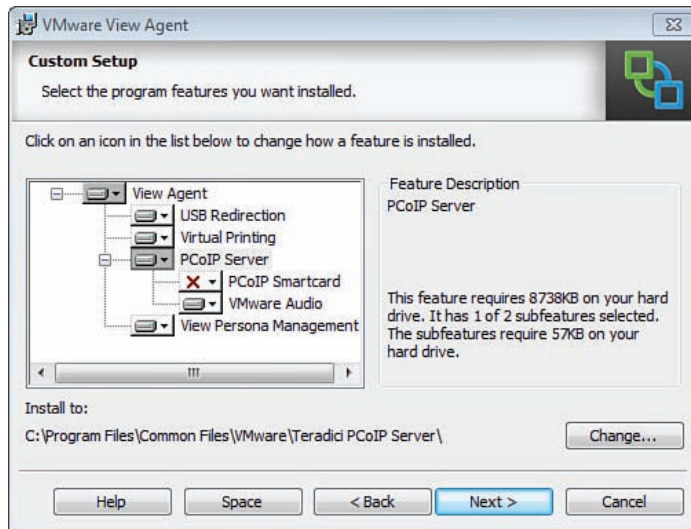
User Account	Default Permissions	Minimum Permissions Required
Everyone	Read only	No permissions
Security group of users needing to put date on share	N/A	Full control

The NTFS permissions on each user persona folder are shown in Table 5.4.

**Table 5.4** User Persona Folder Permissions

User Account	Default Permissions	Minimum Permissions Required
%username%	Full Control, Owner of Folder	Full Control, Owner of Folder
Local System	Full Control	Full Control
Administrators	No Permissions	No Permissions
Everyone	No Permissions	No Permissions

After creating the Share, you need to ensure that View Persona is loaded when the agent is installed on the virtual desktop (see Figure 5.28). Because we covered the installation of the View Agent in the section “Manually Installing the VMware View Agent,” we do not cover the installation again here. Ensure the View Persona Management is installed (it is by default).

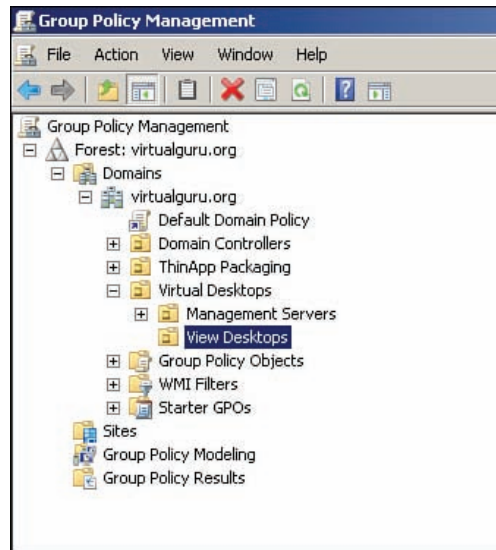


**Figure 5.28** Ensure that View Persona is loaded.

To enable View Persona management, you import the policy template and set the policy to Enable. By default, the View Persona administrator templates are located on the VMware View Server at `install_directory\VMware\VMware View\Server\extras\GroupPolicyFiles`. There are many additional settings that you can fine tune. Let's go through the steps to turn on View Persona management and then look at the more common configurations.

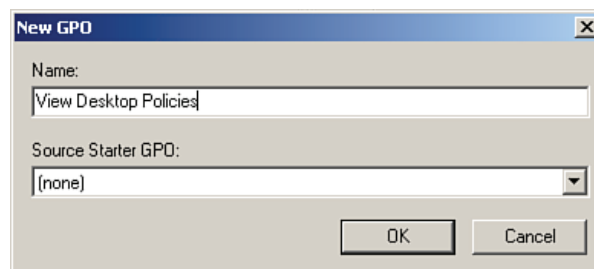
1. Run the Group Policy Management Utility and select the OU that will contain your VMware View desktops (see Figure 5.29).





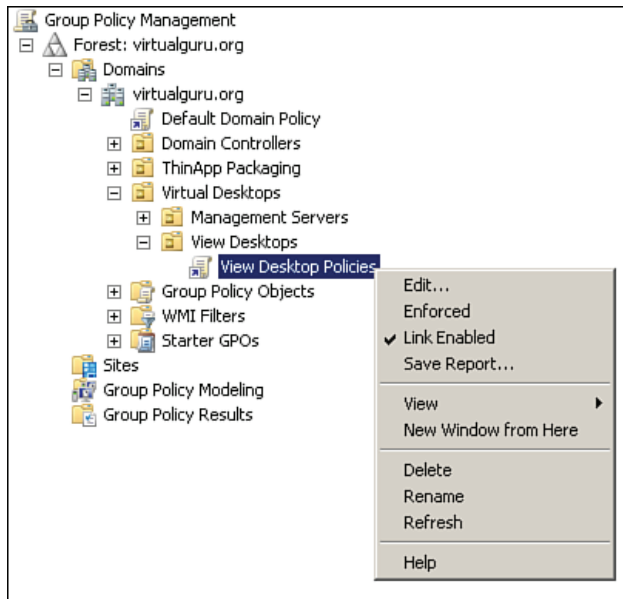
**Figure 5.29** Select your View desktop OU.

2. Create a new GPO and provide a descriptive name, as shown in Figure 5.30; then click **OK**.



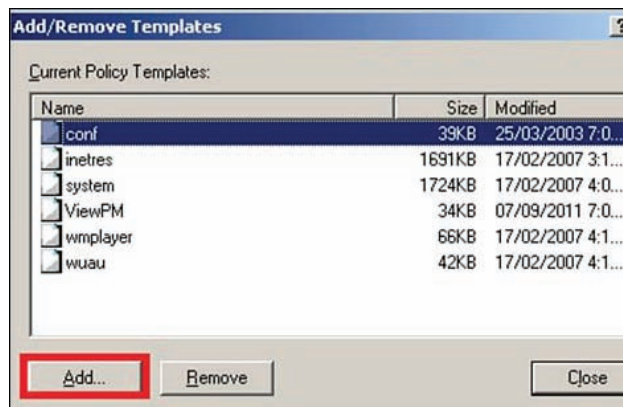
**Figure 5.30** Name the new GPO.

3. Right-click the newly created GPO, as shown in Figure 5.31, and click **Edit**.



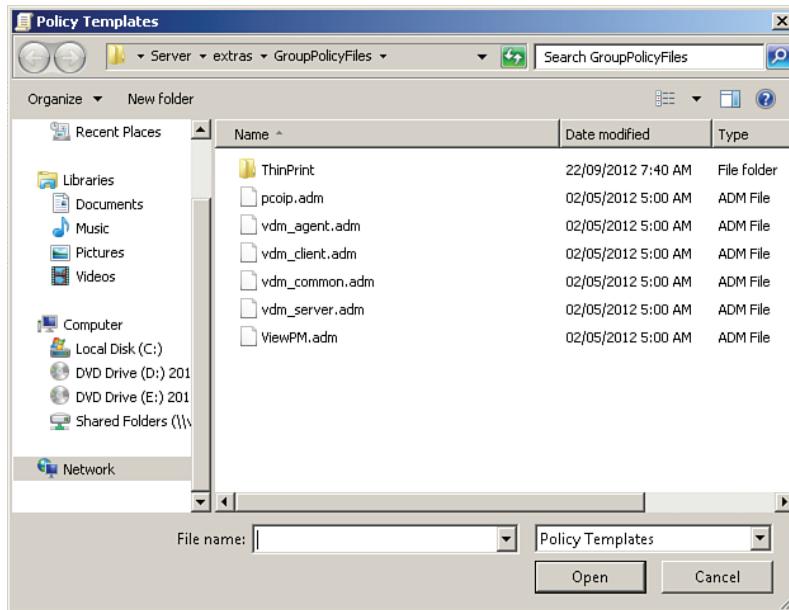
**Figure 5.31** Edit the Policy.

4. Under Group Policy Object, expand Computer Configuration and select Administrative Template. Right-click and select **Add/Remove Templates**; then click **Add**, as shown in Figure 5.32.



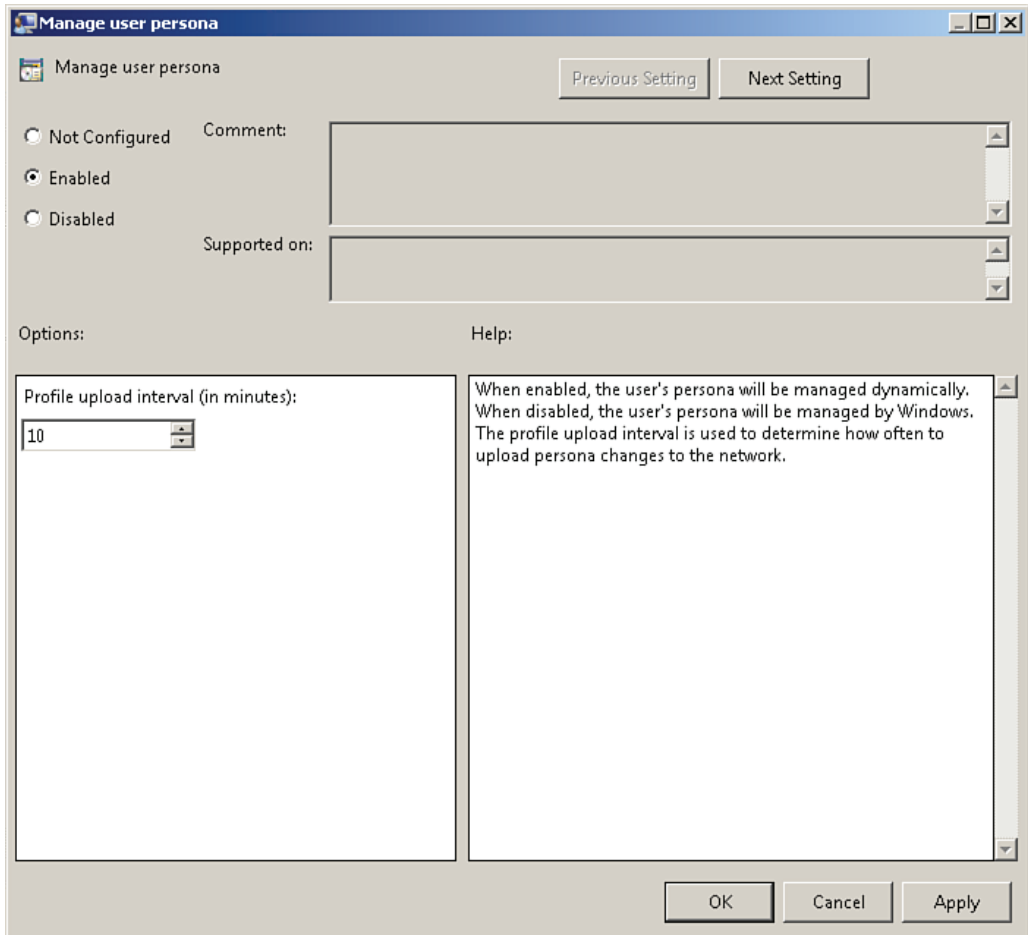
**Figure 5.32** Add an administrator template.

- By default, the View Persona administrator template is located on the VMware View Server at `install_directory\VMware\VMware View\Server\extras\GroupPolicyFiles`. Browse to this location (see Figure 5.33), select the **ViewPM.adm** file, and click **Open** and then **Close**.



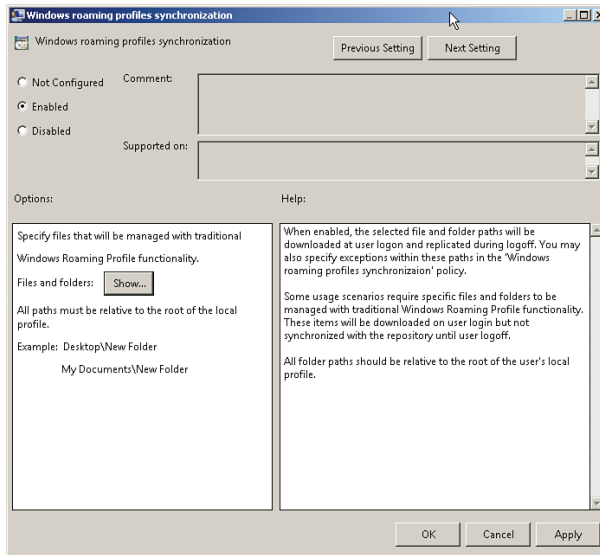
**Figure 5.33** Select ViewPM.adm.

- If you browse under `Computer Configuration\VMware View Agent Configuration\Roaming & Synchronization` and enable the `Manage User Persona` setting, by default, the internal synchronization takes place every 10 minutes (see Figure 5.34), but you can adjust it to reduce the amount of data that has to be synced. Shorter intervals require less data to be synchronized; extending the interval means more data has to be synchronized.



**Figure 5.34** Update Interval.

Perhaps the most common configuration is integrating Persona Management into an existing roaming profile environment or transitioning to Persona from roaming. In this case, you can selectively separate which folders are managed by Windows profiles and View. To do this, you simply set the Windows roaming profiles synchronization properties (see Figure 5.35) and define the paths of the folders you would like to remain under Windows roaming profile management functionality. You can find this policy under Computer Configuration\VMware View Agent Configuration\Roaming & Synchronization.



**Figure 5.35** Windows roaming profile synchronization.

For a deep dive into Persona Management, you might want to check out some good additional reading at <http://www.vmware.com/files/pdf/view/VMware-View-Persona-Management-Deployment-Guide.pdf>.

## View Persona Management: A New Approach

In a perfect world, everybody would be doing a stateless deployment, or what a lot of people in the industry call it now, a *dynamic desktop*. To achieve this, as you might know from reading previous chapters, you need to manage the data and the applications outside the base image. One of the unspoken use cases that we are seeing more and more often to be able to support a true stateless or dynamic desktop is to put the ThinApp packages in the user data repositories. Doing this, although different, gives you two main benefits. The first is the fact that the OS image will be smaller, will be easier to manage, and should have less “clutter” in the base OS. The second one is that a pool operation like a recompose operation will not lose any user-specific applications that are traditionally installed in the base operating system, by putting these applications in a user partition managed outside that base OS.

You have to balance the size of the application with the size of the user data disk, but it can be done, and more and more customers with very remote sites to manage are leaning toward this configuration.

## Completing the Cycle of Persona Management

One of the new features in VMware View 5.1 is Persona Management being able to manage physical desktops. In most VDI projects, you start from an existing state, which means that you have a lot of physical desktops with user data on them. Some of these environments are not able to survive a migration to the virtual world. Users have a habit of storing huge and unreasonable amounts of data under My Documents. However, if processes are in place to educate users around the purpose of VDI, the migration is possible and should be fairly smooth.

You can now use a command-line tool to do a one-time conversion of user profiles from either a physical or virtual Windows XP to a virtual Windows 7. If migration to Windows 7 is not possible yet, you could also use this command to get your users off their physical desktop into their XP View environment.

The last use case, although seldom used, is to use Persona Management to sync user profiles between a physical desktop and a virtual desktop. You might have a few users who need to go back and forth, for valid reasons, between the virtual world and physical world. In that instance, you could synchronize by putting Persona Management on the physical PC. Again, this is a very rare use case but important to note because you have an additional tool in your belt to use during your VDI implementation to shorten the transition.

For a good blog post specifically on the new features of Persona Management in VMware View 5.1, check out <http://blogs.vmware.com/euc/2012/05/vmware-view-persona-management-features-new-5-1.html>.

---

## Summary

In this chapter, we looked at many of the ways to build a virtual desktop for use in a View environment. In addition, we looked at ways to tune that desktop. Part of that tuning includes making sure that user data persists between logins by integrating View Persona. We also looked at a less common way of integrating Windows 2008 R2 Servers into a View environment to reduce costs while making it appear as a native Windows 7 desktop. You should now have an understanding of the View Management components, ThinApp, and how to build the View desktop.

The next chapter, “View Operations and Management,” looks at some of the things you need to know to properly maintain the components in your environment. You also learn how to take groups of desktops or pools and tailor the feature set to match the requirements of the users. The chapter reviews how to control the behavior of the desktop when it is deployed and when the user is logged in and what happens when the user logs off. The information in this chapter is by no means all inclusive, as there is new information published all the time on additional ways to tune your View desktop. I recommend that you also check the VMware website for updates to optimizing your virtual desktops in a way that delivers a great end-user experience.