VMware® Horizon View™ Optimization Guide for Windows 7 and Windows 8

OPTIMIZATION GUIDE

vmware®

Table of Contents

About This Guide

This guide provides guidelines for configuring a standard Windows image for use in a VMware® Horizon View™ infrastructure. It gives administrators the information necessary to create a standard Windows image, whether by leveraging the Microsoft Deployment Toolkit (MDT) or by utilizing a script-based approach to optimize traditionally installed Windows virtual machines. The recommended configuration settings optimize the operating system to enhance overall scalability and performance in a Horizon View implementation.

The procedures described in this guide apply to the Windows 7 and Windows 8 operating systems. Scripts and task sequences to optimize both operating systems are included.

Horizon View 5.2 supports Microsoft Windows 8 and the Metro style user interface. Windows 8 offers more options for security and personalization as well as new built-in desktop virtualization capabilities. The new Group Policy templates for Windows 8 enable more control and consistency for desktop users and greatly enhance the Horizon View virtual desktop experience.

Horizon View also supports basic gestures in a View Client running on Intel-based Surface tablets. In Windows 8 there is now a services state change where only the necessary services are running at system startup, with most services marked as Manual (Triggered Start). In this scenario, services are started only when the user accesses a component that requires the triggered service to be started. This improves Windows performance.

Organization

This guide is organized into distinct sections:

About This Guide discusses the overall process of optimization and the optimization aids provided.

Creating an Optimized Windows Image gives step-by-step procedural guidance for both methods of optimization, MDT and script-based.

Windows 7 and Windows 8 OS Customizations provides background information on the specific optimizations and techniques used by the optimization aids.

Managing VMware Horizon View Desktops offers guidance and considerations for optimizing the environmental aspects on an ongoing basis.

Additional reference material, files, and other useful items are located in the Appendixes, and two especially useful scripts are attached to the PDF file.

Process Overview

You can accomplish the goal of building your standard image and applying desired customizations in a number of ways. This guide provides two methods for IT organizations to utilize, each requiring a different level of effort and yielding different benefits. Figure 1 illustrates the workflow of both methods.

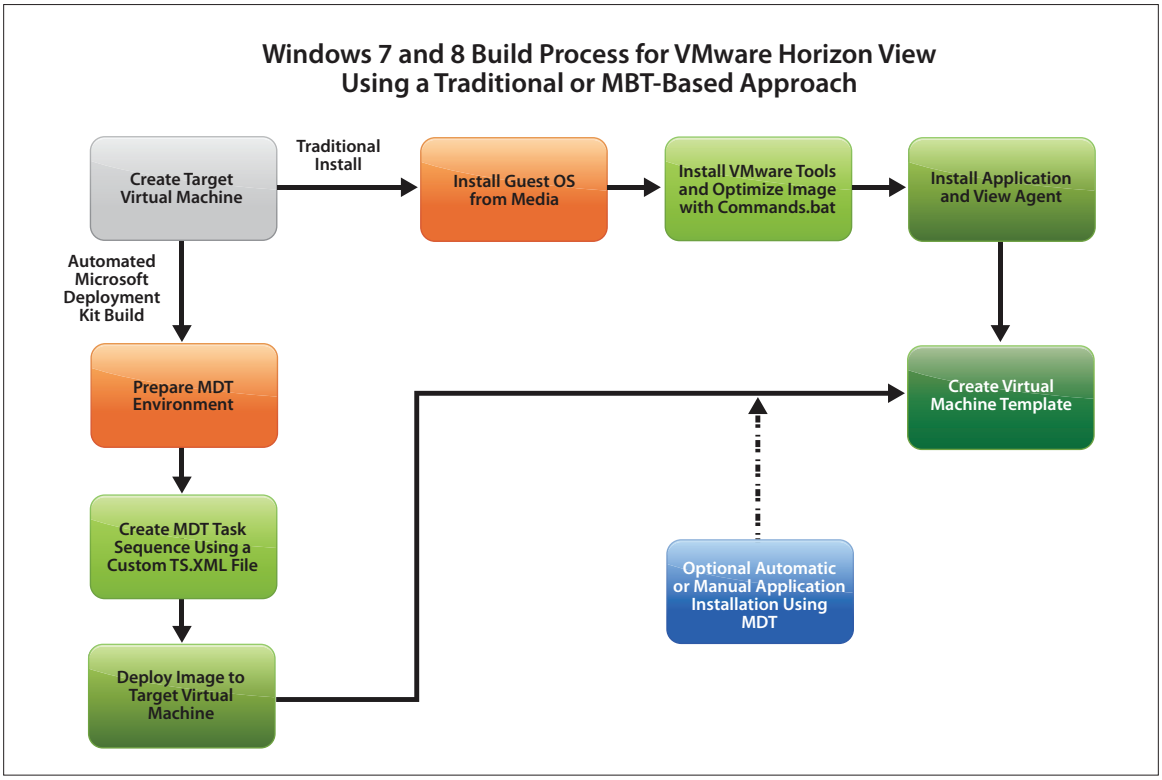

Figure 1: Horizon View Virtual Machine Workflow Using Traditional and MDT Build Process

Traditional Install Method

You can optimize a traditional install with a minimum set of tools. It takes very little effort to create a standardized and optimized process for customizing a Windows 7 or Windows 8 virtual machine. Administrators create the virtual machine with the specified parameters, load the operating system from media, and then use a command script for the appropriate operating system to apply optimizations. The `Commands.bat` script, attached to this guide, is distributed as a choice of `CommandsPersonaManagement.txt` or `CommandsNoPersonaManagement.txt` (see Appendix B).

Microsoft Deployment Toolkit Method

The Microsoft Deployment Toolkit (MDT) provides a framework for building and maintaining a defined process that is modular and applicable to both physical and virtual desktops. The benefits of this solution are derived from the prescriptive guidance and repeatable processes included in the tool for building and maintaining standardized images. While you may invest more time up front when using this method, there are long-term advantages. In many cases, an IT organization may already use some of the tools and processes described. This method involves leveraging the MDT and Windows Automated Installation Kit (WAIK) to create a standard image-build and customization process that leverages a robust task sequence engine. You can use the MDT approach to automate application installation, manage driver injection into different operating system versions, and use a GUI to create system builds and customize events.

Optimization Aids

This guide provides two ways to optimize the Windows image. As shown in Figure 1, you can leverage a script file or the MDT to implement the customizations. While these optimization aids contain recommended configurations, each IT organization should investigate and evaluate the benefits—there is sometimes a trade-off between productivity and optimization. Appendix A lists all the optimizations, using an asterisk ('*') to highlight discretionary changes. You should review these for applicability to your organization's specific use cases.

Commands.bat

`Commands.bat` is a script file that can be executed manually or by using an automated scripting mechanism. The script utilizes standard operating system mechanisms to manipulate the registry using Registration Entry (REG) syntax; adjust services using PowerShell; and optimize other miscellaneous items, such as Scheduled Tasks (see Appendix B.) The script is distributed as a choice of `CommandsPersonaManagement.txt` or `CommandsNoPersonaManagement.txt`, included as attachments to this guide for both Windows 7 and Windows 8.

To save the commands text file, go to the **Adobe Reader View** menu, select **Show/Hide** > **Navigation Panes** > **Attachments**, and then **Save**. After saving, rename the file to `Commands.bat`.

If you are implementing View Persona Management, or plan to use VMware Horizon Mirage™ to manage the desktop image, use the `CommandsPersonaManagement.txt` file. If you are not implementing Persona Management, use the `CommandsNoPersonaManagement.txt` file included for both operating systems.

Caution: Open the script on a Windows machine. Use a script editor or WordPad to avoid possible line-break issues with Notepad.

If you have already optimized an image designed for use without Persona Management, and you want to deploy Persona Management or Horizon Mirage image management on that desktop image, create a `BAT` file on your virtual machine template from the supplied `CommandsDesktopsReadyForPersonaManagement.txt` files. Run this script as an administrator (right-click **Run as Administrator**). Reboot the computer when the BAT file completes (See Appendix C).

Microsoft Deployment Toolkit and TS.xml

The `TS.xml` file is used by the MDT task sequence engine to provide a sequence of tasks to execute when deploying the Windows image. You can use the `TS.xml` file to perform tasks such as joining a domain, stopping or disabling a service, and installing applications or packages. Replacing the default `TS.xml` file with the one provided with this guide provides a GUI interface for viewing and editing the recommended customizations. The customizations included in the provided `TS.xml` file are equivalent to the `Commands.bat` script file described in Commands.bat.

The `TS.xml` file is referenced in Appendix D and included in this guide as an attachment called `MDT 2012 Task Sequences Files.zip.txt`. This ZIP file contains a set of customized `TS.xml` files. To save this set of `TS.xml` files, go to the **Adobe Reader View** menu, select **Show**/**Hide** > **Navigation Panes** > **Attachments**, select the file, and click **Save**. After the `MDT 2012 Task Sequence Files.zip.txt` file is saved to the machine, change the extension to `.zip`. Then unzip the file and use the appropriate `ts.xml` file.

Note: If you are using Windows and have file extensions turned off, the `.txt` suffix does not appear in the downloaded file. Open a command window and navigate to the directory where you saved the `.zip.txt` file from Adobe Reader. Type

```
move "MDT 2012 Task Sequence Files.zip.txt" "MDT 2012 Task Sequence Files.zip"
```

Creating an Optimized Windows Image

The procedures for creating an optimized Windows image are described in the following sections.

Administrative Rights for Users

The methods and optimization aids provided in this guide customize the parent virtual machine that end users' desktops are based on. End users can undo these optimizations if they have administrative rights to start services and modify the registry.

Note: It is important to use Group Policy Objects (GPOs) to reinforce these settings and control desktops where end users have administrative rights.

Image Version Tracking and Managing Windows Updates

Optimizing the operating system configuration is an iterative process. As images progress through the normal life cycle, it can become difficult to determine which image configuration and subsequent optimizations a particular VMware Horizon View guest virtual machine is leveraging. As the VMware View Composer™ Recompose and Refresh updates Horizon View desktops, the virtual machines are linked to parent virtual machines and snapshots. Careful management of snapshot names enables some tracking ability; but you can also use an identifier in the operating system for identification, using the script or system management processes. For this reason, you should add an additional registry setting to track the version of an image, as well as any other helpful information your organization may find useful, such as date, type, and author. The modifications provided in the `TS.xml` and `Commands.bat` files include a marker key for this purpose in `HKEY Local Machine\Software\Image`.

Applying Windows updates is an important step in the process to verify that your parent virtual machine always stays as up to date as possible; however, the Windows Update service should be set to Disabled by default to avoid pulling updates down to virtual machines in your Horizon View environment after they are deployed. The custom task sequence provided with this document applies all applicable Windows updates that are available at the time the target virtual machine is built. It subsequently disables the Windows Update Service to prevent your Horizon View virtual machines from downloading updates from Microsoft. It is considered a best practice to manage your updates for your virtual machines on the parent virtual machine and recompose that virtual machine to update all linked clones. To apply updates manually to your parent virtual machine, re-enable the Windows Update Service, then run Windows updates or apply updates leveraging your enterprise patch-management process.

Creating the Target Virtual Machine

The initial virtual machine parameters create a virtual hardware profile, which is used for subsequent virtual machines. You can convert an existing physical or virtual machine using VMware Converter, but it is best to create a new virtual machine using the VMware vSphere® Client. Administrators can use the built-in VMware vCenter™ wizard to create a new virtual machine or select the parameters on their own. Specific recommendations are listed in Table 1 and described in the paragraphs that follow.

PARAMETER	COMMENTS
Guest Operating System	Microsoft Windows 7 (32-bit or 64-bit)
SCSI Controller	LSI Logic SAS
Hard Disk	Disks for templates or parent virtual machines can utilize Thin Provisioning.
Video Card	No need to specify as settings are provided by View Manager.
Floppy	Remove the floppy drive
CD/DVD	Set to client device used for VMware Tools install, Windows 7 ISO, or Windows PE boot ISO with MDT.
NIC Adapter Type	VMXNET 3. Apply the Microsoft hotfix patch (see VMware Horizon View Administration).
Memory Specifications	32-bit, 1 – 3GB (no more than 3GB) 64-bit, 1 – 4GB (depends on use case, such as Kiosk, Task Worker, or Knowledge Worker)
BIOS – Disable Ports	Go to the **Options** tab of Virtual Machine Properties and select **force entry into BIOS** to disable unnecessary LPT and COM ports.

Table 1: Virtual Machine Parameters

Virtual Machine Parameters

The parameters are explained in further detail in the following paragraphs:

Disk Controller

VMware recommends using the LSI Logic SAS controller for Windows 7 and Windows 8 virtual machines.

NIC Adapter Type

The Network Interface Card (NIC) needs to be VMXNET 3. Failure to set the proper NIC type prevents Windows Preinstallation Environment (Windows PE) from correctly acquiring an IP address and gaining access to the network for resources required during imaging. The traditional install method uses the VMXNET 3 virtual network adapter to provide the most efficient networking stack for Windows 7 and Windows 8. Apply the Windows hotfix (see VMware Horizon View Administration).

Video Parameters
Setting specific video parameters of the video card is not necessary in the virtual machine properties. Leave the video card settings at Auto-detect video settings. The values used for video memory are set and managed by VMware View Manager.

Memory Specifications
For x86 Windows 7 and 8 operating systems, no more than 3GB of memory should ever be allocated. Memory specifications are dependent upon the supporting virtualization infrastructure. However, you should provide at least 1GB of memory to the standard virtual machine template leveraged for Windows 7 and 8. An ideal allocation is 2GB of memory, providing for more bursting of memory when needed for heavier end-user applications. This setting is completely dependent upon the environment and use case scenarios. Sufficient use case mappings should be done to determine the optimum memory settings for your organization.

Disable HotAdd/HotPlug
If HotAdd/HotPlug is enabled for the base image virtual machine (the default), the end user can eject critical components, such as the NIC and SCSI controller. To prevent this from happening, disable HotAdd/HotPlug for the base image virtual machine by setting the `devices.hotplug` parameter for that virtual machine to `false`, either through the vSphere Client or by directly editing the virtual machine's `.vmx` file. For details on using either of these two methods, see the VMware Knowledge Base article, Disabling the HotAdd/HotPlug capability in ESX/ESXi 4.x and ESXi 5.0 virtual machines (KB 1012225).

Choosing Your Windows Installation Method

At this point, you should determine whether to do a traditional installation of Windows by mounting the media to the virtual machine (see Traditional Install Method) or to utilize the MDT (see Using the Microsoft Deployment Toolkit to Optimize Windows) to install Windows into the target virtual machine.

Why Use the Microsoft Deployment Toolkit 2012 Update 1?
The Microsoft Deployment Kit (MDT) can best be described as a collection of scripts and processes that supports a defined framework to create a standard, repeatable, and flexible image for an organization. This approach creates a prescriptive, standardized build process that is:

- **Flexible** – You can enable, disable, or build on logic when certain commands are executed, depending upon existing scenarios.
- **Easy** – The Task Sequencer provides pre-built components for adding reboots, partitioning, command lines, and other logic in an intuitive GUI interface.
- **Updatable** – As drivers, applications, and other updates are needed within the standard build process, you can update the Task Sequencer in a point-and-click configuration for all new image builds in one interface.
- **Cross-platform** – You can leverage the same MDT framework for both virtual and physical machine builds.

Note: For details on how to use the MDT, see Using the Microsoft Deployment Toolkit to Optimize Windows.

Traditional Install of Windows Operating Systems

The following section outlines the process for a traditional install of Windows using an ISO image mounted on a datastore accessible by the target virtual machine. After the installation of the operating system is complete, `Commands.bat` is used to optimize the configuration. Installation of applications and the View Agent can be performed either automatically or manually.

Install Guest OS from Media
1. Verify that the CD/ROM device is set to **Connect at Power on** and directed to the Windows ISO image.
2. Connect to the virtual machine console and answer the prompts for the operating system Setup Wizard.
3. Restart as necessary.
4. Remove any unnecessary components, such as Tablet PC components, from the operating system.

Update Windows and Install VMware Tools

1. Once the operating system installation is complete, perform Windows Update as necessary.
2. From the virtual machine console menu or from VMware vCenter, initiate and complete the installation of VMware Tools.
3. Restart as necessary.
4. Execute the optimization file from the desktop after the installation of the operating system has been completed.

Install Applications and VMware View Agent

1. Install applications as needed in the base image.
2. You can either join the Active Directory domain or not to install applications. If you do not join the domain, mount the application installers on a protected share outside the domain so that you can load them while not in the domain.
3. Install the VMware View Agent manually or utilize a silent installation command as provided, substituting the appropriate values, such as the following:

```
VMware-viewagent.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1 ADDLOCAL=ALL"
```

4. Restart as necessary.
5. In vCenter, edit the properties of the virtual machine to disconnect the installation media and remove the CD/DVD drive from the virtual machine.

For more information on how to install the VMware View Agent, see *Install View Agent Silently* in VMware Horizon View Administration.

Optimize the Image with Commands.bat

1. Use the Adobe attachment panel to save and copy the appropriate script to the `Commands.bat` file.
   a. Use the `CommandsNoPersonaManagemant.txt` file for pools not using Persona Management.
   b. Use the `CommandsPersonaManagemant.txt` file for pools using Persona Management.
   c. Use the `CommandsDesktopsReadyForPersonaManagemant.txt` file to modify a base image already optimized for no Persona Management so it can be used with Persona Management.

   Caution: Open the script on a Windows machine. Use a script editor or WordPad to avoid possible line-break issues with Notepad.
2. Open a command prompt window with administrative privileges, execute the `Commands.bat` file, and monitor for errors.
3. Restart to affect the changes in Windows services.
4. Go to Using the Target Virtual Machine to Create VMware Horizon View Desktops.

Using the Microsoft Deployment Toolkit to Optimize Windows

The MDT 2012 Update 1 is a free toolkit provided by Microsoft to organizations wanting to build and deploy a standard image in a Lite-Touch process. The toolkit enables organizations to standardize and automate the process of creating golden master images.

Using Windows System Image Manager with the MDT

Some organizations may already be leveraging the Windows System Image Manager to customize their Windows images with the `unattend.xml` file. This is most often done through the MDT framework and can be integrated into this process. Some of the settings referenced in this document can be accommodated through that tool and applied directly to `unattend.xml` if desired. For more information on the features and capabilities of WSIM, see the Windows System Image Manager Technical Reference.

Prepare the Microsoft Deployment Toolkit 2012 Update 1 Environment

Preparation of an MDT environment may require the creation of a separate virtual machine that utilizes the MDT, Windows Deployment Services (WDS), Windows Automated Installation Kit (WAIK), and the set of customized `TS.xml` files included with this guide. This section covers the MDT installation, creating the Deployment Share, staging the OS media, and injecting drivers from VMware Tools into the image. The deployment share is used for storing all the standard configurations and customizations leveraged for building a Windows 7 or Windows 8 image. This process was tested on both MDT 2010 and MDT 2012 with Update 1.

1. Create a separate virtual machine for the MDT, unless an MDT environment already exists.
2. Review the system requirements, and verify that the system being leveraged meets the minimum. See the Microsoft Download Center for Microsoft Deployment Toolkit (MDT) 2012 Update 1.

Note: Check the Solution Accelerators site for the latest links and information on MDT.

Download and install the Windows Automated Installation Kit, latest PowerShell version, and the appropriate version of the MDT for your operating system (x86, x64) from the link above.

Note: Pay close attention to the installation directory for MDT during the install. Verify that it is on a drive with sufficient space to hold images, source media, and any line of business applications needed for your standard image.

3. Once the installation for MDT is complete, launch the Workbench by going to the Start Menu and navigating to **Start** > **All Programs** > **Microsoft Deployment Toolkit** and selecting **Deployment Workbench**.
4. Validate that all required components are installed by navigating to **Information Center** > **Components** in the Deployment Workbench and ensuring that any item marked with **Required** in the **Status** column is showing under the **Installed** section.

Note: You can download and install components from inside the Workbench if not already installed.

5. Navigate to the node **Deployment Shares** in the Deployment Workbench, right-click and select **New Deployment Share**.
6. Name the Deployment Share, for example, MDS1.
7. You can leverage defaults for this wizard, but pay close attention to **Deployment Share Path** to verify that you are placing your source files in a location with sufficient space. If you selected an OS drive for the installation of the MDT, select a data volume (non-boot partition) during this step to store deployment data.
8. Select the **Deployment Share** you just created, and click **Properties**. On the **Rules** tab, add or edit the following lines, and click **Apply**.

   These settings streamline the process of building the target virtual machine.

   ```
   SkipCapture=Yes

   SkipUserData=Yes

   SkipBitLocker=Yes

   DoNotCreateExtraPartition=Yes
   ```

   This line prevents adding the 100–300MB system partition for BitLocker.

Staging OS Media

This section describes the process of importing Volume License source media for Windows. In order to build the initial Windows image, source media needs to be obtained and imported into the Deployment Workbench.

1. To import Volume License media for Windows 7 or Windows 8, navigate to **Deployment Shares** > **MDT Deployment Share** > **Operating Systems**, right-click **Operating Systems**, and select **Import Operating System**.
2. Select **Full set of source files**, and click **Next**.
3. Mount the Windows 7 or Windows 8 ISO to the MDT virtual machine, or point to a network location that houses the extracted Windows source files.
4. The media are validated on import to verify that files at the root directory represent an install source for the Windows operating system files.
5. You can select **Move the files to the deployment share instead of copying them**.

   This is useful if you are leveraging a virtual machine for your MDT server and want to avoid copying data, because moves are instantaneous, while copying can take several minutes. Select **Next** to continue.
6. The destination directory is the directory to be created under the `Deployment Share\Operating Systems` directory.
7. Name the directory, for instance `OS-Win8forView` or `OS-Win7forView`, and select **Next** on the remaining screens to finish the import.

Importing Drivers into the Workbench to Support VMware Virtual Machines

To successfully connect to the network and see storage when booting to Windows PE, you may need to import NIC and storage drivers into the workbench. After drivers are imported, they are injected into the Windows PE boot media when the Deployment Share is updated (discussed in step 12 of Create a Custom Task Sequence with TS.xml below).

1. For vSphere 5.0 and later versions, locate the drivers by browsing to the `C:\Windows\System32\DriverStore\FileRepository` directory on an existing Windows 7 or Server 2008 virtual machine installed with VMware Tools.

Note: For vSphere VMware Tools earlier than version 5.0, the directory is located at `C:\Program files\VMware\VMware Tools\Drivers`.

2. From the `File Repository` directory, locate and copy the `vm…` driver directories (especially the network directories, `vmxnet3ndis6.inf_x86` or `x64…`) to a location that can be accessed from the virtual machine running MDT.
3. In the Deployment Workbench, navigate to **Deployment Shares** > **MDT Deployment Share** > **Out-of-Box Drivers**. Right-click **Out-of-Box Drivers**, and select **Import Drivers**.
4. Point to the directory containing the VMware drivers, and select **Next** to import the drivers into the Deployment Workbench.

Note: This process automatically interrogates the `.inf` and `.cab` files to locate and import the appropriate driver files.

Create a Custom Task Sequence with TS.xml

This section discusses leveraging the MDT to create a *task sequence*. A task sequence is a series of commands combined to create an automated process, directly from the Deployment Workbench interface, that is easy to update as the environment changes. A task sequence also removes much of the manual effort required to generate a customized image for a VMware Horizon View environment. The following steps guide you through the process of creating a task sequence for a Windows operating system image. They utilize the set of customized `TS.xml` files included in this document to import a customized task sequence that optimizes this operating system image for Horizon View environments.

The process described below is identical for Windows 7 and Windows 8 operating system images.

1. In the Deployment Workbench, navigate to **Deployment Shares** > **MDT Deployment Share** > **Task Sequences**.
2. Right-click **Task Sequences**, and select **New Task Sequence**.
3. Enter a task sequence ID. This ID must be unique. It determines the directory name that is created with customizations in the `\\MDT\MDS1\control` folder. For example, using Win8forView as the task sequence ID creates the `\\MDT\MDS1\control\Win8forView` directory.
4. Enter a task sequence name, then click **Next**.

   This name must be unique. It is the name that shows up in a list of task sequences to choose from when you build the golden image. For example, use Win8forView as the task sequence name.
5. Select **Standard Client Task Sequence**, and click **Next**.
6. Select the operating system that you imported, as described in Staging OS Media, then click **Next**.
7. Answer the remaining questions, and complete the task sequence definition.
8. Replace the default `TS.xml` (created in the `Win8forView` custom task sequence directory) with the customized `TS.xml` attached to this guide.

   The `TS.xml` file is referenced in Appendix D and included in this guide as an attachment called `MDT 2012 Task Sequences Files.zip.txt`. This ZIP file contains a set of customized `TS.xml` files. To save this set of `TS.xml` files, go to the **Adobe Reader View** menu, select **Show**/**Hide** > **Navigation Panes** > **Attachments**, select the file, and click **Save**. After the `MDT 2012 Task Sequence Files.zip.txt` file is saved to the machine, change the extension to `.zip`. Then unzip the file and use the appropriate `ts.xml` file.

   Note: If you are using Windows and have file extensions turned off, the `.txt` suffix does not appear in the downloaded file. Open a command window and navigate to the directory where you saved the `.zip.txt` file from Adobe Reader. Type

   ```
   move "MDT 2012 Task Sequence Files.zip.txt" "MDT 2012 Task Sequence Files.zip"
   ```

   Move the customized `TS.xml` to the correct location, such as `\\MDT\MDS1\control\Win8forView`.
9. Return to the Deployment Workbench, select the **Task Sequence**, and right-click to see the properties.
10. Select the **Task Sequence** tab (this generates an error). Click **OK**, then navigate to **Install** > **Install Operating System**, and set **Operating System to Install** to the imported OS media referenced in Staging OS Media.
11. Verify that the Deployment Share is updated.

    This step generates the boot image to be used for booting to Windows PE and initiating the OS build. To update the **Deployment Share**, navigate to **Deployment Shares** > **MDT Deployment Share**, right-click **Deployment Share**, and select **Update Deployment Share**.
12. Click **Next** twice to start the process of updating the Deployment Share.

Customize the Win8forView Task Sequence (Optional)

This section discusses the optional process of implementing your own configuration changes directly in the MDT Task Sequencer. It lets you apply customizations to the registry, services, and applications programmatically to a Windows 7 or Windows 8 image.

The Task Sequencer also lets you apply changes to configurations that customize HKEY Current User (HKCU) and HKEY Local Machine (HKLM) settings and those service states that need to be disabled. The set of `TS.xml` files provided with this guide creates a starting point for customizations.

1. In the Deployment Workbench, navigate to **Deployment Shares** > **MDT Deployment Share** > **Task Sequences**, right-click **Task Sequences**, and select **Win8ForView.**
2. Right-click **Task Sequence to modify** in the right-hand pane, and select **Properties**.
3. Select any of the recommended customizations, and enable, disable, or change the settings by editing the Properties tab. You can also add tasks or settings that are particular to your environment to the appropriate phase.

   These changes are written to the `TS.xml` file and become part of the standardized build process.
4. You can add a custom task, using the Task Sequence editor to navigate to the **State Restore** > **Custom Tasks** section. Highlight **Custom Tasks**, click **Add**, and navigate to **Add** > **General** > **Run Command Line**.

   This option provides the ability to run command lines during OS installation.

Installing Applications with the Microsoft Deployment Toolkit

Whether to include software packages into a standard image depends upon the organizational need and strategy for application deployment and management. It may be beneficial to create a custom image with the packages already installed into the image. The MDT can accommodate existing packages that have been created within your organization and enable them to be deployed, using a task sequence, to a standard image. Ideally, these packages are silently deployable and created leveraging Microsoft Installer Package (MSI) technology in cases where HKCU application-specific settings need to be included.

The MDT provides the ability to deploy software to a target system during OS deployment as long the installation supports silent switches. The process detailed below adds VMware Tools and VMware View Agent as applications to be used later by a task sequence for automated installation.

The order in which you add applications is important—the task sequence installs them in that order by default. VMware Tools *must* be added first in order for the View Agent to be installed correctly.

Installing a New Application

1. In the Deployment Workbench, navigate to **Deployment Shares** > **MDT Deployment Share** > **Applications**. Right-click **Applications**, and select **New Application**.
2. Select **Application with source files**, and click **Next**.
3. Provide details about the VMware Tools, and click **Next**.

   ```
   Publisher: VMware

   Application Name: VMware Tools

   Version: v9.0.0 (Use the current version number)

   Language: English
   ```
4. Select your source directory by mounting the Windows.ISO image to the MDT virtual machine.

5. Mount the Windows.ISO image by browsing the Datastores to `\vmimages\tools-isoimages`, and click **Connected**.
6. Select the root of the drive where `Windows.ISO` is mounted.
7. Specify the name of the directory, such as `VMwareTools`, to create in your Deployment Share.
8. Specify the command line, and click **Next**.

   For vSphere versions before 5.0, use the following command:

   ```
   msiexec /i "VMware Tools.msi" /qn /norestart
   ```

   For vSphere 5.0 and later versions, use this command instead:

   ```
   Setup.exe /S /v" /qn REBOOT=R ADDLOCAL=ALL REMOVE=Hgfs"
   ```

9. Check **Reboot the computer** after installing this application.
10. Click **Next**, and **Finish** to complete the process.
11. Select the **VMware View Tools** application, right-click to view **Properties**, select the **Details** tab, and place a check on **Reboot the computer after installing this application**.

Adding the VMware View Agent
Follow a similar process to add the VMware View Agent application.

1. In the Deployment Workbench, navigate to **Deployment Shares** > **MDT Deployment Share** > **Applications**, right-click **Applications** and select **New Application**.
2. Select **Application with source files**, and click **Next**.
3. Provide details about the VMware View Agent application, and click **Next**.

   ```
   Publisher: VMware

   Application Name: View Agent

   Version: (Current version number)

   Language: English
   ```

4. Select your source directory, and click **Next**.
5. Browse to the location of the VMware View Agent application.
6. Specify the name of the directory, such as `VMwareViewAgent52`, to create in your Deployment Share.
7. Specify the command line, for instance:

   ```
   VMware-viewagent-BUILDXXXXX.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1"
   ```

8. Click **Next** to complete the process.
9. Select the **VMware View Agent** application.
10. Right-click to view **Properties**, select the **Details** tab, and check **Reboot the computer after installing this application**.

For more information on how to install the VMware View Agent, see *Install View Agent Silently* in VMware Horizon View Administration.

Deploying the Win8 for View OS Instance into the Target Virtual Machine
When the Deployment Share has been updated and the task sequence for the build has been prepared, deploy the OS instance into the target virtual machine and apply the optimizations.

1. From the MDT virtual machine, copy the appropriate Lite-Touch PE ISO (x86 or x64) from the deployment share (`D:\DeploymentShare\Boot`) to a datastore that can be utilized by the target virtual machine.
2. From the target virtual machine created in the Creating an Optimized Windows Image section, modify the CD/DVD properties to locate and connect at power on the appropriate platform Lite-Touch PE boot CD.
3. Boot your virtual machine from the bootable media selected above.
4. Select **Run the Deployment Wizard**, enter credentials to connect to the Microsoft Deployment Share, and then press **Enter**.
5. Select the **Win8 for View** task sequence, and click **Next**.
6. Enter Product Key information.
7. Specify a computer name, and click **Next**.
8. Select **Join a Workgroup**.

VMware View Composer or vCenter customization will join the virtual machine to the domain at a later time.

9. Click **Next** on Language and other preferences.
    a. Select Time Zone, and click **Next.**
    b. Click to select the VMware Tools and View Agent applications from the Application Install window.
10. Enter Administrator Password to be used for login after restart.
11. Click **Next** to begin the process of installing the operating system.

    The virtual machine restarts as necessary and provides visual updates as it progresses through the various stages.
12. Right-click the target virtual machine in vCenter.
13. Under the Guest submenu, install VMware Tools, then shut down the virtual machine.
14. In vCenter, edit the properties of the virtual machine.
15. Disconnect the WinPE bootable ISO, and remove the CD/DVD drive from the virtual machine.

Using the Target Virtual Machine to Create VMware Horizon View Desktops

At this point, the target virtual machine is an optimized Windows 7 or Windows 8 installation that is ready to be used in the Horizon View environment. When using this image for full- or linked-clone pools in Horizon View, you need to join the virtual machine to the target domain and customize the operating system to generate a unique instance for each user. You can use the Microsoft System Preparation Tool (Sysprep), VMware vCenter customizations settings, or the VMware View Manager QuickPrep tool.

Preparation of the Parent Virtual Machine
To use this virtual machine as a parent virtual machine for full clones, run `ipconfig/release`, power down the virtual machine, and convert it to a template. You can then use View Manager to select this virtual machine as the parent virtual machine for a full-clone desktop pool.

To use the target virtual machine as a parent virtual machine for linked clone pools, run `ipconfig/release`, power down the virtual machine, and create a snapshot. For linked clone-based pools, select the parent virtual machine and the specific snapshot to use for creating or recomposing desktop pools.

See VMware Horizon View Administration for details on preparing the parent virtual machine for the creation of desktop pools.

Windows 7 and Windows 8 OS Customizations

The following modifications are provided as recommendations for how to optimize the configuration of the Windows 7 or Windows 8 operating systems in a Horizon View desktop infrastructure. Appendix A provides a complete reference of the recommended customizations and lists the methods available for implementation (GPO, registry, service, command line).

If you apply customizations to the master image, they are persistent only if users cannot change them. If individual users have administrative rights, they can override these customizations. To preserve your customizations, modify the desktops by GPO so that the customizations are enforced.

Windows 7 and Windows 8 Service Modifications

Table 2 outlines the recommended state of services for Windows 7 and Windows 8 virtual machines. Services are common to both operating systems except where noted. Beginning with Windows 8, most unneeded services are in a manual (Triggered Start) state. Even if a service is configured as manual by default, you should still disable the service to avoid any potential issues. You can disable all of these services in your initial image before capturing.

Analyze each service for applicability in your corporate environment. Some Windows 7 and Windows 8 services detailed below, such as Windows 7 Themes, may actually be desired and left at default values.

Discretionary changes are marked with an asterisk ('*'). Non-applicable services for Windows 8 are designated not applicable under Comments.

SERVICE	NAME	DEFAULT	STATE	COMMENTS
Application Experience Lookup Service	AeLookupSvc	Manual Win8 Manual (Triggered Start)	Disable	Automatically applies software updates to programs to make sure that they run on newly released service packs.
*Background Intelligent Transfer Service	bits	Manual	Disable	Transfers files in the background using idle network bandwidth. If the service is disabled, Windows Update and MSN Explorer cannot automatically download programs and other information.
BitLocker Drive Encryption Service	dbesvc	Manual	Disable	Not recommended to encrypt VDI virtual machines.
Block Level Backup Engine Service	wbengine	Manual	Disable	Leveraged for backing up data on a workstation.
BranchCache	PeerDistSvc	Manual	Disable	Used for caching files on server in a branch office.
Computer Browser	Browser	Manual	Disable	Used for browsing computers on the same network.

SERVICE	NAME	DEFAULT	STATE	COMMENTS
*Desktop Window Manager Session Manager	UxSms	Auto	Disable	Disable if Aero is not necessary or desired. Not applicable for Windows 8.
Diagnostic Policy Service	DPS	Auto	Disable	Problem detection and troubleshooting resolution (disabled on Windows 8).
Diagnostic Service Host	WdiServiceHost	Manual	Disable	Problem detection and troubleshooting resolution.
Diagnostic System Host	WdiSystemHost	Manual	Disable	Problem detection and troubleshooting resolution.
Disk Defragmenter	Defragsvc	Manual	Disable	Provides disk defragmenting services for hard drives and can impact performance if run on a virtual machine. Not applicable on Windows 8.
Function Discovery Provider Host	fdPHost	Manual	Disable	The FDPHOST service hosts the Function Discovery (FD) network discovery providers. These FD providers supply network discovery services for the Simple Services Discovery Protocol (SSDP) and Web Services – Discovery (WS-D) protocol.
Function Discovery Resource Publication	FDResPub	Manual	Disable	Publishes this computer and resources attached to this computer so they can be discovered over the network.
Group Policy Client	gpsvc	Auto	Manual/ Triggered	Responsible for applying settings configured by administrator for the computer and users through the Group Policy component.
Home Group Listener	HomeGroupListener	Manual	Disable	Leveraged for Home Networking.
Home Group Provider	HomeGroupProvider	Manual	Disable	Leveraged for Home Networking.

SERVICE	NAME	DEFAULT	STATE	COMMENTS
Hyper-V Data Exchange Service	vmickvpexchange	Manual	Disable	Allows data exchange between virtual machine and operating system running on physical host machine. Windows 8 only.
Hyper-V Guest Shutdown Service	vmicshutdown	Manual	Disable	Facilitates shutdown of the virtual machine from the management interface on the physical computer. Windows 8 only.
Hyper-V Heartbeat Service	vmicheartbeat	Manual	Disable	Monitors the state of the virtual machine by reporting a heartbeat at regular intervals. Windows 8 only.
Hyper-V Remote Desktop Virtualization Service	vmicrdv	Manual	Disable	Provides a platform for communication between the virtual machine and operating system running on the physical computer. Windows 8 only.
Hyper-V Time Synchronization Service	vmictimesync	Manual	Disable	Synchronizes system time of the virtual machine with the system time of the physical computer. Windows 8 only.
Hyper-V Volume Shadow Copy Requestor	vmicvss	Manual	Disable	Coordinates the communications that are required to use Volume Shadow Copy Service to back up applications and data on the virtual machine from the operating system on the physical computer. Windows 8 only.
Family Safety	WPCSvc	Manual	Disable	Stub for Windows Parental Control functionality that existed in Windows Vista. Windows 8 only.

SERVICE	NAME	DEFAULT	STATE	COMMENTS
Windows Biometric Service	wbiosrvc	Manual	Disable	Gives client applications the ability to capture, compare, manipulate and store biometric data without gaining direct access to any biometric hardware or samples. Windows 8 only.
Windows Store Service	WSService	Manual (Triggered Start)	Disable	Provides infrastructure support for Windows Store. Started on demand and if disabled application bought using the Windows Store will not behave correctly. Windows 8 only.
Interactive Services Detection	UI0Detect	Manual	Disable	Displays a dialog box when a service tries to send a message to the console.
*IP Helper	*IP Helper	Auto	Disable	Disable if IPv6 is not leveraged.
Media Center Extender	Mcx2Svc	Manual	Disable	Allows Media Center Extenders to locate and connect to the computer. Not applicable on Windows 8.
Microsoft iSCSI Initiator Service	MSiSCSI	Manual	Disable	Not needed for virtual machines.
Microsoft Software Shadow Copy Provider	swprv	Manual	Disable/ Enable	Leveraged by the VSS for backups. Disable if you are not using System Restore and not using Horizon View Persona Management. Required for Persona Management, but must be enabled when using Persona Management.
*Offline Files	CscService	Manual	Disable	Used for maintenance of Offline Files cache. Should not be disabled for local mode desktops.
Parental Controls	wpcsvc	Manual	Disable	Restricts usage of certain programs based on time of day and duration.

SERVICE	NAME	DEFAULT	STATE	COMMENTS
Reports and Solutions Control Panel Support	wercplsupport	Manual	Disable	Provides support for viewing, sending and deletion of system-level problem reports for the Problem Reports and Solutions control panel.
Secure Socket Tunneling Protocol Service	SstpSvc	Manual	Disable	Used to provide VPN capability.
Security Center	wscsvc	Auto	Disable	Monitors configuration of security-related services.
SSDP Discovery	SSDPSRV	Manual	Disable	Used to discover UPnP devices.
*Superfetch	SysMain	Auto	Disable	Loads applications into memory for faster reload over time. Non-persistent virtual machines will likely not benefit from this setting being enabled.
Tablet PC Input Service	TabletInputService	Manual	Disable	Tablet PC Services.
*Themes	Themes	Auto	Disable	Only if you want to run as "Classic" interface (no "Orb" for start button) on Windows 7. Not applicable on Windows 8.
UPnP Host Service	upnphost	Manual	Disable	Dependent on SSDP Service.
Volume Shadow Copy Service	VSS	Manual	Disable/ Enable	Disable if you are not using System Restore and not using Horizon View Persona Management. Enable if using Persona Management.
Windows Backup	SDRSVC	Manual	Disable	Backs up workstation data.
*Windows Defender	WinDefend	Auto	Disable	Disable if Anti Spyware / Malware isn't needed.
Windows Error Reporting Service	WerSvc	Manual	Disable	Windows Error Reporting.
*Windows Firewall	MpsSvc	Auto	Auto	Do not disable service. Disable firewall profiles.

SERVICE	NAME	DEFAULT	STATE	COMMENTS
Windows Media Center Receiver Service	ehRecvr	Manual	Disable	Used by Media Center. Not applicable on Windows 8.
Windows Media Center Scheduler Service	ehSched	Manual	Disable	Used by Media Center. Not applicable on Windows 8.
Windows Media Center Network Sharing Service	WMPNetworkSvc	Manual	Disable	Used by Media Center. Not applicable on Windows 8.
*Windows Search	WSearch	Auto	Disable	Disable if you are not doing a lot of searching on a virtual machine.
*Windows Update	wuauserv	Auto	Disable	Disable unless needed for updates.
WLAN AutoConfig	Wlansvc	Manual	Disable	For managing wireless networks.
WWAN AutoConfig	WwanSvc	Manual	Disable	Used for Mobile Broadband Devices.

Table 2: Windows 8 and 7 Service Parameters

You can use a script to disable any of the services above programmatically before running `Sysprep` and capturing an image if you execute the following PowerShell syntax for each service:

```
Powershell Set-Service 'Service name' -startuptype "disabled"
```

For proper results, verify that you are using the Service Name, not the Display Name.

The `CommandsNoPersonaManagement` script disables all services listed in Table 2, and the `CommandsPersonaManagement` script disables all except the Microsoft Software Shadow Copy Provider service and Volume Shadow Copy service. Edit those scripts if you prefer not to disable some of these services.

In Windows 7 and Windows 8, the Remote Registry service is set to manual by default. To use the `Perfmon` of the VMware PCoIP Log Viewer tool to troubleshoot a desktop remotely, restart the Remote Registry service manually on that desktop.

Windows Customizations Available Using Group Policy

Customizations can be dynamically applied post-build through the use of GPOs. Many organizations prefer to use GPOs because existing policies that manage physical machines can be leveraged for virtual desktops as well. GPOs provide many benefits for desktop management, but care should be taken in their design and implementation. The following sections describe recommended practices for utilizing GPOs for Horizon View desktops.

Dedicated OU

The recommended approach is to place virtual machines in a dedicated Organizational Unit (OU) within Active Directory, block inheritance, and enforce loopback processing for user-based GPOs, so that any user GPOs applied at your dedicated OU override any other user-based GPOs applied previously.

Blocking Inheritance on an OU

Blocking inheritance is a potentially important step if you want to manage virtual machines. In some cases, a Group Policy being applied for computer accounts in other OUs may have a direct conflict with a setting, such as a wallpaper policy, that you want to apply in your environment. For additional information describing inheritance for Group Policies, see Microsoft's Group Policy Blog entry Tales from the Community: Enforced vs. Block Inheritance.

Loopback Policy Processing

Loopback policy processing is useful when you want to have Group Policies applied to users according to where the computer account is located in Active Directory. If a computer account is located in a special OU that has certain Group Policy settings applied for end users of those systems, leverage loopback policy processing to verify that Group Policies are applied in the expected and preferred fashion. For more information on implementing loopback policy processing, see the *Loopback Processing* section of the Microsoft TechNet Step-by-Step Guide to Understanding the Group Policy Feature Set.

POLICY	POLICY LOCATION	SETTINGS
Action Center Icon Removal	User Configuration > Administrative Templates > Start Menu and Taskbar	Remove the Action Center icon = Enabled
Event Logs	Computer Configuration > Administrative Templates > Event Log Service > Specific Event Log	Maximum application log size = 1024 Maximum security log size = 1024 Maximum system log size = 1024 If you are attempting to set the Security log size to 1024 with this Group Policy setting, you are restricted to 20480 unless you set this using the previous Group Policy Setting valid for Windows XP SP2 and Server 2003 and higher, located under Computer Configuration > Windows Settings > Security Settings > Event Log.
*Firewall	Computer Configuration > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall Properties	Firewall State = On (Recommended), or Off **Note:** Do not disable the Firewall Service. Disable the firewall profiles as needed.
Internet Explorer Settings (cache)	User Configuration > AdministrativeTemplates > Windows Components > Internet Explorer > Internet Control Panel > Advanced Page	Empty Temporary Internet Files folder when browser is closed = Enabled.
Internet Explorer Settings (IE First Run Wizard)	Computer Configuration > Administrative Templates > Windows Components > Internet Explorer	Prevent performance of First Run Customize settings = Enabled.

POLICY	POLICY LOCATION	SETTINGS
Recycle Bin	User Configuration > Administrative Templates > Windows Components > Windows Explorer	Do not move deleted files to the recycle bin = Enable to eliminate user undelete capabilities to save on disk storage, or Disable to preserve user undelete from the recycling bin functionality. The attached batch file scripts disable this parameter which means they enable deleted files to be stored in the recycling bin.
Remote Desktop	Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections	Enables users to connect remotely using Remote Desktop Services = Enabled.
Remote Desktop	Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security	Require user authentication for remote connections by using Network Level Authentication = Enabled.
RSS Feeds	User Configuration > Administrative Templates > Windows Components > RSS Feeds	Turn off background sync for feeds and Web. Slices = Enabled.
*Screen Saver	User Configuration > Administrative Templates > Control Panel > Personalization	Password protect the screen saver = Enabled. Screen saver timeout = 600. Force specific screen saver = %windir%\system32\scrnsave.scr.
System Restore	Computer Configuration > Administrative Templates > System > System Restore	Turn off System Restore = Enabled.

POLICY	POLICY LOCATION	SETTINGS
User Access Control	Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options	User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode = Elevate without prompting. User Account Control: Detect application installations and prompt for elevation = Disabled. User Account Control: Only elevate UIAccess applications that are installed in secure locations = Disabled. User Account Control: Run all administrators in Admin Approval Mode = Disabled.
Wallpaper	User Configuration > Administrative Templates > Desktop > Desktop	Desktop Wallpaper = " ". **Note:** A "space" is required to set the wallpaper to none in the above setting. Optionally, setting to a file that does not exist will actually prevent a user from setting wallpaper at all.
Windows Defender	Computer Configuration > Administrative Templates > Windows Components > Windows Defender	Turn off Windows Defender = Enabled.
Windows Sideshow	Computer Configuration > Administrative Templates > Windows Components > Windows Sideshow	Turn off Windows Sideshow = Enabled.
*Windows Update	Computer Configuration > Administrative Templates > System > Internet Communication Management > Internet Communication Settings	Turn Off Access to All Windows Update Features = Enabled. Turn off Windows Update Device Driver Searching = Enabled. **Note:** If the Windows Update Service is disabled, this setting is not necessary.

Table 3: Windows 7 and Windows 8 Group Policies

Windows 7 and Windows 8 Customizations Using the Registry

Many optimizations can be programmatically applied through modification of the registry. Most of the modifications that directly affect the operating system are contained in the HKEY Local Machine (HKLM) hive. Others can be made in the users' registry to reduce repetitive tasks and improve visual desktop characteristics. The visual desktop settings, such as screensavers and backgrounds, can unnecessarily introduce significant bandwidth into the display stream, which is why they are included as recommended optimizations.

Creating and Modifying the Default User Profile

For years, administrators have been customizing the default profile for a standard image by customizing the profile of the local administrator, and then copying that profile to the default user profile directory, complete with all customizations required for each user who logs into a system. This process was problematic and not officially supported by Microsoft. There is one method, however, that can be leveraged to alter the default user profile using the attached command script files. The best method for an organization is determined by reviewing the available supported solutions and picking the one that is most suited for its needs.

Modify default user profile settings before running Sysprep and capturing the image.

Modifying the Default User Profile

The following methods for modifying the default user profile are supported:

Automated Profile Copy with Sysprep (CopyProfile)

http://technet.microsoft.com/en-us/library/cc748953(WS.10).aspx
http://support.microsoft.com/kb/973289

Scripted Approach

http://support.microsoft.com/?id=284193

The scripts attached to this document use the method recommended in the following blog post:

http://blogs.technet.com/b/deploymentguys/archive/2009/10/29/configuring-default-user-settings-full-update-for-windows-7-and-windows-server-2008-r2.aspx

Group Policy Preferences

http://www.microsoft.com/downloads/details.aspx?FamilyID=42e30e3f-6f01-4610-9d6e-f6e0fb7a0790&displaylang=en

Scripted Approach for Modifying the Default User Profile

`Commands.bat` and `TS.xml` use the following approach to modify the default user profile.

This process is only intended to incorporate default user settings into a standard image.

1. Identify the HKCU settings that need to be included in the default user profile for a Windows 7 standard image. Keep these settings specific to Windows, such as those presented here (default screensaver settings, default wallpaper behavior, and so on).

Microsoft states that not all HKCU settings can be applied programmatically using registry inserts, so your results may vary. For consistent results, establish defaults for your Horizon View virtual machines, using Group Policy whenever possible.

2. Create a batch file, script, or PowerShell command that initiates loading the `NTUser.DAT` file for the default user profile into `regedit` in order to update.

```
REG LOAD hku\Test" "%USERPROFILE%\..\Default User\NTUSER.DAT"
```

   This example assumes the hive for default is loaded into **Test** under `HKEY_Users` in the registry. Execute the command exactly as it is shown, changing only the `hku\Test` to another location, such as `hku\TEMP`, if desired.

3. While the hive is open for editing, insert any registry updates required for the **\Default User\NTUSER.DAT** file using either REG, PowerShell, or **regedit /S** commands. REG is used below to illustrate one way of inserting values.

```
REG ADD
"hku\Test\Software\Microsoft\Windows\CurrentVersion\Policies \
System" /v Wallpaper /d "" /f
```

4. Finally (very important), the registry hive needs to be unloaded to save the changes imported into the default user profile. Failure to do this holds the hive open by the currently logged–on user and prevents updates from being appended.

```
REG unload "hku\Test"
```

The batch file should now resemble the following:

```
REG LOAD "hku\Test" "%USERPROFILE%\..\Default User\NTUSER.DAT"

REG ADD "hku\Test\Software\Microsoft\Windows\CurrentVersion\Policies \
System" /v Wallpaper /d "" /f

REG unload "hku\Test"
```

Verify that there is no domain-wide default user hive in the **\\domain.local\netlogon\Default User.v2** directory, where **domain.local** is the local domain name for the desktop pool. If such a domain-wide default hive file exists, it will be used to apply user registry settings to new users, and the local **\Default Users\ntuser.dat** file will be ignored.

Managing VMware Horizon View Desktops

The goal of optimizing Windows operating systems extends beyond the initial build and deployment of optimized virtual machines. This section reviews settings that are relevant to the ongoing management of Horizon View desktops and optional settings to modify the default behavior of the PCoIP display protocol.

View Manager Idle Settings

VMware View Manager™ provides settings that determine the length of time that idle or disconnected Horizon View desktops continue to consume system resources before going into suspended mode or powering down. These settings can be modified per desktop pool or managed by Horizon View policies. Determining an acceptable length of time can significantly reduce the load on the system hardware. However, putting machines into suspension or setting up users to constantly power on their desktops is counterproductive, so address these settings carefully.

Managing PCoIP Using GPOs

In some cases, part of optimization can include limiting or tuning the PCoIP protocol for certain network environments. The `PCoIP.ADM` file is provided with VMware Horizon View and can be used to deploy these settings to View Clients, using GPOs. For further details, see the Horizon View 5 with PCoIP Network Optimization Guide.

GPO PCoIPImagingMaximumInitialImageQuality
In a limited bandwidth scenario, this setting can be used to configure a preference between higher initial image quality, with larger peaks in bandwidth during large screen changes, or lower initial image quality, with smaller peaks in bandwidth during large screen changes.

If used, consider adjusting the maximum imaging quality before applying a bandwidth limit. Set to a value between 0 – 100 (default is 90). This value must be set lower than the `PCoIPImagingMinimumInitialQuality` value.

GPO PCoIPMaxLinkRate
The PCoIP protocol is designed to take advantage of available network bandwidth and share bandwidth fairly across active users on a link. You should not change this setting unless you have carefully determined the overall effect to be beneficial. Be careful not to set a maximum bandwidth limit so low that individual sessions cannot take advantage of additional link bandwidth when available.

If you use this setting, configure it for all users who share a particular network link.

Set `PCoIPMaxLinkRate` to the desired maximum PCoIP session bandwidth in kilobits per second (that is, 1000 = 1000Kbps = 1Mbps). The default is 1Gbps; 0 = no bandwidth constraints.

References

Configuring PCoIP for Use with View Manager, VMware Knowledge Base article

Group Policy Settings Reference for Windows and Windows Server

Group Policy Registry Table

Using REG to Update the Registry

Horizon View 5 with PCoIP Network Optimization Guide

Horizon View Persona Management Deployment Guide

About the Authors and Contributors

Kaipo Batoon, Senior Technical Marketing Manager in End-User Computing at VMware, edited the scripts for Horizon View 5.2 and refined the specifications for the Volume Shadow Copy Service and Windows Firewall. Kaipo also updated the scripts to be compatible with Horizon View 5.3 Feature Pack 1, and fixed some character-translation / Unicode issues.

Tina de Benedictis, Senior Technical Marketing Manager in End-User Computing at VMware, updated this document to accommodate the Persona Management and 3D graphics features in View 5.0.

Jim Britt of Ensynch, Inc. wrote the original version of this paper with Aaron Black of VMware. Aaron Black is currently a Product Manager in End-User Computing at VMware.

The following VMware technical staff contributed content and tested the scripts: Matthew Mabias, Phillip Helmling, Todd Dayton, Jeff Birnbaum, Charles A. Windom Sr., John Dodge, Marilyn Basanta, Rory Clements, Aaron Black, Timothy Federwitz, Rasmus Jensen, Erik Haire, Linus Bourque, Jason Miles, and Warren Ponder.

To comment on this paper, contact the VMware End-User Computing Solutions Management and Technical Marketing team at twitter.com/vmwarehorizon.

Appendix A (Customizations Reference)

Table 4 lists all recommended settings to optimize Windows 7 and Windows 8 operating systems for your Horizon View desktop infrastructure. The Method column represents the available mechanisms to apply these settings. The method chosen should be based upon organizational restrictions and preferences. Discretionary changes are marked with an asterisk ('*').

TYPE	DESCRIPTION	STATUS	METHOD	HIVE
Customization	Action Center Icon	Disable	GPO, Registry	HKCU
Customization	Set Boot to "No GUI"	Disable	Command Line	HKLM
Customization	Crash Dump	Disable	Registry	HKLM
Customization	Automatically Reboot after crash	Enable	Registry	HKLM
Customization	Crash Dump	Disable	Registry	HKLM
Customization	Log crash event	Disable	Registry	HKLM
Customization	Alert on crash event	Disable	Registry	HKLM
Customization	Disk Timeout Value	Modify	Registry	HKLM
Customization	Event Logs	Modify	GPO, Registry	HKLM
Customization	Hibernation	Disable	Command Line	HKLM
Customization	IE Cache	Disable	GPO, Registry	HKCU
Customization	IE First Run Wizard	Disable	GPO, Registry	HKLM
Customization	IE RSS Feeds	Disable	GPO, Registry	HKCU
Customization	Start_PowerButtonAction	Modify	Registry	HKCU
Customization	Visual Effects	Modify	Registry	HKCU
Customization	Menu Show Delay	Modify	Registry	HKLM
Customization	Terminal Server Client send interval	Modify	Registry	HKLM
Customization	FastSendDatagramThreshold	Modify	Registry	HKLM

TYPE	DESCRIPTION	STATUS	METHOD	HIVE
Customization	Service Startup Timeout	Modify	Registry	HKLM
Customization	View agent debug	Modify	Registry	HKLM
Customization	View agent trace	Modify	Registry	HKLM
Customization	Background Layout Service	Disable	Registry	HKLM
Customization	Machine Account Password Changes	Disable	Registry	HKLM
Customization	TCP/IP Task Offload	Disable	Registry	HKLM
Customization	Hard Error Messages	Disable	Registry	HKLM
Customization	CIFS Change Notifications	Disable	Registry	HKLM
Customization	Customer Experience Improvement Program	Disable	Registry, Command Line	HKLM
Customization	Language Bar	Disable	Command Line	HKLM
Customization	Windows Update Uninstall folders	Delete	Command Line	
Customization	Image Revision	Modify/ Create	Registry	HKLM
Customization	Last Access Timestamp	Modify	Command Line	HKLM
Customization	Network Location Dialogue	Modify	Registry	HKLM
Customization	Recycle Bin	Enable Deleted File Retention	GPO, Registry	HKLM
Customization	Registry Idle Backup	Disable	Command Line	HKLM
Customization	Screensaver	Enable and Configure	GPO, Registry	HKCU
Customization	Wallpaper	Disable	GPO, Registry	HKCU
Customization	WinSAT (Windows System Assessment Tool)	Disable	Command Line	HKLM

TYPE	DESCRIPTION	STATUS	METHOD	HIVE
Feature	User Access Control	Turn off or Configure	GPO, Registry	HKLM
Feature	Windows Sideshow	Disable	GPO, Registry	HKLM
Feature	IPv6	Disable	Registry	HKLM
Feature/Service	System Restore	Disable	GPO, Registry, Services, Command Line	HKLM
Windows Service	*Desktop Window Manager Session Manager	Disable	Services	HKLM
Windows Service	*IP Helper	Disable	Services	HKLM
Windows Service	*Superfetch	Disable	Registry, Services	HKLM
Windows Service	*Themes	Disable	Services	HKLM
Windows Service	*Windows Defender	Disable	GPO, Services, Command Line	HKLM
Windows Service	Tablet PC Input	Disable	Services	HKLM
Windows Service	*Windows Firewall	Configure/ Disable	GPO, Services, Command Line	HKLM
Windows Service	Application Experience Lookup	Disable	Services	HKLM
Windows Service	BranchCache	Disable	Services	HKLM
Windows Service	Block Level Backup Engine Service	Disable	Services	HKLM

Table 4: Customization Reference Table

Appendix B (Commands.bat)

To optimize a Windows 8 or Windows 7 desktop template, you can create a `Commands.bat` file from one of two files attached to this guide: `CommandsPersonaManagement.txt` or `CommandsNoPersonaManagement.txt`. To save one of these text files, go to the **Adobe Reader View** menu, select **Show/Hide** > **Navigation Panes** > **Attachments**, then select the text file of your choice, and select **Save**. Choose the `CommandsPersonaManagement.txt` file if you plan to implement Horizon View Persona Management. Choose `CommandsNoPersonaManagement.txt` if you do not plan to implement Horizon View Persona Management. Rename to `Commands.bat` for batch file execution.

Caution: Open the script on a Windows machine. Use a script editor or WordPad to avoid possible line-break issues with Notepad.

Any HKEY user setting applied to the default user applies only to new profiles created. The administrator's default profile is left untouched. To see the effects of modifications to the default user profile, log in to a different user account than the local administrator's account.

If you are implementing Persona Management, the following two lines have been deleted from the `CommandsNoPersonaManagement.txt` file to create the `CommandsPersonaManagement.txt` file:

```
Powershell Set-Service 'VSS' -startuptype "disabled"

...

vssadmin delete shadows /All /Quiet
```

By deleting these lines, these desktops are ready for Persona Management enablement.

Appendix C (CommandsDesktopReadyForPersona Management.txt)

If you have an existing desktop image without Persona Management, and you want to deploy Persona Management on that desktop image, create a BAT file on your virtual machine template from the attached `CommandsDesktopsReadyForPersonaManagement.txt` file. From the **Adobe Reader View** menu, select **Show/Hide** > **Navigation Panes** > **Attachments** > **Save**, and save the TXT file as a BAT file. Run this script as an administrator (right-click and **Run as Administrator**). Reboot the computer when the BAT file completes.

Caution: Open the script on a Windows machine. Use a script editor or WordPad to avoid possible line-break issues with Notepad.

Appendix D (TS.xml)

The `TS.xml` file, which contains an example task sequence, is included in this guide as an attachment called `MDT 2012 Task Sequences Files.zip.txt`. This ZIP file contains a set of customized `TS.xml` files. To save this set of `TS.xml` files, go to the **Adobe Reader View** menu, select **Show/Hide** > **Navigation Panes** > **Attachments**, select the file, and click **Save**. After the `MDT 2012 Task Sequence Files.zip.txt` file is saved to the machine, change the extension to `.zip`. Then unzip the file and use the appropriate `ts.xml` file.

Note: If you are using Windows and have file extensions turned off, the `.txt` suffix does not appear in the downloaded file. Open a command window and navigate to the directory where you saved the `.zip.txt` file from Adobe Reader. Type

```
move “MDT 2012 Task Sequence Files.zip.txt” “MDT 2012 Task Sequence Files.zip”
```

For step-by-step guidance, see Using the Microsoft Deployment Toolkit to Optimize Windows.

Appendix E (Summary of Script Changes)

The following changes were made to the `CommandsNoPersonaManagement.txt` file and the `CommandsPersonaManagement.txt` file since the previous version of this document.

Removed

```
Rem Remove recycling bin

reg ADD “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
policies\Explorer” /v NoRecycleFiles /t REG_DWORD /d 0x1 /f
```

Added

```
Rem Enable recycling bin

reg ADD “HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer”
/v NoRecycleFiles /t REG_DWORD /d 0x0 /f

rem Set Windows Visual Effects to Optimized for best performance

reg ADD “hku\temp\Software\Microsoft\Windows\CurrentVersion\Explorer\
VisualEffects” /v VisualFXSetting /t REG_DWORD /d 0x2 /f

rem Set the Start Power Button to Log off as the default

reg ADD “hku\temp\Software\Microsoft\Windows\CurrentVersion\Explorer\
Advanced” /v Start_PowerButtonAction /t REG_DWORD /d 0x1 /f

rem Reduce Menu Show Delay

reg Add “hku\temp\Control Panel\Desktop” /v MenuShowDelay /t REG_DWORD /d
120 /f

Rem Lower Terminal Server Client send interval

Reg ADD “hku\temp\Software\Microsoft\Terminal Server Client” /v Min Send
Interval /t  reg_dword /d 1 /f

rem Making modifications to .DEFAULT

rem Disable Screen Saver at Logon/Welcome Screen
```

```
reg ADD “HKU\.DEFAULT\Control Panel\Desktop” /v ScreenSaveActive /d “0” /f

rem Set Wallpaper to blank at Logon/Welcome Screen

reg ADD “HKU\.DEFAULT\Control Panel\Desktop” /v Wallpaper /d “ “ /f

rem Disable Address space layout randomization

reg ADD “HKLM\System\CurrentControlSet\Control\Session Manager\Memory
Management” /v MoveImages /t REG_DWORD /d 0x0 /f

rem Enable “Automatically Reboot”

reg ADD “HKLM\SYSTEM\CurrentControlSet\Control\CrashControl” /v AutoReboot
/t REG_DWORD /d 0x1 /f

rem Disable “Write an event to the system log”

reg ADD “HKLM\SYSTEM\CurrentControlSet\Control\CrashControl” /v LogEvent /t
REG_DWORD /d 0x0 /f

rem Disable “Send an alert”

reg ADD “HKLM\SYSTEM\CurrentControlSet\Control\CrashControl” /v SendAlert /t
REG_DWORD /d 0x0 /f

rem Disable IPv6

reg Add “HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters” /v
DisabledComponents /t REG_DWORD /d 0xffffff /f

rem Increase Service Startup Timeout – Allows up to 120 seconds before
timing out waiting for a service

reg Add “HKLM\System\CurrentControlSet\Control” /v ServicesPipeTimeout  /t
REG_DWORD /d 120000 /f

rem Don’t buffer UDP packets less than 1500 Bytes – improves high bandwidth
video performance

reg Add “HKLM\System\CurrentControlSet\Services\Afd” /v
FastSendDatagramThreshold /t REG_DWORD /d 1500 /f

rem Disable View agent debug

reg Add “HKLM\software\VMware, Inc.\VMware VDM\” /v DebugEnabled /t REG_SZ
/d False /f

rem Disable View agent trace

reg Add “HKLM\software\VMware, Inc.\VMware VDM\” /v TraceEnabled /t REG_SZ
/d False /f

rem Disable Background Layout Service

reg ADD “HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\OptimalLayout” /v
EnableAutoLayout /t  reg_dword /d  0 /f

rem Disable Machine  Account Password Changes

reg ADD “HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters” /v
DisablePasswordChange /t reg_dword /d 0 /f

Rem Disable TCP/IP Task Offload

Reg ADD “HKLM \SYSTEM\CurrentControlSet\Services\TCPIP\Parameters” /v
DisableTaskOffload /t REG_DWORD /d 1 /f

Rem Hide Hard Error Messages
```

```
Reg ADD “HKLM\SYSTEM\CurrentControlSet\Control\Windows” /v  ErrorMode /t
REG_DWORD /d 0 /f

Rem Disable CIFS Change Notifications

reg ADD “HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer”
/v  NoRemoteRecursiveEvents /t Reg_dword /d 1 /f

rem Disable customer experience improvement program

Reg ADD “HKLM\Software\Microsoft\SQMClient\Windows” /v CEIPEnable /t REG_
DWORD /d 0 /f

rem Application Experience Lookup Service

Powershell Set-Service ‘AeLookupSvc’ -startuptype “disabled”

Rem BranchCache

Powershell Set-Service ‘PeerDistSvc’ -startuptype “disabled”

rem Computer Browser

Powershell Set-Service ‘Browser’ -startuptype “disabled”

rem Diagnostic Service Host

Powershell Set-Service ‘WdiServiceHost’ -startuptype “disabled”

rem Diagnostic System Host

Powershell Set-Service ‘WdiSystemHost’ -startuptype “disabled”

rem Problem Reports and Solutions Control Panel Support

Powershell Set-Service ‘wercplsupport’ -startuptype “disabled”

rem Parental Controls

Powershell Set-Service ‘wpcsvc’ -startuptype “disabled”

rem Windows Media Center Sharing Service

Powershell Set-Service ‘WMPNetworkSvc’ -startuptype “disabled”

Rem Disable Interactive Services Detection

Powershell Set-Service ‘UI0Detect’ -startuptype “disabled”

Rem Background Intelligent Transfer

Powershell Set-Service ‘bits’ -startuptype “disabled”

rem  Function Discovery Resource Publication

Powershell Set-Service ‘FDResPub’ -startuptype “disabled”

rem  Media Center Extender Service

Powershell Set-Service ‘Mcx2Svc’ -startuptype “disabled”

rem Disable the Language Bar

Regsvr32.exe /u /s msutb.dll

rem Delete hidden Windows Update uninstall folders

del /A:H /S /F /Q %WINDIR%\$Nt*
```

```
rem disable Customer Experience Improvement Program tasks

schtasks /change /tn “microsoft\windows\Application Experience\AitAgent”/
disable

schtasks /change /tn “microsoft\windows\Application Experience\
ProgramDataUpdater” /disable

schtasks /change /tn “microsoft\windows\Customer Experience Improvement
Program\Consolidator” /disable

schtasks /change /tn “microsoft\windows\Customer Experience Improvement
Program\KernelCeipTask” /disable

schtasks /change /tn “microsoft\windows\Customer Experience Improvement
Program\UsbCeip” /disable
```

The Volume Shadow Copy Service (VSS) and the Windows Firewall require special treatment when optimizing Windows 7 and Windows 8 desktops.

Managing Volume Shadow Copy Service

In an environment where Persona Management is not being used, we recommend deleting shadow copies and disabling the VSS service. In the current version of the `CommandsNoPersonaManagement.txt` script, any existing shadow copies are deleted before the service is disabled.

In an environment where Persona Management is being used, we require the VSS services. In the `CommandsPersonaManagement.txt` script, the VSS service remains enabled.

Modifications (CommandsNoPersonaManagement.txt Script)

```
REM *************************************************************

REM *****************  No Persona Management Start

rem ***

rem *** Delete shadows and Disable the Volume Shadow Copy Service and the
Shadow Copy Protection Service if not using Persona Mgmt

vssadmin delete shadows /All /Quiet

Powershell Set-Service ‘swprv’ -startuptype “disabled”

Powershell Set-Service ‘vss’ -startuptype “disabled”

rem ***

rem ****************** No Persona Management End

REM *************************************************************
```

Managing Windows Firewall

It is recommended that you enable Windows Firewall with the `DomainProfile` disabled. The remaining firewall profiles, `PrivateProfile` and `PublicProfile`, can be enabled depending on your corporate security policy.

The following modifications were made to the `CommandsNoPersonaManagement.txt` and `CommandsPersonaManagement.txt` scripts since the previous version of this document.

Modifications (CommandsNoPersonaManagement.txt and CommandsPersonaManagement.txt Scripts)

```
rem ************************************************************
rem *** Set Firewall Domain profile off
rem *** Set Firewall Private profile on
rem *** Set Firewall Public profile on
netsh advfirewall set publicprofile state on
netsh advfirewall set privateprofile state on
netsh advfirewall set domainprofile state off
rem ***
rem ************************************************************
```

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com