Windows XP Deployment Guide

For VMware® View™

WHITE PAPER

vmware®

VMware® View™ transforms the way customers use and manage desktop operating systems. Desktop instances can be deployed rapidly in secure datacenters to facilitate high availability and disaster recovery, protect the integrity of enterprise information, and remove data from local devices that are susceptible to theft or loss. Isolating each desktop instance in its own virtual machine eliminates typical application compatibility issues and improves users' personal computing environments.

About This Guide

This guide suggests best practices for creating Windows XP–based templates for use with View 5 and later.

Creating the Initial Virtual Machine

The initial virtual machine establishes a virtual hardware profile for rapid deployment of other virtual desktop instances. You can create the initial virtual machine from scratch, as described in this guide, or convert a physical machine to a virtual machine, using either the standalone version of VMware vCenter™ Converter™ or the version integrated with VMware vCenter. VMware Converter images the target PC and migrates it into VMware vSphere®. When the migration is complete, you can convert the virtual machine to a template and then use it as the basis for deploying future virtual desktops.

To create the initial virtual machine from scratch, follow these steps:

1. Use the vSphere Client™ to connect to your vCenter server.
2. Use the console to configure the initial virtual machine or template.
3. Install the OS using the console.

When you establish a connection with your vSphere datacenter, create a new virtual machine from inventory. When you create a virtual machine, the New Virtual Machine wizard appears. Use the custom configuration parameters in Table 1 as baseline settings for the template. If you use View 5.x as your virtual desktop manager for deploying pooled virtual desktops, you can change these settings at deployment time.

Table 1. Custom Configuration Parameters

PARAMETER	COMMENTS
Name and Location	This can be a generic name, such as **`xptemplate`**. The location can be any folder within your datacenter inventory.
Host/Cluster	The VMware ESX®/VMware ESXi™ server or cluster of server resources that will run this virtual machine. It can be changed at any time. This location does not necessarily specify the location of future virtual machines created from this template.
Resource Pool	If the physical ESX/ESXi server resources are divided granularly using resource pools, they can be assigned to this virtual machine.
Datastore	The location where you want to store the files associated with the virtual machine.
Guest Operating System	The operating system that will be installed.
CPUs	The number of virtual processors that will be presented to the virtual machine. For most View users, a single processor is sufficient.

PARAMETER	COMMENTS
Memory	The amount of memory to allocate to each virtual machine created from this template (in most cases, 512MB, for Windows XP).
Network	The number of virtual network adapters that will be used. One is usually enough. As a best practice, make the network name consistent across vSphere. An incorrect network name in a template can cause failures during the instance customization phases.
I/O Adapters	The LSI Logic adapter issued for deployments based on View is recommended; however, the LSI Logic driver is not included as part of the Windows XP installation procedure. Download and add it during the OS installation.
Disk	Creates a new disk when you create the initial virtual machine or template. Specify the amount of local storage to allocate to each user. Allow at least enough for the OS installation, patches, and locally installed applications. A best practice is to store as much of the user's information, profile, and documents on network shares as possible, rather than locally. Doing so can greatly reduce the need for disk space and management of local data.

Installing Windows XP

Virtual machines behave like physical machines, so Windows XP installation is essentially the same on both. Although it is possible to image your virtual machine using some type of cloning technology, this guide focuses on a fresh Windows XP installation.

Preparation

LSI storage controller drivers are not available on the Windows XP installation CD, so be sure to complete the following tasks before starting the installation:

1. Download the LSI 53C1030 drivers from the LSI Web site.
2. Using MagicISO or other third-party solutions, create an .flp image containing the LSI Logic drivers.
3. Use SCP to transfer the floppy image to the virtual machine's ESX/ESXi host. If you are using vCenter, you can use the vSphere Client to upload the file to the datastore.
4. Be sure you have a Windows XP CD or ISO image that is accessible from the virtual machine.

Preinstallation Modifications to the Virtual Machine

Make the following modifications to the virtual machine hardware profile before starting the Windows XP installation:

1. Using the vSphere Client, connect to vCenter.
2. Locate the virtual machine you created earlier.
3. Edit the following hardware settings:
    a. Ensure that there is a floppy drive present.
    b. Configure the floppy drive to connect at power on.
    c. If using a floppy image, ensure that the device type is set to use a floppy image and is pointing to the LSI Driver image.
    d. Check that the CD/DVD drive is present and configured to connect at power on.
    e. Configure the CD/DVD device type to point to the Windows XP CD or ISO image.

Installation

After you complete the preinstallation preparation and modifications, you can install Windows XP:

1. From the vSphere Client, connect to vCenter.
2. Power on the virtual machine created earlier.
3. Use the console to view the boot process and to send input to the virtual machine.
4. As the Windows setup process begins, press F6 to add another SCSI driver. This lets you specify the LSI Logic driver on the floppy image.

The Windows setup process copies all the necessary files to the virtual disk. Complete the setup just as you would for any normal Windows XP installation. Because this image will be used as a template, however, it is a good idea to make the configuration as generic as possible. (For information on customization, see Creating a Guest Customization.)

After completing the Windows setup, perform the following tasks before you finalize the image. Some of these steps will vary from organization to organization, depending on your Windows imaging standards; some are optional. Many can be managed using a group policy (see Managing Virtual Desktops Using Common GPOs).

Recommended Steps

1. If SP2 has not been applied to the installation CD, install SP2 and the most recent Microsoft updates.
2. Install and configure the VMware Tools.
3. Install View Agent.
4. Install and configure any additional third-party or in-house applications needed.
5. Set the Windows screen saver to "blank."
6. Configure the default color setting for the Windows Remote Desktop Client Connection. By default, Windows XP uses 16-bit color for Remote Desktop. You can enable and manage 24-bit color centrally by using a group policy or by making the following registry change:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp`
   Change the color depth to 4.

Optional Steps

1. Disable any unused hardware, such as COM1 and COM2.
2. Turn off theme enhancements.
3. Adjust **My Computer** > **Properties** > **Advanced tab** > **Performance section** > **Settings** for best performance.
4. Set the blank screen saver to **Password protect on resume**.
5. Ensure that hardware acceleration is enabled.
   Start > **Control Panel** > **Display** > **Settings tab** > **Advanced button** > **Troubleshooting tab**
6. Delete any hidden update uninstall folders in the `C:\Windows directory`.
   For example: `$NtUninstallKB893756$`
7. Disable Indexing Services:
   Start > **Control Panel** > **Add Remove Windows Components** > **Indexing Service**
   Note: Indexing improves searches by cataloging files. For users who search a lot, indexing may be beneficial and should not be disabled.
8. Disable indexing of the **C:** drive in **Properties.**
9. Remove or minimize System Restore points:
   Start > **Control Panel** > **System** > **System Restore**
10. Disable any unwanted services.
11. Run Disk Cleanup:
    My Computer > **C:** drive in **properties**
12. Run Disk Defrag:
    My Computer > **C: properties** > **Tools**

After the preparations and installation are complete, you can power off the virtual machine and get ready to enable it as a deployment template for other virtual desktops.

Converting a Virtual Machine to a Template

Templates standardize the creation of virtual desktops and reduce the risk of human error. Many organizations use separate templates for different types of users or workgroups, such as Finance, HR, and Sales, where each group typically uses a unique software or virtual hardware configuration. Templates help you automate and manage desktop provisioning.

- Any virtual machine can be *converted* to a template: just connect to vCenter using the vSphere Client, locate the virtual machine in the inventory, and select **Convert to Template**.
- Any virtual machine can also be *cloned* to a template. Cloning creates a copy of the virtual machine, leaving the original in place.

Cloning is helpful if you update the template and redeploy desktops often—for instance, if you deploy nonpersistent desktops or if you use a profile solution to separate the user profiles from the desktop environment. Cloning enables you to convert a template to a virtual machine, update it, and then convert it back to a template at any time.

Creating a Guest Customization

Guest customization enables you to customize virtual desktops as they are created. Using Microsoft Sysprep, vCenter guest customization automates configuration tasks such as the following:

- Adding registration information
- Assigning a unique computer name
- Adding your product key
- Setting the administrator password
- Setting the time zone
- Adding any custom run-once scripts
- Defining the network configuration
- Joining a domain
- Generating a new SID

VMware View works with any existing predefined guest customization specification. You can select which guest customization file to use, if any, to customize the pool of virtual desktops.

To create a guest customization specification, follow these steps:

1. Connect with vCenter using the vSphere Client.
2. Select **Edit > Customization Specifications**.
3. When the Customization Specification Manager starts, select **New**.

If you prefer, you can import an existing custom `sysprep.ini` file and use it in the Guest Customization wizard. As a best practice when using View and a guest customization specification, set the **Computer Name** portion of the guest specification to **Use the Virtual Machine Name**. This ensures that the computer name is consistent across View, vCenter, Active Directory, and Local Computer Name.

When your initial virtual machine, template, and guest customization are complete, the virtual desktop template is ready, and you can use it when deploying virtual desktops.

Managing Windows XP View Desktops

The following sections focus on best practices for simplifying and standardizing some common desktop management tasks.

Adding Users to the Local Remote Desktop Users Group

You need to add users to the Windows XP local group Remote Desktop Users, so that they will be able to access individual or pooled desktops. There are several ways to add users or groups to the local Remote Desktop Users group. One approach is to use a login script. Another approach leverages the Restricted Groups GPO in Active Directory.

When leveraging Restricted Groups, you can add users individually, or you can create a group, add users to it, and then add that group to the Restricted Group you are managing. Here are the steps for configuring a Restricted Group using the Default Domain Policy:

1. Using your Microsoft Management Console (MMC) with the Group Policy console for your domain, create a new group called View Users under **Active Directory** > **Users and Computers**.
2. Add users to this group who need to access the virtual desktops.
3. Edit your Default Domain Policy.
4. Under **Computer Configuration** > **Windows Settings** > **Restricted Groups**, add the Remote Desktop Users Group.
5. Add the View Users group to the Restricted Remote Desktop Users group.

This approach ensures that the View Users group is always added to the local Remote Desktop Users group of each virtual desktop joined to the domain. When provisioning new users, an administrator or helpdesk technician must only ensure that users are added to the View Users group in Active Directory.

Managing Virtual Desktops Using Common GPOs

There are several Group Policy objects (GPOs) that can be used for central control of the configuration of your virtual desktops. Because users access their virtual desktops with Remote Desktop, the most commonly used GPOs are the Terminal Server GPOs under **Computer** or **User Configuration** > **Administrative Templates** > **Windows Components** > **Terminal Services**. Several of the GPOs are specific to Terminal Server and do not apply to Remote Desktop sessions. Some of the commonly used GPOs for deploying Windows XP in a View environment are described in Table 2 and Table 3. Many of these GPOs are optional but recommended. Naturally, use cases and environments vary depending on your organization's standards and policies.

Table 2. GPOs Under Terminal Services

SERVICE	DESCRIPTION
Enforce removal of Remote Desktop wallpaper = Enable	This setting can greatly enhance the user experience, especially over low-bandwidth connections.
Limit maximum color depth = Enable	This setting lets you set the color depth for Remote Desktop sessions.
Allow users to connect remotely using Terminal Services = Enable	This setting ensures that the local policy enabling Remote Desktop connections is configured.
Remote Windows security item from Start Menu = Disable	The Disable setting ensures that users have a logout mechanism.
Remove Disconnect option from Shut down dialog = Enable	This setting minimizes the possibility of users disconnecting rather than logging out.
I/O adapters	The LSI Logic adapter issued for deployments based on View is recommended; however, the LSI Logic driver is not included as part of the Windows XP installation procedure. Download and add it during the OS installation.

Table 3. GPOs Under Terminal Services > Sessions

SERVICE	DESCRIPTION
Set time limit for disconnected sessions = Enable	This setting logs out any disconnected sessions that occur after the specified time. Combined with View virtual machine power policies, this setting can be used to create a dynamic and powerful solution for suspending or powering off disconnected virtual desktops. When unneeded desktops are suspended or powered off, the resources are made available to other desktops.
Set a time limit for active but idle Terminal Services sessions = Enable	This setting logs out any idle sessions that occur after the specified time. Combined with View virtual machine power policies, this setting can be used to create a dynamic and powerful solution for suspending or powering off disconnected virtual desktops. When unneeded desktops are suspended or powered off, the resources are made available to other desktops.

Note: A Windows XP bug may prevent the idle tracker from working. A hotfix is available from Microsoft upon request. See KB890864.

Managing the View Client Using GPOs

One of the components provided with VMware View is the View Client, an application that is installed on the client and which provides the client-side component for connecting with virtual desktops. On some clients, the View Client also enables the ability to redirect additional USB devices not supported by native RDP device redirection.

Also included with View is a Group Policy Administrative Template for managing and configuring View Client settings from a central location with Group Policy. Using this administrative template, you can manage the following client-side settings:

- Enable the shade
- Pin the shade
- Don't check monitor alignment on spanning
- Color depth
- Desktop background
- Show contents of window while dragging
- Menu and window animation
- Themes
- Cursor shadow
- Font smoothing
- Desktop composition
- Audio redirection
- Redirect drives
- Redirect printers
- Redirect serial ports
- Redirect smart cards
- Redirect clipboard
- Redirect supported plug-and-play devices
- Bitmap caching
- Shadow bitmaps
- Cache persistence active
- Enable compression
- Windows key combination redirection
- Bitmap cache file size

Take the following steps to start configuring the View Client settings:

1. Locate the `vdm_client.adm` file in **<install_directory>\VMware\VMware View\Server\extras\GroupPolicyFiles**. This file is located on any View Connection Server that has been installed.
2. Copy this file to the management station you use to manage GPOs. By default, Group Policy looks for administration templates in `C:\WINDOWS\inf`. You can copy the `vdm_client.adm` file to that location or any other location accessible from your management station.
3. Using your Microsoft Management Console (MMC) with the Group Policy Editor snap-in loaded, locate the group policy you want to add the template to.
4. From the policy, expand **User Configuration**, select **Administrative Templates**, and select **Add/Remove Templates**.
5. Locate the `vdm_client` template and add it to the policy.

When you complete these steps, you are ready to configure your policy to manage View Client settings. When managing the View Client settings for another device, such as a thin client using its own RDP client and configuration, any GPO settings for Remote Desktop will override the client side. For example, if the client is configured to use 24-bit color and the Remote Desktop GPO is configured for a maximum of 16-bit color, the connection will connect using 16-bit color.

Supporting Multiple Monitors

If you use the Microsoft Remote Desktop client command-line option `/span`, a Remote Desktop session can span multiple displays with a maximum resolution of 4096 x 2048. However, spanning does not create a desktop experience identical to that of a workstation with a multiport graphics card. To achieve a true multimonitor experience, you need a third-party tool, such as SplitView or iShadow Desktop.

VMware View also enables users to configure their desktops by spanning the Remote Desktop session across multiple monitors. Individual users can configure this preference with the View Client or View Web Access.

About the Author

Warren Ponder, Director of Product Management, Enterprise Desktop, End User Computing, VMware, wrote this paper while in the role of Senior Technical Marketing Engineer.

Release Notes

Tina de Benedictis, Technical Marketing Manager, Enterprise Desktop, End User Computing, VMware, made minor updates to this paper. The paper does not fully reflect the current capabilities of View with PCoIP.

References

http://technet.microsoft.com/en-us/sysinternals/default.aspx

http://technet.microsoft.com/en-us/windowsxp/default.aspx?wt.svl=leftnav

http://technet2.microsoft.com/windowsserver/en/library/b9546edf-751f-4a09-835a-f3397caef2361033.mspx?mfr=true

http://technet2.microsoft.com/windowsserver2008/en/library/fc0b405b-07ef-4767-8716-198d7f0949011033.mspx?mfr=true

http://www.ishadow.com/

http://www.splitview.com/

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