CREATING AN OPTIMIZED WINDOWS IMAGE FOR A VMWARE HORIZON VIRTUAL DESKTOP

VMware Horizon
# Table of Contents

## Introduction
- Overview
- Advantages of an Optimized Image
- Tested Operating Systems
- Infrastructure Prerequisites

## Initial VM Creation
- Create a Virtual Machine
- Install Windows
- Configure Windows Server Systems for VDI or RDSH
- Install VMware Tools
- Update Windows and Run Ngen and DISM
- Run the VMware OS Optimization Tool
- Optimize the VM Hardware

## Image Generalization
- Prepare the OS for Generalization
- Run Sysprep to Create a Generic Image

## Installation of Virtual Desktop Agents and Applications
- Install Horizon Agent
- Install the Dynamic Environment Manager Agent
- Install the App Volumes Agent
CREATING AN OPTIMIZED WINDOWS IMAGE FOR A VMWARE HORIZON VIRTUAL DESKTOP

- Install Applications in the Base Image

Free Additional Disk Space and Remove Host Information

- Clean Up Disk Space and Zero-Out the Virtual Hard Disk
- Clear KMS and Release the IP Address

Preparation for Use

- Clone the VM to Adjust Disk Size and Virtual Hardware
- Take a VM Snapshot
- Create OUs and User Groups in Active Directory
- Set Other Common Group Policies
- Set Policies for RDSH Server VMs
- Add Users to the Local Remote Desktop Users Group
- Turn Off Hardware Graphics Acceleration in Commonly Used Applications

Conclusion

- In Conclusion
- Additional Resources
- About the Authors and Contributors
Creating an Optimized Windows Image for a Virtual Desktop (update)

Introduction

Overview

Considerations you must take into account when creating a Windows system image are much different if you plan to deploy virtual desktops rather than physical desktops:

- **Physical desktops** – Resource usage on a physical machine impacts only the user who is using that machine. The operating system on a physical machine determines whether or not resources are available. One-time actions impact the user only the first time they are performed because the machine is never refreshed. For example, a user typically gets a new user profile the first time they log on, and they continue to use that same profile with all subsequent logons.

- **Virtual desktops** – In contrast, in a virtual environment, the guest operating system behaves as if it has exclusive access to the CPU cores, but in reality the cores are shared between 2 to 8 virtual machines. When using nonpersistent VMs or user profiles, the actions that are intended to run only once could run every time a user logs on.

Therefore, with virtual desktops, one-time system actions must be configured in the base image, and one-time user actions must be configured in the default user profile. In addition, to reach a higher consolidation ratio, increasing the number of VMs hosted on a single VMware vSphere® host, VMware recommends turning off features that are not needed.

JMP Next-Generation Desktop and Application Delivery Platform

JMP (pronounced jump), which stands for Just-in-Time Management Platform, represents capabilities in VMware Horizon® 7 Enterprise Edition that deliver Just-in-Time Desktops and Apps in a flexible, fast, and personalized manner. JMP is composed of the following VMware technologies:

- VMware Instant Clone Technology for fast desktop and RDSH provisioning
- VMware App Volumes™ for real-time application delivery
- VMware Dynamic Environment Manager™ for contextual policy management

JMP allows components of a desktop or RDSH server to be decoupled and managed independently in a centralized manner, yet reconstituted on demand to deliver a personalized user workspace when needed. JMP is supported with both on-premises and cloud-based Horizon deployments, providing a unified and consistent management platform regardless of your deployment topology. The JMP approach provides several key benefits, including simplified desktop and RDSH image management, faster delivery and maintenance of applications, and elimination of the need to manage “full persistent” desktops.

**Note:** Installing the components of JMP is required only if you want to use that functionality. Similarly, installing the Horizon Agent is required only if you plan to use the image for VMware Horizon desktop or application pools.

Purpose of This Guide

*C latticeing an Optimized Windows Image for a Virtual Desktop provides step-by-step procedures for creating optimized images. These procedures include creating a VM, installing and configuring a Windows operating system, optimizing the OS, and installing the various VMware agents required for desktop pool deployment.

**Important:** The procedures in this guide are sequential and build on one another, so make sure to complete each procedure in each chapter before moving on to the next.
Intended Audience

This guide is intended for IT administrators and product evaluators who are familiar with VMware vSphere and VMware vCenter Server®. Familiarity with networking and storage in a virtual environment, Active Directory, identity management, and directory services is assumed. Knowledge of other technologies, such as Horizon 7 is also helpful.

Advantages of an Optimized Image

Optimizing the master image is well worth the time and effort involved. Savings are returned on a variety of fronts.

Initial Deployment Time Savings

By trimming the image, you can reduce the amount of required disk space by up to 80 percent, which translates to a significant reduction in the time it takes to create desktop pools (up to 3 times faster).

By default, Windows generates native images and performs disk cleanup actions after being idle for 10 minutes, which can use a full core for up to an hour. When deploying a large pool, this means that the cluster might not be usable for up to an hour after deployment. With image optimization, however, this process could be reduced to 30 seconds.

User Logon Time Savings

When a user logs on, the portion of logon time devoted to creating a standard user profile can take up to 30 seconds, but when optimized, this portion of logon time could be reduced to 2.5–8.5 seconds.

Host Memory Savings

A default deployment can use up to 2 GB of active memory, but with optimization, memory requirements can be reduced significantly (up to 50 percent).

Host CPU Savings

An optimized deployment can reduce CPU usage by up to 40 percent, allowing for up to a 40-percent increase in VM density on the physical vSphere host.

Storage and IOPS Savings

Because of the earlier-mentioned disk-space savings, you realize cache-usage improvements as well. Disabling unneeded features and compressing the OS files means a larger portion can fit in the cache, which can reduce the amount of IOPS required by up to 250 percent.

Tested Operating Systems

The following operating systems have been tested using the procedures included in this guide. The table shows the example sizing and login duration that we achieved in our testing.

Only 64-bit operating systems where tested, but any 32-bit operating system that has a corresponding 64-bit version listed should work in the same way. All operating systems were tested with all updates available as of late September 2019. For a complete list of supported Windows 10 operating systems, see the VMware knowledge-base article Supported versions of Windows 10 on Horizon Agent Including All VDI Clones (Full Clones, Instant Clones, and Linked Clones on Horizon 7) (2149393).

Note: Most screenshots in this guide are from Windows 10 1803. If you have a different OS version, some screens might look slightly different, but in general they are quite similar.

Important: Use an OS version that has a Microsoft Windows volume license key using the Key Management Service (KMS). KMS treats each activated clone as a computer with a newly issued license. In a production environment, you must activate Windows. In an
evaluation environment, you can create the VM and log in without activating Windows.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Version</th>
<th>Edition</th>
<th>Architecture</th>
<th>Used Space</th>
<th>New Profile Login Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10</td>
<td>1607</td>
<td>LTSB*</td>
<td>x64</td>
<td>8.37 GB</td>
<td>7 S</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1709</td>
<td>Education</td>
<td>x64</td>
<td>7.72 GB</td>
<td>8 S</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1709</td>
<td>Enterprise</td>
<td>x64</td>
<td>7.88 GB</td>
<td>8 S</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1709</td>
<td>Professional</td>
<td>x64</td>
<td>7.68 GB</td>
<td>8 S</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1803</td>
<td>Education</td>
<td>x64</td>
<td>6.97 GB</td>
<td>8 S</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1803</td>
<td>Enterprise</td>
<td>x64</td>
<td>7.19 GB</td>
<td>8 S</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1803</td>
<td>Professional</td>
<td>x64</td>
<td>6.91 GB</td>
<td>8 S</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1809**</td>
<td>Education</td>
<td>x64</td>
<td>5.81 GB</td>
<td>7 S</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1809**</td>
<td>Enterprise</td>
<td>x64</td>
<td>5.83 GB</td>
<td>7 S</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1809**</td>
<td>LTSC*</td>
<td>x64</td>
<td>5.41 GB</td>
<td>7 S</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1809**</td>
<td>Professional</td>
<td>x64</td>
<td>5.63 GB</td>
<td>7 S</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1903**</td>
<td>Education</td>
<td>x64</td>
<td>5.78 GB</td>
<td>7 S</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1903**</td>
<td>Enterprise</td>
<td>x64</td>
<td>5.77 GB</td>
<td>7 S</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1903**</td>
<td>Professional</td>
<td>x64</td>
<td>5.69 GB</td>
<td>7 S</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1909**</td>
<td>Education</td>
<td>x64</td>
<td>5.98 GB</td>
<td>7 S</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1909**</td>
<td>Enterprise</td>
<td>x64</td>
<td>5.96 GB</td>
<td>7 S</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1909**</td>
<td>Professional</td>
<td>x64</td>
<td>5.87 GB</td>
<td>7 S</td>
</tr>
<tr>
<td>Windows Server 2016</td>
<td>1607</td>
<td>Datacenter</td>
<td>x64</td>
<td>9.79 GB</td>
<td>3.5 S</td>
</tr>
<tr>
<td>Windows Server 2016</td>
<td>1607</td>
<td>Standard</td>
<td>x64</td>
<td>9.44 GB</td>
<td>3.5 S</td>
</tr>
<tr>
<td>Windows 7</td>
<td>SP1</td>
<td>Enterprise</td>
<td>x64</td>
<td>18.79 GB</td>
<td>5 S</td>
</tr>
<tr>
<td>Windows 7</td>
<td>SP1</td>
<td>Professional</td>
<td>x64</td>
<td>18.77 GB</td>
<td>5 S</td>
</tr>
<tr>
<td>Windows 8.1</td>
<td>Enterprise</td>
<td>x64</td>
<td>10.35 GB</td>
<td>4.5 S</td>
<td></td>
</tr>
<tr>
<td>Windows 8.1</td>
<td>Professional</td>
<td>x64</td>
<td>11.46 GB</td>
<td>4.5 S</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2012 R2</td>
<td>Datacenter</td>
<td>x64</td>
<td>10.67 GB</td>
<td>2.5 S</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2012 R2</td>
<td>Standard</td>
<td>x64</td>
<td>10.82 GB</td>
<td>2.5 S</td>
<td></td>
</tr>
</tbody>
</table>
CREATING AN OPTIMIZED WINDOWS IMAGE FOR A VMWARE HORIZON VIRTUAL DESKTOP

* LTSB means long-term servicing branch. LTSC means long-term servicing channel. This edition receives only security updates but no feature updates. OS upgrades are released only once every three years or so. This edition does not include Edge or any Microsoft Store (Universal Windows Platform, or UWP) apps, or Cortana, the voice-activated digital assistant. This edition is meant for specialized systems that perform a single important task—such as PCs that control medical equipment, point-of-sale systems, and ATMs.

** For 1809+ vSphere 6.7 U3 is recommended as there are known problems with earlier versions of vSphere.

Infrastructure Prerequisites
Before you can perform the procedures in this guide, you must have the following infrastructure components installed and configured:

- VMware vSphere and vCenter Server. We used vSphere 6.7 and vCenter Server 6.7 in our testing. For information and installation instructions, see the VMware vSphere documentation.
- VMware ESXi™ host or hosts configured in the vCenter Server instance.
- An authentication infrastructure that includes Active Directory, DNS, and DHCP.
- If you intend to use VMware App Volumes™, you must have the host name or IP address of the server on which App Volumes Manager is installed or will be installed. You will enter this information when you install the App Volumes Agent on the master VM image.

If you plan to create Horizon 7 desktop pools, ideally at this point you would also have Horizon 7 Connection Server installed and configured. We used Horizon 7 version 7.5. For installation instructions, see the Horizon 7 Installation guide.

Initial VM Creation

Create a Virtual Machine
Each desktop pool or RDSH server farm uses a master virtual machine (VM), which serves as the model for the deployed virtual desktops. You use VMware vSphere® Web Client to create the master VM.

Prerequisites
Before you complete this procedure, you will need the following:

- **Windows ISO file** – You must have uploaded an ISO file to a vSphere datastore. The ISO file must contain a supported version of the Windows operating system. You will point to this file when completing the New Virtual Machine wizard. For a list of the operating systems we tested, see Tested Operating Systems. For a complete list of supported Windows 10 operating systems, see the VMware knowledge-base article Supported versions of Windows 10 on Horizon Agent Including All VDI Clones (Full Clones, Instant Clones, and Linked Clones on Horizon 7) (2149393).

  **Important**: Use an OS version that has a Microsoft Windows volume license key using the Key Management Service (KMS). KMS treats each activated clone as a computer with a newly issued license. In a production environment, you must activate Windows. In an evaluation environment, you can create the VM and log in without activating Windows.
- **User account** – When you log in to vSphere Web Client, the account you use must have the privileges required to create a VM. See the "Prerequisites" section of the product documentation topic Create a Virtual Machine with the New Virtual Machine Wizard.

1. Start the New Virtual Machine Wizard in the vSphere Web Client
In vSphere Web Client, right-click a data center, cluster, host, or VM folder.


2. Select the New Virtual Machine Creation Type
1. Select Create a new virtual machine.
2. Click NEXT.

3. Select a VM Name and Folder
1. Provide a name in the **Virtual machine name** field.
2. Select a location.
3. Click **NEXT**.

### 4. Select a Cluster or Host
1. Select a cluster or host as the compute resource.
2. Click NEXT.

5. Select a Datastore for the VM
1. Select a datastore or datastore cluster where you would like to store the VM.
2. Click NEXT.

6. Select the vSphere Compatibility Level
1. Select the lowest version of ESXi that this VM would be deployed to. 
   Tip: See Hardware Features Available with Virtual Machine Compatibility Settings.
2. Click NEXT.

7. Select the Windows Version and Architecture
1. Select the **Guest OS Version** with the correct architecture (32- or 64-bit) and, when required, enable VBS.
2. Click **NEXT**.

### 8. Specify Virtual Hardware Settings
1. Select 4 CPUs. (Use 4 CPUs for the creation of the image. We will adjust this to production values later.)
2. Select 4 GB of memory.
   **Note:** The table that follows describes the small amount of RAM on the ESXi host that is required for video overhead in addition to system memory. This VRAM size requirement depends on the display resolution and number of monitors configured for end users.
3. Choose an appropriate hard disk size.
4. Select the appropriate network and expand the section and select VMXNET3 as type.
5. Browse to the Windows ISO file and select **Connect**.
6. Choose the appropriate video card settings.
7. Click **NEXT**.
## Display Resolution Standard

<table>
<thead>
<tr>
<th>Display Resolution Standard</th>
<th>Width, in Pixels</th>
<th>Height, in Pixels</th>
<th>1-Monitor Overhead</th>
<th>2-Monitor Overhead</th>
<th>3-Monitor Overhead</th>
<th>4-Monitor Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td>VGA</td>
<td>640</td>
<td>480</td>
<td>1.20 MB</td>
<td>3.20 MB</td>
<td>4.80 MB</td>
<td>5.60 MB</td>
</tr>
<tr>
<td>WXGA</td>
<td>1280</td>
<td>800</td>
<td>4.00 MB</td>
<td>12.50 MB</td>
<td>18.75 MB</td>
<td>25.00 MB</td>
</tr>
<tr>
<td>1080p</td>
<td>1920</td>
<td>1080</td>
<td>8.00 MB</td>
<td>25.40 MB</td>
<td>38.00 MB</td>
<td>50.60 MB</td>
</tr>
<tr>
<td>WQXGA</td>
<td>2560</td>
<td>1600</td>
<td>16.00 MB</td>
<td>60.00 MB</td>
<td>84.80 MB</td>
<td>109.60 MB</td>
</tr>
<tr>
<td>UHD (4K)</td>
<td>3840</td>
<td>2160</td>
<td>32.00 MB</td>
<td>78.00 MB</td>
<td>124.00 MB</td>
<td>Not supported</td>
</tr>
</tbody>
</table>

9. Complete the Wizard
Click FINISH.

Install Windows

After you boot the VM, installation of the Windows OS begins automatically. You will accept most of the default settings and specify that you are doing a new installation rather than an update.

1. Open a Remote Console for the VM
1. Select the newly created Windows VM in the inventory list.

2. Click **Launch Remote Console**.
   
   **Note**: To launch a remove console, you must have downloaded and installed the VMware Remote Console. If necessary, you can click the "i" button to download and install it.

2. **Power on the VM**
3. Boot the VM from the Virtual CD

Press any key to boot from CD or DVD.

4. Select Settings for Your Region
1. Select the correct regional options.
2. Click Next.

5. Begin Installing Windows
6. Select the Edition
This screen is only shown for an ISO that contains multiple editions.


   **Important:** For Windows Server 2012 R2, select either of the following “Server with GUI” editions:
   - Windows 2012 R2 Standard (Server with a GUI)
   - Windows 2012 R2 Datacenter (Server with a GUI)

   For Windows Server 2016, select either of the following “Desktop Experience” editions:
   - Windows Server 2016 Standard (Desktop Experience)
   - Windows Server 2016 Datacenter (Desktop Experience)

2. Click Next.

7. Accept the License Agreement
1. Select the **I accept the license terms** check box.
2. Click **Next**.

8. **Select the Custom Installation**
Select Custom: Install Windows only (advanced).

9. Use the Default Location
10. Monitor Installation Progress
Wait for Windows to be installed.

11. Enter Audit Mode by Pressing CTRL+SHIFT+F3

After the Windows operating system is installed, you need to enter audit mode.

The screen at which you enter audit mode depends on which Windows operating system you are using. For example, some operating systems will automatically log in to Windows after a restart operation, while others will prompt for user credentials. If prompted, use Administrator for the user name and leave the password field blank.

11.1. If You Are Not Prompted for Credentials Enter Audit Mode by Pressing CTRL+SHIFT+F3
When you are prompted with **Let's start with a region** or to **Get going fast**, or **Personalize**, or **Customize Settings**, or **Setup Windows**, press CTRL+SHIFT+F3 to switch to audit mode.

**Note**: Different Windows operating systems provide different prompts after the initial installation. This example shows Windows 10 1803.

**11.2. If You Are Prompted for Credentials Leave the Password Blank and Press CTRL+SHIFT+F3**
If prompted for credentials, use Administrator for the user name, ignore the password prompt, and press CTRL+SHIFT+F3 to switch to audit mode. This example shows Windows Server 2016.

**Configure Windows Server Systems for VDI or RDSH**

Complete this procedure if you are working with Windows Server 2012 R2 or 2016.

**Note:** The following editions are supported for Windows Server installations:

For Windows Server 2012 R2, use either of the following "Server with GUI" editions:

- Windows 2012 R2 Standard (Server with a GUI)
- Windows 2012 R2 Datacenter (Server with a GUI)

For Windows Server 2016, use either of the following "Desktop Experience" editions:

- Windows Server 2016 Standard (Desktop Experience)
- Windows Server 2016 Datacenter (Desktop Experience)

**1. Open the Server Management Properties Dialog Box**
On the Windows Server system, start Server Manager, and select Manage > Server Manager Properties.

2. Select the Option to Not Start Server Manager at Logon

3. Turn Off IE Enhanced Security
1. Select **Local Server**.
2. Click on **On** next to **IE Enhanced Security Configuration**.
3. Select **Off** for both **Administrators** and **Users**.
4. Click **OK**.

### 4. Start the Add Roles and Features Wizard

1. Select **Dashboard**.
2. Click **Add roles and features**.
3. In the wizard, for **Installation Type**, use the default selection, which is **Role-based or feature-based installation**.
4. Follow the prompts to the **Server Roles** page.

### 5. Install the Remote Desktop Services Role for RDSH Servers
1. If you plan to use this server as an RDSH server, to create published applications and published desktops (rather than single-user VDI desktops), select **Remote Desktop Services** on the Server Roles page.
2. Click **Next**, and click **Next** on the pages that follow until you come to the Role Services page.

6. **Add the Remote Desktop Session Host**
Select the check box for the Remote Desktop Session Host service, and confirm that you want to add the applicable management tools, before clicking Next.

7. Install the Desktop Experience Feature on Windows Server 2012 R2

1. On Windows Server 2012 R2 servers, on the Features page, install the Desktop Experience feature. This feature is already installed on Windows Server 2016 (Desktop Experience) installations.
2. Click Next.

8. Complete the Wizard

For Windows Server 2016, open a command prompt and enter the following command to enable Adobe Flash Player run.

Note: To display the command in this document, we had to add a line break after Packages, but you should enter the command all on one line:

```
dism /online /add-package /packagepath:"C:\Windows\servicing\Packages\Adobe-Flash-For-Windows-Package~31bf3856ad364e35~amd64~~10.0.14393.0.mum"
```

**Install VMware Tools**

VMware Tools is a set of services and modules that enable several features in VMware products for better management of, and seamless user interactions with, guests operating systems.

For example, VMware Tools can run scripts that automate OS operations and can synchronize the time in the guest operating system with the time on the vSphere host. You must install VMware Tools in VMs used for desktop and application pools.

**1. Use vSphere Web Client to Mount the VMware Tools Virtual DVD Drive**
Select the VM in the inventory list.
1. Click Install VMware Tools, and click MOUNT when prompted.

Alternatively, you can select the VM and select ACTIONS > Guest OS > Install VMware Tools.

2. Start the Installation Wizard

1. Open a console for the VM, and in Windows Explorer, select DVD Drive (D:) VMware Tools.
2. To start the wizard, double-click Setup64.exe (or Setup.exe for a 32-bit OS).
3. Click Next on the Welcome Page

4. Select the Typical Setup Type
Leave the **Typical** setup selected, and click **Next**.

### 5. Start the Installation

Click **Install**.

### 6. Complete the Wizard
7. Restart the VM

Click Yes.

Update Windows and Run Ngen and DISM

After you install the latest Windows OS updates, you will use the Native Image Generator (Ngen.exe) command-line tool to improve the performance of managed applications. You will use the Deployment Image Servicing and Management (DISM.exe) command-line tool to save space on the Windows image by running the operating system and other system files from compressed files.

1. Select the Update & Security Settings
Press Windows Key+I, to open Windows Settings, and click Update & Security or, for Windows 8.1 or Windows Server 2012 R2 and earlier, navigate to Control Panel > System and Security > Windows Update.

**Important**: Currently (as of July 2018), Windows Update is not working on Windows 8.1 and 2012R2. Use Microsoft Baseline Security Analyzer 2.3 to identify missing updates, and manually download and install them from the Microsoft Download Center.

2. Select Check for Updates
Note: For non-LTSB Windows 10 versions, click Advanced options first and select Defer feature upgrades so that new features are not downloaded and installed. When a new feature upgrade has been available for more than 365 days, Microsoft offers wushowhidediag.cab, which allows you to hide the upgrade. Deferring feature upgrades does not affect security updates.

Click Check for updates and wait for the updates to be installed.

3. Restart the VM
1. After the VM restarts, log in, press Windows Key+R and type `cmd.exe`.  
2. Click OK.

4. Open a Command Prompt
5. Run the Ngen Tool

1. Type `cd \` and press Enter.
2. Type `cd Windows\Microsoft.NET\Framework\v4` and press Tab, and then press Enter.
3. Type `ngen executequeueditems` and press Enter. This command executes queued compilation jobs.

6. Run the DISM Tool
1. Type `dism /online /cleanup-image /startcomponentcleanup /resetbase` and press Enter.
   
   **Note:** This command might take a long time to complete and is not available on Windows 7 or Windows Server 2008. On these operating systems, run `cleanmgr.exe` and select **Windows Update Cleanup**. When the process is complete, reboot.

2. Optionally, on Windows 10/Server 2016, you can also run `compact /compactos:always`, which has a positive effect on the amount of IOPS required for storage with cache and a negligible CPU impact.

3. Close the command prompt.

---

### Run the VMware OS Optimization Tool

The **VMware OS Optimization Tool** fling helps optimize Windows 7/8/10 and Windows Server 2008 R2/2012/2016 systems for use with Horizon 7. The optimization tool includes customizable templates to enable or disable Windows system services and features, according to VMware recommendations and best practices, across multiple systems. Because most Windows system services are enabled by default, the optimization tool can be used to easily disable unnecessary services and features to improve performance.

---

1. **Download the OS Optimization Tool**
Go to the VMware OS Optimization Tool page to download and start it.

2. Check for Updates to the Template
1. To check for updates to the template for your Windows version, select the **Public Templates** tab.
2. Select **Update Only**.
3. If there is an update, click **Update**.
   In the screen shot for this example, there is an update only for the templates provided by Login VSI, not the default VMware one.

3. **Analyze Recommended System Optimizations to Apply**

   ![VMware OS Optimization Tool](image)

   1. Select the **Analyze** tab.
   2. Click **Analyze**.

4. **Select the Optimizations to Apply**
1. Select the appropriate optimizations from the extensive list. For most VDI environments, use the default selection. For Windows 8.1 and 2012 R2, de-select SMB v1.
2. Click Optimize.

5. Shut Down the VM When Optimization Is Complete
Monitor the optimization results, and when the process is complete, close the VMware OS Optimization Tool and shut down the VM.

**Optimize the VM Hardware**

Because we no longer need the virtual CD/DVD drive, we can remove that as well as any other unnecessary virtual hardware devices.

### 1. Open the Edit Settings Dialog Box
In the vSphere Web Client, right-click the VM and select **Edit Settings**.

### 2. Remove Devices That You Plan Not to Use
To remove the virtual CD/DVD drive from the VM, click the X that appears when you hover your pointer over CD/DVD drive 1 row. If you do not plan to use USB redirection, do the same with the USB xHCI controller.

Click OK and edit the VM again.
3. Remove the SATA Controller

1. To remove the virtual SATA controller from the VM, click the X that appears when you hover your pointer over the SATA controller.
Controller 0 row.
2. Click OK.

4. Open the Add Configuration Parameter Dialog Box

Note: In the next step, you are going to disable the hotplug feature. With hotplug enabled, NICs and SCSI controllers appear as removable devices, and the Safely Remove Hardware option for the virtual hardware appears in the Windows System Tray (notification area). To prevent this option from appearing, we will disable the capability.

5. Add a Parameter to Disable Hotplug Functionality
Click ADD CONFIGURATION PARAMS
1. For Name, type devices.hotplug, and for Value, type false.
2. Click OK.

6. Disable Floppy, IDE, LPT, and COM Devices

If you are not using Windows 10 or Windows Server 2016 systems that, by default, use UEFI rather than BIOS to boot, you can disable more devices in the BIOS.

6.1. Configure the VM to Boot into the BIOS Setup Screen
1. Expand Boot Options.
2. Select During the next boot, force entry into the BIOS setup screen.
3. Click OK.
4. Power on the VM and open a remote console.

6.2. Open I/O Device Configuration Options
1. Go to the Advanced tab.
2. Select I/O Device Configuration and press Enter.

### 6.3. Disable the Devices

<table>
<thead>
<tr>
<th>I/O Device Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial port A:</td>
</tr>
<tr>
<td>Serial port B:</td>
</tr>
<tr>
<td>Parallel port:</td>
</tr>
<tr>
<td>Floppy disk controller:</td>
</tr>
</tbody>
</table>

Set everything to Disabled and press ESC.

### 6.4. Disable the Local Bus IDE Adapter

1. On the Advanced tab, select Local Bus IDE adapter and press Enter.
2. Select Disabled and press Enter.

### 6.5. Exit BIOS Setup

1. Go to the Exit tab.
2. Select Exit Saving Changes and press Enter.
Image Generalization

Prepare the OS for Generalization

Generalizing a Windows image means removing computer-specific information so that the image can be deployed throughout an enterprise. Before we can generalize the image, we need to remove any Windows Store applications that are not needed. In our example, these include all the Windows Store applications that can be deleted.

Note: When preparing the master image, we do not join the machine to a domain. Joining a machine to a domain is part of the deployment process, not part of image creation and optimization. This way, the image can be used across domains. Also some optimization steps will not work if the image is joined to a domain.

1. Disable Password Complexity Requirements on Windows Server

2. Double-click `Password must meet complexity requirements`.
3. Click `Disabled` and click `OK`.

For Windows Server operating systems disable `Password must meet complexity requirements`. Desktop operating systems already have this setting. When using this image later the domain policies will overwrite this setting, but for the Master this allows the use of an empty administrator (which should also be disabled by the domain policy) password.

2. Create a Sysprep Answer File
Create a new file with the name `unattend.xml` in the `c:\windows\system32\sysprep` directory.

### 3. Add the Content of the Answer File

Open the `unattend.xml` file with a text editor, and add the following content:

**Note:** If you copy the following text from a Web (HTML) page, the line breaks will most likely be preserved, but if you copy the lines from a PDF file, the line breaks will not be correct. Be sure to copy the text from an HTML page.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
  <settings pass="generalize">
      <SkipRearm>1</SkipRearm>
    </component>
  </settings>
  <settings pass="specialize">
      <RunSynchronous>
        <RunSynchronousCommand wcm:action="add">
          <Order>1</Order>
          <Path>net user administrator /active:yes</Path>
        </RunSynchronousCommand>
      </RunSynchronous>
    </component>
      <TimeZone>Mountain Standard Time</TimeZone>
      <ComputerName>*</ComputerName>
    </component>
  </settings>
</unattend>
```
<settings pass="oobeSystem">
             xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" name="Microsoft-Windows-International-Core"
             processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS">
    <InputLocale>en-us</InputLocale>
    <SystemLocale>en-us</SystemLocale>
    <UILanguage>en-us</UILanguage>
    <UserLocale>en-us</UserLocale>
  </component>
             xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" name="Microsoft-Windows-Shell-Setup"
             processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS">
    <AutoLogon>
      <Enabled>true</Enabled>
      <LogonCount>1</LogonCount>
      <Username>Administrator</Username>
    </AutoLogon>
    <OOBE>
      <HideEULAPage>true</HideEULAPage>
      <NetworkLocation>Work</NetworkLocation>
      <HideLocalAccountScreen>true</HideLocalAccountScreen>
      <HideOEMRegistrationScreen>true</HideOEMRegistrationScreen>
      <HideOnlineAccountScreens>true</HideOnlineAccountScreens>
      <ProtectYourPC>3</ProtectYourPC>
    </OOBE>
    <UserAccounts>
      <LocalAccounts>
        <LocalAccount wcm:action="add">
          <Description>Local Administrator</Description>
          <DisplayName>Administrator</DisplayName>
          <Group>Administrators</Group>
          <Name>Administrator</Name>
        </LocalAccount>
      </LocalAccounts>
    </UserAccounts>
  </component>
</settings>

Important: Take the following version-specific guidelines into account when creating this file:

- When using a 32-bit operating system, replace the instances of amd64 with x86.
- When using Windows 7, delete the lines with HideLocalAccountScreen, HideOEMRegistrationScreen, and HideOnlineAccountScreen.

4. Create a UseProfilePathExtensionVersion Registry Entry for
Certain Versions of Windows
For Windows Server 2012 R2 and Windows 8.1, run the following command:

```cmd
reg add "HKLM\System\CurrentControlSet\Services\ProfSvc\Parameters" /v UseProfilePathExtensionVersion /t REG_DWORD /d 1 /f
```

This command helps avoid compatibility issues between Windows Server 2012 R2 or Windows 8.1 and default user profiles created using a different version of Windows.

Run Sysprep to Create a Generic Image
Now that you have created a Sysprep answer file, you can run an unattended installation using the System Preparation tool.

Open a Command Prompt and Run Sysprep

For all versions except Windows 7, open a command prompt and execute the following command from the directory where sysprep.exe is installed. For Windows 7, because the /mode:vm option is not available, run the command without it.

```cmd
c:\windows\system32\sysprep\sysprep.exe /oobe /generalize /mode:vm /unattend:c:\windows\system32\sysprep\unattend.xml /reboot
```

In this command, /generalize removes computer-specific information, /oobe restarts the computer into out-of-box-experience mode, /mode:vm skips driver installation, and /unattend points to the answer file to use during an unattended installation. For details about these options and others, see the Microsoft article Sysprep Command-Line Options.

Installation of Virtual Desktop Agents and Applications

Install Horizon Agent
If you plan to create VMware Horizon desktop or application pools, you must install Horizon Agent on the master VM so that VMware Horizon servers can communicate with and manage the desktops that you deploy. The Horizon Agent also communicates with VMware Horizon® Client™ on end users’ computers to provide features such as connection monitoring, virtual printing, access to the local file system, and access to locally connected USB devices.

Prerequisites for Installing Horizon Agent
To perform this procedure, you need the following:

- **User account** – When you log in to the OS of the master image to run the installer, the account you use must have local administrative privileges.
• **Installer** – 32-bit and 64-bit Horizon View Agent installer (.exe) files are available from the [Download VMware Horizon](https://example.com) page. You must download the file and copy it to the system where it will run or to a location accessible to the system.

• **VM with supported Windows OS** – The virtual machine must be running a Windows operating system that Horizon Agent supports. For a list of the systems we tested, see [Tested Operating Systems](https://example.com). For a complete list of supported Windows 10 operating systems, see the VMware knowledge-base article [Supported versions of Windows 10 on Horizon Agent Including All VDI Clones (Full Clones, Instant Clones, and Linked Clones on Horizon 7)](https://example.com) (2149393).

**Important**: If you install Horizon Agent on a Windows Server machine on which the Remote Desktop Services (RDS) role is not installed, the wizard will prompt you to **Install VMware Horizon Agent in ‘desktop mode’**. Selecting this option configures the Windows Server machine as a single-user virtual desktop rather than as an RDS host. If you intend the machine to function as an RDS host, cancel the Horizon Agent installation, install the RDS role on the machine, and restart the Horizon Agent installation.

1. **Start the Horizon Agent Wizard**

Log in to the OS of the master VM as an Administrator, and double-click the installer file to start the wizard, and click **Next** on the Welcome page.

2. **Accept the License Agreement**
Select I accept the terms in the license agreement, and click Next.

3. Select Whether to Use IPv4 or IPv6
Select the protocol, and click **Next**.

The environment must be either IPv6 only or IPv4 only. Horizon 7 does not support a mixed IPv6 and IPv4 environment.

### 4. Enable the USB Redirection Feature

Enable the USB Redirection feature, and click **Next**.

You can later control use of the feature by setting group policies or by using Horizon Smart Policies for granular control. For example, you can set a condition for the Smart Policy so that users can access USB devices only when connecting from inside the corporate network.

### 5. Disable Installation of the View Composer Agent
Because the View Composer Agent cannot be installed if you plan to install the Instant Clone Agent, disable the **VMware Horizon View Composer Agent**, and click **Next**.

6. Enable Installation of the Instant Clone Agent
Enable the **VMware Horizon Instant Clone Agent**, and click **Next**.

**Instant Clone Technology** enables single-image management with automation capabilities. You can rapidly create instant-clone desktop pools and automated RDSH server farms that contain thousands of VMs.

**Note**: Even though you install this feature, you can still use this master image to create full-clone desktop pools in addition to instant-clone desktop pools.

### 7. Disable the Persona Management Feature
Because the Persona Management feature cannot be installed if you plan to install the Instant Clone Agent, disable the **VMware Horizon Persona Management** feature, and click *Next*.

**Note**: For some operating systems, this component might not appear in the list.

### 8. Enable the Performance Tracker
Enable installation of the Horizon Performance Tracker, as well as any other features you might require, and click Next.

VMware Horizon Performance Tracker is a utility that runs in a remote desktop or RDSH server and monitors the performance of the display protocol and system resource usage.

Note: For a description of each of the features in the list, see Horizon Agent Custom Setup Options.

9. Enable the Remote Desktop Capability
If the Remote Desktop Protocol page appears, select **Enable the Remote Desktop capability on this computer**, and click **Next**. This wizard page might not appear if you have already enabled this feature in Windows Firewall.

If you select the **Do not enable the Remote Desktop capability on this computer** option, you can manually enable the remote desktop feature later and configure the firewall exceptions.

**10. Click Install**
Now that all the correct components are configured to be installed, click **Install**.

### 11. Click Finish When Installation Is Complete
Click **Finish** to close the installer.

### 12. Restart the VM

When prompted to restart, click **Yes**.

**Install the Dynamic Environment Manager Agent**

Dynamic Environment Manager (formerly called *User Environment Manager*) provides profile management by capturing user settings for the operating system and applications. Unlike traditional application profile management solutions, Dynamic Environment Manager captures only the settings that the administrator specifies. This reduces login and logout time because less data needs to be loaded. User data is managed through folder redirection.

FlexEngine, the Dynamic Environment Manager agent component, applies the policies that the IT administrator creates with the Dynamic Environment Manager Management Console. To install this component, you run the same VMware Dynamic Environment Manager Setup wizard that you run to install the management console.
Prerequisites for FlexEngine Installation

To perform this exercise, you need the following:

- **User account** – When you log in to the OS to run the installer, the account you use must have administrative privileges.
- **Installer** – If necessary, you can download the installer from the VMware Downloads page. The installer is an architecture-specific (x86 or x64) MSI file. You must download the file and copy it to the system where it will run or to a location accessible to the system.
- **Internet access** – The installation process includes a certificate revocation check to verify the digital signature of the MSI file. This check requires Internet access.
- **VM with supported Windows OS** – The machine must be running a supported Windows version. For a list of the systems we tested, see Tested Operating Systems. For a complete list of supported Windows 10 operating systems, see the VMware knowledge-base article Supported versions of Windows 10 on Horizon Agent Including All VDI Clones (Full Clones, Instant Clones, and Linked Clones on Horizon 7) (2149393).

**Note:** When you install the Dynamic Environment Manager agent on a VM where Horizon Agent is already installed, you are not required to specify a Dynamic Environment Manager license file. However, you are required to have purchased Dynamic Environment Manager. This component is included with Horizon 7 Enterprise Edition.

Running the Installer

To use the Dynamic Environment Manager wizard to install the agent, double-click the installer file and follow the prompts to perform a Typical Setup type of installation. The typical setup installs the VMware UEM FlexEngine agent component, along with the optional components: Application Migration and Self-Support.

**Note:** Because you are installing the Dynamic Environment Manager agent on a VM where Horizon Agent is already installed, you are not required to specify a Dynamic Environment Manager license file.

The product documentation for this procedure can be found in the Installing and Configuring VMware Dynamic Environment Manager guide.

Install the App Volumes Agent

App Volumes delivers applications that are not in the master VM image. Application containers, called AppStacks, are assigned to a user, group, OU, or machine and mounted each time the user logs in to a desktop. With this strategy, user changes can persist between sessions.

App Volumes can also provide user-writable volumes, which allow users to install their own applications and have those applications follow the user as they connect to different virtual desktops.

You install the App Volumes Agent on the master VM so that the App Volumes Manager can communicate with the desktops you deploy and attach the correct applications when a user logs in.

**Note:** Installing the App Volumes Agent is an optional step. Install this agent only if you plan to use this functionality.

Prerequisites for Installing the App Volumes Agent

To perform this exercise, you need the following:

- **User account** – When you log in to the OS of the master image to run the installer, the account you use must have local administrative privileges.
- **Installer** – App Volumes is included with Horizon 7 Enterprise Edition, available from the Download VMware Horizon page. The App Volumes installer is distributed as an ISO file. You can mount the ISO on the machine where you want to create the App Volumes component, or you can also extract the ISO contents to a shared folder. This option allows you to install each component without mounting the ISO each time.
- **VM with supported Windows OS** – The machine must be running a supported Windows version. For a list of the systems we...
CREATING AN OPTIMIZED WINDOWS IMAGE FOR A VMWARE HORIZON VIRTUAL DESKTOP

tested, see Tested Operating Systems. For a complete list of supported Windows 10 operating systems, see the VMware knowledge-base article Supported versions of Windows 10 on Horizon Agent Including All VDI Clones (Full Clones, Instant Clones, and Linked Clones on Horizon 7) (2149393).

- **App Volumes Manager server information** – During agent installation, you will be prompted to enter the host name or IP address and port number of the App Volumes Manager that this agent will communicate with.

## Running the Installer

To use the App Volumes Agent installation wizard to install the agent, double-click the installer file and follow the prompts.

**Note**: On the Server Configuration page, ensure that Disable Certificate Validation with App Volumes Manager is not selected.

The product documentation for this procedure can be found in the VMware App Volumes Installation Guide.

## Install Applications in the Base Image

Although our primary application-delivery mechanism is App Volumes, it might be desirable to install select applications in the master VM so that all clones get those applications in their base disk.

Many applications have integrated auto-update functionality. Install these applications and update them to the latest version, and then turn off or disable the auto-update functionality to prevent the clones from updating individually.

## Free Additional Disk Space and Remove Host Information

### Clean Up Disk Space and Zero-Out the Virtual Hard Disk

The Disk Cleanup utility frees unused disk space, and running the Secure Delete tool with the \(-z\) option zeros-out free disk space.

### 1. Open the Disk Cleanup Utility

1. Press Windows Key+R and type `cleanmgr.exe`.
2. Click OK.

### 2. Select File Types to Delete
1. Select all items.
2. Click OK.

3. Confirm File Deletion

   Are you sure you want to permanently delete these files?

   Click Delete Files.

4. Download and Run SDelete
Download the Sysinternal SDelete Tool and run the following command from a command prompt:

- For 64-bit operating systems: sdelete64 -z c:
- For 32-bit operating systems: sdelete.exe -z c:

This command overwrites all empty disk space with zeroes so that we can shrink the VMDK (virtual machine disk file) later.

**Clear KMS and Release the IP Address**

In this procedure, you use the Windows Software Licensing Management Tool (slmgr.vbs), which is a Visual Basic script, to clear the KMS (Key Management Service) host information from the image. You also release the IP address and shut down the machine.

Run the following commands:

slmgr.vbs /ckms
slmgr.vbs /ckhc
ipconfig /release
shutdown /s /t 0 /c "Image Ready"

slmgr.vbs /ckms clears the name of the KMS server.
slmgr.vbs /ckhc disables KMS host caching.
ipconfig /release releases the IP address.
shutdown /s /t 0 /c "Image Ready" shuts down the local computer, with 0 seconds between the time the command is given and the time the shutdown occurs, and leaves the comment "Image Ready."

Preparation for Use

Clone the VM to Adjust Disk Size and Virtual Hardware

If you used the same settings as shown in Specify Virtual Hardware Settings when you created the master VM, your VM has 40 GB of disk space and 4 GB of RAM. The storage usage of the VM can amount to the size of the disk as specified plus the amount of RAM.

Using the cloning process described in this article, we can select the thin-disk option and shrink the size of the VM according to the amount of zeroes written during the procedure Clean Up Disk Space and Zero-Out the Virtual Hard Disk.

Cloning also offers a good opportunity to adjust the virtual hardware specifications to better suit production usage.

1. Open the Clone VM Wizard

   1. Using vSphere Web Client, right-click the VM in the inventory list, and select Clone.
   2. Select Clone to Virtual Machine.

2. Specify a VM Name and Location
1. Type a descriptive name; for example, Win10-1803-Master-v1.
2. Select a location.
3. Click NEXT.

3. Select a Cluster or Host
1. Select a cluster or host as the compute resource.
2. Click NEXT.

4. Select a Datastore and Disk Format
1. Select a datastore or datastore cluster where you would like to store the VM.
2. Select Thin Provision.
3. Click NEXT.

5. Open the Customize VM Hardware Page
6. Adjust Virtual Hardware Settings
The actual values you use should be tested in a pilot, but the following settings are a good starting point:

1. For CPU, select 2.
2. For Core per Socket, select 1.
3. For Memory, type 2.5.
4. Click NEXT.

7. Click Finish
To begin the cloning process, click **FINISH**.

For the example in this procedure, the storage usage shrank from 44.2 GB to 10.84 GB, which represents a 75 percent savings.
Take a VM Snapshot
To create a desktop pool of cloned VMs, or to create a farm of cloned RDSH server VMs, you need to create a frozen state, or base image, from which the clone can be derived.

- For instant-clone pools and server farms, and for linked-clone pools, you achieve this state by taking a VM snapshot of the master VM.
- For full-clone pools, you achieve this state by cloning the master VM to a VM template.

This procedure describes taking a VM snapshot. For information about cloning a VM to a VM template, see Clone a Virtual Machine to a Template.

Prerequisites for Taking a Snapshot
Although it is possible to take a snapshot of a VM that is powered on, for the purposes of creating a base image for a Horizon 7 desktop pool or server farm, the VM must be shut down and powered off.

1. Open the Take Snapshot Dialog Box

   1. Using vSphere Web Client, right-click the VM in the inventory list, and select Snapshots.
   2. Select Take Snapshot.

2. Take the Snapshot
Create OUs and User Groups in Active Directory

Much of the initial configuration and ongoing management of virtual desktops, RDSH server farms, feature enablement, and end-user experience is performed by creating and applying group policies in Active Directory. Some standard Microsoft Group Policy Object settings are required to configure virtual desktops and applications, as described later in this guide.

If you use Horizon 7, you can also use VMware-provided GPO administrative templates for fine-grained control of access to features. See Using Horizon 7 Group Policy Administrative Template Files.

OUs for VMs

You should create an organizational unit (OU) specifically for your virtual desktops and an OU for your RDSH server VMs. An OU is a subdivision in Active Directory that contains users, groups, computers, or other OUs.

To prevent group policy settings from being applied to other Windows servers or workstations in the same domain as your desktops or server farms, you can create a GPO for group policies and link it to the OU that contains your VMs.

You can also delegate control of the OU to subordinate groups, such as server operators or individual users.

User Groups

You should also create groups for different types of users in Active Directory. For example, you can create a group called End Users for your end users and another group called Horizon Administrators for users that will administer virtual desktops and applications.

Later in this guide, you will add a user group containing end users to the local Remote Desktop Users group in AD. Then members of the group will be able to connect to any VM that is joined to the domain.
Set Other Common Group Policies

For both virtual desktop VMs and RDSH server VMs, create a GPO for the OU in Active Directory, and use the Group Policy Management Editor to apply the following GPO settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computer Configuration &gt; Policies &gt; Administrative Templates &gt; System &gt; Group Policy</strong></td>
<td><strong>Enabled</strong>&lt;br&gt;Set Mode to Replace</td>
</tr>
<tr>
<td>Configure user Group Policy loopback processing mode</td>
<td><strong>Enabled</strong>&lt;br&gt;Set Mode to Replace</td>
</tr>
<tr>
<td>Configure Logon Script Delay</td>
<td><strong>Disabled</strong></td>
</tr>
<tr>
<td><strong>Computer Configuration &gt; Policies &gt; Administrative Templates &gt; System &gt; Logon</strong></td>
<td><strong>Disabled</strong>&lt;br&gt;Always wait for the network at computer startup and logon</td>
</tr>
<tr>
<td>Show first sign-in animation</td>
<td><strong>Disabled</strong>&lt;br&gt;Always wait for the network at computer startup and logon</td>
</tr>
</tbody>
</table>

If you use Horizon 7, you can also use VMware-provided GPO administrative templates for fine-grained control of access to features. See Using Horizon 7 Group Policy Administrative Template Files.

Set Policies for RDSH Server VMs

If you plan to use the image for creating RDSH server VMs, create a GPO for the RDSH server OU in Active Directory, and use the Group Policy Management Editor to apply the following GPO settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computer Configuration &gt; Policies &gt; AdministrativeTemplates &gt; Windows Components &gt; Remote Desktop Services &gt; Remote Desktop Session Host &gt; Licensing</strong></td>
<td><strong>Enabled</strong>&lt;br&gt;(Comma-separated list of license servers to use)</td>
</tr>
<tr>
<td>Use the specified Remote Desktop license server</td>
<td><strong>Enabled</strong>&lt;br&gt;(Comma-separated list of license servers to use)</td>
</tr>
<tr>
<td>Set the Remote Desktop license mode</td>
<td><strong>Enabled</strong>&lt;br&gt;(Choose the correct Per Device or Per User mode for your CALs)</td>
</tr>
<tr>
<td><strong>Computer Configuration &gt; Policies &gt; Administrative Templates &gt; System &gt; User Profiles</strong></td>
<td><strong>Enabled</strong>&lt;br&gt;Delete cached copies of roaming profiles</td>
</tr>
</tbody>
</table>

If you use Horizon 7, be sure to review the VMware-provided administrative templates for RDSH server management. See Using Remote Desktop Services Group Policies.

Add Users to the Local Remote Desktop Users Group

To connect to a remote desktop or RDSH server, users must belong to the local Remote Desktop Users group of the virtual desktop or RDSH server. You can use the Restricted Groups policy in Active Directory to add users or groups to the Remote Desktop Users group.

The members of the Remote Desktop Users group are always added to the local Remote Desktop Users group of every virtual desktop or RDSH server that is joined to your domain. When adding new users, you need only add them to the Remote Desktop
Prerequisites for Adding Users to the Restricted Groups Policy

Before you can perform the procedure in this article, you must have created one or more user groups in Active Directory that contain the end users who will connect to the virtual desktops and RDSH servers.

1. Open Group Policy Management

On the domain controller (AD machine), click the Start button, and navigate to Windows Administrative Tools > Group Policy Management.

2. Edit the Default Domain Policy

1. Expand your domain.
2. Right-click Default Domain Policy.
3. Select Edit.
3. Open the Add Group Dialog Box

1. In the Group Policy Management Editor, expand Computer Configuration.
2. Expand Windows Settings.
4. Right-click Restricted Groups.
5. Select Add Group.

4. Add the Remote Desktop Users Group

1. In the Add Group dialog box, enter Remote Desktop Users.
2. Click OK.
5. Add User Groups to the Remote Desktop Users Group

1. Right-click the Remote Desktop Users group that you just added to Restricted Groups.
2. Select Properties.
3. Click Add.
4. Add a group of end users.
5. Click OK in the Add Member dialog box.
6. Click OK in the Remote Desktop Users Properties dialog box.

**Turn Off Hardware Graphics Acceleration in Commonly Used Applications**

If the VMs are not using a physical GPU in the ESXi hosts, you can reduce CPU usage by not emulating hardware graphics in applications. We recommend using Dynamic Environment Manager configuration files to control these application settings.

For more information about having VMs use physical GPUs, see Deploying Hardware-Accelerated Graphics with VMware Horizon 7.

1. Internet Explorer
1. To turn off hardware graphics acceleration for Internet Explorer, open the Internet Options dialog box by clicking the Tools icon and selecting Internet Options.
2. Click the Advanced tab.
3. From the Accelerated graphics list, select Use software rendering instead of GPU rendering.
4. Click OK.

2. Microsoft Office
1. To turn off hardware graphics acceleration for Microsoft Office, open the Options dialog box by selecting **File > Options** in the application (in this example, Microsoft Word).
2. Select **Advanced**.
3. Scroll down to the Display section.
4. Select **Disable hardware graphics acceleration**.

### 3. Adobe Reader
1. To turn off hardware graphics acceleration and disable other CPU-intensive display options for Adobe Reader, open the Preferences dialog box by selecting **Edit > Preferences**.

2. Select **Page Display**.

3. In the Rendering section, deselect the following options:
   - Smooth imaging
   - Smooth line art
   - Use page cache
   - Enhance thin lines

4. In the Page Content and Information section, deselect **Use smooth zooming**.

For more information, see the Adobe documentation about **General Application Settings in the Windows Registry**.

**4. Google Chrome**
To turn off hardware graphics acceleration for Chrome, navigate to `chrome://settings`.

1. Scroll down to the System section, and turn off `Use hardware acceleration when available`.

2. Continue running background apps when Google Chrome is closed

**Conclusion**

**In Conclusion**

With the image optimization procedures in this guide, you are able to achieve a significant reduction in the amount disk space, CPU, and memory used by virtual desktop and RDSH server VMs and their vsphere hosts. The result is a corresponding savings in initial deployment time, user logon times, and IOPS.

Image optimization techniques included:

- Disabling unneeded Windows services and features
- Deleting unnecessary files and folders, such as event logs and temporary files
- Compressing OS files
- Zeroing out free disk space and shrinking the disk

Using the **VMware OS Optimization Tool** fling greatly simplifies many of these tasks.

This guide also provided step-by-step instructions for configuring the Windows image to perform optimally in a virtual environment, where CPU cores are shared among many VMs, and where users might be accessing a new VM every time they log in, though they probably will not realize it.

Twenty discreet versions of the Windows OS were tested using the procedures in this guide, including 12 versions of Windows 10.

The procedures in this guide help you create an optimized Windows image that you can use in a VMware Horizon implementation or in other types of deployments. End users will have a great experience, whether they access their personalized virtual desktops or remote applications from company laptops, their home PCs, thin client devices, Macs, tablets, or smartphones.

**Additional Resources**

For more information about the VMware products mentioned in this guide, you can explore the following resources:

- Evaluate VMware Products
- Horizon Support Center
- Horizon 7 Documentation
- Dynamic Environment Manager Documentation
- App Volumes Documentation
- VMware Product Guide
About the Authors and Contributors

**Hilko Lantinga** is a Staff End-User Computing Architect in VMware Technical Marketing, with a focus on 3D, Horizon Windows Desktops and RDSH, Linux, and Applications. Previously, he was a Senior Consultant in VMware Professional Services, leading large-scale EUC deployments in EMEA and has over 18 years of experience in end-user computing.

**Caroline Arakelian** is a Senior Technical Marketing Manager, End-User-Computing Technical Marketing, VMware.

The following people contributed to the review of this paper:

- **Graeme Gordon**, Senior Staff End-User-Computing (EUC) Architect in End-User-Computing Technical Marketing, VMware
- **Jim Yanik**, Senior Manager, End-User-Computing Technical Marketing, VMware

To comment on this paper, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.