Deploying Microsoft Windows 7 Virtual Desktops with Windows Server 2008 R2 Hyper-V

Applied Best Practices
Copyright © 2010 EMC Corporation. All rights reserved.

Published August, 2010

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com. All other trademarks used herein are the property of their respective owners.

Deploying Microsoft Windows 7 Virtual Desktops with Windows Server 2008 R2 Hyper-V Applied Best Practices

P/N h8041
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable boot graphic</td>
<td>19</td>
</tr>
<tr>
<td>Chapter 3</td>
<td></td>
</tr>
<tr>
<td>Default User Profile Customization</td>
<td>21</td>
</tr>
<tr>
<td>Creating a Custom Default User Profile</td>
<td>22</td>
</tr>
<tr>
<td>Create an answer file</td>
<td>22</td>
</tr>
<tr>
<td>Windows profile customizations</td>
<td>25</td>
</tr>
<tr>
<td>Audit mode</td>
<td>25</td>
</tr>
<tr>
<td>Change the default theme</td>
<td>25</td>
</tr>
<tr>
<td>Adjust for best performance</td>
<td>25</td>
</tr>
<tr>
<td>Disable the screen saver</td>
<td>25</td>
</tr>
<tr>
<td>Turn off system sounds</td>
<td>25</td>
</tr>
<tr>
<td>Complete the default profile</td>
<td>25</td>
</tr>
<tr>
<td>Post Installation</td>
<td>26</td>
</tr>
<tr>
<td>Disk cleanup</td>
<td>26</td>
</tr>
<tr>
<td>Defrag the hard drive</td>
<td>26</td>
</tr>
<tr>
<td>Appendix A</td>
<td></td>
</tr>
<tr>
<td>Sizing Memory for Virtual Machines</td>
<td>27</td>
</tr>
<tr>
<td>Virtual machine active memory (working set)</td>
<td>28</td>
</tr>
<tr>
<td>Assigning RAM to virtual machines</td>
<td>28</td>
</tr>
</tbody>
</table>
This applied best practices guide discusses how to configure Microsoft Windows 7 for optimal performance in a Virtual Desktop Infrastructure (VDI) implementation. This document provides an overview on how to configure various subsystems of Windows 7 to minimize the performance requirements on the shared storage and Hyper-V environment.

**Audience**

This applied best practices document is intended for all parties responsible for planning, architecting, configuring, deploying, and maintaining the VDI.

**Related documents**

The following document, located on EMC® Powerlink®, provides additional and relevant information. Access to this document is based on the login credentials. If you do not have access to the following document, contact your EMC representative:

♦ *EMC Performance Optimization for Microsoft Windows XP for the Virtual Desktop Infrastructure – Applied Best Practices*

The following third-party documents, located on the respective website, also provide useful information:


♦ *Pushing the Limits of Windows: Virtual Memory* at [http://blogs.technet.com](http://blogs.technet.com)
This chapter presents this topic:

Virtual Desktop Infrastructure design challenges

--------------------------------------------------------------------------------------------------- 8
Virtual Desktop Infrastructure design challenges

Organizations face many challenges when designing a Virtual Desktop Infrastructure (VDI) that can absorb the bursts of input/output (I/O) users place on a network. The act of centralizing users also centralizes the workload of those users. Centralized user workloads tend to be very dynamic, yet somewhat coordinated in nature. This is because the highly volatile workload of thousands of virtual desktop images can cause periodic performance issues.

A flawed design plan can lead to periods of erratic and unpredictable virtual desktop performance. Users can adapt to slow performance, however, unpredictable performance is sure to quickly frustrate them. A well thought-out design and implementation plan is critical to building a successful environment that provides predictable performance within a VDI infrastructure.

A well thought-out design and implementation plan:

♦ Has enterprise-wide, departmental agreement on the design, test, validation, and user acceptance plans.

♦ Can handle the I/O load from the clients without causing excessive increases in the response time as measured by the user.

Figure 1 shows resource utilization of a typical server and a VDI workload.

In small-to-medium size VDI deployments, most of the issues are about the client experience and total cost of ownership (TCO) of the solution. However, in large scale deployments storage scaling is the primary issue that prevents production implementations. This is because
deployments with thousands of VDI images on a single array synchronous I/O spikes from all the virtual desktops can potentially cause performance issues.

This applied best practices guide provides a set of implementation guidelines to increase virtual machine performance and reduce the I/O burden of the OS significantly. This can also reduce the amount of storage required to support the VDI infrastructure, which in turn, can reduce the initial capital expenditure and operational expenditure outlays. These reductions can significantly increase the return on investment (ROI) of the solution.

Many of the configuration adjustments described in this guide can substantially improve the performance of a virtual machine. However, performance comes at the cost of features. It is the responsibility of the desktop engineering team to find a suitable balance between the features required by users and the performance of their environment.

**Group policy**

This guide assumes that a Microsoft Windows domain that is running on Windows Server 2008 R2 is configured to house the Hyper-V users and desktops.

Many of the optimizations mentioned in this guide are accomplished by using Microsoft Active Directory (AD) Group Policy Objects (GPO) or by editing the registry directly. Use the AD GPOs to manage user desktops that log in to the same virtual desktop. This practice allows administrators to enforce domain policies on the desktops even if users are given the necessary permissions to make changes to the local policy of their machines.

For deployments where user changes are discarded after logging off, use local policy objects (LPO) in the master image instead of AD-based GPOs. When administrators use LPOs instead of GPOs, they have the ability to significantly reduce the load on domain controllers at higher desktop counts.

Do not implement desktop policy directly through the registry. This method is prone to error and high management overhead.

For more information on using group policy effectively, see the Windows Server Group Policy homepage at [http://technet.microsoft.com](http://technet.microsoft.com).
Optimizing
Windows 7 for VDI Overview
This chapter presents these topics:

- Introduction ................................................................. 12
- Virtual machine configuration ....................................... 12
- Windows optimizations .................................................. 13
Introduction

The Windows boot process creates a brief period of extremely heavy read activity as the OS is loaded into memory. During the boot process, Windows loads drivers, fonts, applications, processes, and other runtime components. Each component, driver, service, and application that is loaded represents IOs that must be serviced from the backend storage.

The management of large VDI deployments at scale requires effective use of tools available to the domain administrator. Many of the settings can be applied by binding GPOs to the organizational units (OU) containing the virtual desktops. This can be done using the Group Policy Management Console. The examples in this chapter assume that all desktops are contained in an OU named HyperV_VDI.

Virtual machine configuration

Microsoft Hyper-V Server 2008 R2 is a stand-alone product that provides a reliable and optimized virtualization solution. This section includes recommendations for configuring virtual machines hosted on Hyper-V Server 2008 R2.

Memory size

The minimum recommended configuration of RAM for Windows 7 is 512 MB. This is not enough space to hold the entire active working set of applications in memory that most users require. When enough RAM is available, Windows 7 caches binaries and data in memory. This is also referred to as client-side caching, a feature that stores frequently used information on the client's machine, which is key in reducing unnecessary read activity from the guest OS.

Refer to Appendix A for more information about client-side caching and how to adequately size the memory configuration for Windows 7 virtual desktops. For initial testing 2 GB is a preferred value.

Disk size

Create a virtual hard disk (VHD) file that is large enough to hold the OS and any applications that will be installed in a virtual desktop. Use roaming profiles to redirect data out of the virtual desktop and folder redirection to an EMC Celerra® CIFS share. This enables VDH files to consume less space and allows for centralized management and data protection for user’s files. VHD files are thinly provisioned when created and dynamically expand to the maximum size specified during creation of the VHD.

Storage controller

For virtual desktops use the default Integrated Drive Electronics (IDE) controller that requires more than four disks need to be attached to the image. Because the storage subsystem uses a filter driver, the performance of the IDE and SCSI controllers are very similar.

CPU count

Use as few virtual CPUs (vCPUs) as possible while providing the required amount of CPU resources to the guest OS. Increasing the number of vCPUs increases the work required by the hypervisor to coschedule CPU resources on the physical CPU cores.

If the Hyper-V server is installed on a Non-Uniform Memory Access (NUMA) architecture with more than one physical processor, do not assign more vCPUs to the virtual desktop than exist in a single NUMA node. Doing so can greatly hamper performance in CPU intensive loads.
Integration components

Integrations components (ICs) are sets of drivers and services that help virtual machines perform better by enabling the guest to use synthetic devices instead of emulated hardware devices. Although Windows 7 comes with ICs as part of the base operating system image, ensure that the latest revision has been loaded.

The IC install is initiated by opening the console GUI and selecting Action > Insert Integration Services Setup Disk.

Network adapter

If Citrix Provisioning Services or other third-party PXE imaging delivery applications will not be used for virtual desktop deployment, then select a single synthetic network adapter for virtual desktop images. A single network adapter is recommended for simplicity if network performance or fault-tolerance is not a priority for the user environment.

If Citrix Provisioning Services will be used, then use a dual network adapter configuration that consists of a legacy network card and a synthetic network card. With Hyper-V, the legacy network card is required for supporting PXE with Provisioning Services. After the virtual machine boots, the synthetic NIC has precedence over the legacy network card. The driver sets the route metric for the synthetic NIC to be lower than the legacy NIC.

In this dual NIC configuration, the legacy adapter will be used to support a PXE boot of when the OS is powered on. During the boot process the OS will load the integration components which include the synthetic NIC driver. Once this driver is active, the synthetic adapter will carry the virtual machine traffic on the network.

Windows optimizations

This section provides instructions for modifying Window features to increase performance.

Disable error reporting

When an application or an OS crashes, Windows compiles error reports and attempts to contact Microsoft to debug the issue. Typically, users can safely disable error reporting.

To disable error reporting by using a group policy object,

1. Edit the HyperV_VDI GPO.
Disable automatic updates

The preferred method of updating virtual desktops is to update the master image and create new virtual desktops from the updated master. This method provides a measure of change control and limits the extreme I/O overhead potentially caused by “patch Tuesday” or other events that cause the entire desktop population to simultaneously download and apply updates.

To configure this option:

1. Edit the HyperV_VDI GPO.
3. Set the Configure Automatic Updates to Disabled.

To provide additional space for previously downloaded updates, delete the C:\Windows\SoftwareDistribution\Download folder.

Note: Do not delete the SoftwareDistribution folder itself.

Note: Do not disable automatic updates through group policy in environments that use System Center Configuration Manager (SCCM) because it will prevent SCCM updates from being installed.

Remove unnecessary applications

Many applications load boot-time processes to aid with application performance by caching and prefetching specific data into memory ahead of any actual user request. Examples of this are the boot-time stubs loaded by QuickTime, Real Player, Adobe Acrobat, and others.

Remove Windows components

Remove any Windows components that are not required in the environment such as MSN Explorer or Tablet PC components:

1. Navigate to Control Panel > Programs and Features > Turn Windows features on or off.
2. Remove any unneeded components.

Change NTFS behavior

There are several NTFS options than can be tuned using the fsutil command to minimize file system overhead. These options include the ability to disable the creation of DOS style 8.3 filenames and disabling the “last accessed” time stamp. The “last accessed” option can reduce write workload for users who run applications that access many files.

To disable these features, open a command window and type the following commands:

fsutil behavior set disablelastaccess 1
fsutil 8dot3name set 1

Disable hibernation

Given the high I/O cost of writing the contents of the systems RAM to the C:\hiberfil.sys file, do not allow virtual desktops to go into a hibernation state due. Since the hiberfil.sys file size is equivalent to the RAM allocated to the virtual machine, removing it can save space.

To disable hibernation, open a command prompt and type powercfg /hibernate off.
Disable system restore

Since most VDI environments do not require system restore, this feature can safely be disabled. This practice is acceptable, because users’ data should be moved out of the virtual machine by using folder redirection. In the event the virtual machine becomes corrupt, a replacement can be quickly provisioned to save on I/O overhead of creating and maintaining snapshot data on the virtual machine and also save a significant amount of space.

To disable system restore:
1. Right click My Computer.
2. Select Properties > Advanced System Settings > System Protection > System Protection.
3. Click the Configure button.
4. Under the Restore Settings section, select Turn off System Protection.

Disable paging the executive

By default, Windows writes kernel-mode drivers and system code to the Windows page file when not in use to make more memory available for the system. If the virtual machine is assigned sufficient memory, you may disable this function to save the additional I/O overhead of writing and then reading system code into the Windows page file.

To disable paging of the executive:
1. Open regedit.exe on the master image.
2. Select HKLM > System > CurrentControlSet > Control > Session Manager > Memory Management Find the DisablePagingExecutive key.
3. Change the value from 0 (default) to 1.

Properly size virtual machine RAM

Setting RAM for the virtual machine has an immediate effect on the size of a virtual machine due to the space required to store the Windows page file. Windows creates the C:\pagefile system file based on the RAM installed which can be expanded on demand to meet the virtual memory requirements of the Windows OS.

Appendix A on page 27 provides details about sizing virtual machine RAM. Pushing the Limits of Windows: Virtual Memory by Mark Russinovich provides more details (http://blogs.technet.com).

Set page file to fixed size

By default, Windows dynamically expands and shrinks the Windows page file as required. This can lead to fragmentation of the page file and unnecessary I/O overhead. Set the page file to a fixed size.

The section entitled “How big should I make the paging file” in Pushing the Limits of Windows: Virtual Memory at http://blogs.technet.com provides guidance in determining the fixed page file size.
Disable indexing

Indexing can create I/O overhead for a virtual machine as it builds the index cache. If the environment does not require indexing, it should be disabled to save I/O overhead.

To disable indexing of the local disk

1. From **My Computer**, highlight the C:\ drive and select **Properties**.
2. On the General tab clear the **Allow Indexing Service to index this disk for fast file searching** checkbox.
3. Navigate to **Indexing Options**.
4. Open the **Control Panel** and click the **Modify** button.
5. Deselect all locations in the list.

Disable unnecessary services

Since services are not useful in a virtualized instance of the OS, disable unnecessary services such as WWAN AutoConfig serve. Services can be disabled by launching the Services MMC plug-in by running **START\RUN\services.msc**.

The following is a list of services that can be considered for disabling in a VDI environment.

- Telephony
- Shell Hardware detection
- Machine Debug Manager (MDM)
- Remote Registry
- Task Scheduler
- Network Location Awareness
- Windows Audio
- Themes
- WWAN AutoConfig
- WLAN AutoConfig
- Windows Update
- Windows Connect Now

For a comprehensive list of services and configuration options review [http://www.blackviper.com](http://www.blackviper.com).

SuperFetch

Window 7 uses SuperFetch to manage the random access memory on a machine and helps it run efficiently. To do this SuperFetch analyzes usage patterns and based on repeated user action it are pre-populate RAM with programs the user is likely to launch.

For systems with small memory configurations, disable SuperFetch to keep as much free memory available as possible and to avoid extra disk accesses. SuperFetch also allocates system RAM for its use which can increase memory pressure on the host if RAM is heavily overcommitted.

For desktops with larger memory configurations, leave SuperFetch enabled so that Windows 7 can optimize the disk layout of the prefetch data and proactively load user binaries into memory to make the desktop more responsive.
Managing Processes with Process Explorer

Another useful tool for managing services and processes is Sysinternals Process Explorer which provides an interface for viewing processes that are currently running on the desktop. Process Explorer is also a powerful troubleshooting tool that can be used to investigate performance issues, slow logon/logoff performance, and other related issues. An example of how Process Explorer was used to solve issues with slow logons can be found by searching for “The Case of the Slow Logons” at http://blogs.technet.com/b/markrussinovich/.

Other examples of how to use these tools is in “The Case of the Unexplained” series hosted by Mark Russinovich at: http://technet.microsoft.com/en-us/sysinternals/bb963887.aspx.

Microsoft also offers the Sysinternals Live service which enables execution of the Sysinternals tools directly from the Internet without searching for and manually downloading them. Enter a tool's Sysinternals Live path into Windows Explorer or a command prompt as http://live.sysinternals.com/<toolname> or \live.sysinternals.com\tools\<toolname>. The entire Sysinternals Live tools directory is available through a browser at http://live.sysinternals.com.

The Process Explorer interface can be seen in Figure 2.

![Figure 2 Process Explorer](image-url)
Streamline Windows with autoruns

Autoruns is a program developed by Mark Russinovich and Bryce Cogswell of Microsoft. The program enables an administrator to streamline components of Windows 7 that would otherwise be difficult and error prone to configure. The Autoruns GUI is a powerful tool that exposes services, drivers, shell extensions, scheduled tasks and other features normally masked from view. The interface is shown in Figure 3.

There is also a command line version autorunsc that can be run via command line for reporting.

![Figure 3 Autoruns GUI](image)

Disable success logging

By default, Windows records both successful and failed login attempts. For some environments, the overhead of logging successful logons is not required and can be disabled. This could be considered a potential security issue.

To disable successful login events so that they are not written to the security log:

1. Edit the HyperV_VDI GPO.
3. When the Audit account logon events setting Properties dialog box appears, click the Security Policy Setting tab.
4. Select the Failure checkbox.
Group policy refresh interval

By default, all computers in the domain will attempt to refresh their group policy settings every 90 minutes with a 30 minute offset. This can be extended to limit the amount of network bandwidth that is consumed when refreshing group policy. By default, group policy is also updated at every boot of the OS.

To change the group policy refresh interval:

1. Edit the HyperV_VDI GPO.
3. When the Group Policy refresh interval for computers dialog box appears, click the Enabled button.
4. In the Options area, set how often the Group Policy will be applied to computers by typing or selecting the number of Minutes.
5. Optionally, in the same area, set the amount of random time to be added to the Group Policy refresh interval by typing or selecting the number of Minutes.

Disable scheduled defrag

By default Windows 7 is set to run a scheduled defrag every week. This is not desirable for the end clients.

To disable the scheduled defrag:

1. Open the properties for the C:\ drive.
2. Select the Tools tab.
3. Click Defragment now to display the Disk Defragmenter dialog box.
4. Click Configure schedule.
5. Clear the Run on a schedule checkbox.

Remove tablet PC components

The handwriting input drivers packaged with the Tablet PC Components are not necessary for Windows 7 instances deployed as virtual desktops.

To remove these components:

1. Select Control Panel > Programs and Features.
2. Click Turn Windows features on or off.
3. In the Windows Features dialog box clear the Tablet PC Components checkbox.

Disable boot graphic

Windows 7 draws a startup animation during the boot process. This will not be seen by users who are not connected to the console and it needlessly consumes resources.

To disable it:

1. Start the msconfig.exe program.
2. Select the Boot tab.
3. Under the Boot options, select No GUI boot and Base video.
4. Clear the Boot log checkbox, unless this functionality is desired.
This chapter presents these topics:

Creating a Custom Default User Profile........................................................................................................22
Windows profile customizations ......................................................................................................................25
Post Installation................................................................................................................................................26
Creating a Custom Default User Profile

This section describes the procedures to set up the default user profile for the golden image virtual machine. The process to create a default user profile under Windows 7 is different from the Windows XP setup. An altered profile to the default can no longer be copied user space from the Windows 7 User Profiles dialog box under System Properties.

This chapter provides an overview of the procedure to create a default user profile. This is accomplished by doing the following:

♦ Create an answer file.
♦ Run `sysprep.exe` and boot to audit mode.
♦ Make customizations for the default user.
♦ Run `sprep.exe` with custom answer file to copy administrator profile to the default user.

Create an answer file

To create and manage an answer file, the Windows System Image Manager (WSIM) must be installed on a workstation. WSIM is part of the Windows Automated Install Kit (AIK) and can be found by searching for “Windows 7 AIK” at [http://www.microsoft.com/downloads/](http://www.microsoft.com/downloads/).

To create an answer file:

1. Open WSIM and under the Windows Image header, right-click and select Select Windows Image as shown in Figure 4.

![Select image dialog box](image)

Figure 4 Select image dialog box
2. In the open dialog box, browse to the sources directory of a Windows 7 DVD or mounted ISO file and select the install.wim file as shown in Figure 5.

This will load the Windows 7 installation image structure into WSIM. Now that the Windows 7 install image is loaded, the answer file can be created.

![Select a Windows Image](image)

**Figure 5** Select the install image

3. From WSIM select **File > New Answer File** to create a blank answer file.

4. Save this file as sysprep.xml.

5. Under the **Windows Image** header, expand **Components**.

6. Locate the name that is similar to `x86_Microsoft-Windows-Shell-Setup_6.1.7600.16385_neutral`.

**Note:** If this is a 64-bit image, the key name will be prefixed with `amd64` instead of `x86`. 
7. Right-click this key and select **Add Setting to Pass 4 specialize** as shown in Figure 6.

![Figure 6 Adding components to Pas 4 specialize](image)

8. In **Answer File** pane, expand **4 specialize** and select `x86_Microsoft-Windows-Shell-Setup_neutral`

9. Change the **Copy Profile** option to **true** as shown in Figure 7.

![Figure 7 Setting CopyProfile to true](image)

10. Save the answer file as `sysprep.xml`.

11. **Copy the file to the golden image under c:\Windows\system32\sysprep.**

**Note:** There are many other options that can be configured, but **CopyProfile** is the only option required to copy the administrator profile over the default user profile.
Windows profile customizations

This section contains procedures to customize the Windows profile.

Audit mode

When a valid sysprep.xml file is present the golden image machine must be booted into audit mode. To boot the machine in audit mode during an install of Windows 7, press Ctrl + Shift + F3. When the Welcome screen to reboot the machine and put Windows in audit mode. If Windows 7 has already been installed on a machine audit mode can be invoked by running `c:\windows\system32\sysprep /audit`.

After the system reboots into audit mode, it automatically logs in with the local administrative user account. At this point, customization of the administrator account can begin. Note that sysprep removes the machine from the domain to place Windows in audit mode. After the system is resealed, it must be rejoined to the domain.

Change the default theme

Windows Themes controls how the desktop is rendered. The default theme uses many optimizations to paint a more graphically complex user interface which creates increased processor and network overhead. The Classic theme is suggested for VDI environments due to its lower overhead. If the Themes service has been disabled, the user interface (UI) defaults to the Windows Classic theme.

To manually enforce the Windows Classic theme using the group policy:

2. Set the Force a specific visual style file or force Windows Classic option to Enabled.

Adjust for best performance

Some of the more advanced UI features, such as menu fading and animations, require extra CPU and memory resources to use. To turn off these effects select:


Disable the screen saver

The screen saver is not needed in a VDI environment because users do not directly connect to the console of the virtual machine. To disable it for all VDI users:

1. Edit the HyperV_VDI GPO.
3. Set Enable Screen Saver to Disabled.

Turn off system sounds

To turn off the system sounds:

1. Select Control Panel > Sound > Sounds.
2. Set the Sound scheme to No Sounds.

Complete the default profile

After all require changes have been made under the local administrator account, sysprep must be run again to copy the account over the default user account. Assuming the sysprep.xml file
created previously is located in C:\windows\system32\sysprep and is named sysprep.xml the system can be resealed by running C:\windows\system32\sysprep\sysprep.exe /generalize /oobe /shutdown /unattend:C:\windows\system32\sysprep\sysprep.xml.

This causes Windows to copy the administrator profile over the default user profile and shut down. Now any user logging into the virtual machine will inherit the changes made to the default user profile. The default user profile can also be copied to a network share if so desired.

**Post Installation**

After the user configuration is complete; perform before a disk cleanup, defrag the hard drive, and take a snapshot of the virtual machine to deploy the linked clones.

**Disk cleanup**

Run the disk cleanup wizard to find and delete any files that have accumulated in the image that do not absolutely have to be present in the image.

To perform a disk clean up:
1. Select the C:\ drive and right-click.
2. Select Properties > General tab.
3. Click Disk Cleanup.
4. Remove all files that do not need to be part of the image.

**Defrag the hard drive**

The golden image should have its disk defragmented before being used for image deployment.

<table>
<thead>
<tr>
<th>Note:</th>
<th>NEVER defragment deployed virtual desktops.</th>
</tr>
</thead>
</table>

Do not defragment deployed virtual desktops for the following reasons:

- Defragging a drive creates a very high I/O overhead and can quickly cause sufficient I/O to the shared storage to cause performance issues.
- If the VHDs are thinly allocated, defragmenting the virtual machine hard drive will cause the virtual machine hard disk to quickly expand in size. For example, running defragmentation on a virtual machine that was using only 600 MB of space after deployment can balloon up to 4 GB or more of allocated space.

To defragment the hard drive:
1. Select the C:\ drive and right-click.
2. Select Properties > Tools tab.
3. Click Defragment now.
This appendix presents these topics:

Virtual machine active memory (working set) ................................................................. 28
Assigning RAM to virtual machines ................................................................................. 28
The amount of RAM allocated to a virtual machine directly effects the number of factors that impact both capacity and performance requirements for a virtual machine. This appendix briefly explains on how to allocate RAM to Windows 7 virtual machines.

Virtual machine active memory (working set)

The amount of RAM activity by a virtual machine is referred to as the active working set. This can be seen by observing the In Use counter in Resource Monitor. A virtual machine with 2 GB of RAM with the max working set size is 1 GB (In Use == 50%), then the virtual machine is using 50 percent of its allocated RAM.

Assigning RAM to virtual machines

The goal in selecting the appropriate RAM size for the golden image virtual machines is to give the virtual machines enough memory to hold the entirety of the working set in memory. Properly sizing the amount of RAM assigned to the virtual machines has the following benefits:

- Reducing page file usage. If Windows 7 has sufficient RAM to hold the active working set, it will not need to utilize virtual memory as often.
- Reduce I/O requirements. By reducing virtual memory activity, disk accesses are reduced.
- Maximize consolidation ratio. Accurately sizing the RAM for virtual machines can lead to higher consolidation ratios on the Hyper-V host.

To determine how much RAM to allocate to the golden image virtual machine, the guest OS should be placed under load. With the peak load running on the virtual machine, the amount of memory in use needs to be measured. This is the active working set size.

For the best balance between performance and memory utilization the virtual machine should have at least 25 percent more RAM allocated than the maximum memory load witnessed by the VM. This extra RAM helps Windows avoid writing data to its page file which keeps the active working set for the virtual machine in RAM instead of virtual memory space.

As an example, if the golden image virtual machine has a peak active memory threshold of 600 MB, then the virtual machine should have at least 750 MB of RAM allocated.