Deploying Microsoft Windows 7 Virtual Desktops with VMware View

Applied Best Practices

EMC NAS Product Validation
Corporate Headquarters
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

Published September, 2010

Deploying Microsoft Windows 7 Virtual Desktops with VMware View Applied Best Practices

P/N h8043.1

Contents

About this Document

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 ESX 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:

- *Windows XP Deployment Guide* at *http://www.vmware.com*
- *VMware VDI Storage Considerations* at *http://www.vmware.com*
- *Recommendations for Aligning VMFS Partitions* at *http://www.vmware.com*
- *Pushing the Limits of Windows: Virtual Memory* at *http://blogs.technet.com*
- *Understanding Memory Management* at *http://vpivot.com*

Chapter 1 Optimizing Windows 7 for VDI Overview

This chapter presents this topic:

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.

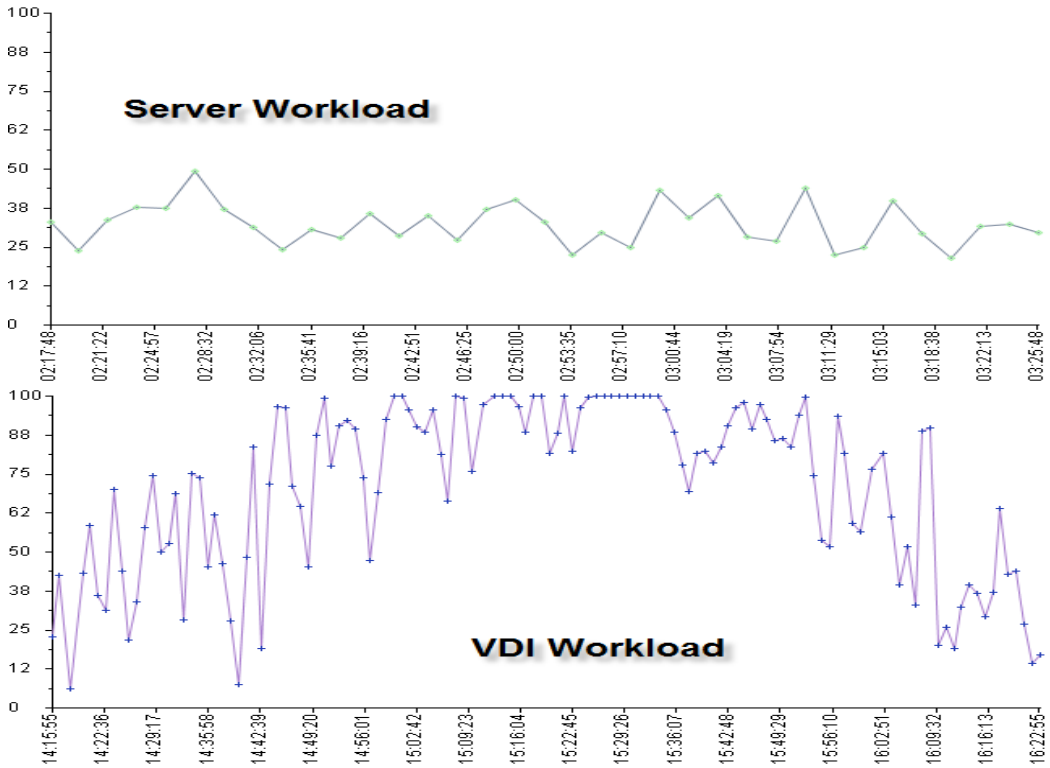

Figure 1 VDI workload – Example

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 VMware View 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.

Chapter 2 Customizing the Virtual Machine

This chapter covers the basic configuration to perform on the virtual machine before you can create a base image for use in a VDI deployment. Follow the procedures in this chapter to create a Windows 7 virtual machine.

This chapter presents this topic:

Configure the virtual machine settings

Windows 7 compatibility

In order to run Windows 7 virtual desktops, ensure the ESX servers can support the virtual desktops as a guest OS type. Windows 7 support is included with the ESX as of ESX 4 update 1. Additionally, VMware View Manager 4.5 is required for official support of Windows 7 virtual desktops. EMC also recommends that you use version 7 virtual machines.

vCPU 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 co-schedule CPU resources on the physical CPU cores. Be sure to allocate adequate CPU resources are allocated to the virtual machine, verify that the average CPU utilization reported by the virtual machine is less than 70 percent, and the %RDY counter for the virtual machine is less than 10 percent.

If the virtual machine reports low CPU utilization and the %RDY value is higher than 10 percent, the virtual machine vCPU is waiting for free physical CPU resources to schedule its workload. This can be an indication of over-provisioned physical CPUs on the ESX host. Move some virtual machines off the ESX host to free up physical CPU resources.

Virtual machine memory

The minimum recommended configuration of RAM for Windows 7 is 512 MB. For most users this will not be adequate to hold the entire active working set of applications in memory. If enough RAM is available, Windows 7 will cache binaries and data in memory. This caching is referred to as client side caching and it is key in reducing unnecessary read activity from the guest operating system. Appendix A has more information on how to adequately size the memory configuration for Windows 7 virtual desktops. For initial testing, 1.5 GB is a safe value to use.

SCSI controller

The default small computer system interface (SCSI) controller for new Windows 7 virtual machines is the LSI Logic SAS controller. This controller provides good performance and Windows 7 includes the drivers in its image.

Disable virtual machine logging

Every time a virtual machine is powered on, it logs diagnostic information to the data store hosting its VMDK file. For large concentrations of virtual machines, this overhead can be significant.

To disable logging, clear **Enable logging** from the **Settings** pane in the **Options** tab as shown in Figure 2 below. This option sets the **`logging = "FALSE"`** option in the VMX file for the virtual machine.

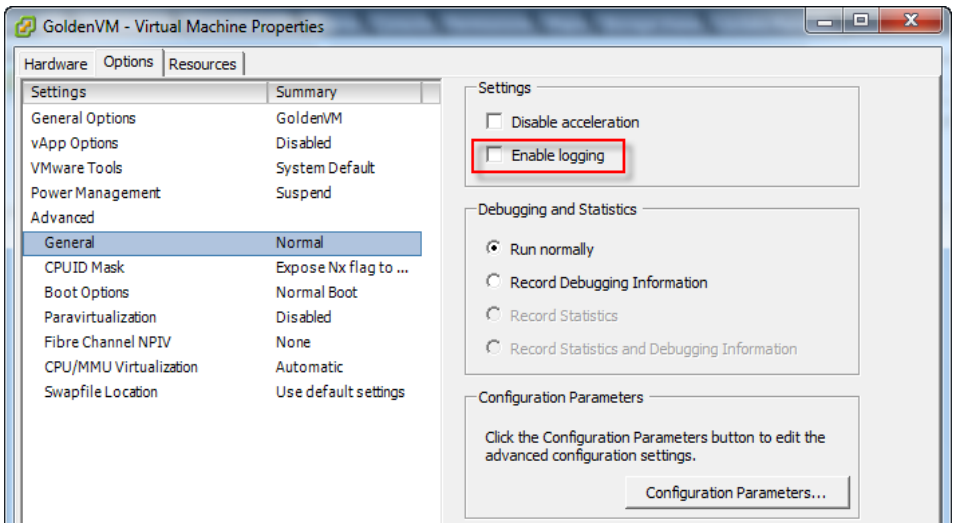

Figure 2 Virtual Machine Properties dialog box

Edit BIOS settings

Any device attached to the virtual machine requires resources to load during startup. Disabling devices that the virtual machine will not use frees more resources for use by the ESX server.

To disable unneeded BIOS devices for a virtual machine,

1. Select **Boot Options** in the Virtual Machine Properties screen.
2. Select the **Force BIOS Setup** checkbox, as shown in Figure 3 below.

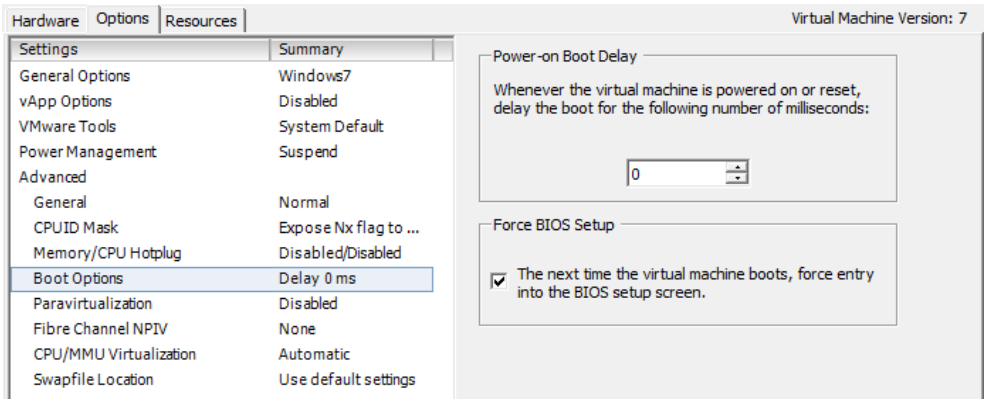

Figure 3 Forcing the virtual machine into BIOS

3. Click **OK** to close the **Virtual Machine Properties** dialog box and start the virtual machine. The virtual machine will now boot to the BIOS menu.
4. In the BIOS menu, click the **Advanced** tab.
5. Select **I/O Device Configuration**.
6. In this menu, disable the serial and parallel ports for the virtual machine if they are not needed.

7. Press **F10** to save the configuration and exit the BIOS.

Install using 8 KB allocation size

EMC has seen increased performance with Windows 7 when formatting the boot volume with an allocation size of 8192 bytes instead of 4096 bytes. Currently the Windows installer does not support creating an 8 kilobyte allocation size during the installation with the graphical interface.

To install Windows 7 with an 8 kilobyte allocation size perform the following steps.

1. Boot from the Windows 7 ISO image or CD and proceed through the install steps until the **Where do you want to install Windows** dialog appears.
2. Press Shift-F10 to bring up a command window.
3. In the command window, enter the following commands:
    a. Diskpart
    b. Select disk 0
    c. Create partition primary size=400
    d. active
    e. format fs=ntfs label="System Reserve" quick
    f. Create partition primary
    g. Format fs=ntfs label=OS_8k unit=8192
    h. Assign
    i. Exit
4. Click the **Refresh** button to refresh the **Where do you want to install Windows** screen.
5. Select **Disk 0 Partition 2.**
6. Complete the install to the second disk formatted with the 8192 allocation size, as shown in Figure 4 below.

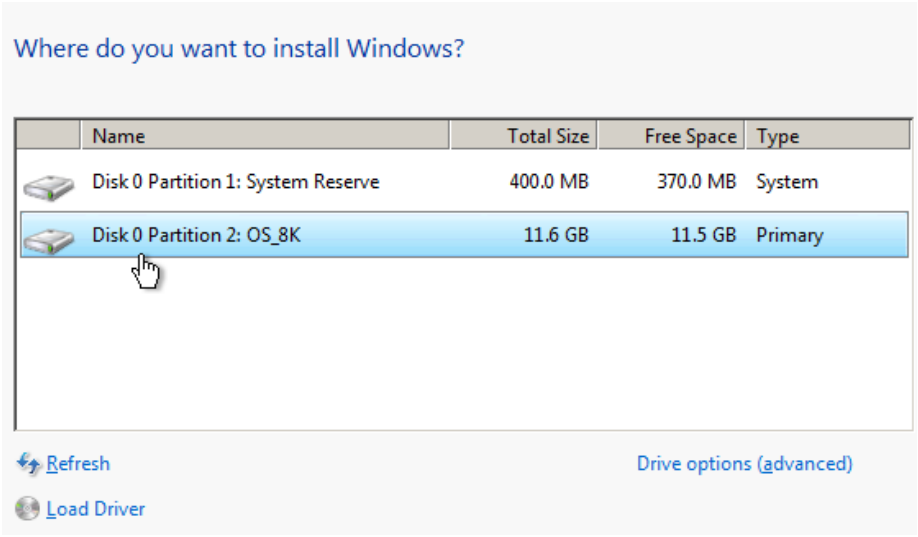

Figure 4 Install on 8K partition

Chapter 3 Windows 7 Operating System Optimization

This chapter presents these topics:

VMware optimizations

The Windows boot process creates a brief period of extremely heavy read activity while 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 loaded represents IOs that must be serviced from the backend storage.

VMware View allows for both persistent and non-persistent (or floating pool) desktop pool types. Persistent pools map users to unique a unique desktop which remains assigned to that user until the desktop is deleted. For these types of desktops, maintain features that help maintain personality of the desktop, such as search history, browser cookies, and other personalized information.

For non-persistent or floating pools, users are not assigned unique desktops and the desktops are deleted after a single use. In this case, there is no need to maintain any user state information on the virtual desktop at all and more aggressive methods can be used to reduce the I/O footprint of the virtual desktop. For non-persistent pools EMC recommends enforcing domain policies through LPOs set in the master image.

Managing large VDI deployments at scale requires effectively using tools available to the domain administrator. For persistent pools, many of these 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. For the examples provided this chapter, it is assumed that all desktops are contained in an OU named VMware_View.

Each optimization in this chapter will be recommended for one or both types of desktop pools in order to provide a good balance of user personalization and performance for the virtual desktop. The optimizations will be recorded as follows:

- [A] – Both persistent and non-persistent pools
- [NP] – Recommended for non-persistent (floating) pools

Install VMware tools [A]

Install the latest version of VMware tools to ensure that the virtual desktops are running the latest drivers. These drivers should be a part of the base image. You can also update VMware tools post-deployment with VMware Update Manager.

Windows optimizations

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

Disable error reporting [NP]

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 **VMware_View GPO**.
2. Select **Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Error Reporting**.
3. Set **Disable Windows Error Reporting** to **Enabled**.

Disable automatic updates [NP]

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 **VMware_View GPO**.
2. Select **Computer Configuration** > **Policies** > **Administrative Templates** > **Windows Components** > **Windows Update**.
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 SoftwareDistibution 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 [A]

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 [A]

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 [A]

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 [A]

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 [A]

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 [A]

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 [A]

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 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 [A]

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 [NP]

Indexing can create I/O overhead for a virtual machine as it builds the index cache. If the environment does not require indexing, is not needed 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 [A]

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.

Disable SuperFetch [NP]

For non-persistent pools where the desktops are deleted after use disable the SuperFetch service. SuperFetch analyzes usage patterns and based on repeated user action it and pre-populates RAM with programs the user is likely to launch. This causes unnecessary I/O as any optimizations are destroyed along with the desktop when a user disconnects. SuperFetch also allocates more of the system RAM for its use which can increase the pressure on the host if RAM is heavily overcommitted.

For persistent desktops with larger memory configurations it is recommended to 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.

Note: On systems where the storage is able to achieve more than 8 MB/s random read performance during the Windows System Assessment Tool (WinSAT) tests the SuperFetch service may be proactively disabled. WinSAT is generally run during the out of box experience (OOBE) system preparation stage after deployment. Windows 7 will do this under the assumption that with very fast storage it is more efficient to pull data from disk than to pre-populate it into memory.

To view the status of the last WinSAT test, an administrator should invoke the invoking **winsat query** from the command prompt in a Windows 7 command prompt window.

Managing Processes with Process Explorer [A]

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 5 below.

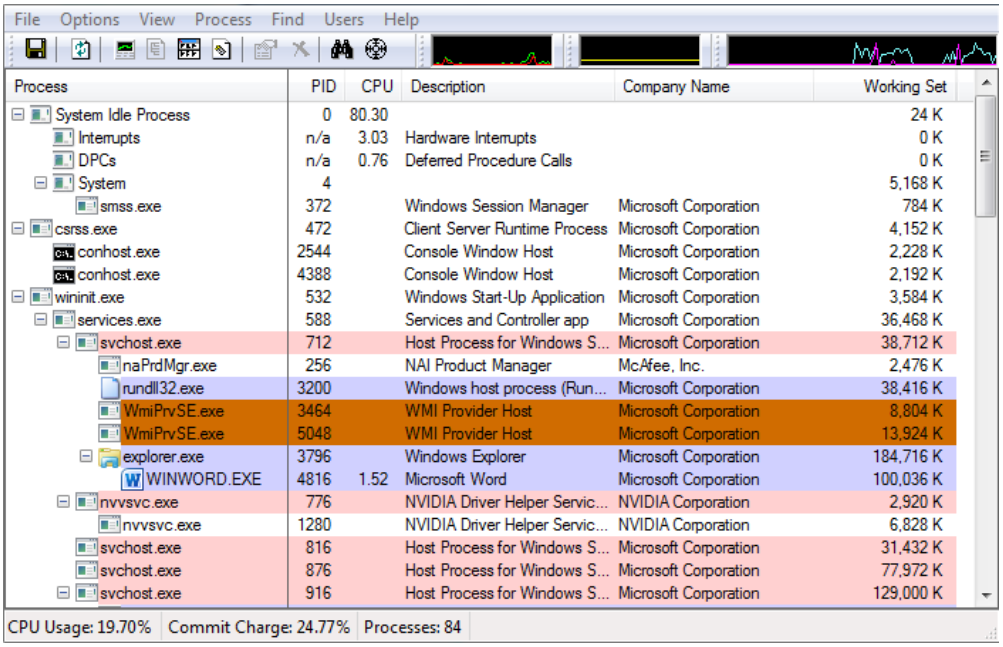

Figure 5 Process Explorer

Streamline Windows with Autoruns [A]

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 6 below.

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

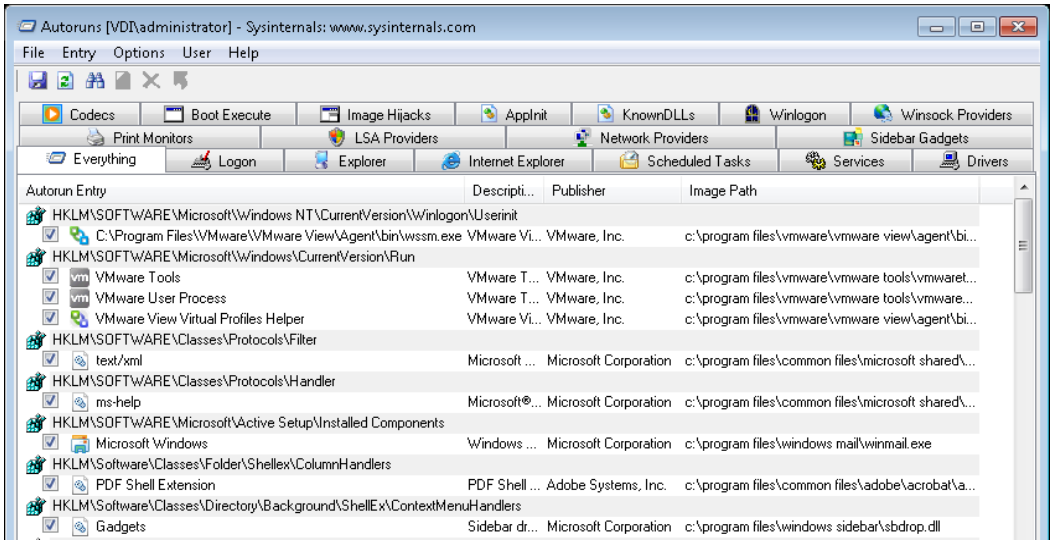

Figure 6 Autoruns GUI

Disable success logging [NP]

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 **VMware_View GPO**.
2. Select **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **Audit Policy**.
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 [A]

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 **VMware_View GPO**.
2. Select **Computer Configuration** > **Policies** > **Administrative Templates** > **System** > **Group Policy**.

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 [A]

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 [A]

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 [A]

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 lo**g checkbox, unless this functionality is desired.

Chapter 4 Default User Profile Customization

This chapter presents these topics:

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/.

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 7 below.

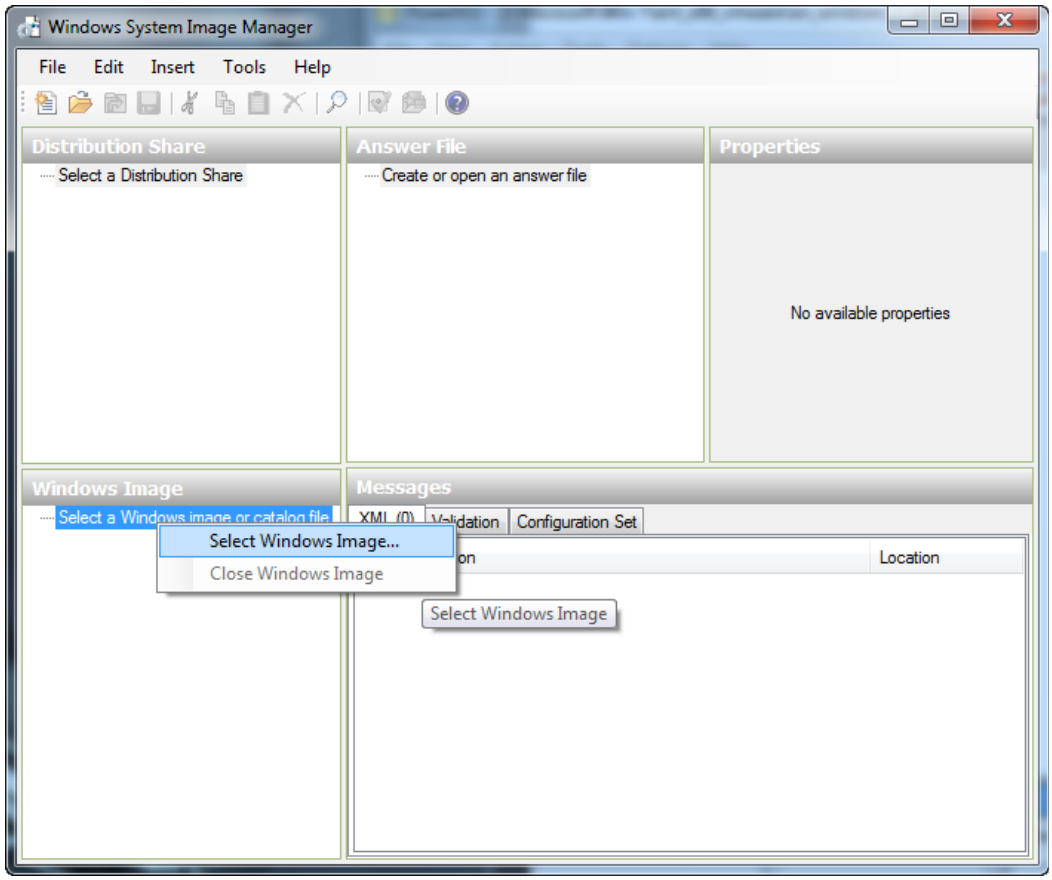

Figure 7 Select image dialog

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 8 below.

   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.

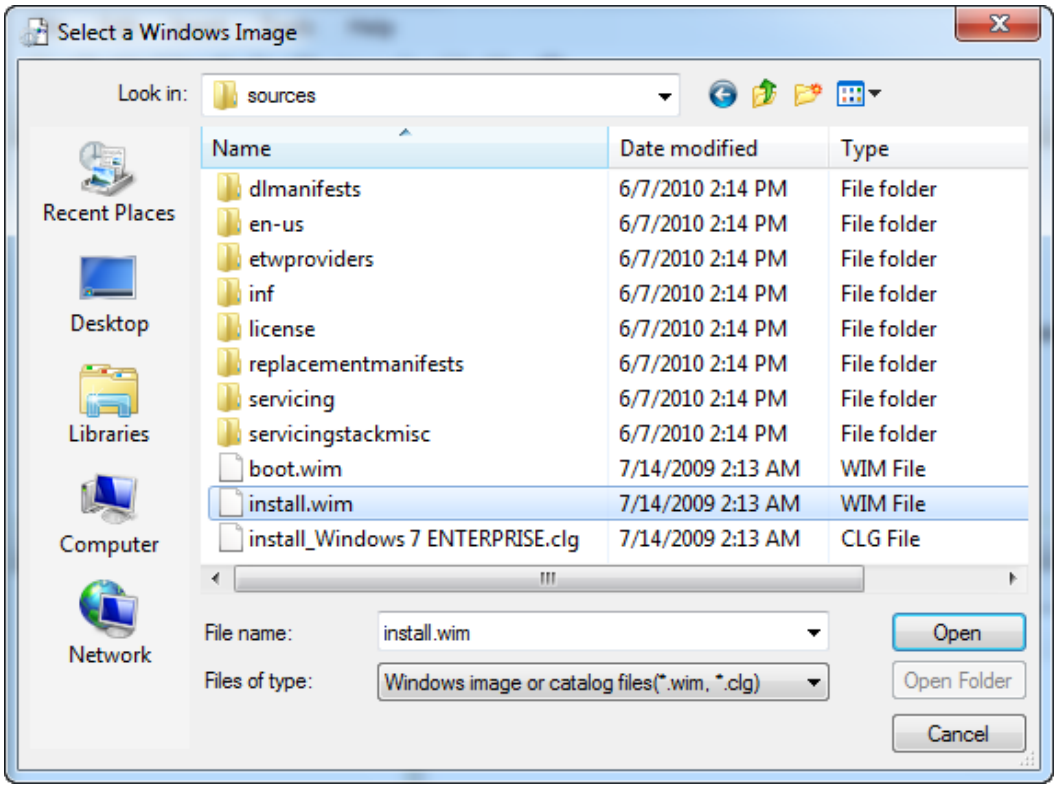

Figure 8 **Select the install image**

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 9 below.

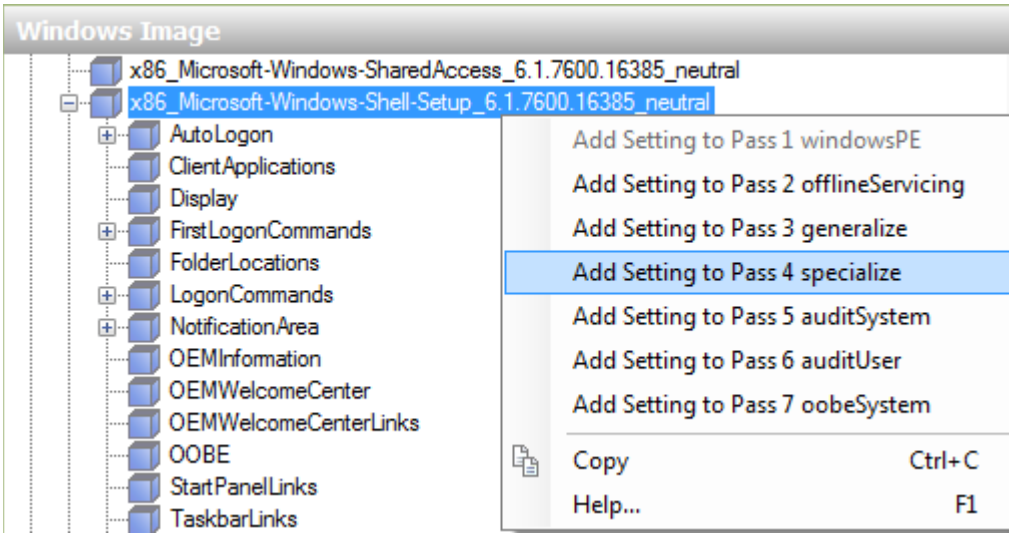

Figure 9 Adding components to specialize pass

8. In **Answer File** pane, expand **4 specialize** and select x86_**Microsoft-Windows-Shell-Setup_neutral**

9. Change the **CopyProfile** option to **true** as shown in Figure 10 below.

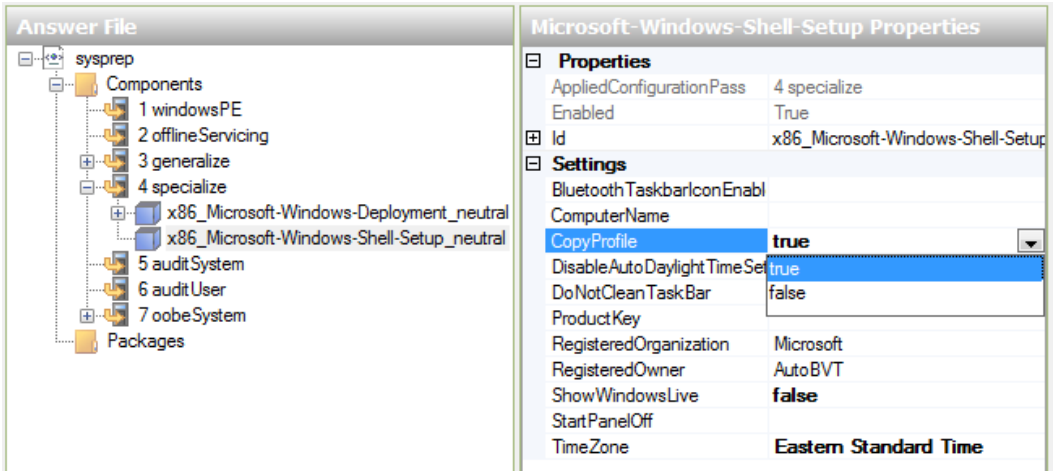

Figure 10 Setting CopyProfile to true

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:

1. Select **User Configuration** > **Policies** > **Administrative Templates** > **Control Panel** > **Personalization**.
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:

1. **My Computer** > **Properties** > **Advanced** > **Performance**.
2. Select **Adjust for best performance**.

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 **VMware_View GPO**.
2. Select **User Configuration** > **Policies** > **Administrative Templates** > **Control Panel** > **Personalization**.
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.

Note:	NEVER defragment deployed virtual desktops.

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**.

Appendix A Sizing Memory for Virtual Machines

This appendix presents this topic:

Introduction

The amount of RAM allocated to a virtual machine has a direct effect on a number of factors that impact both capacity and performance requirements for a virtual machine. This appendix briefly explains how to allocate RAM to Windows 7 virtual machines. For the sake of simplicity, memory overhead of the ESX host will not be included in any calculations.

This appendix also assumes that users have a good understanding of ESX memory management technologies such as memory over-commitment, transparent page sharing (TPS) and vswap usage. More information can be found in the *vSphere Resource Management Guide* found at www.vmware.com.

As an advanced configuration consideration, if you do not over-commit memory, then it is possible to disable TPS which will free up CPU cycles which the virtual machines can use. TPS can be disabled by setting **Mem.ShareScanGhz** to zero under the advanced settings for an ESX host. This can provide a 5 percent performance boost to the virtual machines on the host.

Virtual Machine Active Memory (Working Set)

The amount of RAM that is actively used by a virtual machine is referred to as the active working set. This can be seen with the %ACTV counter in esxtop or the "Active" memory counter in vCenter under the **Resource Allocation** tab. On a virtual machine with 2 GB of RAM, if the max working set size is 1GB (%ACTV == 50%) then the virtual machine is using 50 percent of its allocated RAM. Assuming other virtual machines exhibit similar behavior, a 2:1 over-commit ratio could be used without causing excessive swapping by the ESX host.

On the ESX server, if the active working set for all virtual machines is less than the total available host memory, then all the virtual machines run at full speed because each virtual machine is able to address all the RAM it requires without the hypervisor ballooning or swapping virtual machine memory pages to disk.

Conversely, when the sum of all active working sets on the host exceeds the amount of available RAM on the ESX host, the hypervisor will be forced to swap pages from the virtual machine memory to vswap. The hypervisor has no knowledge of which pages are in the active working set of the virtual machine and will swap the pages to meet the memory demands placed on the ESX host. This will lead to very poor performance of the virtual machine and should be avoided at all times.

Refer to Table 1 for an example in which a host with 32 GB of RAM is hosting virtual machines each configured for 2 GB of RAM. Each virtual machine has on average 50 percent active memory.

Table 1 Memory over-commit

VM Count	Active Memory in host	Comments
16	16 * 2 GB * 50% = 16 **GB**	Without memory over-commit, only 50% of the host's memory is actively in use.
32	32 * 2 GB * 50% = **32GB**	Memory is over-committed by 200% but active memory is equal to host memory. Virtual machines will run at full speed until usage exceeds 100% of host memory.
48	48 * 2 GB * 50% = **48 GB**, limited to**32 GB** by host	These virtual machines want 48 GB of RAM but are limited to the 32 GB that is installed on the host. ESX must swap to allow these machines to run and performance will be degraded.

When used appropriately, the memory over-commit feature allows virtual infrastructure administrators to drive the ESX hosts to high memory utilization without degrading performance which is not possible with most physical systems.

Assigning RAM to virtual machines

The goal in choosing 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 while keeping the memory over-commit ratio as low as possible. This avoids Windows having to page because there is not enough RAM available in the guest OS. It also avoids ESX having to swap because it cannot reclaim memory from active guests fast enough when experiencing sufficient memory demand.

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

There are several methods to measure the active working set size. In esxtop, look at the %ACTV memory counter. This will display the active working set size as a percentage of allocated memory. If this value never approaches 100 percent then the virtual machine is not actively using all RAM allocated to it.

In vCenter it is reported as **Active** under the **Guest Memory** section on the **Resource Allocation** tab. Alternatively, for more accurate measurement launch **VM Statistics Logging** on the VM and observe the **Memory Active** counter under **VM Memory**.

For the best balance between performance and memory utilization it is suggested that the virtual machine have at least 25 percent more RAM allocated than the maximum active load the VM witnessed to avoid having Windows write data to its page file. This keeps the active working set for the virtual machine in RAM instead of virtual memory space.

For 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. The maximum number of virtual machines to load on the host can be calculated by dividing the maximum amount of ESX host memory by the maximum active memory of the golden virtual machine. In this case it would be 32,768 / 600 = 54 virtual machines. This provides a safe over-commit ratio of approximately 1.25 to 1 if you do not factor in virtual machine and ESX memory overhead.

Additionally, when Windows is booted it zeros out its memory space. This causes the %ACTV memory to briefly run up to 100 percent. This can lead to periods of vswap usage if multiple virtual machines are rebooted in concert as could happen in the event of an ESX host failure, or when VMware HA is enabled for the cluster.