Abstract
This white paper describes how to configure various subsystems of Microsoft Windows in a virtual desktop implementation to minimize the performance demands on the shared storage and VMware vSphere environment.

February 2016
Contents

Executive summary........................................................................................................................................ 4
EUC design challenges.................................................................................................................................. 5
Microsoft Group Policy .................................................................................................................................... 6
Hypervisor settings ......................................................................................................................................... 6
Windows installation settings ....................................................................................................................... 8
Optimizing EUC desktop pools .................................................................................................................. 10
Creating a default user profile .................................................................................................................... 21
Sizing memory for virtual machines .......................................................................................................... 25
References ..................................................................................................................................................... 28
Executive summary

Business case
Organizations face many challenges when designing an end-user computing (EUC) infrastructure that can absorb the bursts of I/O that users place on a network and its accompanying systems. The act of centralizing desktop resources also centralizes the associated workloads. Centralized EUC workloads tend to have high peaks of demand at predictable times. This high-volume workload of thousands of virtual desktop images can cause periodic performance issues.

A poorly designed implementation plan can lead to periods of erratic and unpredictable virtual desktop performance. Users can adapt to slow performance, but unpredictable performance is sure to frustrate them quickly.

A well thought-out design and implementation plan:
- Is critical to building a successful environment that provides predictable performance within an EUC infrastructure
- 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 experienced by the user

Document purpose
This white paper provides EMC configuration recommendations for Microsoft Windows 7, Windows 8, and Windows 10 virtual desktop environments to enable best performance in an EUC implementation. It provides an overview on how to configure various Windows subsystems to minimize the performance demands on the shared storage and VMware vSphere environment. This paper is a starting point for image optimization and not a definitive reference on the topic. The recommendations represent best practices at the time of publication.

Audience
This paper is intended for all parties responsible for planning, designing, configuring, deploying, and maintaining EUC infrastructures and desktop master images.

We value your feedback!
EMC and the authors of this document welcome your feedback on the documentation. Contact EMC.Solution.Feedback@emc.com with your comments.

Authors: John Moran, David Hu, Ye Dai, Kathleen McCarthy
EUC design challenges

Desktop workload

Figure 1 shows a sample of the SAS disk I/O for both a server workload and an EUC workload. Each of the two I/O datasets represents a single disk in a storage pool that is used to provide storage for the indicated resource.

![Figure 1: Sample server and EUC workloads](image)

While the sample server workload shows a consistent amount of disk I/O across the sample time period, the EUC workload experiences frequent peaks in disk utilization. Proper configuration of the virtual desktop master image is critical to minimizing these I/O fluctuations and to maintaining expected levels of performance.

In EUC environments, deployments with thousands of virtual desktop images on a single array are common. In such environments, users often perform tasks at similar times, causing the relatively small utilization spikes for one user to be multiplied by the number of users doing the same tasks. This can potentially cause significant performance issues.

Image optimization

One key way to help mitigate significant performance issues is to optimize the desktop image that is deployed. Any optimizations that are applied to the master image will propagate to all the desktops deployed from that master and can yield significant savings in the I/O operations required of the system.

This document provides a set of implementation guidelines to improve virtual machine performance and reduce the I/O burden on the OS significantly. Following these guidelines can reduce:

- Amount of storage that is required to support the EUC infrastructure
- Initial capital expenditure and operational expenditure outlays
These reductions can significantly increase the return on investment (ROI) of a solution.

Many of the configuration adjustments that are described in this paper substantially improve the performance of a virtual machine. However, performance often comes at the cost of features. The desktop engineering team must find a suitable balance between the features required by users and the performance of the user environment.

**Microsoft Group Policy**

Many of the optimization practices that are described in this paper are accomplished by using Microsoft Active Directory Group Policy objects (GPOs). Use Active Directory GPOs to manage user desktops that log in to the same persistent 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.

**Note:** This paper assumes a Microsoft Windows domain that is running on Windows Server 2008 R2, or later, and that is configured to manage system users.

For deployments where user changes are discarded after logging off, use local policy objects (LPOs) in the master image instead of Active Directory GPOs. This practice can significantly reduce the load on domain controllers at higher desktop counts.

For more information about using Group Policy effectively, see the Windows Server Group Policy home page on [Microsoft TechNet](https://technet.microsoft.com).

**Note:** Some of the optimization practices that are described in this document do involve editing the Windows registry. Read the instructions carefully, follow them exactly, and always back up the registry before making any changes.

**Hypervisor settings**

**Windows version compatibility**

To run Windows virtual desktops, ensure that the hypervisor can support the virtual desktops as a guest OS type.

**vCPU count**

The number of virtual CPUs (vCPUs) that should be used in a virtual desktop depends on numerous factors:

- Use as few 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.
- Allocate adequate CPU resources to the virtual machine.
- Verify that the average CPU utilization reported by the virtual machine is less than 70 percent.
- Verify that the CPU ready (%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 vSphere host. Move some virtual machines off the hypervisor host to free up physical CPU resources.

**Virtual machine memory**

The minimum recommended configuration of RAM for Windows is 1 GB for 32-bit systems and 2 GB for 64-bit systems. The minimum configuration can vary with different versions of Windows, and you should consult the relevant documentation from Microsoft if you have concerns. For most users, the minimum configuration is not adequate to hold the entire active working set of applications in memory. If enough RAM is available, Windows 10 will cache binaries and data in memory. This caching is referred to as client-side caching and is key to reducing unnecessary read activity from the guest operating system. **Sizing memory for virtual machines** on page 25 has more information on how to adequately size the memory configuration for Windows 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 virtual machines is the LSI Logic SAS controller. This controller provides optimal performance, and Windows includes the driver in its image.

**Virtual machine logging**

Every time a virtual machine is powered on, it logs diagnostic information to the datastore hosting its Virtual Machine Disk (VMDK) file. For large concentrations of virtual machines, this overhead can be significant.

To disable logging, clear Enable logging in the Virtual Machine Properties dialog box, as shown in Figure 2. This option sets the logging = "FALSE" option in the VMX file for the virtual machine.

![Virtual Machine Properties dialog box](image-url)
Attached devices

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

To disable unneeded BIOS devices for a virtual machine:

1. In the Virtual Machine Properties dialog box, select Options > Boot Options.
2. Select Force BIOS Setup.

![Figure 3. Forcing a virtual machine into BIOS setup](image)

3. Click OK.
4. Start the virtual machine.
   The virtual machine displays the BIOS menu.
5. In the BIOS menu, click the Advanced tab.
6. Select I/O Device Configuration, and disable the serial and parallel ports for the virtual machine if they are not needed.
7. To save the configuration and exit the BIOS, press F10.

Windows installation settings

Allocation size

EMC has seen improved performance with Windows desktops when formatting the boot volume with an allocation size of 8,192 bytes instead of 4,096 bytes. Currently the Windows installer does not support creating an 8-KB allocation size during installation with the graphical interface.
To install Windows with an 8-KB allocation size, perform the following steps on the master desktop image:

1. Start the virtual machine from the Windows ISO image or CD and continue through the install steps until the **Where do you want to install Windows** dialog box appears.

2. To bring up a **command** window, press **Shift-F10**.

3. In the command window, type the following commands:
   ```
   diskpart
   select disk 0
   create partition primary size=100
   active
   format fs=ntfs label="System Reserve" quick
   create partition primary
   format fs=ntfs label=OS_8k unit=8192 quick
   assign
   exit
   ```

4. To refresh the **Where do you want to install Windows** screen, click **Refresh**.

5. Select **Disk 0 Partition 2:OS_8K**, as shown in Figure 4.

   ![Figure 4. Installing Windows on an 8-KB partition](image)

6. Complete the installation to the disk formatted with the 8,192-byte allocation size.

**VMware Tools**

Install the latest version of VMware Tools to ensure that the virtual desktops are running the latest drivers preconfigured in the base image. Update VMware Tools post-deployment with VMware vSphere Update Manager.
Optimizing EUC desktop pools

Overview

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 that is loaded represents I/O that must be serviced from the backend storage.

Many EUC platforms support both persistent and non-persistent (or floating) desktop pool types. For non-persistent desktop pools:

- Users are not assigned unique desktops and the desktops are refreshed to a previous state after a single use.
- Due to the refresh operation, maintaining user state information on a virtual desktop is unnecessary.
- More aggressive methods are used to reduce the I/O footprint of the virtual desktop.
- EMC recommends enforcing domain policies through LPOs set in the master image, rather than Active Directory enforced GPOs.

Persistent desktop pools map users to a unique desktop that remains assigned to that user until the desktop is deleted or assigned to someone else. Persistent desktops retain features that help preserve the personality of the desktop—for example, search history, browser cookies, and other personalized information.

Managing large EUC deployments at scale requires effective use of tools available to the domain administrator. For persistent desktop pools, many of these settings are applied by binding GPOs to the organizational units (OUs) containing the virtual desktops. This action is done using the Group Policy Management Console. For the examples provided in this document, it is assumed that all desktops are contained in an OU named **EUC_Desktops**.

Optimization recommendations based on type of desktop pool

The following sections describe how to optimize these two types of desktop pools to provide a good balance of user personalization and performance for the virtual desktop:

- Non-persistent pools
- Pools that are both persistent and non-persistent

These recommendations might apply differently to different pools in a real-world environment, so take care to align the optimization practices with the appropriate user communities. Table 1 provides a summary of the recommendations by desktop pool type.
## Table 1. Optimization recommendations for desktop pools, by pool type

<table>
<thead>
<tr>
<th>Type of desktop pool</th>
<th>Optimization recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-persistent only</td>
<td>Disable error reporting</td>
</tr>
<tr>
<td></td>
<td>Disable automatic updates</td>
</tr>
<tr>
<td></td>
<td>Disable content indexing of the C drive</td>
</tr>
<tr>
<td></td>
<td>Disable indexing of remaining file locations</td>
</tr>
<tr>
<td></td>
<td>Disable SuperFetch</td>
</tr>
<tr>
<td></td>
<td>Disable success logging</td>
</tr>
<tr>
<td>Both persistent and non-persistent</td>
<td>Remove unnecessary applications</td>
</tr>
<tr>
<td></td>
<td>Remove Windows components</td>
</tr>
<tr>
<td></td>
<td>Change NTFS behavior</td>
</tr>
<tr>
<td></td>
<td>Pre-compile .NET Framework assemblies</td>
</tr>
<tr>
<td></td>
<td>Disable hibernation</td>
</tr>
<tr>
<td></td>
<td>Disable system restore</td>
</tr>
<tr>
<td></td>
<td>Disable paging the executive</td>
</tr>
<tr>
<td></td>
<td>Correctly size virtual machine RAM</td>
</tr>
<tr>
<td></td>
<td>Set page file to fixed size</td>
</tr>
<tr>
<td></td>
<td>Disable unnecessary services</td>
</tr>
<tr>
<td></td>
<td>Remove unnecessary scheduled tasks</td>
</tr>
<tr>
<td></td>
<td>Remove unnecessary Metro applications</td>
</tr>
<tr>
<td></td>
<td>Manage processes with Process Explorer</td>
</tr>
<tr>
<td></td>
<td>Streamline Windows with Autoruns</td>
</tr>
<tr>
<td></td>
<td>Change the Group Policy refresh interval</td>
</tr>
<tr>
<td></td>
<td>Disable scheduled defragment</td>
</tr>
<tr>
<td></td>
<td>Disable startup graphic</td>
</tr>
</tbody>
</table>

### Optimizing non-persistent desktop pools

**Disable error reporting**

When an application or 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 GPO:

1. Select the **Edit** option for the **EUC_Desktops** GPO.
2. Select **Computer Configuration > Administrative Templates > Windows Components > Windows Error Reporting**.
3. Set **Disable Windows Error Reporting** to **Enabled**.

### 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 events that cause the entire desktop population to simultaneously download and apply updates.

To configure this option:

1. Select the **Edit** option for the **EUC_Desktops** GPO.
2. Select **Computer Configuration > Administrative Templates > Windows Components > Windows Update**.
3. Set **Configure Automatic Updates** to **Disabled**.
4. To provide additional space for previously downloaded updates, delete the `C:\Windows\SoftwareDistribution\Download` folder.

**Note:** Do not disable automatic updates through Group Policy in environments that use Microsoft System Center Configuration Manager (SCCM) because it prevents SCCM updates from being installed.

### Disable content indexing of the C drive

Indexing creates I/O overhead for a virtual machine as it builds the index cache. If the environment does not require indexing, disable it to eliminate the 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 files on this drive to have contents indexed in addition to file properties** checkbox.
3. Click **OK** to begin the change, and then click **OK** again to update the indexing settings using the default option (Apply changes to Drive C:\, subfolders and files).
4. During the application of the new indexing settings, select **Ignore All** if an error message states that a file is in use.

### Disable indexing of remaining file locations

Windows indexes a number of system and user specific folders by default. To reduce the I/O overhead that is associated with this indexing operation, remove any unneeded folder locations from the index list.

To disable indexing of the remaining default locations:

1. Open the Windows Control Panel.
2. Select **Indexing Options**.
3. Select **Modify**. The **Indexed Locations** dialog box opens.
4. Clear the selections for all locations or folders in the list. Click OK to save the changes.

**Disable SuperFetch**

For non-persistent desktop pools, disable the SuperFetch service. SuperFetch analyzes usage patterns and, based on repeated user action, pre-populates RAM with programs the user is likely to launch. This causes unnecessary I/O because any optimization is 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, leave SuperFetch enabled so that Windows 10 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 run during the out of box experience (OOBE) system preparation stage, after deployment. Windows 10 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, run the invoking winsat query from the Windows 10 command prompt.

**Disable success logging**

By default, Windows records both successful and failed login attempts. For some environments, logging successful logins is not required and can be disabled to reduce overhead. This is considered a potential security issue as this information might be required to audit desktop access.

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

1. Select the Edit option for the EUC_Desktops GPO.
3. When the Audit account logon events setting Properties dialog box appears, click the Security Policy Setting tab.
4. Select the Failure checkbox.

**Remove unnecessary applications**

Many applications load boot-time processes to aid 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 Adobe Air and other similar applications.
**Windows 10 native applications**

One of the most obvious differences between Windows 8 and Windows 10 is the number of pre-installed free applications. Windows 10 includes dedicated applications for news, weather, sports, finance, Skype, maps, and so on. All these applications consume some resources in a system, due to the way Windows 10 uses them, even if the user has not started them. We recommend disabling applications that users do not need. Which applications to disable depends on the specific user environment, and identifying such applications is beyond the scope of this document. For the purposes of this paper, EMC testing of Windows 10 EUC environments was conducted with all default applications enabled so that any optimization in this area will only improve performance.

**Remove Windows components**

Remove any Windows components that are not required in the environment such as Internet Printing Client:

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

**Change NTFS behavior**

Several NTFS options can be tuned using the `fsutil` command to minimize file system overhead. These options include disabling the creation of DOS style 8.3 file names and disabling the “last accessed” timestamp. The “last accessed” option reduces write workload for users who run applications that access many files.

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

```
fsutil behavior set disablelastaccess 1
fsutil 8dot3name set 1
```

**Pre-compile .NET Framework assemblies**

Windows compiles .NET framework assemblies on an as needed basis when .NET dependent programs are launched for the first time. This process can be both CPU and disk intensive, so it is preferable to pre-compile all .NET Framework assemblies before deployment of the desktop image.

To pre-compile all .NET Framework assemblies:

1. Open an elevated command prompt.
2. Browse to the C:\Windows\Microsoft.NET\Framework\v4.0.30319 folder.
3. Run the command `ngen.exe executequeueditems`. This process may take several minutes to complete.

**Note:** Microsoft .NET 3.5 is not installed by default in Windows 10. If Microsoft .NET 3.5 is required on the desktop image, it should be installed before running the `ngen.exe executequeueditems` command. Microsoft .NET 3.5 can be installed using the Control Panel option Programs and Features > Turn Windows features on or off.
**Disable hibernation**

Given the high I/O cost of writing content for the system's RAM to the `C:\hiberfil.sys` file, do not allow virtual desktops to go into a hibernation state. Since the `hiberfil.sys` file size is equivalent to the RAM allocated to the virtual machine, remove the file to save space.

To disable hibernation:

1. Open an elevated command prompt.
2. Run the command, `powercfg /hibernate off`.

**Disable system restore**

Since most EUC environments do not require system restore, this feature can safely be disabled. This practice is acceptable because user data should be moved out of the virtual machine using techniques such as folder redirection. If the virtual machine becomes corrupt, a replacement can be quickly provisioned. This method is preferred over system restore due to the I/O resources required to create, store, and maintain virtual machine snapshot data.

To disable system restore:

1. Right-click *My Computer*.
2. Select *Properties > Advanced System Settings > System Protection*.
3. Click *Configure*.
4. Under the *Restore Settings* section, select *Disable System Protection* (or *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, 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`. Locate the `DisablePagingExecutive` key.
3. Change the value from 0 (default) to 1.

**Correctly size virtual machine RAM**

Allocating RAM for a virtual machine has an immediate effect on the size of the 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.
Sizing memory for virtual machines provides details about sizing virtual machine RAM. Pushing the Limits of Windows: Virtual Memory (Microsoft TechNet Blog by Mark Russinovich) provides more details.

**Set page file to fixed size**

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

The “How big should I make the paging file” section in Pushing the Limits of Windows: Virtual Memory (Microsoft TechNet Blog by Mark Russinovich) provides guidance for determining the fixed page file size.

**Disable unnecessary services**

Many Windows services are unnecessary in a virtualized instance of the OS. Disable such services by launching the Services Microsoft Management Console (MMC) plug-in and running services.msc.

Consider disabling the following services in your EUC environment:

- Diagnostic Policy Service
- IP Helper
- Network Location Awareness
- Security Center
- Shell Hardware Detection
- SSDP Discovery
- SuperFetch
- Telephony
- Touch Keyboard and Handwriting Panel Service
- Themes
- Windows Defender Service
- Remote Registry
- Windows Audio
- Windows Connect Now – Config Registrar
- Windows Update
- WLAN AutoConfig
- WWAN AutoConfig

For a comprehensive list of Windows 10 services and configuration options, see Black Viper's Windows 10 Service Configurations.

**Remove unnecessary scheduled tasks**

Windows has a number of scheduled tasks that are either undesirable or not required in an EUC environment. These tasks can be removed or disabled using the Windows Control Panel Schedule tasks utility (or Task Scheduler utility) or an elevated command prompt. The following is a list of tasks that should be reviewed to determine if they are required within the EUC environment; if not, they should be disabled or removed.

**Note:** Different versions of Windows include different scheduled tasks by default. Not all Task Scheduler options listed below are available in all Windows versions. Check the list against your version of Windows.
This list is a superset of commonly disabled items across Windows 7, 8, and 10.

- \Microsoft\Windows\Application Experience\AitAgent
- \Microsoft\Windows\Application Experience\ProgramDataUpdater
- \Microsoft\Windows\Application Experience\StartupAppTask
- \Microsoft\Windows\Autochk\Proxy
- \Microsoft\Windows\Bluetooth\UninstallDeviceTask
- \Microsoft\Windows\Customer Experience Improvement Program\BthSQM
- \Microsoft\Windows\Customer Experience Improvement Program\Consolidator
- \Microsoft\Windows\Customer Experience Improvement Program\KernelCeipTask
- \Microsoft\Windows\Customer Experience Improvement Program\UsbCeip
- \Microsoft\Windows\Defrag\ScheduledDefrag
- \Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticDataCollector
- \Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticResolver
- \Microsoft\Windows\FileHistory\File History (maintenance mode)
- \Microsoft\Windows\Live\Roaming\MaintenanceTask
- \Microsoft\Windows\Live\Roaming\SynchronizeWithStorage
- \Microsoft\Windows\Maintenance\WinSAT
- \Microsoft\Windows\Mobile Broadband Accounts\MNO Metadata Parser
- \Microsoft\Windows\MobilePC\HotStart
- \Microsoft\Windows\Power Efficiency Diagnostics\AnalyzeSystem
- \Microsoft\Windows\Ras\MobilityManager
- \Microsoft\Windows\SideShow\AutoWake
- \Microsoft\Windows\SideShow\GadgetManager
- \Microsoft\Windows\SideShow\SessionAgent
- \Microsoft\Windows\SideShow\SystemDataProviders
- \Microsoft\Windows\SpacePort\SpaceAgentTask
- \Microsoft\Windows\SystemRestore\SR
- \Microsoft\Windows\UPnP\UPnPHostConfig
- \Microsoft\Windows\Windows Defender\Windows Defender Cache Maintenance
- \Microsoft\Windows\Windows Defender\Windows Defender Cleanup
Optimizing EUC desktop pools

- \Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan
- \Microsoft\Windows\Windows Defender\Windows Defender Verification
- \Microsoft\Windows\Windows Error Reporting\QueueReporting
- \Microsoft\Windows\Windows Media Sharing\UpdateLibrary
- \Microsoft\Windows\WindowsBackup\ConfigNotification

Details about each task are available in the Windows Control Panel **Schedule tasks** utility (or **Task Scheduler** utility). To remove a task using an elevated Windows command prompt, use a command similar to the following example:

```
SCHTASKS /Delete /TN "\Microsoft\Windows\Application Experience\AitAgent" /F
```

**Remove unnecessary Metro applications**

Windows 8 and 10 include a number of Metro applications that might not be required in an EUC environment. In addition, some Metro applications are active even if they are not being used by the end user, placing unnecessary load on the EUC infrastructure.

You can view the full list of installed applications by using the PowerShell command **Get-AppxPackage**.

The following PowerShell commands uninstall Windows Metro applications related to Bing, Xbox, Zune, and SkyDrive. Additional Metro applications are removed by using the same command syntax and replacing the **-name** portion of the command with the name of the application you want to remove.

```
get-appxpackage -name Microsoft.Bing* | Remove-AppxPackage
get-appxpackage -name Microsoft.XBox* | Remove-AppxPackage
get-appxpackage -name Microsoft.Zune* | Remove-AppxPackage
get-appxpackage -name Microsoft.microsoftsky* | Remove-AppxPackage
```

**Manage processes with Process Explorer**

Another useful tool for managing services and processes is Windows Sysinternals Process Explorer. This tool provides an interface for viewing processes currently running on the desktop. Process Explorer is also a powerful troubleshooting tool for investigating performance issues, slow logon and logoff performance, and other related issues. Figure 5 shows the Process Explorer interface.
The Microsoft Technet blog post The Case of the Veeerrry Slow Logons (by Mark Russinovich) provides an example of how to use Process Explorer to solve logon issues. The Case of the Unexplained webcast series by Mark Russinovich provides further examples of using Sysinternals and other advanced tools.

Microsoft also offers the Sysinternals Live service, which enables you to run the Sysinternals tools directly from the Internet without searching for and manually downloading them. Enter the path of a Sysinternals Live tool in Windows Explorer or at 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.

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 10 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 that are normally masked from view, as shown in Figure 6.

A command line version, autorunsc, can be run for reporting.
Optimizing EUC desktop pools

Figure 6. Autoruns GUI

Change the Group Policy refresh interval

By default, all computers in a domain attempt to refresh their Group Policy settings every 90 minutes with a 30 minute offset. This policy is intended to limit the amount of network bandwidth that is consumed when refreshing Group Policy. By default, Group Policy is also updated at every startup of the OS.

To change the Group Policy refresh interval:

1. Edit the EUC_Desktops GPO.
3. When the Group Policy refresh interval for computers dialog box appears, click Enabled.
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 defragment

By default Windows is set to run a scheduled defragment every week. This is not desirable in an EUC environment.

To disable the scheduled defragment:

1. Open the properties for the C: drive.
2. Select the Tools tab.
3. Click Optimize to display the Optimize Drives dialog box.
4. Click Change settings.
5. Clear **Run on a schedule**.

The schedule defragment can also be disabled by executing the following command at an elevated command prompt:

```
SCHTASKS /Delete /TN "\Microsoft\Windows\Defrag\ScheduledDefrag" /F
```

**Disable startup graphic**

Windows draws an animation during the startup process. Users who are not connected to the console do not see the animation and it needlessly consumes resources.

To disable the startup animation:

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 wanted.

**Creating a default user profile**

**Overview**

This section describes the procedure to set up a default user profile for the golden or master image virtual machine. The process varies between versions of Windows. You may not be able to copy an altered profile, other than the default, to user profiles. Refer to the appropriate version of Windows documentation for more information.

The procedure to create a default user profile includes the following high-level steps:

1. Load the Windows System Image Manager.
2. Create an answer file.
3. Start the golden image machine in audit mode.
4. Customize the default user profile.
5. Copy the administrator profile to the default user.
6. Prepare the final image for deployment.

**Loading the Windows System Image Manager**

To create and manage an answer file, which is an XML-based file that contains setting definitions and values to use during Windows setup, install the Windows System Image Manager (WSIM) on a workstation. WSIM is part of the Windows Assessment and Deployment Kit (ADK) and is found by searching for “Windows ADK” at [http://www.microsoft.com/downloads/](http://www.microsoft.com/downloads/).

To load the Windows installation image structure into WSIM:

1. Copy the **sources** directory located on the root of a Windows installation DVD, or mounted ISO, to a writable location.
2. Open WSIM and under the **Windows Image** header, right-click and select **Select Windows Image**.
Creating a default user profile

3. In the open dialog box, browse to the sources directory you previously copied and select the install.wim file.

   If this is the first time you have used WSIM to load the installation image structure, you are prompted to create a catalog file.

4. If you are prompted to create a catalog file, select Yes.

The Windows installation image structure is now loaded into WSIM and the answer file can now be created.

Creating an answer file

   To create an answer file:

1. From WSIM, select File > New Answer File, and save the file as sysprep.xml.

2. Under the Windows Image header, expand Components, and find the name that is similar to x86.Microsoft-Windows-Shell-Setup_6.2.9200.16384_neutral.

   Note: If this is a 64-bit image, the key name will be prefixed with amd64 instead of x86.

3. Right-click the key and select Add Setting to Pass 4 specialize, as shown in Figure 7.

   Figure 7. Adding components to specialize pass

4. In the Answer File window, expand 4 specialize and select x86.Microsoft-Windows-Shell-Setup_neutral.

5. Change the CopyProfile option to true, as shown in Figure 8.
Creating a default user profile

**Figure 8. Setting CopyProfile to true**

6. Save the answer file
7. Copy the file to the golden image under `C:\Windows\system32\sysprep`.

**Note:** Many other options can be configured, but `CopyProfile` is the only option that is required to copy the administrator profile over the default user profile.

When a valid `sysprep.xml` file is present, the golden image machine must be booted into audit mode.

To start the machine in audit mode during an install of Windows:

1. Press `Ctrl+Shift+F3`.
2. When the **Welcome** screen appears, reboot the machine and put Windows in audit mode. If Windows has already been installed on a machine, invoke audit mode by running `C:\windows\system32\sysprep /audit`.

After the system restarts in audit mode, it automatically logs in with the local administrative user account.

You can now customize the administrator account.

**Note:** `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.

### Adjust for best performance

Some of the more advanced UI features, such as menu fading and animations, require extra CPU and memory resources.

To turn off these features:

1. Select **My Computer > Properties > Advanced > Performance**.
2. Select **Adjust for best performance**.
Creating a default user profile

**Disable the screen saver**

An EUC environment does not require the screen saver because users do not directly connect to the console of the virtual machine.

To disable the screen saver for all EUC users:

1. Edit the `EUC_Desktops` GPO.
2. Select `User Configuration > 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`.

**Copying the administrator profile to the default user**

After making all required changes under the local administrator account, you must rerun `sysprep` 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`, you can reseal the system by running:

```
C:\windows\system32\sysprep\sysprep.exe /generalize /oobe /shutdown /unattend:C:\windows\system32\sysprep\sysprep.xml
```

This command causes Windows to copy the administrator profile over the default user profile and then shut down. Any user logging in to the virtual machine inherits the changes made to the default user profile. You can also copy the default user profile to a network share.

**Preparing the final image for deployment**

Perform the following tasks to prepare the final image for deployment:

1. 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:
   a. Right-click the `C:\drive`.
   b. Select `Properties > General`.
   c. Click Disk Cleanup.
   d. Remove all files that do not need to be part of the master image.
2. Defragment the hard drive:
   a. Right-click the `C:` drive.
   b. Select `Properties > Tools`.
   c. Click `Optimize`.
The golden image should have its disk defragmented before being used for image deployment.

**Note:** Do *not* defragment deployed virtual desktops for the following reasons:

- To defragment a drive creates a large amount of disk I/O, which can result in performance issues with the shared storage.
- If the VHDs are thinly allocated, defragmenting the virtual-machine hard drive causes it to quickly expand in size. For example, running defragmentation on a virtual machine that is using only 600 MB of space after deployment can expand the drive to 4 GB or more.

3. Power off the desktop.

**Sizing memory for virtual machines**

The amount of RAM allocated to a virtual machine has a direct effect on a number of factors that affect both capacity and performance requirements for a virtual machine. This section briefly explains how to allocate RAM to Windows virtual machines. For simplicity, the calculations do not include memory overhead of the vSphere host.

This section also assumes that users have a good understanding of vSphere memory management technologies such as memory over-commitment, transparent page sharing (TPS), and vswap usage. For more information, see the *vSphere Resource Management Guide* on the [vSphere documentation page](https://www.vmware.com/support/pubs/vsphere_pubs.html).

As an advanced configuration consideration, if you do not over-commit memory, disable TPS to free up CPU cycles, which the virtual machines can use. You can disable TPS by setting `Mem.ShareScanGhz` to zero under the advanced settings for a vSphere host. This can provide a 5 percent performance boost to the virtual machines on the host.

The amount of RAM that is actively used by a virtual machine is referred to as the active working set. This usage is seen with the `%ACTV` counter in esxtop or the `Active` memory counter in vCenter under the Resource Allocation tab. If the maximum working set size is 1 GB (%ACTV == 50%) on a virtual machine with 2 GB of RAM, 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 vSphere host.

If the active working set for all virtual machines is less than the total available host memory on the vSphere server, then all the virtual machines will run at full speed. Each virtual machine can 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 vSphere host, the hypervisor is 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 pages to meet the memory demands placed on the vSphere host. This activity leads to poor performance of the virtual machine and should be avoided always.
Table 2 shows an example of a host with 32 GB of RAM that is hosting virtual machines, each of which is configured for 2 GB of RAM. Each virtual machine has on average 50 percent active memory.

<table>
<thead>
<tr>
<th>Virtual machine count</th>
<th>Active Memory in host</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>16 * 2 GB * 50% = 16 GB</td>
<td>Without memory over-commit, only 50% of the host memory is actively in use.</td>
</tr>
<tr>
<td>32</td>
<td>32 * 2 GB * 50% = 32 GB</td>
<td>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.</td>
</tr>
<tr>
<td>48</td>
<td>48 * 2 GB * 50% = 48 GB, limited to 32 GB by host</td>
<td>These virtual machines want 48 GB of RAM but are limited to the 32 GB that is installed on the host. vSphere must swap to allow these machines to run, and performance will be degraded.</td>
</tr>
</tbody>
</table>

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

### Assigning RAM to virtual machines

Choosing the appropriate RAM size for the golden-image virtual machine ensures that the virtual machines can 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 the guest OS does not have enough available RAM. It also avoids vSphere having to swap because it cannot reclaim memory from active guests fast enough when experiencing significant memory demand.

To determine how much RAM to allocate to the golden-image virtual machine, place the guest OS under load. With the peak load running on the virtual machine, measure the amount of active memory. This is called the active working set size.

Several methods exist for measuring the active working set size. In esxtop, review the %ACTV memory counter. This counter displays the active working set size as a percentage of allocated memory. If this value never approaches 100 percent, the virtual machine is not actively using all RAM allocated to it.

In VMware vCenter, the active working set size is reported as Active under the Guest Memory section on the Resource Allocation tab. Alternatively, for a more accurate measurement, launch VM Statistics Logging on the virtual machine and observe the Memory Active counter under VM Memory.

For the best balance between performance and memory utilization, allocate at least 25 percent more RAM to the virtual machine than the maximum active load observed. Doing so avoids having Windows write data to its page file, which 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, the virtual machine should have at least 750 MB of RAM allocated. The maximum number of virtual machines to be loaded on the host can be calculated by dividing the maximum amount of vSphere host memory by the maximum active memory of the golden-image virtual machine. In this example, the calculation 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 vSphere memory overhead.

At startup, Windows zeros out its memory space, which causes the %ACTV memory to briefly run up to 100 percent. This can lead to periods of vswap usage if multiple virtual machines are restarted in concert, as could happen if a vSphere host fails or when vSphere High Availability is enabled for the cluster.
References

The following documentation on [EMC.com](https://www.emc.com) or [EMC Online Support](https://www.emc.com/support) provides additional and relevant information. Access to documents depends on your login credentials. If you do not have access to a document, contact your EMC representative.

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

VMware documentation

The following documentation on the [VMware website](https://www.vmware.com) provides additional and relevant information:

- *Storage Considerations for VMware View*
- *Server and Storage Sizing Guide for Windows 7 Desktops in a Virtual Desktop Infrastructure*
- *vSphere Resource Management Guide*

Microsoft documentation

The following documentation on the [Microsoft TechNet website](https://technet.microsoft.com) provides additional and relevant information:

- *Pushing the Limits of Windows: Virtual Memory*
- *The Case of the Unexplained*
- *The Case of the Veeerrry Slow Logons*

Other documentation

The following additional third-party documents provide useful information:

- *Misunderstanding Memory Management*
- *Windows Service Configuration Information*
- *Black Viper's Windows 10 Service Configurations*