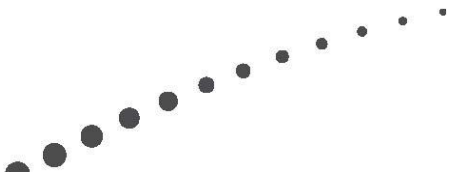


Windows 2008 R2 Optimization Guide

For Desktop Virtualization with XenApp 6 / 6.5



Contents

Overview 3

Windows 2008 R2 Configuration 4

User Settings 19

Revision History 23

Overview

When considering desktop virtualization with Citrix FlexCast technologies, one method for delivering services to end-users is through the use of hosted shared desktops using Citrix XenApp. Hosted shared desktops can deliver a locked down, streamlined and standardized environment ideally suited for task workers where personalization is not required. Delivering hosted shared virtual desktop requires proper planning and configuration to maximize the scalability of server resources while providing users with an optimized and functional desktop environment. This document outlines optimizations for XenApp 6 on Windows Server 2008 R2 to meet these goals.

These configurations typically add value by enhancing the user experience and increasing system performance. For example, some of the changes optimize the user experience by enabling faster logons, reducing unnecessary prompts, and quicker screen updates. Others optimize performance and increase scalability by reducing unnecessary processor, memory, disk and network usage.

However, certain modifications allow for greater scalability but at the cost of the user experience. As many organizations will demand a user experience similar to the traditional desktop, care must be taken when applying optimization settings. Many of these settings are identified within the remainder of the document.

A note on Registry Settings:

Many of the configurations recommended in this document are changes to the registry. Registry changes can be implemented in a number of ways and there is not necessarily one way that is best for all deployments. The simplest way to implement many of these is to modify the registry manually using "regedit.exe" or creating and executing a ".REG" file. Automated ways of modifying the registry, including Group Policy or other third-party tools, are also possible. All registry modifications listed in this document use the ".REG" file syntax so that they can be easily copied and pasted into a customized ".REG" file.

Caution*: All of the registry settings mentioned in this document must be analyzed for benefit and risk to your environment. Modifying the registry incorrectly can cause serious problems that may require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrectly modifying the registry can be solved. Modify the registry at your own risk. Backup the registry or disk image before making changes.*

Windows 2008 R2 Configuration

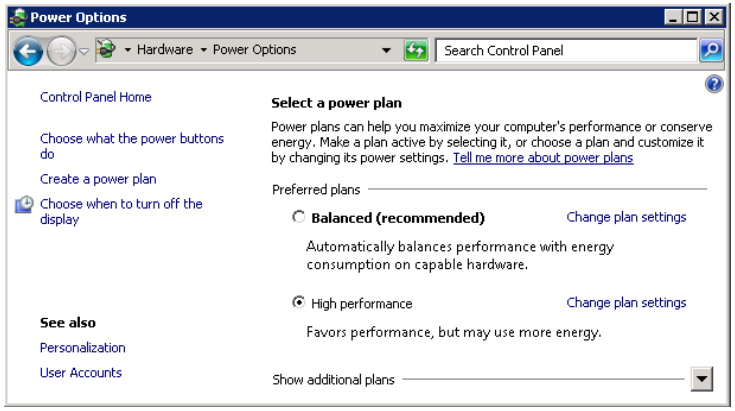
General

The following items, which are configurable by means of Group Policies, are recommended for all deployment scenarios and would almost always be desirable in a XenApp hosted shared desktop implementation:

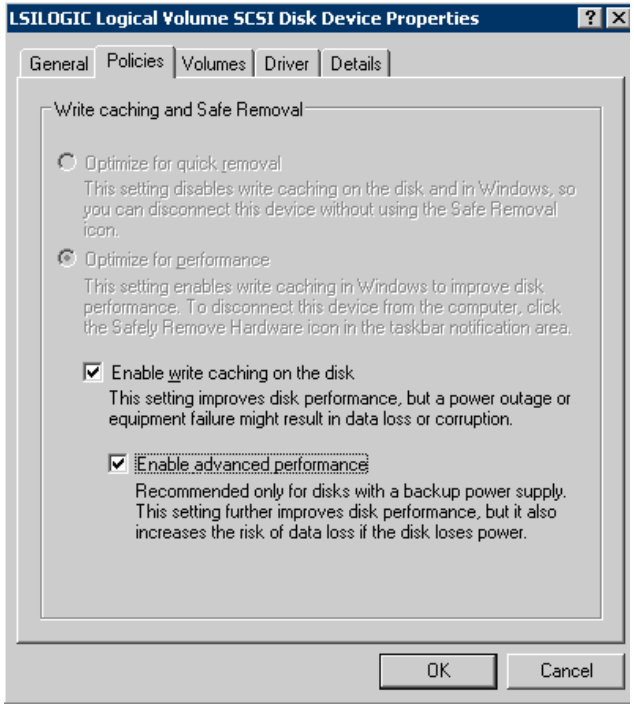
Item	Path (Computer Configuration)	Justification
Error Reporting	Administrative Templates – Windows Components – Windows Error Reporting Disable Windows Error Reporting: Enabled	Generates application crash dumps to be sent to Microsoft. Should be safe to disable unless troubleshooting application.
Disable Customer Experience Improvement Program (CEIP)	Administrative Templates – System – Internet Communication Management – Internet Communication Settings Turn off Windows Customer Experience Improvement Program: Enabled	Minimize background traffic by opting out of diagnostics feedback programs.
Windows Update	Administrative Templates – Windows Components – Windows Updates Configure Automatic Updates: Disabled	Windows updates should only be done on the base desktop image and not by users.
System Restore	Administrative templates – System – System Restore Turn off System Restore: Enabled	Not needed due to the nature of desktop virtualization and single image management.
RDP Listener – Printer mapping	Disable printer mapping for RDP sessions. Administrative Templates – Windows Components – Remote Desktop Services – Remote Desktop Session Host – Printer Redirection Do not allow client printer redirection: Enabled	Mapping printers in administrative RDP sessions can cause printer drivers to be installed. This can cause heterogeneous server configurations and increase complexity for troubleshooting.

The following registry changes and manual configurations are recommended for all deployment scenarios and would almost always be desirable in a XenApp hosted shared desktop implementation:
Note: Windows Group Policy Preferences are a very elegant way of applying registry changes.

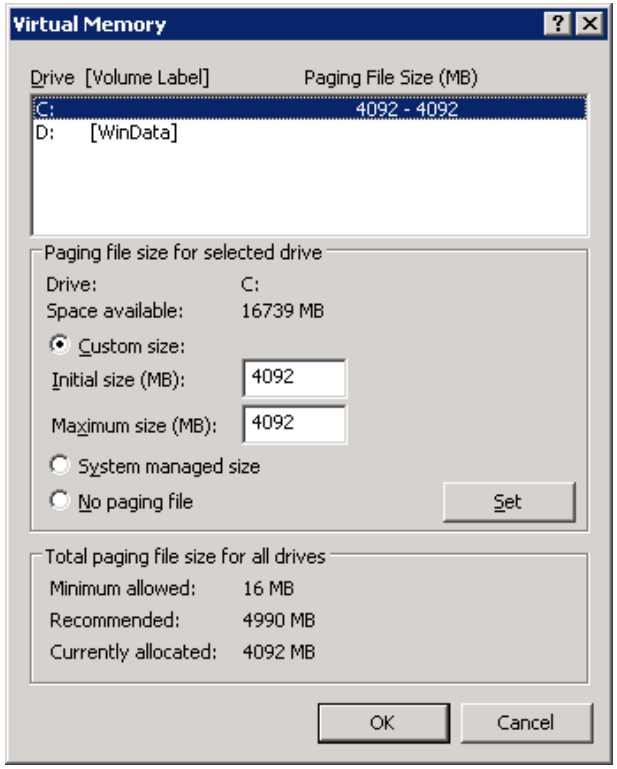
Configuration	Optimizer*	Recommendation / Registry Key	Justification
Hide System Hard Error Messages	No	HKLM\System\CurrentControlSet\Control\Windows "ErrorMode"=dword:00000002	When Windows or an application generates a hard error message, a dialog with the error usually appears with an "OK" or "Continue" button. These messages are usually cryptic for the end user and they can cause a session to hang if the user gets disconnected, but there is an error awaiting response. The system can be configured to suppress these messages by writing them to the Event Log and automatically selecting "OK" for the user.
Spooler Warning Events	No	HKLM\System\CurrentControlSet\Control\Print\Providers "EventLog"=dword:00000001	The Spooler service can quickly fill up the System Event Log with useless warning events. These happen whenever an ICA Auto Created Printer is created or deleted, which can generate thousands of events per day. The Spooler should be configured to write only errors.
Paging of the Executive	No	HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management "DisablePagingExecutive"=dword:00000001	In order to increase performance, kernel mode drivers and other system components can be configured to that they are not paged to disk.

Edit Run and RunOnce Registry keys	No	HKLM\Software\Microsoft\Windows\CurrentVersion\Run HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce	The Run and RunOnce registry keys define programs that run in each users' context at login. In a multi-user system, these can contribute significantly to processor utilization and therefore reduce scalability. It is recommended that any programs that can run once within a system context, such as Java scheduler and antivirus modules, be removed from these keys.
Windows Power Plans	No	High Performance Power Plan 	Processors are always locked at the highest performance state.
BIOS Power Schemes	No	Choose maximum performance scheme when possible.	Recent server hardware often includes BIOS level power savings settings, which can cause the CPUs of a server to be clocked with a frequency lower than maximum. It is recommended to select the maximum performance scheme for Citrix related servers.

Scheduled Tasks	No	Verify the scheduled tasks and randomize execution time. Typically the following scheduled tasks can be disabled: • Application Experience → AitAgent • Application Experience → ProgramDataUpdater • Autochk → Proxy • Customer Experience Improvement Program → everything under this node (Consolidator, KernelCeipTask, UsbCeip, ServerCeipAssistant, ServerRoleCollector, ServerRoleUsageCollector) • DiskDiagnostic → Microsoft-Windows-DiskDiagnosticDataCollector • Power Efficiency Diagnostics → AnalyzeSystem • Server Manager → ServerManager • Windows Error Reporting → QueueReporting	Scheduled tasks should be used carefully only and the execution time should be randomized, to prevent any negative impact on central infrastructures such as storage or database systems.
Disable Logon Screensaver	No	HKEY_USERS\.DEFAULT\Control Panel\Desktop "ScreenSaveActive"="0"	Prevents a screensaver to be shown at the server console, which can improve performance.
Disabled Boot Animation	No	Disable bcdedit /set bootux disabled (need to be run from the Windows Command Prompt)	Disabling the animation, which no user will see, saves resources plus speeds up the entire boot process. **Note:** Disabling the boot animation disables all UI feedback until the Windows logon screen appears. This behavior can increase to complexity for troubleshooting.
Disable all application auto-updates	No	Java updates can be controlled via the Control Panel. SAP updates are disabled in the CCS ADM(X) template.	Auto-updates should be managed to prevent changes being made to the environment by end users.

Defragmentation	No	Run defragmentation	Disk defragmentation should be done before capturing the desktop image (in case Provisioning Services is used) or at regular intervals to ensure the disk is optimized. When a scheduled defragmentation is used, ensure that the schedule does not conflict with business times (default every Wednesday at 1am).
Antivirus	No	Optimize	Follow the Best Practices as outlined here.
Write Cache (Operating System)	No	Device Manager → Disk Drive Properties → Policies tab  Additional settings:	For hardware on which write cache is unavailable, Windows write back caching can be enabled through Device Manager on the properties of the drive. RegistryLazyFlushInterval should also be configured especially if no hardware write cache is available.

		HKLM\System\CurrentControlSet\Control\Session Manager\Configuration Manager\ "RegistryLazyFlushInterval"=dword:00000060 (dec)	
Write Cache (Hardware)	Hardware drive controllers can store device writes and reads in a cache so that the data can be written or read in an optimal fashion. When enabled, the controller immediately informs the operating system that data has been written or read, allowing it to continue normal operation. Citrix Consulting recommends configuring hardware based write caching to 100% write.		
Worker Threads	No	HKLM\System\CurrentControlSet\Control\Session Manager\Executive\ "AdditionalCriticalWorkerThreads"=dword:00000064 (dec)	This value affects the number of threads that the file system cache uses for read-ahead and write-behind requests. Raising this value can allow for more queued I/O in the storage subsystem and can improve I/O performance, particularly on systems with many processors and powerful storage hardware
8.3 Name Creation	No	HKLM\System\CurrentControlSet\Control\FileSystem\ "NTFSDisable8dot3NameCreation"=dword:00000001	The default is 0. This parameter determines whether NTFS generates a short name in the 8.3 (MS DOS®) naming convention for long file names and for file names that contain characters from the extended character set. If the value of this entry is 0, files can have two names: the name that the user specifies and the short name that NTFS generates. If the user-specified name follows the 8.3 naming convention, NTFS does not generate a short name.

			Changing this value does not change the contents of a file, but it avoids the short-name attribute creation for the file, which also changes how NTFS displays and manages the file.
Page File	No	My Computer properties → Advanced → Performance Settings → Advanced tab → Change Virtual Memory 	The page file is a physical file on the disk where virtual memory can be stored. This allows the system to allocate and commit more virtual memory than there is physical memory. The page file should be optimized as follows: Have the same min-max size to minimize fragmentation. **Note:** Further information about determining the appropriate size of the page file, can be found here.

SMB 1.0 Client Optimization **Note:** Tuning SMB 1.0 is required in mixed (2003 / 2008 R2) environments, where SMB 2.0 cannot be used.	No	HKLM\SYSTEM\CurrentControlSet\Services\Lanman workstation\Parameters "MaxCmds"=dword:00002048 (dec) HKLM\SYSTEM\CurrentControlSet\Services\MRxSmb \Parameters "MultiUserEnabled"=dword:00000001 HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies\Explorer NoRemoteRecursiveEvents"=dword:00000001 HKLM\SYSTEM\CurrentControlSet\Services\ Lanmanserver\Parameters "MaxWorkItems"=dword:00008192 (dec) "MaxMpxCt"=dword:00002048 (dec) "MaxRawWorkItems"=dword:00000512 (dec) "MaxFreeConnections"=dword:00000100 (dec) "MinFreeConnections"=dword:00000032 (dec)	File Sharing in a Microsoft Environment is based on an application protocol called Server Message Block (SMB). When a device connects to a Microsoft file share on another computer it is acting as an SMB client. By default the SMB 1.0 Client network redirector can have only 50 outstanding SMB requests/commands open to a single file server. This is controlled by the MaxCmds registry value. All connections to remote servers are per computer not per user. This means all users on a Terminal Server open files over the same SMB session. A single SMB Client Session can only have 16383 open files. This is controlled by the MultiUserEnabled registry value. When you map a drive to a UNC path and have Windows Explorer open to the network drive, Explorer submits an always open SMB command to request notification when a file changes anywhere on the network drive. These are called SMB Change Notify events. In order to reduce network traffic, resource utilization and SMB commands and to overcome a

			potential screen flicker issue for certain file sharing scenarios, the policy for NoRemoteRecursiveEvents should be enabled. This Prevents change notifications from being sent for anything other than the root folder. **Note:** Further information can be found within this blog.
SMB 2.x Client Tuning	No	HKLM\System\CurrentControlSet\Services\ LanmanWorkstation\Parameters "DisableBandwidthThrottling"=dword:00000001 "DisableLargeMtu"=dword:00000000 HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies\Explorer NoRemoteRecursiveEvents"=dword:00000001	By default, the SMB redirector throttles throughput across high-latency network connections in some cases to avoid network-related timeouts. Setting the DisableBandwidthThrottling registry value to 1 disables this throttling, enabling higher file transfer throughput over high-latency network connections. By default, the SMB redirector does not transfer payloads larger than approximately 64 KB per request. Setting the DisableLargeMtu registry value to 0 enables larger request sizes, which can improve file transfer speed. **Note:** Further information can be found within this blog.

***Note:** The Optimizer column indicates whether this registry change is included in the XenConvert Optimizer tool that is installed with the Provisioning Services target device software.*

Provisioning Services based servers

The next set of registry changes are recommended for images deployed using standard mode vDisk images with Citrix Provisioning services. Standard mode images are unique in that they are restored to the original state at each reboot, deleting any newly written or modified data. In this scenario, certain processes are no longer efficient. These configurations may also apply when deploying persistent images and in many cases should be implemented in addition to the changes recommended in the preceding section.

Configuration	Optimizer*	Recommendation / Registry Key	Justification
Disable Clear Page File at Shutdown	Yes	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management] "ClearPageFileAtShutdown"=dword:00000000	Clearing the Windows Pagefile at shutdown can delay the shutdown procedure and therefore increase the time required for a complete reboot cycle.
Disable Offline Files	Yes	HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\NetCache "Enabled"=dword:00000000	The offline file feature is not required for XenApp scenarios.
Disable Background Defragmentation	Yes	HKLM\SOFTWARE\Microsoft\Dfrg\ BootOptimizeFunction "Enable"="N"	Defragmentation is not necessary for Provisioning Services vDisks.
Disable Background Layout Service	Yes	HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\OptimalLayout "EnableAutoLayout"=dword:00000000	The Layout Service is responsible for rearranging files on the hard drive to increase performance. This does not apply to Provisioning Services vDisks.
Disable Hibernation	Yes	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Power "Heuristics"=hex:05,00,00,00,00,01,00,00,00,00,00,00,00,00,00,00,00,3f,42,0f,00	Hibernation is not required for XenApp scenarios.
Disable Mach. Acct. Password Changes	Yes	HKLM\SYSTEM\CurrentControlSet\Services\Netlogon \Parameters "DisablePasswordChange"=dword:00000001	Disabling the automatic machine account password change is required for the Active Directory integration of Provisioning Services Target Devices.

Redirect Event Logs	No	HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application "File"="D:\EventLogs\Application.evtx" HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security "File"="D:\EventLogs\Security.evtx" HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\System "File"="D:\EventLogs\System.evtx"	Redirecting Windows Eventlogs to a persistent drive (such as D:\) eases troubleshooting and satisfies certain security monitoring requirements.
Disable Large Send Offload	No	HKLM\SYSTEM\CurrentControlSet\Services\BNNS\Parameters "EnableOffload"=dword:00000000	Disabling Large Send Offloads is required for Provisioning Services vDisk streaming.
Disable TCP/IP Offload	No	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters "DisableTaskOffload"=dword:00000001	Disabling TCP/IP Offloads is required for Provisioning Services vDisk streaming.
Increase Service Startup Timeout	No	HKLM\SYSTEM\CurrentControlSet\Control "ServicesPipeTimeout"=dword:00060000(dec)	In certain peak load scenarios Windows services might take longer than 30 seconds to start. This setting increases the timeout value to 10 minutes.
Scheduled Defrag	No	Disable the scheduled defragmentation of the hard disks. Task Scheduler - Defrag → ScheduledDefrag	Defragmenting the vDisks from a standard target device is not possible (disk is mapped read only), but can significantly increase to load on the PVS Server as well as the write cache.

***Note:** The Optimizer column indicates whether this registry change is included in the XenConvert Optimizer tool that is installed with the Provisioning Services target device software.*

Services

Windows Server 2008 R2 includes a set of services, many of which are enabled as default. When using the system as Citrix XenApp server, some of these services provide little value increases but significantly increase the memory footprint of the OS. Therefore the following services could potentially be disabled.

Service	Recommendation	Justification
Desktop Windows Manager Session Manager	Potential	This service is responsible for Windows 7 Aero theme. Organizations need to determine if Aero theme is something they wish to support at a later date.
Multimedia Class Scheduler	Disable	Not required for XenApp use cases.
Network List Service	Disable	The network location of a XenApp Server is unlikely to change over time. Thus automatic network location detection is not required.
Network Location Awareness	Disable	
Themes	Potential	Allows users to manage the themes, which includes backgrounds, sounds and visual effects. Although this service does take resources and will impact overall scalability, each organization needs to determine if this functionality should be supported. It does allow the user to better personalize the environment and helps improve acceptance.
Windows Defender	Disable	Most enterprise deployments will have their own anti-malware solutions. As the corporate version will most likely be used, the integrated service should be disabled.

Windows Update	Potential	For XenApp servers based on a Provisioning Services vDisk or in case an Enterprise Software Deployment Systems is used to deploy Windows hotfixes, the Windows Update Service is not required.

File Servers

The following registry changes are recommended for all Windows File Server deployment scenarios in order to enable the XenApp Server side SMB tuning parameters:

Configuration	Recommendation / Registry Key	Justification
SMB 1.0 Tuning **Note:** Tuning SMB 1.0 is required in mixed (2003 / 2008 R2) environments, where SMB 2.0 cannot be used.	HKLM\SYSTEM\CurrentControlSet\Services\ Lanmanserver\Parameters "MaxWorkItems"=dword:00008192 (dec) "MaxMpxCt"=dword:00002048 (dec) "MaxRawWorkItems"=dword:00000512 (dec) "MaxFreeConnections"=dword:00000100 (dec) "MinFreeConnections"=dword:00000032 (dec)	File Sharing in a Microsoft Environment is based on an application protocol called Server Message Block (SMB). When a device connects to a Microsoft file share on another computer it is acting as an SMB client. The SMB client interacts with the network redirector, which is responsible for sending file requests to the proper location (local file system, CIFS/SMB, Netware, CDM, etc…). The client sends SMB commands to the server for execution. These commands include requests to read, write or delete files and folders as well as commands to list directories and subscribe to change events (such as when someone else creates a new file and it automatically appears in your Explorer window). By default the SMB or CIFS service on the file server only allows 50 outstanding SMB requests/commands open from a single client at any given time. This is controlled by the MaxMpxCt registry value (by default, does not exist).

SMB 2.x Tuning	HKLM\System\CurrentControlSet\Services\ LanmanServer\Parameters "TreatHostAsStableStorage"=dword:00000001 "MaxThreadsPerQueue"=dword:00000064 (dec) HKLM\System\CurrentControlSet\Control\Session Manager\Executive "AdditionalCiticalWorkerThreads"=dword:00000064 (dec)	The "TreatHostAsStableStorage" key controls the processing of write flush commands from clients. Disabling this functionality can improve client responsiveness. The "MaxThreadsPerQueue" and "AdditionalCiticalWorkerThreads" keys control the number of threads allocated to file I/O requests. These are the values recommended by Microsoft for file servers with sufficient processing capabilities. Refer to http://download.microsoft.com/download/3/2/A/32A70368-1457-4972-8CDD-08A496198361/Perf-tun-srv-R2.docx for additional information.

User Settings

Unlike machine settings, user settings must be applied to each user and typically cannot be applied as part of the base image. In addition, user settings typically do not depend on whether the image is deployed in private or standard mode; however, the method in which the settings should be applied can be influenced by the image mode. None of the configurations in this section are included in the XenConvert Optimizer tool. These factors make user settings more difficult to implement.

As a recommended approach for the application of the user settings is to utilize group policy settings and/or preferences, as they provide administrators a central site for configuration and allow for greater customization based on the desktop.

Recommended Configurations – Windows specific

The following registry changes and Group Policy based modifications should be evaluated for all deployment scenarios and would almost always be desirable in a XenApp hosted shared desktop implementation. As some of the settings will significantly impact the personalization capabilities for users it is highly recommended to perform user acceptance testing (in addition of general functionality testing) prior to production rollout.
Note: Windows Group Policy Preferences are a very elegant way of applying registry changes.

Configuration	Optimizer*	Recommendation	Justification
Internet Explorer – Force Offscreen Composition	No	HKEY_CURRENT_USER\Software\Microsoft\ Internet Explorer\Main "Force Offscreen Composition"=dword:00000001	Overcomes a potential screen flicker issue for certain websites. **Note:** This setting applies to IE8 and earlier only.
Disable Recycle Bin	No	User Configuration - Administrative Templates – Windows Components – Windows Explorer Do not move deleted files to the Recycle Bin: Enabled	As the Recycle Bin is part of the user profile in Windows 2008 R2 it should be disabled in roaming profile scenarios, to prevent profile bloat.
Reduce Menu Show Delay	No	HKEY_CURRENT_USER\Control Panel\Desktop "MenuShowDelay"="150"	Reduces the delay Windows sets for menus. Provides better user experience.

Disable all Visual Effects except "Use common tasks in folders" and "Use visual styles on windows and buttons"	No	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\VisualEffects "VisualFXSetting"=dword:00000003 HKEY_CURRENT_USER\Control Panel\Desktop\WindowMetrics "MinAnimate"="0" HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced "ListviewAlphaSelect"=dword:00000000 "TaskbarAnimations"=dword:00000000 "ListviewWatermark"=dword:00000000 "ListviewShadow"=dword:00000000 HKEY_CURRENT_USER\Control Panel\Desktop "FontSmoothing"="0" "UserPreferencesMask"=binary:90,12,01,80 ,10,00,00,00	Provides a better user experience. Note: The UserPreferenceMask changes based on the settings selected in the System Properties – Performance Options configuration page.
Disable Screen Saver	No	User Configuration - Administrative Templates – Control Panel – Personalization Enable Screen Saver: Disable	Running a server side screen saver consumes resources on the XenApp servers. In case a screen saver is required, running it locally on the end point device would be a better option.
Documents History	No	User Configuration - Administrative Templates – Start Menu and Taskbar Do not keep history of recently opened documents: Enable Remove Balloon Tips on Start Menu items: Enable Remove frequent program list from Start Menu: Enable	Minimize the effect on CPU usage when you are running many XenApp sessions and to improve user logon times.

Auto End Tasks	No	HKCU\Control Panel\Desktop "AutoEndTasks"=REG_SZ = "1" "WaittoKillAppTimeout"=REG_SZ= "20000"	Sometimes an application will hang or become unresponsive. This often happens when closing applications or logging off. The system will often present a dialog that asks the user to "Wait" or "End Task." This dialog can be suppressed and the "End Task" automatically selected for the user.
Background Spell Checking	No	Disable using Group Policy	Background spell and grammar checking can cause significant CPU load.
Sound Scheme	No	Disable Windows Logon / Logoff notification sounds HKCU\AppEvents\Schemes\Apps\.Default\WindowsLogon\.Current "(Default)"=REG_SZ="" HKCU\AppEvents\Schemes\Apps\.Default\WindowsLogoff\.Current "(Default)"=REG_SZ=""	Playing a sound notification upon every logon/logoff increases the bandwidth consumption and can also increase the logon/logoff times. **Note:** It might be desirable to disable further sounds.

Recommended Configurations – XenApp specific

The following performance related XenApp specific Group Policy based modifications should be evaluated for all deployment scenarios and would almost always be desirable in a XenApp hosted shared desktop implementation:

Category (within the XenApp Policy)	Setting	Justification
Desktop UI	Desktop Wallpaper: Prohibited Menu animation: Prohibited View window content while dragging: Prohibited	By prohibiting these settings the server memory footprint as well as the network bandwidth utilization per user session will be decreased.
Visual Display\Moving Images	Progressive compression level: Low (min. setting)	By enabling the progressive display compressing the network bandwidth utilization per user is decreased significantly.
Printing\Drivers	Automatic Installation of in-box drivers: Disabled	Although this setting is not performance related, it is highly recommended, as it prevent Windows from installing Printer Drivers on demand. This can cause printing related functionality and stability issues as well as complicate the troubleshooting.

Revision History

Revision	Change Description	Updated By	Date
1.0	Document created	Andy Baker – Architect Brendan Lin – Architect Daniel Feller – Lead Architect Rich Meesters – Architect Thomas Berger – Architect	December 02, 2011
1.1	Document updated	Thomas Berger – Architect	December 12, 2011

About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is a leading provider of virtual computing solutions that help companies deliver IT as an on-demand service. Founded in 1989, Citrix combines virtualization, networking, and cloud computing technologies into a full portfolio of products that enable virtual work styles for users and virtual datacenters for IT. More than 230,000 organizations worldwide rely on Citrix to help them build simpler and more cost-effective IT environments. Citrix partners with over 10,000 companies in more than 100 countries. Annual revenue in 2010 was $1.87 billion.

©2011 Citrix Systems, Inc. All rights reserved. Citrix®, Access Gateway™, Branch Repeater™, Citrix Repeater™, HDX™, XenServer™, XenApp™, XenDesktop™ and Citrix Delivery Center™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.