

Windows 8/8.1 Virtual Desktop Optimization Guide

Prepared by:
Worldwide Consulting
Desktops and Apps Group



TABLE OF CONTENTS

Overview	3
Registry-Based Optimizations	3
Optimization Testing.....	4
Processor.....	5
Memory	5
Disk.....	6
Network	6
Optimizations.....	7
Image Preparation	7
Runtime Optimizations	8
Services	12
Scheduled Tasks	16
General Recommendations	18
System Performance.....	20
User Experience	21
Application Optimizations	22
Revision History	23
Contributors	23
Feedback.....	23

Overview

As organizations start to migrate to Windows 8 / 8.1, it is expected many will leverage desktop virtualization to simplify and streamline the migration and ongoing maintenance process. Delivering a Windows 8 / 8.1 system as a virtual desktop requires proper planning and configuration to provide the users with an optimized and functional desktop environment. The Windows 8 / 8.1 optimizations identified within this document are intended to provide a leaner and more responsive desktop for users.

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 fast logons, reducing unnecessary prompts, and smoother screen updates. Others optimize performance and increase scalability by reducing unnecessary processor, memory, disk and network usage. However, certain optimizations 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.

Note: *It is important that optimizations are thoroughly tested prior to being implemented in production. Most software vendors perform their testing using default rather than optimized desktops.*

Registry-Based Optimizations

Many of the optimizations within this document require updates to be made to the computer or user portions of the registry. There are several techniques that can be used to apply these optimizations including updates to the default user hive, regedit, scripts, Group Policy Preference and third-party tools.

The preferred option is to use Group Policy Preference so that registry-based optimizations can be applied without updating the master image or having to run a script each time a computer starts or a user logs on. For more information on Group Policy Preference, please refer to the Microsoft TechNet article – [Configure a Registry Item](#).

Caution: *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.*

Optimization Testing

A XenDesktop 7.1 environment was built to determine the performance gains that these settings can help achieve. A baseline was established by testing a Windows 8.1 x64 image with the optimizations that are included in the XenDesktop VDA installation by default (many of which are noted in this document). Additional tests were then performed with the recommendations in this document applied. Metrics were captured using Microsoft Performance Monitor.

Note: Not all of the effects of the optimizations in this guide could be captured due to the nature of the testing. These include boot time optimizations and the effects of anti-virus exclusions. Results may vary depending on your environment and image delivery solution.

The table below summarizes the base hardware and machine resources used in testing the optimizations in this guide as well as the baseline desktop performance.

Test Environment	
Model	HP BL460c Gen8
Processor	16 Core Intel Xeon @ 2.60 GHz
Memory	192 GB
Storage	EMC VNX5500 Storage Array
Hypervisor	Hyper-V 3 on Server 2012 R2
Number of desktops per test run	80
vCPU per desktop	2
Memory assigned per desktop	2GB (Static)
Delivery method	Provisioning Services 7.1

Table 1 Test Environment

The table below summarizes the performance gains achieved from applying the optimizations documented within this guide. The testing was done using leveraging the LoginVSI 4.0 Medium workload. For official documentation on LoginVSI, please refer to their [website](#).

Metric	Default Average	Optimized Average	% Improvement
Hypervisor % Total Runtime	55%	42%	24%
Hypervisor Context Switches	201,000	177,000	12%
Disk Mbytes Total/Sec	9.6	8.4	13%
Disk Transfers/Sec	634	595	6%
VM Available Memory (MB)	458	644	40%
Guest Machine Network Traffic (Mbps)	120	92	23%

Table 2 Performance Metrics

Processor

The graphic below shows that the CPU utilization was substantially lower for the optimized tests throughout the entire Login VSI Medium workload. This is consistent throughout the login process and remains during steady-state processing.

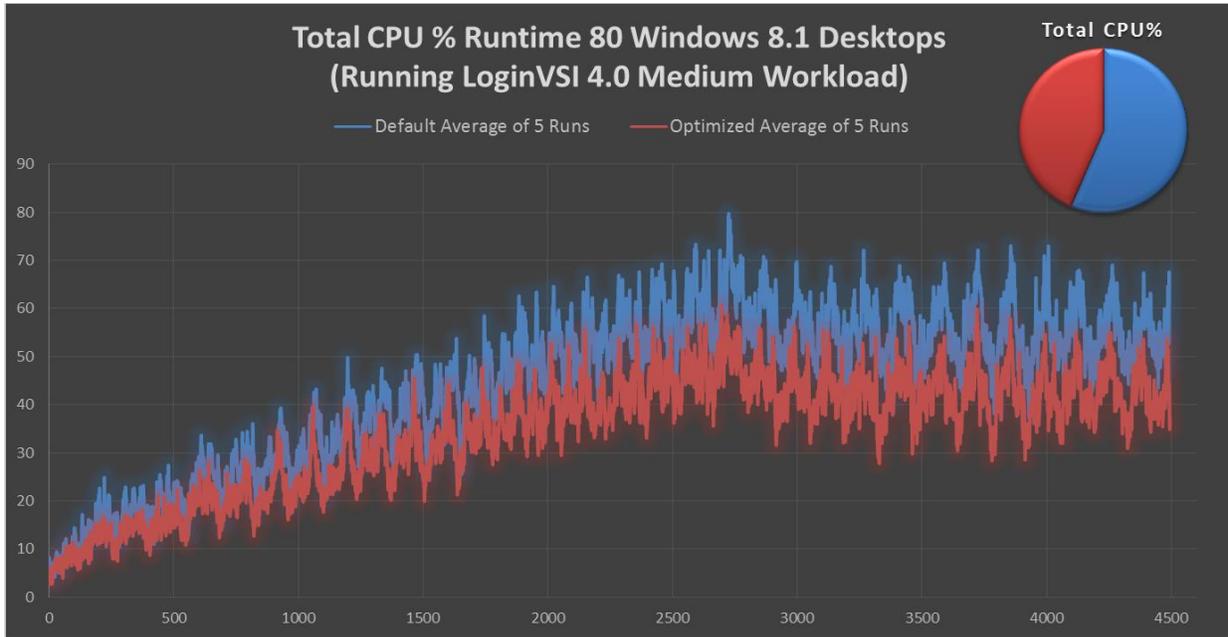


Figure 1 Total CPU % Runtime on the Hyper-V Host

Memory

The graphic below shows a comparison of available memory consistent with all the virtual desktops tested. Each machine was given 2GB of statically allocated memory. As can be seen below the Optimized desktop had almost 200MB of additional memory through the entire LoginVSI 4.0 Medium workload.

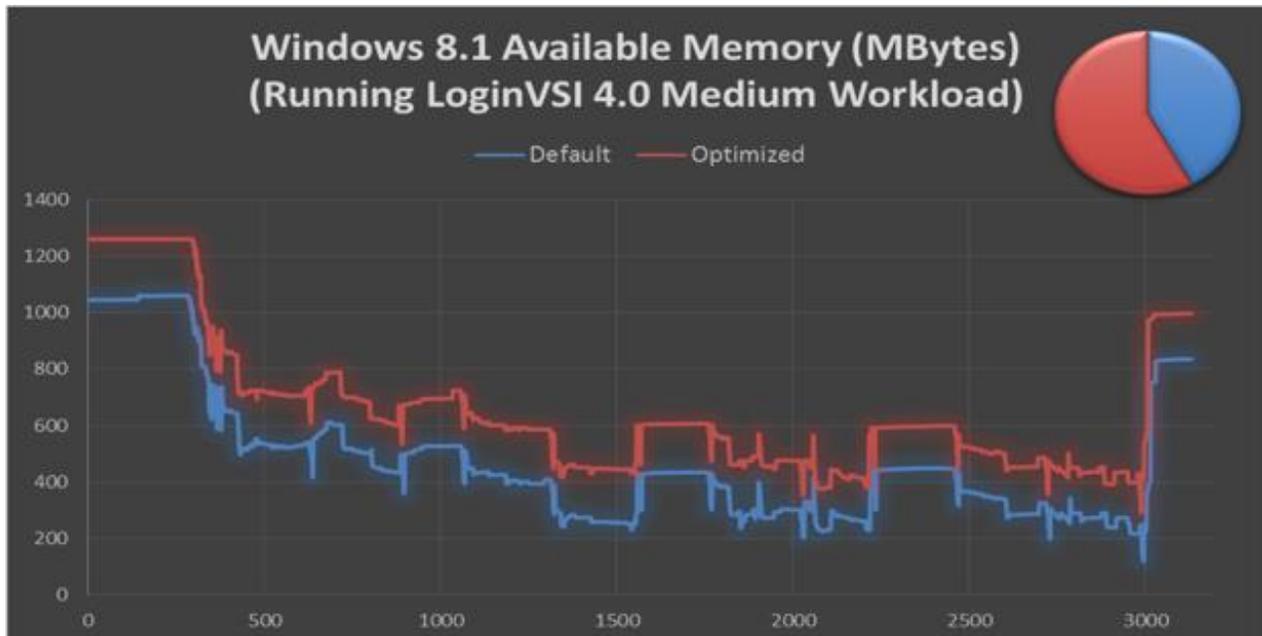


Figure 2 Available memory on the Windows 8.1 Desktop

Disk

Below is a graphic showing the total disk Mbytes/sec on the Provisioning Services write cache storage hosted in an EMC storage array. The test runs using the optimized image consistently stressed the storage less than the test runs using the default image. Note that in the image below the majority (>90%) of the disk operations were write operations. This is typical in a Provisioning Services deployment.

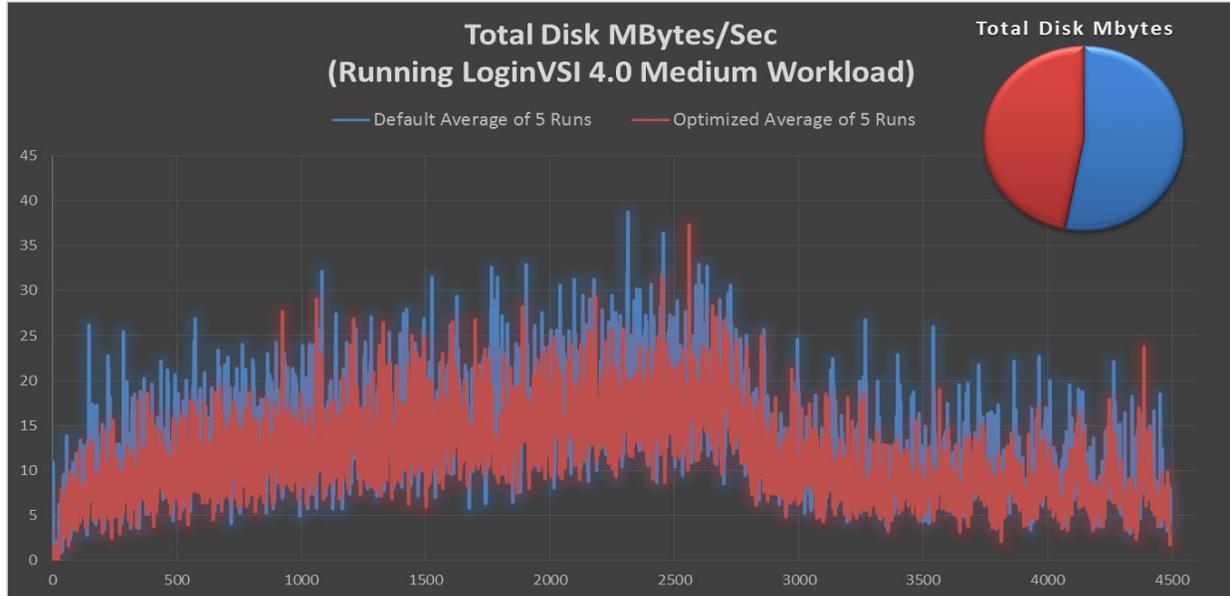


Figure 3 Total Disk MBytes/Sec on the write cache storage

Network

The network traffic pictured below is the total traffic to and from the desktops. It includes the streaming traffic of the vDisk through Provisioning Services as well as the video streaming throughout the workload. As can be seen below, the network traffic is consistently lower for the test runs using the optimized image.

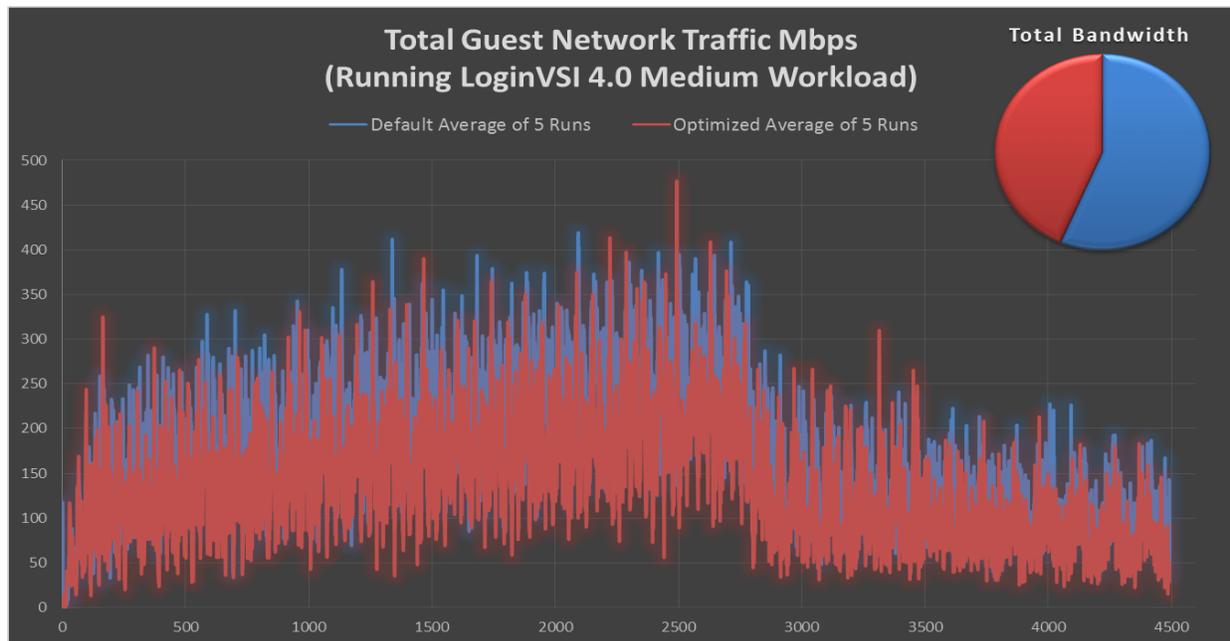


Figure 4 Total guest network traffic for 80 Windows 8.1 desktops

Optimizations

Image Preparation

The following tasks should be performed for each Machine Creation Services or Provisioning Services master image. If no desktop provisioning technology is used, these tasks should be performed on all virtual desktops.

Item	Configuration / Registry Key	Description/Justification
During initial installation		
Prevent creation of BitLocker drive (350MB) (Done before OS installation)	<ol style="list-style-type: none"> 1. Press Shift+F10 to open CMD 2. Type "diskpart" to enter the utility 3. Type "list disk" to see the disks available 4. Select the disk to create the partition, for example "select disk 0" 5. Type "create partition primary" to create a partition without the 350MB Bitlocker drive 6. Exit diskpart and continue with normal installation 	<p>Bitlocker drive is not needed in virtual desktop environment. Drive can be removed to minimize disk space requirements.</p> <p>Can be done manually or through MDT Understand (and Get Rid of) the Mysterious Small Partition</p>
Remove unnecessary Windows features	Windows 8: Control Panel > Programs and Features	Minimizes disk space requirements.
Before rolling out to production		
Reboot the virtual machine at least two times	-	Ensures that pending installations, file updates and configurations are complete.
Update virus definitions and perform a full scan for viruses on all local hard disks	-	Ensures that the golden image does not contain any viruses. Also minimizes the virus scanner overhead during normal runtime since files which have already been scanned will not be scanned again if not changed (in some scenarios).
Run the Disk Cleanup Wizard	Disk Properties > Disk Cleanup	Clean up files and system restore points to minimize disk space requirements.
Defragment the hard disk	Windows Explorer > Optimize Drives Wizard	<p>Disk defragmentation should be completed before the initial rollout and at regular intervals to ensure that the disk is optimized, for example – following updates to a golden PVS or MCS image.</p> <p>When a scheduled defragmentation is used – for example in a persistent desktop – ensure that the schedule does not conflict with business times (default is every Wednesday at 1am).</p>

Table 3: Image Preparation

Runtime Optimizations

The following optimizations can help to improve performance and scalability. These optimizations should be considered for each Machine Creation Services or Provisioning Services master image. If no desktop provisioning technology is used, these tasks should be performed on all virtual desktops unless specifically noted.

Note: Optimizations marked ¹ are applied automatically during the XenDesktop VDA installation as outlined in [CTX125874](#).

Note: Optimizations marked ² should be applied to non-persistent desktops only.

Item	Configuration / Registry Key	Description/Justification
Disable Last Access Timestamps ¹	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem] "NtfsDisableLastAccessUpdate"=dword:00000001	Disabling the last access timestamp will help to minimize I/O operations.
Disable default system screensaver	HKEY_USERS\DEFAULT\Control Panel\Desktop "ScreenSaveActive"=dword: 00000000	This setting disables the screensaver when no user is logged on. This will save system resources when no users are logged into the desktop.
Disable bootlog and boot animation	bcdedit /set {default} bootlog no bcdedit /set {default} quietboot yes	Disabling the boot animation, which no user will see, helps to speed up the boot process. Note: Disabling the boot animation disables all UI feedback until the Windows logon screen appears. This behavior can increase troubleshooting complexity.
Enable "High Performance" scheme in Windows Power Plans	Select the "High Performance" power plan under "Control Panel\System and Security\Power Options" Or alternatively run command powercfg -s 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c	Processors are always locked at the highest performance state.
Antivirus	Follow the best practices outlined in CTX127030 – Guidelines for Antivirus Software Configuration .	

Page File	<p>My Computer Properties → Advanced → Performance Settings → Advanced tab → Change Virtual Memory</p> <p>Set the initial size to be equal to the maximum size.</p>	<p>The page file is a physical file on the disk where virtual memory can be stored. The page file allows the system to allocate and commit more virtual memory than there is physical memory available.</p> <p>The optimal size of the page file should be determined during pilot testing. The memory-to-committed bytes performance counter can be used to monitor how much committed virtual memory is on the system. When the value of this counter reaches close to the total combined size of physical memory and page file, memory allocation begins to fail. So the physical memory or the page file would need to be increased.</p> <p>The initial size of the page file should be equal to the maximum size of the page file to prevent fragmentation.</p> <p>Note: For more information on determining the appropriate size of the page file, please refer to the Microsoft knowledgebase article - KB2860880 and Citrix blog post - The Page File Done right! .</p>
Disable unnecessary Desktop Notification Icons	<p>Manually remove the components from the startup list or hide the notification icons by means of GPO</p> <p>In Windows 8, startup items can be controlled in Task Manager</p> <p>GPO is configured via;</p> <p>Administrative Templates > Start Menu and Taskbar > Hide the notification area</p>	<p>Notification icons on the desktop can have fairly expensive refreshing mechanisms. Therefore it is best to disable unnecessary notifications.</p>

<p>SMB 1.0 Client Optimization</p> <p>Note: Tuning SMB 1.0 is required in mixed environments where Windows 2012 / 8 and Windows 2003 or earlier systems connect.</p> <p>For more information on how to check your SMB version usage, please refer to the Microsoft blog post – Which version of the SMB protocol are you using?</p>	<p>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanworkstation\Parameters</p> <p>"MaxCmds"=dword:00002048 (dec)</p> <p>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxSmb\Parameters</p> <p>"MultiUserEnabled"=dword:00000001</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer</p> <p>NoRemoteRecursiveEvents"=dword:00000001</p> <p>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\Parameters</p> <p>"MaxWorkItems"=dword:00008192 (dec)</p> <p>"MaxMpxCt"=dword:00002048 (dec)</p> <p>"MaxRawWorkItems"=dword:00000512 (dec)</p> <p>"MaxFreeConnections"=dword:00000100 (dec)</p> <p>"MinFreeConnections"=dword:00000032 (dec)</p>	<p>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.</p> <p>By default the SMB 1.0 Client network redirector can only have 50 outstanding SMB requests/commands open to a single file server. This is controlled by the MaxCmds registry value.</p> <p>All connections to remote servers are per computer and not per user. This means all users on a Terminal Server open files over the same SMB session. A single SMB Client Session can have a maximum of 16,383 open files. This is controlled by the MultiUserEnabled registry value.</p> <p>When a drive is mapped to a UNC path and Windows Explorer is open to the network drive, it will submit 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.</p> <p>Note: For more information, please refer to the Citrix blog post – SMB tuning for XenApp and File Servers on Windows Server 2008.</p>
--	--	--

<p>SMB 2.x Client Tuning</p> <p>Note: Tuning SMB 2.0 is required in mixed environments where Windows 2012 / 8 and Windows 2008 / 2008 R2 systems connect.</p> <p>For more information on how to check your SMB version usage, please refer to the Microsoft blog post – Which version of the SMB protocol are you using?</p>	<p>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters</p> <p>“DisableBandwidthThrottling”=dword:00000001</p> <p>“DisableLargeMtu”=dword:00000000</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer</p> <p>NoRemoteRecursiveEvents”=dword:00000001</p>	<p>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.</p> <p>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.</p> <p>Note: For more information, please refer to the Citrix blog post – SMB tuning for XenApp and File Servers on Windows Server 2008.</p>
<p>Disable Background Disk Defragmentation ^{1,2}</p>	<p>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Dfrg\BootOptimizeFunction]</p> <p>“Enable”=“N”</p>	<p>Not required for MCS or PVS based non-persistent virtual desktops. File system changes are discarded after reboot.</p>
<p>Disable Background Auto-Layout ^{1,2}</p>	<p>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\OptimalLayout]</p> <p>“EnableAutoLayout”=dword:00000000</p>	<p>Not required for MCS or PVS based non-persistent virtual desktops. File system changes are discarded after reboot.</p>
<p>Disable Superfetch ^{1,2}</p>	<p>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SysMain]</p> <p>“Start”=dword:00000004</p> <p>The Optimizer tool disables the Superfetch service by registry change. Alternatively the Superfetch service can be disabled in the services dialog.</p>	<p>Tries to improve system performance over time by “learning” the typical user activity. This information is stored within the operating system, which means it is deleted upon each reboot and provides little value in a virtual desktop environment.</p> <p><i>Windows 8/8.1 should disable the SuperFetch service automatically in pooled virtual desktops.</i></p>
<p>Disable System Protection ²</p>	<p>System Properties > System Protection > Configure</p>	<p>System restore points are lost on reboot using MCS or PVS non-persistent desktops. Should be considered for other scenarios as well to save on disk requirements.</p>
<p>Disable Scheduled Disk Optimization ²</p>	<p>Local Disk Properties > Tools > Optimize</p>	<p>Not required for non-persistent virtual desktops. File system changes are discarded after reboot.</p>
<p>Disable UAC Secure Desktop Prompt</p>	<p>[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System]</p> <p>“PromptOnSecureDesktop”=dword:00000000</p>	<p>The secure desktop prompt partially dims the screen and consumes additional CPU and network traffic.</p> <p>Note: Disabling the UAC prompt will reduce security.</p>

<p>Disable Windows Defender Service</p> <p><i>Note: In Windows 8 and 8.1 the VDA Optimizer tool will not disable Defender Service.</i></p>	<p>Manually on master image:</p> <ol style="list-style-type: none"> 1. Navigate to Start->Apps->Windows Defender 2. Go to the settings tab 3. Under the administrator tab uncheck the box labeled "Turn on this app" <p>Through GPO: Computer Configuration->Administrative Templates->Windows Components->Windows Defender "Turn off Windows Defender"</p>	<p>Windows Defender can be disabled if using another anti-virus solution. <i>Windows Defender should disable itself if another anti-virus solution is detected.</i></p>
<p>Disable Hibernation¹</p>	<p>Execute "powercfg -h off" with elevated user rights.</p>	<p>Not required for virtual desktop environments. The hibernation file is unnecessary and requires storage.</p>

¹ Optimization applied automatically during XD7 VDA installation as outlined in [CTX125874](#)

Table 4: Runtime Optimizations

Services

Many Windows services within a virtual desktop environment and can be disabled to save resources. Below is a list of potential services to disable in hosted virtual environment. Some of these services are dependent on each other and dependencies should be considered for any required service. Note that some 3rd party applications may potentially rely on some services so testing should be carried out to ensure no lost functionality.

Services can be disabled in the master image (MCS or PVS), on individual desktops, or through Group Policy. Group Policy is the preferred method for large environments for easy rollback and minimal interference to the base image. System Services can be configured under Computer Configuration->Windows Settings->Security Settings->System Services.

Service Name	Recommended Configuration	Description/Justification
Application Experience	Disabled	Not required in managed corporate environments.
Application Layer Gateway Service	Disabled	Provides support for 3rd party protocol plugins for Internet Connection Sharing. This service is used for mobile devices and is not needed for virtual desktops.
Background Intelligent Transfer Service (BITS)	Consider Disabling	Used by Windows Update. Virtual desktops which are based off a PVS or MCS golden image do not typically require this service. Note: This service is required by many 3 rd party applications such as AppSense. If required, consider limiting the bandwidth usage of BITS through GPO.
BitLocker Drive Encryption Service	Disabled	Drive encryption is not typically desired in virtual desktop environments.
Block Level Backup Engine Service	Disabled	Windows backup is not typically needed for virtual desktop deployments.
Bluetooth Support Service	Disabled	Bluetooth support is not typically needed for virtual desktop environments.
BranchCache Service	Disabled	BranchCache is typically used for network savings to a WAN and is not needed in the virtual desktop environment.

Computer Browser Service	Disabled	Maintains an updated list of computers on the network and supplies this list to computers designated as browsers. If this service is stopped, this list will not be updated or maintained. If this service is disabled, any services that explicitly depend on it will fail to start.
Device Association Service	Disabled	Enables pairing between the system and wired or wireless devices.
Device Setup Manager Service	Disabled	Enables the detection, download and installation of device-related software. If this service is disabled, devices may be configured with outdated software, and may not work correctly.
Diagnostic Policy Services	Disabled	The Diagnostic Policy Services enables problem detection, troubleshooting and resolution for Windows components. If this service is stopped, diagnostics will no longer function. Unless the diagnostic facilities of Windows is required, this service can be disabled.
Distributed Link Tracking Client Service	Disabled	Maintains links between NTFS files within a computer or across computers in a network. This service may be required for certain editions of AVG Anti-Virus.
Encrypting File System Service	Disabled	Provides the core file encryption technology used to store encrypted files on NTFS file system volumes. If this service is stopped or disabled, applications will be unable to access encrypted files.
Family Safety Service	Disabled	Service provides backwards compatibility to Vista parental control and can be disabled in a virtual corporate environment.
Fax Service	Disabled	Disable if fax services are not needed from virtual desktop.
Function Discovery Resource Publication Service	Disabled	Publishes this computer and resources attached to this computer so they can be discovered over the network. If this service is stopped, network resources will no longer be published and they will not be discovered by other computers on the network.
Home Group Listener	Disabled	Used to establish Home Groups, not used with virtual machines in a corporate environment
Home Group Provider	Disabled	Used to establish Home Groups, not used with virtual machines in a corporate environment
IP Helper	Disabled	Provides tunnel connectivity using IPv6 transition technologies. Not required unless IPv6 is used within the datacenter.
Microsoft iSCSI Initiator Service	Disabled	Manages Internet SCSI (iSCSI) sessions from this computer to remote iSCSI target devices. This should not be needed within a virtual desktop.

Microsoft Software Shadow Copy Provider Service	Consider Disabling (Disable after PVS imaging)	Manages software-based volume shadow copies taken by the volume shadow copy service. If this service is stopped, software-based volume shadow copies cannot be managed. <i>Do not disable this service if using personal vdisk. This service is often required by other 3rd party applications.</i>
Optimize Drives Service ²	Disabled	Drive optimization should be performed on the master image during scheduled maintenance.
Secure Socket Tunneling Protocol Service	Disabled	Provides support for the Secure Socket Tunneling Protocol (SSTP) to connect to remote computers using VPN. If this service is disabled, users will not be able to use SSTP to access remote servers.
Security Center	Disabled	Used to monitor and report security health settings on a system.
Sensor Monitoring Service	Disabled	Monitors various sensors in order to expose data and adapt to system and user state.
Shell Hardware Detection Service	Disabled	Provides autoplay functionality not typically needed in a virtual desktop environment.
SNMP Trap Service	Disabled	Receives trap messages generated by local or remote Simple Network Management Protocol (SNMP) agents and forwards the messages to SNMP management programs running on this computer. If this service is stopped, SNMP-based programs on this computer will not receive SNMP trap messages. May be required for certain monitoring tools.
SSDP Discovery	Disabled	Discovers network devices and services that use the SSDP protocol. SSDP discovery is not typically used in corporate environments.
SuperFetch ¹ (Non-persistent desktops only)	Disabled	All cached files which are used to determine SuperFetch behavior are deleted on pooled desktops. <i>Windows 8 should disabled this service automatically for non-persistent desktops.</i>
Telephony Service	Disabled	Provides Telephony API (TAPI) support for programs that control telephony devices on the local computer and, through the LAN, on servers that are also running the service.
Themes Service Note: Unlike in Windows 7, Desktop Composition does not require the themes service	Disabled	Provides user experience theme management. In Windows 8 the Desktop Window Manager still runs if the themes service is disabled. <i>Disabling the themes service can alter the appearance of the desktop. (Disables taskbar transparency)</i>
UPnP Device Host Service	Disabled	Allows UPnP devices to be hosted on the computer. Is dependent on the SSDP Discovery service above.

Volume Shadow Copy Service	Consider Disabling (Disable after PVS Imaging)	Manages and implements volume shadow copies used for backup and other purposes. If this service is stopped, shadow copies will be unavailable for backup and the backup may fail. <i>Do not disable this service if using personal vdisk. This service is often required by other 3rd party applications.</i>
Windows Color System Service	Disabled	The WcsPlugInService service hosts third-party Windows color system color device model and gamut map model plug-in modules. These plug-in modules are vendor-specific extensions to the Windows color system baseline color device and gamut map models.
Windows Connect Now – Config Registrar Service	Disabled	Not required in virtual desktop environments as virtual machines typically do not use wireless internet.
Windows Error Reporting Service	Disabled	Allows errors to be reported when programs stop working or responding. Also allows logs to be generated for diagnostic and repair services. If this service is stopped, error reporting might not work correctly and results of diagnostic services and repairs might not be displayed.
Windows Media Player Network Sharing Service	Disabled	Shares Windows Media Player libraries to other systems. This is typically not required in corporate environments.
Windows Search ¹	Consider Disabling <i>High User Impact</i>	Remove all files and folders (default is Start Menu and local User Profiles) from index options. Doing so enables user to search for file contents on Windows file servers running the Windows Search service. If this functionality is not required, the Windows Search service can be disabled.
Windows Update ¹	Depends	Not required for PVS or MCS based environments, or if Windows Update has been replaced with an alternative deployment solution. <i>Note that Windows Update can also be configured by group policy as described in the General Recommendations Section below.</i>
WLAN Service	Disabled	Not required in virtual desktop environments as virtual machines typically do not use wireless internet.
WWAN Service	Disabled	Not required in virtual desktop environments as virtual machines typically do not use wireless internet.

Table 5: Windows Services

Scheduled Tasks

Windows includes a large number of scheduled tasks, many of which are enabled by default. These tasks may increase the CPU and memory footprint of the operating system, especially in a virtual desktop environment.

Scheduled tasks can be controlled through the master image (MCS or PVS), on each individual desktop, or preferably through Group Policy. For more information on scheduled tasks and group policy please refer to the following Microsoft TechNet article – [Scheduled Tasks Extension](#).

The following scheduled tasks could potentially be disabled on the virtual desktops.

Task	Description/Justification
Application Experience \ AitAgent	Aggregates and uploads Application Telemetry information if opted-in to the Microsoft Customer Experience Improvement Program.
Application Experience \ ProgramDataUpdater	Collects program telemetry information if opted-in to the Microsoft Customer Experience Improvement Program
Application Experience \ StartupAppTask	Scans startup entries and raises notification to the user if there are too many startup entries.
AutoCHK \ Proxy	This task collects and uploads autochk SQM data if opted-in to the Microsoft Customer Experience Improvement Program.
Bluetooth \ UninstallDeviceTask	This tasks uninstalls the PnP device associated with a specified Bluetooth service ID.
CHKDSK \ Proactive Scan	NTFS Volume Health Scan
Customer Experience Improvement Program \ Consolidator	If the user has consented to participate in the Windows Customer Experience Improvement Program, this job collects and sends usage data to Microsoft.
Customer Experience Improvement Program \ KernelCeipTask	The Kernel CEIP (Customer Experience Improvement Program) task collects additional information about the system and sends this data to Microsoft. If the user has not consented to participate in Windows CEIP, this task does nothing.
Customer Experience Improvement Program \ BthSQM	The Bluetooth CEIP (Customer Experience Improvement Program) task collects Bluetooth related statistics and information about your machine and sends it to Microsoft. The information received is used to help improve the reliability, stability, and overall functionality of Bluetooth in Windows.
Customer Experience Improvement Program \ Uploader	This job sends data about windows based on user participation in the Windows Customer Experience Improvement Program
Customer Experience Improvement Program \ UsbCeip	The USB CEIP (Customer Experience Improvement Program) task collects Universal Serial Bus related statistics and information about your machine and sends it to the Windows Device Connectivity engineering group at Microsoft. The information received is used to help improve the reliability, stability, and overall functionality of USB in Windows. If the user has not consented to participate in Windows CEIP, this task does not do anything.

Diagnosis \ Scheduled	The Windows Scheduled Maintenance Task performs periodic maintenance of the computer system by fixing problems automatically or reporting them through the Action Center.
DiskDiagnostic \ Microsoft-Windows-DiskDiagnosticDataCollector	The Windows Disk Diagnostic reports general disk and system information to Microsoft for users participating in the Customer Experience Program.
DiskDiagnostic \ Microsoft-Windows-DiskDiagnosticResolver	This task warns users about faults that occur on disks that support Self-Monitoring and Reporting Technology.
Defrag \ ScheduledDefrag	This task optimizes local storage drives.
FileHistory \ File History	Protects user files from accidental loss by copying them to a backup location when the system is unattended
Location \ Notifications	Location Activity
Maintenance \ WinSAT	Measures a system's performance and capabilities
Mobile Broadband Accounts \ MNO Metadata Parser	Mobile Broadband Account Experience Metadata Parser
MobilePC \ HotStart	Launches applications configured for Windows HotStart
PerfTrack \ BackgroundConfigSurveyor	Performance Tracing Idle Task: Background configuration surveyor
Power Efficiency Diagnostics \ AnalyzeSystem	This task analyzes the system looking for conditions that may cause high energy use.
RAC \ RacTask	Microsoft Reliability Analysis task to process system reliability data.
RAS \ Mobility Manager	Provides support for the switching of mobility enabled VPN connections if their underlying interface goes down.
Registry \ RegIdleBackup	Registry Idle Backup Task
Shell \ FamilySafetyMonitor	Initializes Family Safety monitoring and enforcement.
Shell \ FamilySafetyRefresh	Synchronizes the latest settings with the Family Safety website.
SlideShow \ AutoWake	This task automatically wakes the computer and then puts it to sleep when automatic wake is turned on for a Windows SideShow-compatible device.
SlideShow \ GadgetManager	This task manages and synchronizes metadata for the installed gadgets on a Windows SideShow-compatible device.
SlideShow \ SessionAgent	This task manages the session behavior when multiple user accounts exist on a Windows SideShow-compatible device.
SlideShow \ SystemDataProviders	This task provides system data for the clock, power source, wireless network strength, and volume on a Windows SideShow-compatible device.
SystemRestore \ SR	This task creates regular system protection points.
TaskScheduler \ IdleMaintenance	Maintenance Scheduler Launcher Task
TPM \ Tpm-Maintenance	This task supports the Trusted Platform Module (TPM) by performing background actions on behalf of the OS.
UPnP \ UPnPHostConfig	Sets the UPnP service to autostart.

WDI \ ResolutionHost	The Windows Diagnostic Infrastructure Resolution host enables interactive resolutions for system problems detected by the Diagnostic Policy Service. It is triggered when necessary by the Diagnostic Policy Service in the appropriate user session. If the Diagnostic Policy Service is not running, the task will not run
Windows Backup \ ConfigNotification	This scheduled task notifies the user that Windows Backup has not been configured.
Windows Defender \ Windows Defender Cache Maintenance	Can be disabled in case an alternative virus and malware protection has been implemented.
Windows Defender \ Windows Defender Cleanup	
Windows Defender \ Windows Defender Scheduled Scan	
Windows Defender \ Windows Defender Verification	
Windows Filtering Platform \ BfeOnServiceStartTypeChange	This task adjusts the start type for firewall-triggered services when the start type of the Base Filtering Engine (BFE) is disabled.
Windows Media Sharing \ UpdateLibrary	This task updates the cached list of folders and the security permissions on any new files in a user's shared media library.

Table 6: Scheduled Tasks

General Recommendations

The following items, which are configurable by means of Group Policies, do not provide immediate performance increases but can improve system stability and user experience for virtual desktop implementations.

The following optimizations should be applied using default Group Policy settings. Some of these settings can be achieved by disabling the associated service or manually on the virtual machine image. Use Group Policy whenever possible for ease of management.

Item	Configuration / Registry Key	Description/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 Administrative Templates – Windows Components – Windows Updates Remove access to use all Windows Update features	Windows updates should be performed 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. Non-persistent desktops do not maintain system restore points. Persistent desktops require additional storage for system restore.
Windows Search <i>Note: If Search is not available in Group Policy the .ADMX file may need to be imported from a machine with Windows Search enabled.</i> <i>For more on Windows Search Policies see Microsoft TechNet article Group Policy For Windows Search</i>	Administrative Templates – Windows Components – Search Prevent Indexing Certain Paths	Disabled indexing on the machine but enables users to perform searches on Windows file servers running the Windows Search service. If this functionality is not required, the Windows Search service can be disabled.

Table 7: General Recommendations - GPO

The following general recommendations are configurable by means of registry changes.

Item	Configuration / Registry Key	Description/Justification
Increase Service Startup Timeout	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control] "ServicesPipeTimeout"= dword:0002bf20	In certain peak load scenarios Windows services might take longer than 30 seconds to start. This setting increases the timeout value to 10 minutes.
Redirect or Disable CrashDump ¹ (Non-persistent desktop only)	To redirect CrashDump: Advanced System Settings->Start Up and Recovery: "Complete Memory Dump" Dump File "Small Memory Dump" Small Dump Directory To disable CrashDump: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl] "CrashDumpEnabled"= dword:00000000 "LogEvent"=dword:00000000 "SendAlert"=dword:00000000	On reboot, non-persistent virtual desktops will start from the pristine state and all information about the crash will be wiped. Either redirect the memory dump to a persistent disk or if not required, disable it entirely. Note: The <i>TargetOSOptimizer</i> tool disables the crashdump.
Disable Windows Autoupdate ¹	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update] "AUOptions"=dword:00000001 "ScheduledInstallDay"=dword:00000000 "ScheduledInstallTime"=dword:00000003	Not required for PVS or MCS based environments where updates should be applied on the master image, or if Windows Update has been replaced with an alternative deployment solution.

Disable Offline Files ¹	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\NetCache] "Enabled"=dword:00000000	Not applicable to virtual desktop scenarios as desktops are never offline.
Hide Hard Error Messages	[HKEY_LOCAL_MACHINE\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. The system can be configured to suppress these messages by writing them to the Event Log and automatically selecting "OK" for the user.
Increase Disk I/O Timeout to 200 seconds	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Disk] "TimeOutValue"=dword:000000C8	In peak scenarios the disk may be heavily strained. This setting allows for a timeout of 200 seconds.

¹ Optimization applied automatically during XD7 VDA installation as outlined in [CTX125874](#)

Table 8: General Recommendations - Registry

System Performance

The following registry changes can improve system performance and user experience but may have a small impact on the appearance of the desktop. This is done by removing resource intensive animations which in a virtual desktop, can add considerable bandwidth requirements. Note that many of the optimizations below affect the explorer shell and therefore must either be implemented in the Default profile or if using Group Policy Preferences or logon script, they will take effect only upon reboot. For more on customizing the default user profile see Microsoft support article - [Customize the default local user profile when preparing an image of Windows](#).

Item	Configuration / Registry Key
Settings "Visual Effects to Custom"	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\VisualEffects] "VisualFXSetting"=dword:00000003
Disable "Show translucent selection rectangle"	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced] "ListViewAlphaSelect"=dword:00000000
Disable "Show shadows under windows"	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced] "ListViewShadow"=dword:00000000
Disable "Animate windows when minimizing and maximizing"	[HKEY_CURRENT_USER\Control Panel\Desktop\WindowMetrics] "MinAnimate"="0"
Disable "Animations in the taskbar"	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced] "TaskbarAnimations"=dword:00000000

Disable "Enable Peek"	[HKEY_CURRENT_USER \\Software\\Microsoft\\Windows\\DWM] "EnableAeroPeek"=dword:00000000
Disable "Save Taskbar Thumbnail Previews"	[HKEY_CURRENT_USER \\Software\\Microsoft\\Windows\\DWM] "AlwaysHibernateThumbnails"=dword:00000000
Disable "Smooth edges of screen fonts"	[HKEY_CURRENT_USER \\Control Panel\\Desktop] "FontSmoothing"="0"
Disable "Use drop shadow for icon labels on the desktop"	[HKEY_CURRENT_USER \\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Advanced] "ListViewShadow"=dword:00000000
Disable the rest of the visual effects	[HKEY_CURRENT_USER \\Control Panel\\Desktop\\] "UserPreferencesMask"=RegBin: "90,12,01,80"
Disable "Cursor blink"	[HKEY_CURRENT_USER \\Control Panel\\Desktop] "CursorBlinkRate"="-1"

User Experience

The following items, which are configurable by means of registry changes, do not provide immediate performance increases but can improve user experience for virtual desktop implementations:

Item	Configuration / Registry Key	Description/Justification
Disable the Windows 8 First Logon Animation	[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System] "EnableFirstLogonAnimation"=dword:00000000	Disable the first logon sequence for a user on a Windows 8 machine. Note: This can also be disabled through machine local group policy Administrative Templates->System->Logon "Show first sign-in animation"
Disable Internet Explorer First Run Wizard	[HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Microsoft\\Internet Explorer\\Main] "DisableFirstRunCustomize"=dword:00000001	Disables the pop-up for Internet Explorer for users first logging onto the machine.
Reduce menu show delay	[HKEY_CURRENT_USER\\Control Panel\\Desktop] MenuShowDelay", "0"	Reduces the delay Windows sets for menus. Provides better user experience.
Disable Action Center	[HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer] "HideSCAHealth"=dword:00000001	Disables the action center icon which may display messages to users that they cannot react to.
Turn off Network Location Wizard	[HKEY_CURRENT_USER \\Software\\Microsoft\\Windows NT\\CurrentVersion\\Network\\NwCategoryWizard\\Show]	The network location should not change in a corporate VDI environment and can be confusing for users. For more information, please refer to the Microsoft TechNet article - Turn off the Network Location Wizard .

Table 9: User Experience

Application Optimizations

Many commercial applications are not optimized for virtual desktops and can consume excess resources with little or no benefit. Some vendors provide guides on optimizing the performance of applications that can be reviewed to ensure lean and scalable systems:

- [How to optimize Word 2007 and Word 2010](#)
- [Slow Display Performance](#)
- [Office 2013 Video Performance](#)

Check with your application vendor for guidelines on optimizing their application for virtual desktops. In addition, custom internal applications should also be optimized to ensure they do not unnecessarily degrade performance.

Revision History

Revision	Change Description	Updated By	Date
1.0	Initial Document Creation	Thomas Berger Amit Ben-Chanoch	2/24/2014

Contributors

We would like to thank the Citrix Solutions Lab for providing both hardware and support for the testing as well as EMC for providing the VNX5500 storage array.

The following individuals have helped contribute to the making of this guide:

Andy Baker

Roger LaMarca

Martin Zugec

Pablo Legorreta

Steven Krueger

Feedback

As we are always looking for ways to improve our content, we welcome and appreciate your feedback. Please provide feedback using the link below.

<https://podio.com/webforms/6040613/470785>

The copyright in this report and all other works of authorship and all developments made, conceived, created, discovered, invented or reduced to practice in the performance of work during this engagement are and shall remain the sole and absolute property of Citrix, subject to a worldwide, non-exclusive license to you for your internal distribution and use as intended hereunder. No license to Citrix products is granted herein. Citrix products must be licensed separately. Citrix warrants that the services have been performed in a professional and workman-like manner using generally accepted industry standards and practices. Your exclusive remedy for breach of this warranty shall be timely re-performance of the work by Citrix such that the warranty is met. THE WARRANTY ABOVE IS EXCLUSIVE AND IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE WITH RESPECT TO THE SERVICES OR PRODUCTS PROVIDED UNDER THIS AGREEMENT, THE PERFORMANCE OF MATERIALS OR PROCESSES DEVELOPED OR PROVIDED UNDER THIS AGREEMENT, OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM, AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR AGAINST INFRINGEMENT. Citrix' liability to you with respect to any services rendered shall be limited to the amount actually paid by you. IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY HEREUNDER FOR ANY INCIDENTAL, CONSEQUENTIAL, INDIRECT OR PUNITIVE DAMAGES (INCLUDING BUT NOT LIMITED TO LOST PROFITS) REGARDLESS OF WHETHER SUCH LIABILITY IS BASED ON BREACH OF CONTRACT, TORT, OR STRICT LIABILITY. Disputes regarding this engagement shall be governed by the internal laws of the State of Florida.

851 West Cypress Creek Road

Fort Lauderdale, FL 33309

954-267-3000

<http://www.citrix.com>

Copyright © 2013 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, Citrix ICA, Citrix XenDesktop, and other Citrix product names are trademarks of Citrix Systems, Inc. All other product names, company names, marks, logos, and symbols are trademarks of their respective owners.