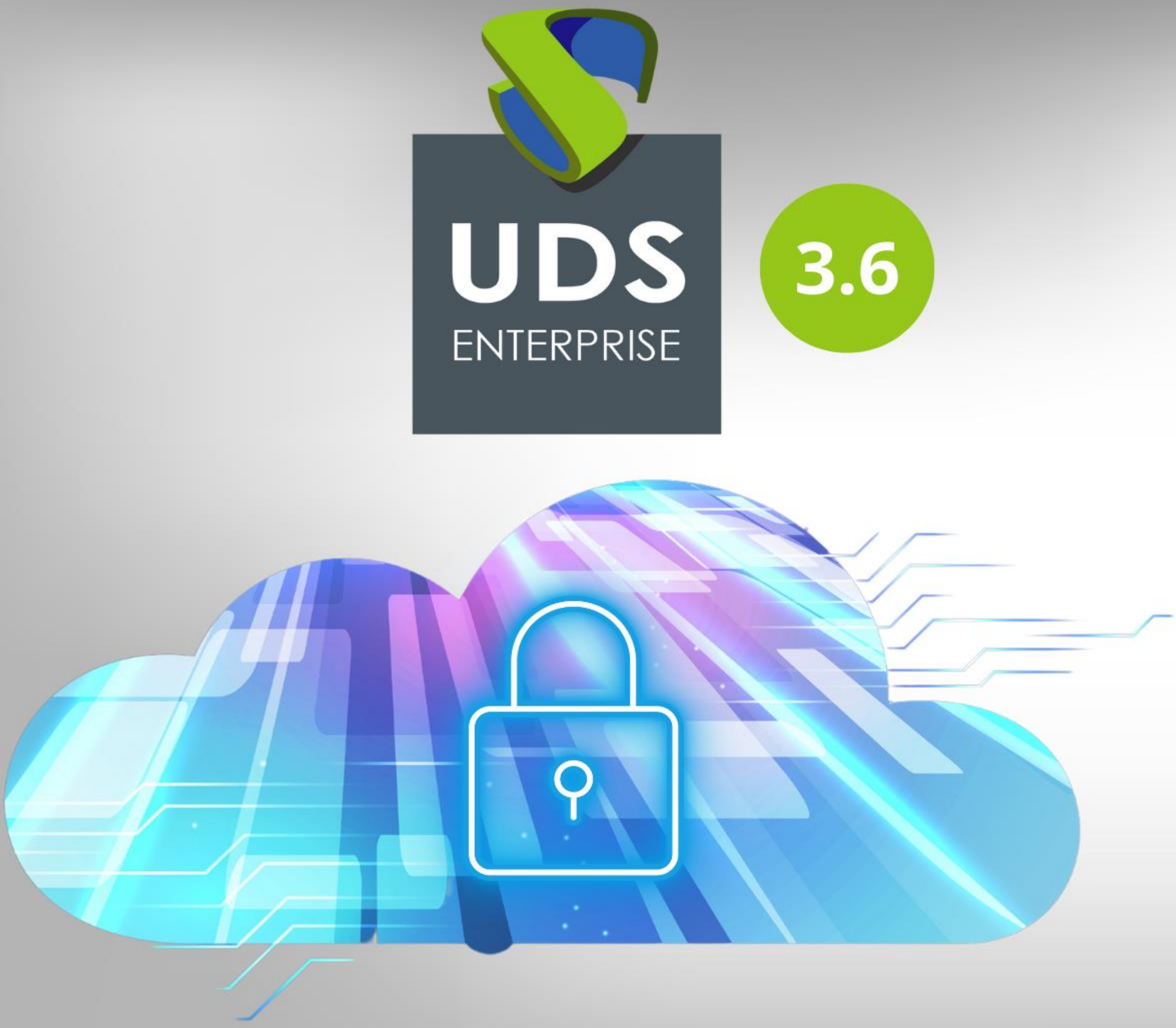
VIRTUAL CABLE

Optimization of UDS Enterprise in Windows 10



Index

Optimizing UDS Enterprise in Windows 10

Deploying virtual desktops with Windows 10 requires planning and configuration that provides users with a secure and optimized virtual desktop platform.

This document describes a series of good practices, referring to the configuration and characteristics of Windows 10, which will allow optimizing the performance and behavior of the provision of virtual desktops deployed for users.

The user configuration will be carried out on the Active Directory group policy objects that directly affect the user profile at the time of loading said source template or golden image.

The rest of the proposed configurations and modifications will be made on the virtual machine image defined as the source template, which will later be used as the basis for deploying virtual desktops. These are modifications to the system registry and to the operating system services.

It should be noted that most of the modifications indicated in this document are recommended, so the system administrator can choose whether or not to disable each of the described features at his convenience. The character of the type of configuration for optimization, recommended or mandatory, is indicated in the title of the corresponding section.

Some of the modifications described in this document are generic and apply to any virtual desktop platform, while others are exclusive to non-persistent virtual desktop platforms.

The proposed configurations and modifications are in no case necessary for the correct operation of a desktop virtualization platform, they simply optimize certain aspects of its operation, the changes adopted and the correct operation of the platform being the responsibility of the system administrator.

VirtualCable and the UDS Enterprise team are not responsible in any way for the possible consequences on the stability of the system once the changes proposed in this document are applied.

User settings

Unlike machine settings, user settings cannot be applied to the base template on which virtual desktops are to be deployed. To make changes centrally, it is recommended to use Group Policy Objects or GPOs.

Recommended Generic User Configurations

Group Policy Objects:It is recommended to apply the following GPO settings on any virtual desktop platform.

Element	Route	Explanation
screensaver	Administrative Templates – Control Panel – Personalization Activate screen saver: Enabled Prevent screen saver changes: Enabled Password Protect Screen Saver: Enabled Screen saver activation time: 600 seconds Force specific screensaver: scrnsave.scr	Using complex screensavers consumes a large amount of resources. Basic screen saver can be used to secure virtual desktop without consuming resources

Virtual machine (VM) configuration or source template

For the configurations described in this section, which involve changes to the Windows registry, it is advisable to take into account the possible implications when making such changes.

Incorrectly modifying the Windows registry can make the system unstable. It is recommended to make a backup of the Windows registry before making any changes to it.

For a correct optimization of the source virtual machine, there are a series of parameters that we can fine-tune in order to improve its performance.

The settings on the source virtual machine go through modifications in three sections: system registry, group policy objects or GPOs, and Windows 10 services.

Recommended generic VM configurations

System Log:The following system registry changes are valid for any virtual desktop platform, persistent or non-persistent. These modifications will reduce the resource consumption of virtual desktops on the hypervisor platform.

Setting	Modification in the registry	Explanation
Disable “Last Access Timestamp”	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem] "NtfsDisableLastAccessUpdate"=dword:00000001	Increases file viewing speed
reduce delay in showing the Menu	[HKEY_CURRENT_USER\Control Panel\Desktop] "MenuShowDelay"="150"	Reduces delay by show the menu Windows. Provides a better user experience
Disable all visual effects except "Using Common Tasks on Folders" and "Using Visual Styles on Buttons and Windows"	[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 "ListviewShadow"=dword:00000000 [HKEY_CURRENT_USER\Control Panel\Desktop] "DragFullWindows"="0" "FontSmoothing"="0"	Provides a better user experience
Hide “Hard” Mistake	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows] "ErrorMode"=dword:00000002	Does not show messages of errors

Recommended VM configurations for non-persistent desktops

System Log:These registry changes are recommended for non-persistent virtual desktops. As can be seen in the following table, the parameters are used to configure event logs, log storage and disk defragmentation, services that are of no use in non-persistent virtual desktops.

Setting	Modification in the registry
Disable Clear Page File at Shutdown	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management] "ClearPageFileAtShutdown"=dword:00000000
Disable Background Defragmentation	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Dfrg\BootOptimizeFunction] "Enable"="N"
Disable Background LayoutService	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\OptimalLayout] "EnableAutoLayout"=dword:00000000
Disable Bug Check memory dump	[HKLM\SYSTEM\CurrentControlSet\Control\CrashControl] "CrashDumpEnabled"=dword:00000000 "LogEvent"=dword:00000000
Disable Memory Dumps	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl] "CrashDumpEnabled"=dword:00000000 "LogEvent"=dword:00000000
Disable Mach. Act. Password Changes	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters] "DisablePasswordChange"=dword:00000001
Redirect Event Logs	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]
Reduce Event Log Size to 64K	HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application] "MaxSize"=dword:00010000 [HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security] "MaxSize"=dword:00010000 [HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\System]

Group Policy Objects:It is recommended to apply the following GPO settings on any virtual desktop platform. These settings are enabled by default in Windows 10. When performing template-based non-persistent virtual desktop deployments, it is not necessary to have these options enabled, since, apart from consuming resources, they are useful when the virtual desktop remains over time.

Element	Route	Explanation
bug report	Administrative Templates – Windows Components – Windows Error Reporting Disable error reporting	It generates application dumps that are sent to Microsoft. It should be disabled unless you have to troubleshoot an application
windows update	Administrative Templates - Windows Components – Windows update Configure automatic	Windows updates should be done on top of the base template
system restore	Administrative Templates – System – system restore Disable System Restore: Enabled	It is not necessary since the virtual desktops will be based on a base template

Required service configuration for non-persistent desktops

Services:Windows 10 includes a series of services activated by default. These services improve performance as the virtual desktop is maintained over time. UDS Enterprise allows, among other functions, to publish non-persistent virtual desktops, so in the face of this type of deployment, having these services active does not make much sense. Below we list the services that can be disabled.

Setting	Recommendation	Justification
Background Intelligent Transfer Service	disabled	This service uses idle network bandwidth for services like Windows Update. As services that depend on BITS are going to be disabled, this service will be disabled
experience with Applications	disabled	Automatically apply updates software to programs. This functionality is typically not required in a virtual desktop environment
Publication of function detection resource	disabled	This service publishes desktop information on the web so that others can find them. This functionality is typically not required in a virtual desktop environment

Encryption Service	disabled	This service is not usually necessary in a
Block Level Backup Module Service	disabled	Windows uses the WBENGINE service to perform backup and recovery operations
examiner of equipment	disabled	Maintains an up-to-date list of equipment in the network and provides this list to computers designated as browsers. This functionality is typically not required in a virtual desktop environment
Group listening Home	disabled	As in most environments the virtual desktops will be associated to a domain HomeGroup functionality is not required
Group Provider Home	disabled	
Service Hyper-V data exchange	disabled	This functionality is not required
closing service guest of	disabled	This functionality is not required
heartbeat service Hyper V	disabled	This functionality is not required
Service Hyper-V Remote Desktop Virtualization	disabled	This functionality is not required
Service Hyper-V time synchronization	disabled	This functionality is not required
applicant for volume snapshots Hyper-V	disabled	This functionality is not required
Child protection	disabled	This functionality is not required
Dashboard Help control of Reports of problems and solutions	disabled	This service provides help to view, submit and clear system-level problem reports to the Problem Reports and Solutions control panel. This functionality is typically not required in a virtual desktop environment.
host device UPnP	disabled	Allows UPnP devices to connect stay in the team. This functionality is typically not required in a virtual desktop environment.

Windows Error Reporting Service	disabled	It allows you to report bugs when programs stop working or responding and provide existing solutions. It also allows you to generate logs for diagnostic and repair services. This service is typically not required in a virtual desktop environment
Volume snapshots	disabled	Manage and deploy Shadow Volume Copies used for backup and other purposes. This service must be disabled
dashboard service handwriting and touch keyboard	disabled	Enable pen and input functionality handwriting pad pen and touch keyboard. This service is typically not required in a virtual desktop environment
SSDP detection	disabled	Detect devices and services on the network that They use the SSDP discovery protocol, just like UPnP devices. This service is typically not required in a virtual desktop environment
Service secure socket tunneling protocol	disabled	Provides tunneling protocol support Secure Sockets (SSTP) to connect to remote computers using VPN. This service is typically not required in a virtual desktop environment
biometric service Windows	disabled	Provides client applications with the ability to capture, compare, manipulate and store biometric data without gaining direct access to any biometric sample or hardware
Store Service windows	disabled	Provides infrastructure support for windows store
Diagnostic Service Host	disabled	The Diagnostic Policy Service uses the Diagnostic Service Host to host diagnostics that need to be run in a Local Service context
system host diagnosis	disabled	The Diagnostic Policy Service uses the Diagnostic Service Host to host diagnostics to be run in a Local Service context
provider host function detection	disabled	The FDPHOST service hosts providers of network detection FD (function detection). This functionality is typically not required in a virtual desktop environment.

Security Center	disabled	When disabled, the service does not report problems with antivirus, malware, or firewall settings. Since many of these elements are disabled in a virtual desktop environment, disabling this service removes the messages that are displayed to users.
Superfetch	disabled	Maintains and improves system performance over time. Since the data of this service is stored with the operating system in non-persistent virtual desktop environments this functionality is not necessary
Topics	disabled	Allows the user to manage the themes of desktop including wallpapers and visual and sound effects that consume machine resources
helper application IP	disabled	Provides tunnel connectivity using IPv6 transition technologies
service of iSCSI initiator	disabled	Manages Internet SCSI sessions (iSCSI). This service must be disabled
Microsoft Software Snapshot Provider	disabled	Manages software-based volume shadow copies taken by the Volume Shadow Copy Service. This functionality is typically not required in a virtual desktop environment.
files without Connection	disabled	The offline file service performs maintenance activities on the offline file cache. This functionality is typically not required in a virtual desktop environment.
Windows Defender	disabled	Most entities have their own antivirus system, for this reason this service should be disabled
Windows Media Player Network Sharing Service	disabled	Unless users are going to share items using Media Player this service can be disabled
Automatic WWAN configuration	disabled	Manages mobile broadband embedded module/data card (GSM and CDMA) adapters and connections using automatic network configuration. It is not usually necessary in virtual desktops

Automatic WLAN configuration	disabled	The WLANSVC service provides the logic necessary to configure, discover, connect to, and disconnect from a wireless local area network (WLAN), as defined in IEEE 802.11 standards. This service must be disabled
Windows Search	disabled	Provides content indexing, property caching, and search results for files, email, and other types of content. This service must be disabled
windows update	disabled	Enables detection, download and installation of Windows updates and other programs. This service must be disabled

common settings

These latter settings optimize the desktop by removing unnecessary items. They are applied to different sections within the OS of the source machine itself. In the case of antivirus, we recommend consulting its manufacturer for this type of optimization.

Setting	Recommendati	Explanation
animation of start	disable with the following command bcdedit /set bootux	Disable animation, reduces the consumption of resources and speeds up the desktop boot process
Eliminate unused Windows components	Windows Media Center DVD Maker Tablet	These components are not used in a VDI environment centralized
file of pagination	match the minimum and the	Keep the paging file a single size prevents its growth by avoiding a high consumption of IO
Cleaning of disk	delete files unnecessary	clean unnecessary files
Defragmentation disk	Carry out disk defragmentatio	Disk defragmentation should be performed as last step in the creation of the base template
anti virus	Optimize	Configure the antivirus to perform a scan of the writes and disable automatic updates. The base template must be scanned before going to production

About VirtualCable

Virtual Cableis a company specialized in the digital transformation of the workplace. The company develops, supports and markets UDS Enterprise. Its team of experts has designed VDI solutions tailored to each sector to provide a unique user experience fully adapted to the needs of each user profile. Virtual Cable professionals have more than 30 years of experience in IT and software development and more than 15 in virtualization technologies. Millions of Windows and Linux virtual desktops with UDS Enterprise are deployed all over the world every day.