

Quest vWorkspace Feature Overview

Prepared by: Patrick Rouse



CONTENTS

Contents

INTRODUCTION	3
CONNECTION BROKER FEATURES	3
PRINTING FEATURES	8
SECURITY FEATURES	9
CLIENT EXPERIENCE FEATURES	11

INTRODUCTION

The objective of this document is to describe the core features of Quest vWorkspace Enterprise and Desktop editions.

CONNECTION BROKER FEATURES

The following are features of the vWorkspace Connection Broker Service. The Connection Broker is the brains of the Quest vWorkspace.

Connection Broker Service	Value-add
<p>1. Single point of access to corporate computing resources. The connection broker service authenticates users against Active Directory, queries the vWorkspace database and provides the client with a list of authorized resources to be accessed by the authenticated user. These resources can be seamless applications, desktops or web content hosted on Windows Terminal Servers, Virtual Desktops or Physical PCs.</p>	<p>Quest vWorkspace empowers IT to provide users with a single point of access to their applications, regardless of the hosting platform. Without this capability IT has to provide end users with connection files and instructions on how to access each application or computing resource. This requires a significant amount of administrative overhead to maintain, frustrates or confuses end users and generates unnecessary helpdesk calls.</p>
<p>2. Single point of management with granular, delegated administration. The vWorkspace Management Console manages Terminal Services, Virtual Desktops, Physical Desktops, Applications, User Profiles, and Printers, all from a single management console. Every setting in the console can be delegated to authorized administrators to support organizations with different types of IT Staff, and different geographical locations or departments.</p>	<p>One of the major drawbacks of competing products is the lack of functionality of the management console, or the number of consoles required to maintain the system. Other vendor's consoles offer all or nothing administration, and offer features useful only to third level IT Staff, with nothing for the helpdesk employee.</p> <p>The vWorkspace Management Console offers a Single Pane of Glass for operating and maintaining the desktop environment. Features can be delegated to first, second and third level IT Staff, where appropriate.</p>

<p>3. Tight integration with popular hypervisors. Quest vWorkspace provides tight integration with four different hypervisors; VMware ESX, Virtual Iron, Microsoft Hyper-V and Parallels Virtuozzo. Quest vWorkspace also supports all other hypervisors, but for others features such as VM cloning, VM deleting and VM Power Management are not supported.</p>	<p>In a perfect world IT would be completely centralized and standardized on a single virtualization infrastructure. The reality is that there are several hypervisors from which to choose and IT may end up having to manage more than one. This may be to support current technology investments, because of mergers and acquisitions or for political reasons. With Quest vWorkspace desktop engineers can manage virtual desktops on any hypervisor without needing to understand the intricacies of the underlying hypervisor. The connection broker utilizes the hypervisor vendor's published SDK to completely automate the lifespan of virtual desktops.</p> <p>Without a connection broker that supports a heterogeneous virtual infrastructure, IT will have to standardize on a single hypervisor or utilize multiple connection brokers.</p>
<p>4. Advanced automation of virtual infrastructures. Because of Quest's tight integration with popular hypervisors, virtually all desktop management can be performed from the vWorkspace Management Console, i.e. cloning, automated virtual machine provisioning, power management, virtual machine deletion and changing VM memory allocation.</p>	<p>Without automation of the hypervisor, many manual administrative tasks need to be performed, such as:</p> <ul style="list-style-type: none"> • Creation of virtual machines, one at a time • Sysprep of Virtual Machines, giving them their personalization and joining them to Active Directory • Reconfiguring the amount of memory is assigned to virtual machines • Writing a scripts to delete virtual machines that haven't been used in some period of time • Powering on machines that were accidentally shut down • Suspending or powering off Virtual Machines that are idle or not in use • Manual assignment of users to specific virtual machines.

<p>5. User Profile Management. Hybrid user profiles are a management feature that allows users to customize only "IT authorized portions" of their Windows User Profile.</p> <p>All unauthorized changes to the User Profile are discarded at logoff. Administrators can specify for which users, and on which Terminal Servers or desktops the settings apply.</p>	<p>This management feature provides consistent working environments, lightning fast logons and users own customized application settings.</p> <p>This eliminates calls to the helpdesk regarding issues like:</p> <ul style="list-style-type: none"> • Incorrect default printer • Slow logon • Wrong Application Settings • Can't logon due to corrupted User Profile <p>User Profile Management allows users to access their desktop and application settings regardless of which system they access, as authorized by IT. This allows for temporary assignment of desktops without using Roaming Profiles.</p>
<p>6. Task Automation. Task automation is a framework that allows IT to schedule the following types of tasks against virtual and physical PCs:</p> <ul style="list-style-type: none"> • Power Management – power on, power off, reset, suspend, resume, sleep, wakeup. • OS Operations – logoff, reset session, restart o/s, shutdown o/s • VM operations – Delete VM, Delete AD Computer Account, Delete VM not accessed in X number of days • Miscellaneous operations – copy file, enable/disable computer, initialize computer, run program or script on computer • MSI Tasks – install, uninstall or update MSI package 	<p>Without vWorkspace Task Automation, IT would have to script these functions, or perform them manually. Neither of these options is better than what IT doing now and neither are centrally managed.</p> <p>Applications would have to be installed manually, via 3rd party application, or via Group Policy.</p> <p>Power Management operations can otherwise only be performed via SDK.</p> <p>Deletion of VMs not accessed in X number of days of days is of importance because users typically ask for resources, access them for a while then stop using them. This feature can automatically delete VMs and the associations AD Computer Account when a VM has been idle for the specified number of days.</p>

<p>7. OS Management. vWorkspace offers the following features (not related to the hypervisor) to ease the management of the desktops.</p> <ul style="list-style-type: none"> • MSI package deployment • management of the local administrators, power users and remote desktop users groups • date and time access control • GUI sysprep editor • Active Directory Computer Account creation and deletion 	<p>Similar to task automation, these features could otherwise only be done manually or via script.</p> <p>Active Directory computer accounts would have to be manually pre-staged, or created in the default Computers OU. Because VMs could be dynamically created, leaving them in the Computers OU, or creating the accounts manually is not an option.</p> <p>Deleting Virtual Machines would not delete the associated computer accounts</p> <p>Applications would have to be installed manually, via 3rd party application, or via Group Policy.</p>
<p>8. Terminal Services Load Balancing. vWorkspace offers granular, intelligent load balancing of terminal services sessions and applications for Windows 2000 Server, Server 2003 and 2008</p>	<p>vWorkspace offers administrators the ability to load balance Windows Terminal Servers using any combination of the following workload evaluators:</p> <ul style="list-style-type: none"> • Context switches /sec • CPU Load • CPU Queue Length • Disk Load • Disk Queue Length • Interrupts per second • Memory Load • Memory Pool Pages Bytes • Number of processes • Number of users • Page faults per second • Pages per second • Redirector current commands <p>The default “number of users” evaluator works fine in a simple load balanced terminal server farms, but the other evaluators are often required as Terminal Server Farms grow in number of applications, servers and types of users.</p>

<p>9. Broad client support. vWorkspace clients exist for Windows, Windows CE, Linux, Java, Wyse Thin OS, Sun Microsystems Sunray, and Linux PXE, USB and CD boot. vWorkspace also provides an AJAX powered ASP.net Web Portal that provides connectivity via Windows or Java Web Client as well as clients for most thin client devices.</p>	<p>Without support for a wide range of client devices, IT budgets will be squandered replacing current, working hardware with devices that work with a less flexible connection broker. Because vWorkspace offers a PXE Boot Client, legacy PCs can be repurposed as diskless thin clients, extending their lifespan and reducing to the cost of the standard desktop refresh cycle.</p>
<p>10. Integration with Expand Networks and Cisco bandwidth optimization appliances. The vWorkspace management console offers a single click setting to configure RDP Settings for integration with Expand Networks and Cisco Bandwidth Optimization and QoS Appliances.</p>	<p>Without this functionality, IT would have to manually set RDP Security Settings on each Virtual or Physical Machine and on each RDP Client.</p> <p>This saves IT hours of labor, and provides a single click method of turning this functionality on or off without having to visit the client device or re-configure the Virtual or Physical Desktops.</p>

PRINTING FEATURES

The following are features of Print-IT, the vWorkspace Universal Printer Driver.

Printing Features	Value-add
<p>1. End-to-end Universal Printer Driver. Print-IT is a 6th Generation Universal Printing Solution that debuted in 2001. It supports all three different modes of printing without installing any printer drivers on the Windows Terminal Server, Virtual Desktops or Physical Desktops:</p> <ul style="list-style-type: none"> • Client Printing – printers defined on a Windows Client can be (if authorized by the administrator) auto created in the user’s session. Per-session bandwidth can be controlled by the administrator, as can the compression level. • Network Printing – printers from a Windows Print Server can be imported to a Print-IT Server. These printers can be assigned to user’s Terminal Services Sessions via policy or Virtual or Physical PCs via logon script. The compression level, share name and print data format are defined by the administrator. • Remote Print Relay – network printers from a remote office can be imported to a Print-IT Server where they can be assigned to user’s Terminal Services Sessions via policy or Virtual Desktop via logon script. Bandwidth available from the Print-IT Server to the remote print relay can be defined by the administrator 	<p>For administrators not familiar with Windows Terminal Services, printing is typically an overlooked necessity of application delivery or desktop virtualization. For Windows Terminal Services a Universal Printer Driver is necessary because many printer drivers are not stable on this multi-user platform, causing system instability. For both Windows Terminal Services and VDI, administrators rarely know what print devices end users have, and can’t install every driver in existence on each host. Additionally, users often are connecting over low bandwidth connections, or shared WAN links where printing a large document could impact the performance of the system, and other services.</p> <p>For remote offices with network printers and thin clients, there is typically no way to install the printers on the thin client devices.</p> <p>In a VDI deployment where desktops are temporarily assigned to users, it would be virtually impossible to support printing without a universal printer driver, as users are typically connected to a different desktop at each logon, and drivers that would be installed by the helpdesk in one session would not persist to the next.</p> <p>Print-IT addresses all of these issues allowing users to print to any printer using a single, battle tested universal printer driver. This dramatically reduces or eliminates printer related helpdesk calls and preserves precious bandwidth.</p>

SECURITY FEATURES

This following are security features of Quest vWorkspace.

Security Features	Value-add
<p>1. SSL Gateway. Secure-IT is a service that is included with both Desktop and Enterprise Editions of Quest vWorkspace. Secure-IT is a Windows Service that acts as an SSL Reverse Proxy for Web, RDP and Connection Broker communication. This means that untrusted clients can connect to the vWorkspace infrastructure via Secure-IT, which is typically deployed in a DMZ. The only port that needs to be open to the untrusted network is port 443. Since this is the default port for HTTPS and SSL communication, it allows users to securely connect to the vWorkspace infrastructure without have to reconfigure their client or corporate firewall rules. Secure-IT can front-end Web Access, the vWorkspace Web Portal, or the connection broker. This means that Secure-IT can be configured to support web, Windows AppPortal or vWorkspace-enabled thin clients. Secure-IT is an optional feature that can be replaced by organizations with investments in SSL VPN hardware.</p>	<p>It is a challenge to provide remote access to Windows Terminal Servers, VDI and physical desktops without compromising security.</p> <p>Quest provides a Reverse SSL Proxy that allows administrators to provide access to any Quest vWorkspace managed desktop or Terminal Server over HTTPS.</p> <p>This means that remote access may be granted without opening ports in the corporate firewall from the public Internet to the private network, and that users can access corporate computing resources without having to alter firewall rules on their client or at the remote network firewall.</p>
<p>2. Authentication. vWorkspace Clients support explicit, pass through, Kerberos, Smart Card and CAC authentication.</p>	<p>Enterprise deployments of Terminal Services and Virtual Desktops need to satisfy the requirements of several access methods, where different authentication requirements are introduced.</p>

<p>3. User Environment Configuration and Lockdown.</p>	<p>Securing the user environment on Windows Terminal Services often involves Group Policies, scripting, registry import/export, and manual configuration.</p> <p>The vWorkspace Management Console provides administrators with a single point of configuration to:</p> <ul style="list-style-type: none"> • Map Network Printers with a single Universal Printer Driver • Map Network Drives via NET USE or SUBST, and optionally with alternate credentials. • Remove clutter from user’s desktops • Restricting access to local or network drive letters • Restrict users to administrator approved applications that may be launched only on an administrator approved schedule. • Restrict users to administrator approved websites and TCP Ports. • Run logon scripts that only apply to Terminal Server Sessions. • Map users to the correct Time Zone • Intercept applications that require a user to be an administrator or power user and redirect the application to write to user portions of the registry or file system where administrative permissions are not required. • Add or delete registry entries or keys • Set the Windows Color Scheme • Set the Desktop Background • Configure applications to use a unique IP address when necessary
<p>4. Windows Group Membership Management.</p>	<p>Management of the local Power Users, Administrators and Remote Desktop Users groups is difficult in environments where users may be logging onto different computers. vWorkspace dynamically manages the membership of these groups without scripting or Group Policies.</p>

CLIENT EXPERIENCE FEATURES

Quest Software is the only VDI and Terminal Services vendor that is both a licensee of the Microsoft RDP Protocol Specification and extends RDP features to dramatically improve all aspects of the end user experience. The following are client experience features that Quest has added to the Microsoft RDP Protocol.

Client Experience Features	Value-add
<p>1. RDP Protocol Graphics Acceleration.</p>	<p>This unique feature not found in any other product provides unprecedented performance and end user experience over even low bandwidth connections.</p> <p>This is of particular importance for WAN or Internet connected clients, or those needing to use programs such as Acrobat, AutoCAD, Flash, Photoshop, PowerPoint, Silverlight... or other programs that are highly graphical in nature.</p> <p>Quest's has extended the Microsoft RDP Protocol to reduce bandwidth requirements and provide an excellent end user experience when connecting to Terminal Services or Virtual Desktop sessions.</p>
<p>2. Enhanced Multi-monitor support</p>	<p>The standard Microsoft Remote Desktop Client and VMware View Clients support spanning the client display across multiple monitors, but do not do anything for:</p> <ul style="list-style-type: none"> • displays of different resolutions or configuration • maximizing applications on specific monitors • pinning the start menu and task bar to the primary monitor

<p>3. Seamless Windows</p>	<p>For users with rich client workstations, a second remote desktop can cause confusion.</p> <p>Quest extends the Microsoft RDP Protocol to allow the administrator to publish individual seamless applications that look and act as if they are running locally on the client. This feature is available for Windows Terminal Services, Virtual and Physical Desktops.</p>
<p>4. Local Text Echo</p>	<p>When working over a latent network connection typing can be challenging because each keystroke is sent across the wire, and is not displayed until it has been received by the RDP Host. This can cause one's typing to words or sentences ahead of what is displayed on the screen.</p> <p>Local Text Echo displays the keystrokes locally on the client when a latent network connection is detected, instead of waiting for them to be received by the remote RDP host.</p>
<p>5. Multimedia Redirection</p>	<p>Windows Media Player content is problematic when rendered via Remoting Protocols like RDP or ICA. It's not possible to deliver the high frame rate that's necessary to provide good performance and end user experience.</p> <p>With this in mind Quest has extended the Microsoft RDP Protocol to redirect Microsoft DirectShow content to the client where it is played with the local CODEC in full fidelity. This provides a local end user experience without taxing server resources to render the multimedia content.</p>

<p>6. Bi-directional Audio</p>	<p>The Microsoft RDP Protocol is capable of only sending audio to the client device, but has no support for client to server audio, which supports microphones.</p> <p>Quest has extended the RDP Protocol with bi-directional audio to support microphone redirection, so one can support voice recognition applications.</p>
<p>7. USB Device Redirection. The ability to support any Windows or Linux client connected USB Device, for example:</p> <ul style="list-style-type: none"> • VOIP Microphone / Headset • Document Scanner • Webcam • Any other device 	<p>Standard USB device support when connected via RDP is limited to mass storage devices and printers.</p> <p>Quest’s USB Device Redirection adds USB over IP support for any client connected USB Device.</p>
<p>8. HP RGS Support. Quest vWorkspace offers the option to broker connections to HP RGS Hosts from HP RGS Receiver Clients.</p>	<p>HP’s RGS (Remote Graphics Software) is a full featured remote display protocol that is well suited for use by professional graphics designers, computer aided designers or engineers that require an uncompromised computing experience. RGS typically requires a LAN speed network connection to provide access to this content.</p>