WHITE PAPER

Virtual Desktop Infrastructure

A Guide to Implementation Best Practices

vmware®

LONG VIEW

Contents

Introduction

Virtualization is a trend that is changing the way that organizations approach IT. The aim is to insert a virtual layer that allows us to obscure the physical components of the infrastructure and simplify interaction between users, applications and physical infrastructure. Over the last few years, virtualization has really taken off in the datacenter space because of the tremendous savings in hardware, space, power and cooling. One reason for this is that most systems running in the datacenter are underutilized and the applications used are, for the most part, not interactive via the keyboard and monitor attached to the servers - instead they are generally accessed by client side applications via the network. Now that server virtualization is becoming mainstream, organizations are revisiting the use of virtualization to deliver desktop applications for users. There are many benefits to virtualizing desktops including simplified management, data security, secure remote access and reduced hardware costs. All of these, coupled with the increased hardware requirements for Microsoft's new desktop operating system, are driving customers to take an opportunity to evaluate their options when it comes to upgrading to Vista.

Virtual Desktop Infrastructure (VDI) is a technology based on multiple existing solutions to achieve access to a "virtual" desktop infrastructure. It is not a stand-alone product, but rather a concept or solution that links components together. Traditional client computing models have put the desktop PC at the client-side. This provides the user with a familiar, full-power computing experience with applications, processing and data storage all located on the desktop. While this model has become increasingly popular as hardware prices have declined over the last decade or more, security and manageability of the individual desktop remains a major cost and issues in the form of security and manageability.

About this White Paper

This white paper addresses the challenges involved in designing and deploying, managing and scaling a Virtual Desktop Infrastructure (VDI) solution. The paper is designed to act as a practical guide to solving both business and technical challenges that customers will face when deploying VMware Virtual Infrastructure to provide desktops to users. This paper assumes that the reader is familiar with the concepts of a VMware virtual infrastructure – namely Virtual Center and the ESX Server hypervisor concepts.

About the Long View and VMware Partnership

Long View Systems, a VMware partner since 2002 and one of the original PREMIER partners, has been an industry leader in helping to drive the adoption of virtualization in North America. Long View is a GOLD Level VMware Authorized Consulting (VAC) Partner and was selected in 2006 as VMware's Technical Partner of the Year for the Americas. Long View has consistently developed great solutions for its clients based on proven consulting methodologies and has been a pioneer in the virtual desktop space. Long View first became involved in the deployment of virtual desktop solutions more than 5 years ago - in fact, they presented a solution on "Enterprise Hosted Desktops" at VMworld 2005 – and before VMware started to position and market VDI to the world. Long View has a tremendously deep and experienced team and has translated their vast

experience in Server Based Computing and the Virtualization space to become leaders in this emerging technology area.

Definitions related to VDI

Connection Broker – At its most basic function, a connection broker is a software component in a VDI solution that acts as a traffic cop to determine who a user is and which VM's they have access to. Once a user has been authenticated and the policies enumerated to determine their access options, then they direct a user to a desktop VM for connection via RDP. When evaluating connection brokers, you should consider a number of things, including:

- User Management and Resource Entitlements (i.e. which users have access to which desktop pools)
- Session Management (i.e. which desktops are in use, logged on but idle, idle, disconnected, etc)
- Virtual Machine Lifecycle Management (i.e. provisioning and decommissioning VM's based on usage and capacity policies)
- Virtual Desktop Pooling (i.e. grouping image types and application sets together to provide access based on group membership)
- SSL Gateway (i.e. encrypting traffic travelling on untrusted networks such as the Internet)

Thin Client – a scaled down PC with no moving parts that is typically used to connect to a Terminal Server to display the users applications

Virtual Desktop – Typically this is a Windows XP or Vista desktop that is installed and running on a Virtual Machine in a centralized datacenter on top of VMware Virtual Infrastructure

ESX Server – This refers to a physical server running the VMware ESX hypervisor and is used to host the virtual desktops.

Presentation Protocol – Typically RDP is used, but this refers to the protocol that is used in a Virtual Desktop Infrastructure to display the output of a users virtual desktop session running in the datacenter. It provides output (video, audio, etc) and accepts input (keyboard, mouse, etc) to conduct a virtual desktop session.

Challenges of Implementing and Managing a Virtual Desktop Solution

Application Support – What if my app doesn't run in Terminal Services or Citrix

One of the biggest reasons for running applications in a virtual desktop environment versus a Citrix/Terminal Services environment is that most applications are not designed for a multi-user environment. The majority of application developers expect that everyone has the same environment as them - i.e. administrative rights to a system that no one else uses. When you try to have multiple users logging on to a system, it can cause a lot of issues if the application wasn't written following Microsoft's recommended best practices (i.e. separate locations for system and user data spaces, file locking issues, and an inability to customize configuration file locations are just some of the challenges presented by a TS environment). By adjusting the model to more closely mimic a standard desktop (i.e. a 1 to 1 relationship between logged on users and operating systems) we can address the majority of these issues. In addition, by changing the operating system from a specialized Terminal Services version of a Windows Server OS to a standard desktop OS, we drastically increase the number of applications that will be supported by vendors who have previously balked at supporting their applications running in a Terminal Services or Citrix environment. On top of this benefit, by sticking with a commodity desktop OS, organizations are able to leverage existing tools and application management packages and procedures that are already in place to manage the application deployment aspect of supporting a VDI infrastructure - thus further driving down the costs by simplifying the people side of the support requirements.

Remote Display Protocols – Graphically Intense Applications

Another challenge with this type of solution is that graphical operations are executed on the centralized VM and need to be "presented" on the end-point device. That means that the output needs to be compressed and sent over the wire to the client side device. This can present some challenges with certain applications that require either specific hardware (such as 3D or OpenGL graphics) or are graphically intense with a lot of screen refreshes. For WAN or remotely connected users, this needs to be a consideration when sizing the bandwidth required to ensure a suitable user experience. This is an area that is evolving quickly and there are some 3rd party solutions available to help with this in addition to steps that VMware is taking to improve the overall user experience and to broaden the spectrum of applications that are suitable for a VDI environment, but some applications are just not a fit as things stand today.

Offline Use - Can I get that to go?

One of the biggest challenges with providing users with a secure, centralized environment to access applications is in regards to how to handle mobile users. Mobile users form an ever-increasing percentage of the population and are providing ever-increasing headaches for the security teams who are tasked with securing and managing the flow of data within an organization. More and more often when watching the news we are seeing examples of companies that have gained notoriety (and not the good kind) for falling victim to the challenges of securing data for mobile workers. It is becoming a

regular occurrence to read stories about how laptops are being stolen that contain sensitive customer and employee data. A centralized solution does a great job of keeping the sensitive information in the secure data center (only the images of the screen are presented to the client - not the actual data), however how do you handle that portion of the user base that require mobility AND access to data? In some organizations that have chosen to deploy VDI, wireless and cellular networking technologies are helping to solve these issues, however they still require that users have some form of connectivity back to the “Mother Ship” in order to provide access to applications and the documents and spreadsheets that so many of us rely on to be productive. What about the truly offline users? While rumors of internet access on airplanes looks to become a reality in the coming years, there are still a number of situations whereby a user might require offline access of their applications and while solutions exist today for "checking out" a virtual desktop to take on the road, they are not yet as elegant and robust as most IT organizations would like.

Local Devices - how do I synch my iPod or upload pictures from my camera?

Another challenge that is often overlooked is the concept of peripherals. With the virtualization of server workloads such as File, Print, SQL, and Exchange IT administrators don't have to worry about connecting local serial and USB devices such as printers, thumb drives or PDA's. When you want to virtualize a user’s desktop, you need to take into account the applications that they are using and ensure that you provide a solution for the most common devices that users connect to their PC's. The majority of new peripheral devices being produced today are using the USB interface to connect so that is something that will need to be solved in order to be able to effectively deploy virtual desktops for anything other than the most basic type of user. A key aspect of being able to connect and use peripheral devices such as USB (besides ensuring that the client-connected device is seen from the centralized virtual machine) is to ensure that the drivers are available and that users can connect a device and have the drivers installed automatically without intervention by an administrator.

TCO and ROI - When do the savings start?

Right now, the majority of VDI implementations are not just about saving money - at least not on the scale of savings when compared to virtualizing the servers in their datacenters. Today's deployments are generally more about providing secure remote access to data and applications that are running in the datacenter or allowing outsourcing partners to gain access to your infrastructure without compromising security or regulatory compliance issues. This trend is changing however as organizations begin to look at rolling out Windows Vista and determine what the hardware requirements are for them to run it, or whether or not their applications are compatible with it yet. Most organizations are looking at this as an opportunity to test the waters to see if there is a better way to solve this problem and many of them are turning to VDI as a possible solution. Besides the potential hardware savings, VDI provides for reduced support costs due to needing fewer desktop support resources in the field (as all desktops are housed in central datacenters, the support staff can very easily work remotely and shadow users sessions to troubleshoot issues). In addition to the centralization of support resources, virtualization provides some great functionality that is quite difficult to achieve with physical hardware in that virtual desktops can be destroyed, recreated and redeployed in seconds by support staff without visiting a user’s desk. Troubleshooting

time can be minimized and after a period of time, the faulty desktop can simply be destroyed by deleting it - a virtual machine is just a file. The user simply logs out and when they log back in, they will be given a fresh new desktop that allows them to continue working. All without a visit to their desktop to swap out hardware (or the time required to re-image a system for those organizations that employ network based image deployment. This results in a huge increase in productivity for users while reducing the cost to support each user. Additional savings can be realized through potentially reduced licensing costs, but this should not form the basis of your TCO argument as each vendor's licensing models are different and are subject to change.

A key aspect of measuring ROI is to conduct proper planning up front before the Design phase of the implementation. It is only with proper sizing and measurement exercises that you can achieve a realistic determination of the hardware, software and services required to implement a VDI solution. One important thing to note is that while you can get a good estimate of the physical requirements of the solution, the perceived performance from an end user is dependent on the applications being delivered and the quality of service of the network transport (i.e. bandwidth and latency). Utilizing tools such as VMware's Capacity Planner or Platespin's PowerRecon can make Capacity Planning a relatively pain-free process. These tools benchmark a physical environment to determine, based on configurable guidelines, how a set of desktops will "stack up" on physical host servers in a virtual infrastructure. These real-world performance figures provide the organization with a better understanding of the workloads being performed on client devices in their environment. While there is no cookie-cutter method for architecting a VDI solution, the infrastructure required to host it generally is predictable using these types of tools and methodologies. The overall design depends on a lot of variables such as the software footprint, connection broker used, the type of thin client used, network architecture and performance, etc. There also are not a lot of tools for properly measuring all of the different models. A real world measurement via a professionally conducted proof of concept is the best method to truly determine which components are required for your environment. Some things to consider when performing capacity planning:

Paradigm Shift - Changing User Habits (and Administrators too)

For some reason, users get quite attached to their PC's. They curse them constantly whenever something is not working, but the minute you try to remove it from under their desk they seem to take a very different approach and really struggle with potentially swapping it out for a thin-client or repurposing it in a thin-client type of configuration. The key to this is to spend some time up front on the design to ensure that you are providing the same functionality. Their attachment is not to the device itself, but to the way in which they do their jobs today - proposing changes to something they barely tolerate today needs to be done carefully and deliberately. If you properly evaluate the way in which they use their systems, there are very few situations where you can't find a method to replace that functionality in a thin client or VDI solution - but it's always better if you build it into your design up front. Users still want to be able to do the same things as before and many of them don't necessarily correlate directly to a business purpose (i.e. listen to CD's, synch their mp3 player, watch video's their friends have emailed to them, etc), but if you don't try to accommodate some of these things, you'll likely have a workforce looking for a mutiny against the oppressive regime that decreed VDI upon them. The good news is that many of these types of non-business related issues also correlate to actual business functions as well (i.e. loading vendor data CD's, synchronizing USB devices such as PDA's, reviewing training videos, etc). If you can

approach the problem with a solution of replacing functionality, rather than taking something away from the user, then you are much more likely to have a successful VDI deployment. The other major type of change that's required is in how we as systems administrators design the user experience. If we can keep the basic look and feel to be as close to what they were used to as before, then users will not notice much change and will likely not take much of an issue with it. By matching the experience with regards to signing on, logon times, persistent user settings across logons, you will be in a better position to make the transition to VDI as seamless as possible for users. It does require planning though - especially with regards to roaming profiles and the locations to which users and applications save data to. Solving these two issues, along with ensuring users can print, will go a long way to providing the same or better user experience.

Printing – But I thought it was a paperless world

Without a doubt, one of the largest challenges of a thin computing solution is allowing the users to print to whatever their preferred local printer is. Depending on the use case for VDI, this can range from simple to complex, but the good news is that it is still simpler than in a Terminal Services or Citrix environment because the drivers don't have to be multi-user aware and because VDI uses a desktop OS (compared to a Windows Server OS for Terminal Services), the native drivers for most printers can be installed a lot more easily than before. The challenges that remain are allowing the user to print and set the properties that they want for the print job (such as duplex, collate, & tray selection) and to ensure that the print job travels to the printer as efficiently as possible (i.e. not in a bloated RAW format). There are numerous third party solutions available to simplify and optimize the printing process for users. As with any local devices, the drivers need to be installed in the centralized desktop VM.

Windows Licensing - Bill's got to eat

This is one of the questions that I am asked most often when discussing VDI solutions with customers. Unfortunately Microsoft's licensing policies were difficult enough to interpret prior to virtualization, but they are constantly changing right now and hopefully once Microsoft's Hyper-V product finally becomes GA (general availability in development lifecycle terms), maybe then they will provide a simple and fair licensing policy with regards to virtual desktops for all customers. As the policy seems to be in a near constant state of flux, I will not dive into it here, but rather I will provide a link to the Microsoft site in the hopes that this white paper can remain relevant without requiring constant updates to this section. The one thing I will say is that I have yet to see Microsoft allow any of Long View's customers to "convert" OEM licenses that a customer purchased with their existing desktop hardware over to a license that is usable within a VDI virtual machine.

At the time of writing this, the relevant Microsoft document is titled "Licensing Vista for Use with Virtual Machine Technologies" and can be found on the Volume Licensing Briefs site located here:

http://www.microsoft.com/licensing/resources/volbrief.mspx

Application Lifecycle Management – one of the largest IT budget items

No matter whether you are deploying physical or virtual desktops, Configuration Management is something that cannot be overlooked, but it is even more important if you are deploying virtual desktops and you want to pool your resources to achieve cost savings. The nature of pooling or sharing desktops means that each user does not always log on to the same virtual desktop each time they log in and as a result, organizations need to properly plan for this version of musical chairs. It is absolutely critical when using pooled VM's (sometimes called dynamic pools) that you have a method of deploying applications and settings to users that is fast, robust and automated. Application installs should be seamless to the user and if possible, applications should be pre-staged to speed deployment and minimize the impact to the users. One of the challenges with pooled VM's is that as the pool of user applications grows, the potential for issues and conflicts within the environment increase considerably due to the complex dependencies that many applications have. If organizations were to properly build, test, stage and regression test all applications before deploying them (or upgrading them), this would be an extremely cumbersome and time consuming task (not to mention a technically monumental task). But alternative paradigms to installing applications have been developing quickly over the last few years and solutions such as Thinstall (VMware), SoftGrid (Microsoft), Ardence (Citrix), SVS (Symantec/Altiris) with AppStream are changing the way that applications are deployed to users and the idea is gaining credibility as a result of these players being swallowed up by much larger organizations that are looking to integrate these solutions into their application delivery frameworks.

Designing, Deploying and Administering VDI Solutions

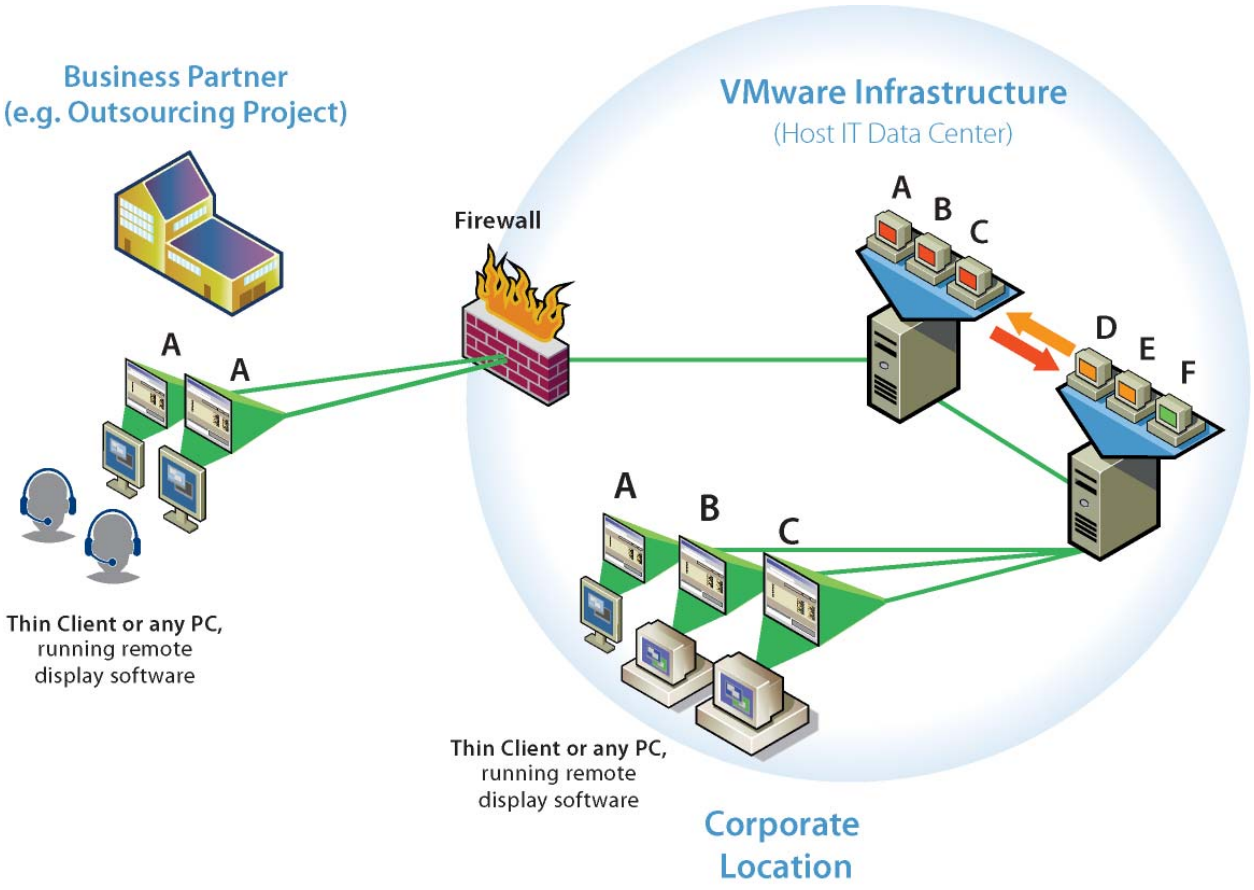


Figure 1. Example Use Cases for users connecting to Virtual Desktop Infrastructure

Strengthening Security

For an external deployment use case, security is going to be a pretty big concern for most organizations. Some connection brokers come with a built-in method for securing the logon and traffic. In other cases a third party VPN will be necessary. This is something that you should definitely keep in mind early on, especially when selecting a thin client device and operating system.

Consider a broker with built in encryption to save the overhead of managing access to an intranet through VPN client software if the client doesn't already have a VPN solution (this is especially relevant when using thin clients as the VPN client software is often not compatible with the Thin Client OS - VPN Client compatibility with Windows XP doesn't necessarily mean compatibility with Windows XP Embedded – the standard OS on Windows based thin-clients).

Network Transport Security – for most organizations, simply encrypting the traffic with Industry Standard SSL encryption is likely to be good enough, but for those that are overly paranoid (or have security policies requiring it), you can encrypt the traffic every step of the way using standard IPSEC encryption in Windows. Keep in mind that this is going to add overhead on the CPU of every virtual machine and thus every ESX server.

I would not recommend using this unless you require it – most organizations don't encrypt traffic on their internal LAN today, so it should be perfectly acceptable to terminate the SSL encryption at the point of entry into the network (generally the DMZ).

Information Security – By the very nature of using VDI or Terminal Services, you are strengthening the security of your environment compared to allowing users to store corporate data on their desktop or laptop hard drives. By controlling where the data resides and what is allowed to leave the data center, you can avoid having sensitive information fall into the wrong hands. Be careful when setting policies around what type of client device mappings (such as local USB devices and hard drives) you allow your users to connect. There are group policy as well as third party solutions available that will allow you granular control over what types of devices users can connect (i.e. USB printer is fine, but a thumb drive is not).

Storage Options for VDI

Like all Virtual Infrastructure deployments, you should strongly consider using centralized storage to take advantage of the functionality provided by features such as VMotion, HA, DRS and DPM to improve efficiencies and decrease costs. Desktops typically don't have a high amount of disk I/O when compared to servers and thus don't necessarily need to be delivered on a high-end SAN infrastructure in order to gain access to these features. By leveraging technologies such as iSCSI and NFS, coupled with larger/cheaper SATA drives to deliver datastores to the ESX Servers, it allows organizations to reduce the infrastructure components required and cut costs. Given that each desktop typically will need about 8 GB of disk space, the storage infrastructure can quickly become cost prohibitive if you try to just extend your Virtual Infrastructure storage platform for use with VDI. Other areas that should be given consideration to drive even further cost savings include thin provisioning, data de-duplication and Volume or LUN cloning. A quick explanation of how to use these advanced storage features is explained below:

Thin Provisioning – if you follow best practices and keep about 20% of the space on a file system available for unexpected data growth, this leaves you with disk utilization that looks something like this:

> If all VM virtual disks are at 80% capacity AND
>
> All VMFS Volumes are at 80% capacity THEN
>
> Your true storage utilization is 64% at best (not including overhead and RAID).

Thin Provisioning allows the provisioned yet unused storage capacity to remain in a global storage pool, thus increasing your capacity available and/or decreasing your capacity requirements.

Data De-duplication – Given that in a VDI environment you are deploying mirror image VM's from a standardized template, the vast majority of the information in the VM's are redundant. By eliminating all the redundant data through de-duplication of the primary file systems, you can typically achieve a 50% or more reduction in the storage capacity required to support your virtual desktops, which significantly decreases the TCO and increases the ROI of the solution.

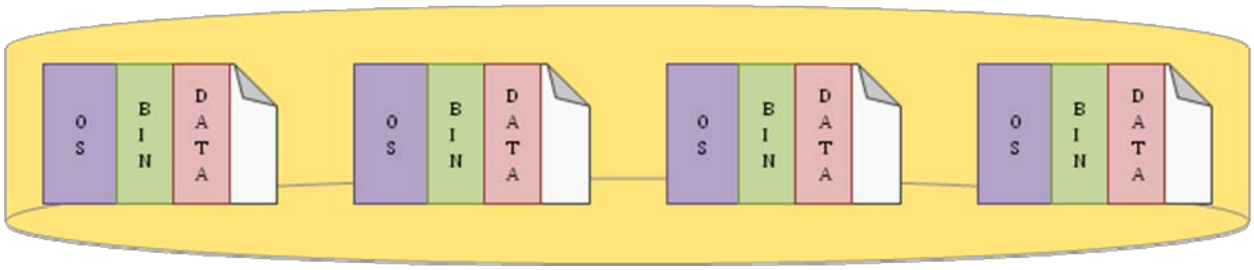


Figure 2. VMFS Volume with 4 VM's (each with OS, Application Binaries, Data and Free Space)

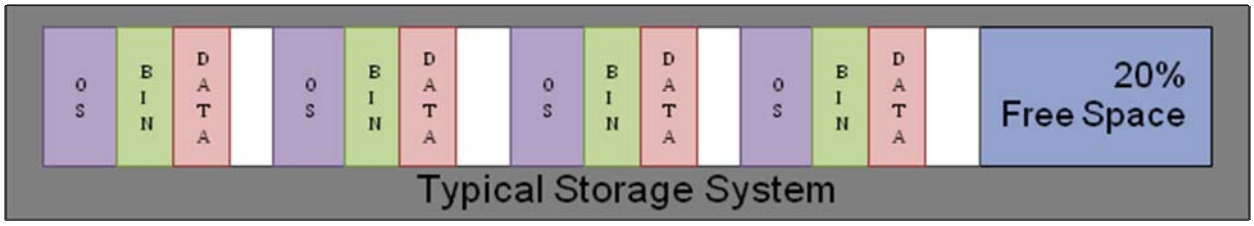


Figure 3. Data Layout of a Typical Storage System Using VMFS

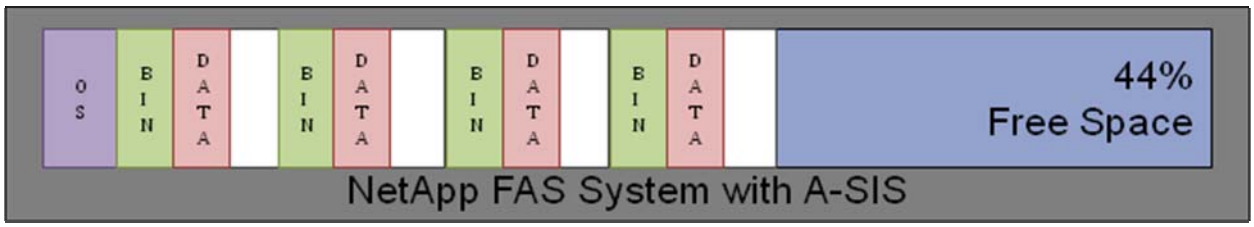


Figure 4. Example of a VMFS De-duplicated VMFS File System that yields 30% increase in storage capacity

Volume or LUN Cloning – Many storage arrays provide the ability to clone and "fork off" a LUN or Volume to allow you to take a snapshot copy of an existing file system and provide a writeable snapshot of that file system to your ESX Server Cluster. The concept is very similar to that of linked clones that are used in VMware Workstation and Lab Manager in that writes for each "copied" volume are written to a different location and the reads reference the "differencing disk" first, and if they don't find the block they are looking for they then look to the original read-only snapshot of the file system. This allows you to provision a lot of virtual machines very quickly (groups of 10 or more at a time in a few seconds to minutes) without taking up much additional disk space on the storage array.

In the example below, the base disks might be 10 GB each, but the "differencing disk" represented by VM1-VM9 may only be a few hundred megabytes in size. Thus in this 9 VM example, if you were to assume a 10GB base disk, 9 VM's would normally require 90 GB of storage. Using Volume/LUN Cloning features you would only need 32.7 GB ((10GB x 3 base disks) + (300MB x 9 differencing disks)). There are some caveats to keep in mind when using Volume or LUN Cloning in that each ESX server can only support up to 256 LUN's, so you may want to group your ESX hosts into clusters based on storage presentation, as well as determining/adjusting the optimal number of VM's to house on an individual "Template VMFS Snapshot" (i.e. 5 VM's per Template VMFS X 256 snapshots = 1280 usable virtual machines). You may need to include 10, 50, 100 or more VM's into the Template VMFS. One other key thing is that because array based cloning tools are typically block based, they don't leverage tools such as Microsoft's Sysprep utility to properly clone the Windows desktop. This can be worked around by creating a single VM and running Sysprep on it, but not powering it up. This way all of the "base disk" VM's are going to run through the Sysprep process when they are powered on and they will all be given unique SID's. You'll want to have a method for auto generating machine names, etc to avoid having to do this manually.

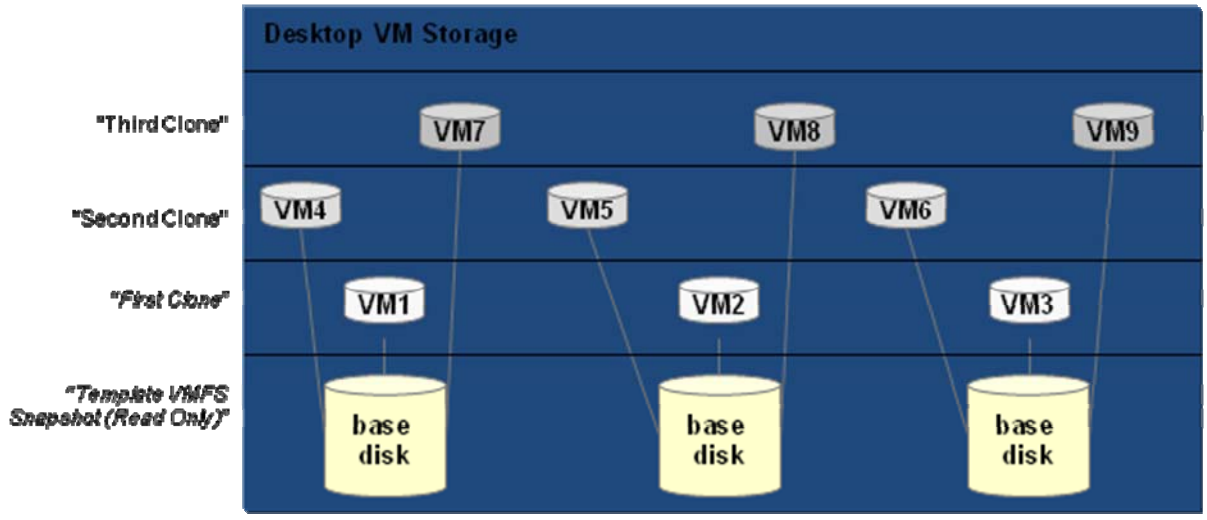


Figure 5. Array based Volume/LUN Cloning Example

Optimizing the user experience

Local Device Support

USB Devices – USB has quickly become a standard for connecting peripherals to users' desktops. From scanners to thumb drives to cameras and printers, USB support is a critical aspect of a Virtual Desktop Infrastructure. USB connections need to be seamless to the user and hopefully just function in the same method they would if a user plugged in a USB device to a traditional desktop. The key to this is to ensure that the drivers for the majority of the device types are pre-installed in the desktop image, or can be easily installed by the user without requiring intervention by the service desk. RDP 6.0 provides support for USB devices, so it is generally a matter of ensuring that the drivers are available in the virtual machine. Given that it is impossible to predict all the devices a user might plug in, there are two ways to handle it. The first method is to standardize on supported device types and to stick to supporting only those devices as much as possible. The other is to provide a method that allows users to install the drivers themselves providing that they have access to the drivers from the desktop VM. In general, standardization is the way to go, but there will always be exceptions so it's best to plan for this up front to determine a methodology to allow users to download the drivers into the VM.

Printers – As discussed, printing is a critical aspect of the user experience so it is highly recommended to use some sort of universal printing solution such as those provided by Provision Networks, Tricerat, ThinPrint, etc to avoid having issues later. Whenever possible, employ network printers for devices connected on the LAN, and use client connected printers for devices connected over the WAN and Internet. This will typically provide the best experience overall and the lowest support costs associated with setting up and troubleshooting printers for users. Third party tools or Login scripts combined with group membership can be used to assign network printers to users (this is sometimes an acceptable solution for WAN printing, especially if third party tools are used to send the print jobs over the WAN in an EMF format rather than RAW).

Serial Devices – Some devices/applications still have a need to connect a client serial port to the remote session. This can be done by mapping the serial ports through the RDP virtual channel to allow communication with the serial attached devices. This can be useful for items such as bar-code scanners or point of sales devices that use COM port connections on the client side.

Local Drives – In some instances, organizations would like to provide their users with the ability to connect local drives such as a hard disk or CD/DVD ROM drive. This can be set easily through the policies of most connection brokers and presentation protocols. It can also be controlled through Active Directory Group Policies. Given that security of information is one of the biggest reasons cited for customers deploying VDI solutions, it's not recommended to enable these drive mappings by default. It is generally better to evaluate requests on a case-by-case basis and have clearly defined policies about which devices, users, client networks, etc can map their client side drives to store or retrieve data.

Graphics Display

Screen Resolution – this is not as much of an issue today as it had been in the past, but the ability to deliver different screen resolutions for the users will further enhance the usability of the solution from the users' perspective.

Multi-Monitor Support – similar to screen resolution, this is something that will enhance the user experience and provide them functionality that matches a traditional desktop deployment. It is highly recommended to perform a proof of concept to help ensure that you have chosen the right solution (specifically the combination of clients, connection brokers, and presentation protocols) to provide the necessary functionality. Some components have multi-monitor support in published app mode, but not in published desktop mode, which can be very confusing and upsetting once the mistake is realized. In addition to this, true multi-monitor support should include windows sizing and placement, message boxes that don't split windows, and actual multi-monitor awareness rather than just spanning multi-monitors but the users has to constantly fiddle with the window sizes and placement in order to be productive.

Multimedia – This is another area that needs to be planned and designed for up front. There are a number of solutions that can support rich media such as streaming video, but they are usually client hardware dependent so if you have requirements around this I strongly suggest that you evaluate products before purchasing to ensure that you have the right solution to fit your needs and your budget.

A solution such as Wyse TCX provides an enrichment component that gets loaded into the desktop VM as well as a client side component on the Thin Client to allow for both multi-monitor capabilities as well as rich audio and video streaming to provide a great user experience.

Creating the Users Application Environment

User Profiles

Profile Types

The three possible types of profiles available for use in a terminal services environment from Microsoft are local, roaming and mandatory roaming profiles. Which profile type an organization decides to go with will be dependent on the decisions made about the overall environment. Local profiles are used when the settings in the profile don't matter as a user roams from desktop to desktop. Roaming profiles allow user settings to be persistent across logins and across machines, ensuring a consistent user experience no matter which desktop a user logs into. A mandatory profile provides groups of users with a single profile and changes to the profile are discarded upon logoff. While each method has its own merits, I recommend using a third party hybrid profile solution that combines the speed and reliability of a mandatory profile while still allowing users to save their applications settings to avoid having to perform repetitive tasks such as setting which tray to print from, etc. Examples of this include FlexProfiles – an "open-source" adaptation of the Microsoft Office Resource Kit and the Provision Networks Profile-IT solution. The combination of hybrid profiles and group policies allows you to define the settings that must be in place as well as suggesting settings for users that can be changed later and saved across logins.

Profile Sizes

Care should always be taken when using roaming profiles as it can severely impact the logon times and performance that a user will experience. Generally, policies do not need to be set to restrict the size of a user's profile, but this generally only applies if certain steps are taken prior to the creation of a user's profile. Administrators have the ability to exclude folders from a profile, while redirecting others to the network, and using policies

to configure settings such as Temporary Internet File Settings to minimize the size of the profile. Roaming, Mandatory, and Hybrid Profiles should all be measurable in KB rather than MB. A properly designed and implemented profile solution will help to ensure quick logon times for users.

Profile Locations

The location of profiles is quite often set to be a network share and this setting is traditionally specified in the properties of the users account. For roaming profiles, this is an excellent solution, however, with a little preplanning, future growth and infrastructure changes can be accomplished with ease instead of requiring planning and resources. By specifying a variable for the users profile server, when the user logs on, it will read that systems environment variable and retrieve the profile from whichever location is contained in the variable. In an organization's initial deployment, this is not an issue because the profiles will reside on a file server, and all of the servers are located in one physical site. When it will make a difference will be when the profiles need to move to another file server (in the event of an upgrade) or when the desktop farm spans multiple sites (and users have the potential to access a desktop in either site – i.e. A Disaster Recovery Site). Using this method will ensure that the users profile is pulled down from the file server that is closest to the desktop that they are logging on to and will ensure the highest level of performance.

Pre-configuring Profiles

I recommend that an organization pre-configure the default user profiles that will be used to build all users profiles the first time that they log on to a system. This will ensure that users will receive the proper basic settings for their application and/or desktop environment, even in the event of a communication problem with the server that is storing the users current profile settings.

Profile Caching

By default, Windows will cache the profiles of users on the desktop even after the user has logged off. This speeds up subsequent logins because only the changes are retrieved from the server. If disk space or profile corruption becomes an issue, an administrator can set the desktops to delete the cached copy upon the user logging off. Given the number of potential users accessing a system, it is recommended to turn this off for dynamic pools – otherwise the registry will begin to bloat and could cause users to not be able to logon until the registry size limit is increased (which requires a reboot).

Group Policies

Group Policy Application

Determining what policies to use and who to apply group policies to is something that should be discussed prior to deployment. Will the policies be applied to all users, including administrators or will policies be configured in such a way that only certain groups of users receive them? It is recommended that at the very least, a group of test users exist to help determine if an application issue is related to a Group Policy or not. Each test user can have a different subset of policies that are applied to it (ranging from no policies to all policies) and this will allow administrators to troubleshoot more quickly and effectively.

Group Policy Settings

Policy settings represent the ability to edit the registry from a GUI and apply those changes to multiple users, possibly on multiple systems. Almost any type of registry setting can be specified in a policy. The default policies provided with Windows give access to the most often configured settings, but customized policy templates or scripting will give an organization the ability to include just about any settings they would like.

Data Locations

Saving Files Locally

While many organizations have already chosen to lock down the desktop to reduce or eliminate the ability for users to store data locally (where it cannot be easily backed up), many have not and users have often created their own filing system on the local hard drive. In a VDI environment, this is not an optimal solution because while you can do it (through static VM assignments and losing the expendable nature of VM's) you lose out on many of the benefits associated with centralizing your infrastructure with VDI. At the very least, you should redirect My Documents and educate users to use a network file share to save their data so that in the event of a users statically assigned desktop VM is undergoing patch maintenance that they will still have access to BOTH their applications and data. By leveraging the user's home drive to store this data, you allow both their settings and data to follow them wherever they may go.

Home Drive Size

The size of a user's home drive is not something that would need to be limited unless there is a shortage of disk space or corporate policies dictate the use of quotas. The Home Drive is the location where you would store most of the folders that you remove or redirect from the Users Profile. The reason for this is that the profile is copied down each time the user logs on, while the home directory is only accessed when required. By relocating or redirecting this to a file share that is accessible via the network, you will maintain a consistent user experience regardless of which desktop they log on to.

Home Drive Location

The Home Drive Location should generally be set in a manner similar to the User Profile location (using an environment variable) to ensure that the Home Drive is always located as close as possible to the desktop that they are logging on to.

Number of Home Drives

Setting the Home Drive location via the environment variable as mentioned above give an organization the flexibility to use multiple home drives with very little difficulty or changes required, should the need arise. This means that users accessing different types of desktops, or desktops in different locations, will not pull the home drive location from the users account properties in Active Directory.

Logon Scripts

Scripting Language

Microsoft has provided a free scripting language that is natively understood by the operating system and is extremely powerful, namely VBScript. VBScript requires no

user interface and thus does not give the user an opportunity to cancel or interrupt the script before it has completed executing. It gives administrators the ability to create login scripts that log information that can be very useful to support staff when trying to troubleshoot an issue for a user. Other scripting languages are available and an organization needs to determine what they plan to use as their Windows Desktop environment moves forward towards production.

Launching Different Scripts for Different Users or Servers

Consolidating the login script into one central location results in reduced administration and ensures that all users will be running the same script revisions. If specific settings need to be specified for users, groups, or servers, then this logic can be built into the script itself.

Launching Scripts

There are numerous ways to launch scripts, and this decision generally depends on the decisions made earlier in this section. Some of the options available are to configure a logon script in the users account properties, via the registry of each desktop, or via a group policy (can be either a user or machine policy or both).

Deploying and Managing Applications

Application Packaging

While most midsize to large organizations today employ the use of application packaging for the purposes of automated deployment, I feel that it still needs to be mentioned when discussing best practices. An increasing number of software vendors are providing their applications with installation routines that are based on the Windows Installer (MSI files). This allows for standardized installation, upgrade, patching and uninstallation routines that can be leveraged by the different application management platforms such as Microsoft SMS or Altiris. The biggest benefit though is that it gives administrators the ability to install software on desktops through a remote and unattended fashion. This is critical in an environment such as VDI where users are potentially logging on to different desktop VM's.

Application Virtualization

Due to the dynamic nature of VDI and the goal of driving efficiencies and cost savings, application management is such a critical aspect of the environment that is too often overlooked. The combination of different users with differing requirements logging on to differing machines can result in a tremendous amount of complexity with regards to application lifecycle management and compatibility issues. It achieves this by isolating applications and thus reducing the interaction between applications through the use of "bubbles" or "sandboxes" that allow users to read and write to virtual file systems and registries that are being redirected somewhere else. By using solutions such as Thinstall, SoftGrid and SVS, you can reduce a large percentage of the issues that you might come across in your environment. Application Virtualization is a topic that can easily take up its own white paper, so I won't go into too much detail here other than to say it should be seriously considered as part of the VDI solution.

Application Streaming

By coupling application streaming with application virtualization, you can get to a point where applications are never truly installed on the desktops, but the users still have full access to the functionality of the applications they require. This makes desktop pooling much easier which allows you to reduce the number of desktops that you require (effectively you are able to oversubscribe your desktops based on the numbers of concurrent users actually logged in and working). VDI, coupled with Application Virtualization and Application Streaming can truly enable the on-demand desktop. Application upgrades can be piloted side by side with the current version and once the pilot has been proven successful, you simply decommission the old application and the next time a user logs in, that application is no longer available to them and they would use the new version. This light switch upgrade capability is huge and allows for tremendous savings in support and regression testing. If a user is having problems with an application, they can simply re-stream it and get back to work.

Printing Architecture

Considerations

When discussing a Virtual Desktop implementation, the architecture and design work involved in customizing a printing solution is extremely important. Printing has a huge impact on performance and stability due to the nature of printing in a Windows environment, not to mention it is a critical aspect to the overall user experience. In the Windows printing process, when an application attempts to render a print job, it creates a non-printer specific Enhanced Metafile (EMF) that is then sent to the spooler and from there, it is rendered in a format specific to the printer being used (based on the driver in use). At this point, it is sent to the printer and the document is printed. The printing process in a VDI environment is not much different, however the raw spool file is sent to the printer via the RDP virtual channel to the client. When using the most Universal Driver solutions provided by third parties such as Provision Networks and ThinPrint, the process is much the same however, the output differs slightly. Instead of getting a large RAW spool file sent down to the client, a much smaller EMF file is sent across the network. This difference in size can have an impact on the performance over slow links due to the amount of data that print jobs contain. These third party solutions intercept the metafile and simply redirect it through the virtual channel to the client where it is sent to the spooler and rendered using the local driver on the client. Using one or both of these solutions increases performance due to decreased bandwidth utilization due to printing, but more importantly, it increases stability and scalability due to lower resource consumption on the physical ESX servers.

Advantages of using EMF based technologies

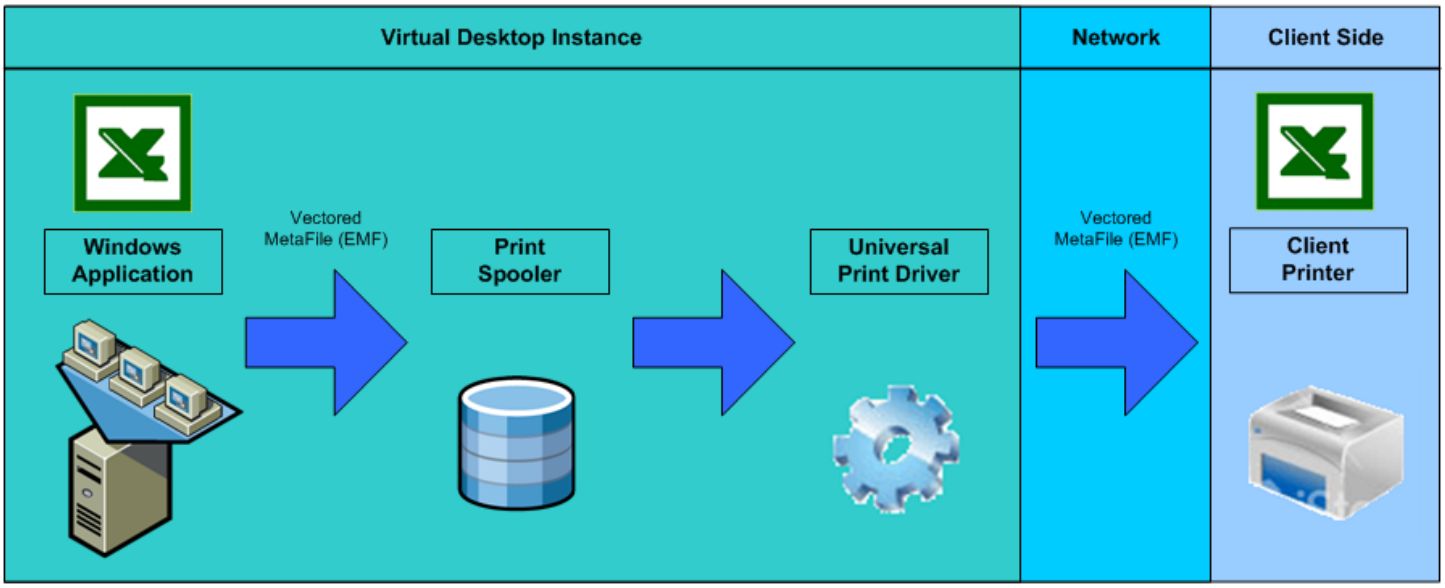
- Increased print speed and session performance due to even smaller print jobs (up to 20:1)
- Reduced Printer Driver Management
- Reduced logon times (due to not mapping fewer client printers)
- 600dpi full color output and increased printer support
- Includes printer bandwidth management functionality on a per client basis

- Reduced Administration with regards to providing printer drivers for installation in the Virtual Machine

Disadvantages of using EMF based technologies

- Requires small software component on server and clients
- Added cost

VDI Printing enhanced with EMF Technology



One caveat that is often overlooked when using Universal Printing Solutions is that they often do not work with thin clients so you need to ensure that there is something on the client side to interpret the print stream and convert it into a RAW format to send to the printer. Some thin client manufacturers work with the printing solution providers to embed their software into the thin client images so keep this in mind when evaluating client devices. The other alternative when using thin clients is to print to network based printers using the universal driver but this uses a lot more bandwidth to print – a concern when talking about a user connected across the WAN, and not an option at all when the user is connected across the internet.

Tips for System Administrators

General Tips

- Enable Quality of Service (QoS) on your routers and switches and increase the priority of RDP traffic
- Set RDP timeouts for idle and disconnected sessions to free up virtual machines for users to log into (only if you are using dynamic pools)
- Standardize the peripherals that you support (and publish and enforce these standards). Failure to do so will result in increased support costs and reduced user satisfaction.

User Profile Optimizations

Whether you use local, roaming or mandatory profiles, be sure that you test each of these settings in your environment to help improve performance and/or stability. You can use group policy, logon scripts, software distribution tools, or just about any method you choose to implement these for your users, but they will generally improve the user experience in a VDI environment.

- Disable the user screensaver in Windows
- Disable Menu Animations
- Disable Desktop Backgrounds
- Disable the requirement to press Ctrl+Alt+Delete before logging in
- Launch Windows Desktop as a Separate Process from Explorer
- Enable Folder Redirection for as many folders as possible to redirect user profile folders to a network drive. The following should be redirected (at a minimum):
    - My Documents (and subfolders)
    - Application Data
    - Desktop
    - Start Menu
- Disable NTFS Timestamps on the virtual machine
- Disable System Beep while printing
- Disable Print Notifications
- Disable the display of the “Last Logged on User Name”

- Enable TCPKeepAlives & TCPMaxDataRetransmissions
- Disable Persistent Network Drive Mapping (so that your logon scripts are the only thing mapping drives for users by default – it will reduce support issues and troubleshooting time down the road)
- Remove Shut Down and Disconnect from the users start menu (through Group Policy)
- Use Volume Licensing for your VM templates to avoid issues with activation and license code requirements after sysprep.
- Disable Sound Schemes – From the Control Panel, open "Sounds and Audio Devices". Click on the Sounds tab, and from the drop down under Sound Scheme, select "No Sounds" (if you feel it is necessary, save the current scheme and name it). This will disable annoying system beeps that just take up unnecessary resources and bandwidth during a user's session.

Virtual Machine Template Optimizations

Listed below are some things that you should consider before declaring your Windows XP Template Image "Ready for Prime Time". I have deliberately excluded some registry tweaks that we often use and recommended in Citrix/Terminal Server Installations (such as DisablePagingExecutive, LargeSystemCache and IOPageLockLimit) because I can't seem to find anything to state that they are supported or improve the experience in a single user Windows XP instance.

- Set NIC to be VMXNET rather than VLANCE
- Disable COM1 & COM2 in the Virtual Machine BIOS
    - Press F2 at virtual machine startup to enter the BIOS (you need to be quick)
    - On the Advanced tab, hit the down arrow until "I/O Device Configuration" is selected. Hit Enter
    - Adjust the values to "Disabled" for "Serial Port A", "Serial Port B", and "Parallel Port".
- Set floppy drive and CD-ROM drive to start disconnected (or remove them from the virtual machine configuration altogether)
- Include tools to optimize the system such as SysInternals PageDefrag which will defragment your page file and system registry hives on boot up. This utility can be scheduled to run at every boot to ensure that files are defragmented before they are loaded (standard defrag tools cannot move files that are in use).
- Clean Up items taking up unnecessary disk space:

  - Click on Start > All Programs > Accessories > System Tools > Disk Cleanup
  - Click on the “More Options” tab
  - Click the “Clean up…” button under System Restore to remove all but the most recent restore point (alternatively you can turn off System Restore altogether)
  - Click on the “Clean up…” button under Windows Components and remove any unnecessary components such as MSN Explorer and Outlook Express.

- Turn off the Logon Screensaver in Windows (see Appendix A)
- Delete the hidden folder and files that would be used by a Service Pack Uninstall:
  - C:\Windows\$NTServicePackUninstall
- For Windows XP, be sure to use SP2 or install MS Q811080
- Disable Unnecessary RDP Virtual Channels (you will need to determine what is necessary). Set a Computer Policy (through Local Policy or AD Group Policy).
  - Computer Configuration > Administrative Templates > Windows Components > Terminal Services > Client/Server data redirection. To disable the settings, you generally ENABLE the policy for each setting that you don’t need such as:
    - Allow Time Zone Redirection
    - Do not allow Clipboard Redirection
    - Do not allow Smart Card Device Redirection
    - Allow Audio Redirection
    - Do not allow Drive Redirection
    - Do not allow COM Port Redirection
    - Do not allow LPT Port Redirection (generally not needed for most RDP printing)
    - Do not allow Client Printer Redirection (probably need this one)
- Disable unnecessary applications from running at System Startup – There are a number of places that applications can hide themselves to get into the System Tray and take up unnecessary processor and memory resources. The easiest way to get rid of these items is to run msconfig.exe and click on the Startup tab. From there you will see a list of all the items scheduled to run automatically when

windows starts. Uncheck any items that are not needed – as a general rule the fewer items left checked, the better the system should perform.

- Turn off Indexing on all hard drives – Open My Computer, right click on the drive (i.e. C:\) and select “Properties”. Uncheck the box at the bottom that says “Allow Indexing Service to index this disk for fast file searching”
- Cleanup Internet Explorer Files – Open a browser, then go to “Tools > Internet Options” and then click on “Delete” under Browsing History. Click on Delete All, then Yes, then Close.
- Be sure you have the latest update to VMware Tools (out of date drivers can sometimes result in slower performance)
- Set Hardware Acceleration to Full (be sure VMware Tools is installed first)
    - Control Panel -> Display -> Settings Tab -> Advanced Button
    - Troubleshooting Tab -> Set acceleration to full
- Remove Unnecessary Windows Components – keep the system image small and clean by only including what users actually need
- Turn off Unnecessary Services – If you don’t need services running, it is best to disable them. Certain Services are not required in most situations that you will experience in a VDI environment. Disable Alerter, Messenger, Computer Browser, Routing and Remote Access, Smart Card, Smart Card Helper, Uninterruptible Power Supply if they are not being used. You can always turn them off and test your machine, before setting them to be disabled on startup. Run "services.msc" from the run box and set the ones you don’t need to be disabled.
- Defragment the hard drive of your XP system template as the last step in your deployment process

Conclusion

While VMware's server focused solutions continue to gain traction in enterprise datacenters, desktop virtualization is an area that has tremendous potential for a large number of organizations and as the old adage goes – "size doesn't matter". Small businesses can benefit just as easily from leveraging a virtual desktop infrastructure to deliver desktops throughout their offices and minimize the amount of IT support that they require. In the near future, you will see offerings that incorporate VDI solutions into SaaS (software as a service) offerings to help minimize the bandwidth and infrastructure requirements for companies.

That said, there are still a large number of design hurdles to overcome, or at the very least consider, when deploying a virtual desktop infrastructure. VDI might be a relatively "new" solution, but its roots are heavily tied to Server Based Computing and it is highly recommended that you engage with an experienced consulting services organization such as Long View Systems or VMware Professional Services to ensure that you get a flexible, scalable infrastructure that can keep up with the changing demands in your business.

As always, the goal should be to try and remove IT as a bottleneck to corporate growth and increased user productivity.

About the Author

Craig Cook is the North American Practice Director of Virtualization and Consolidation for Long View Systems, an IT Solutions & Services company with offices in Denver, Houston, Dallas, Phoenix, Calgary, Vancouver, Victoria and Edmonton. He is responsible for the largest virtualization and consolidation team in North America. With over twelve years of IT experience Craig brings a solid understanding of the challenges faced by IT Infrastructure teams from the desktop to the datacenter. He also appreciates the technology and budget restraints smaller enterprises operate within. Craig has helped customers across Canada, the United States and Europe develop innovative and cost effective IT solutions for their business needs. Craig remains active consulting with customers on strategies regarding desktop, server, storage, and datacenter consolidation, all while keeping an eye on the bottom line. He has lead consolidation initiatives for many Fortune 500 companies.

Acknowledgements

I would like to thank Matthew Allen and Adam Lippitt, both from Long View Systems, for their efforts in helping to build the structure and flow of this white paper and for contributing their expertise in the fields of Server Based Computing and Virtual Desktop Infrastructures.

Appendix A – Sample Registry Settings for a Virtual Desktop

```
Windows Registry Editor Version 5.00
;*****************************************
;Set Default Domain Name (Replace YOUR_NETBIOS_NAME)
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"DefaultDomainName"="YOUR_NETBIOS_DOMAIN"
;*****************************************
;Set Dialing Preferences to avoid pop-ups (Replace YOUR_COMPANY_NAME and
YOUR_AREA_CODE)
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Telephony\Locations]
"NextID"=dword:00000002
"LocationListVersion"=dword:00000002
"CurrentID"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Telephony\Locations\L
ocation1]
"Country"=dword:0000006b
"Flags"=dword:00000001
"Name"="YOUR_COMPANY_NAME"
"AreaCode"="YOUR_AREA_CODE"
"DisableCallWaiting"=""
"LongDistanceCarrierCode"=""
"InternationalCarrierCode"=""
"LongDistanceAccess"=""
"OutsideAccess"=""
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Telephony\Locations\L
ocation1\AreaCodeRules]
;*****************************************
;Disable Dr Watson
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug]
"DebuggerOld"="drwtsn32 -p %ld -e %ld -g"
"Debugger"=""
;*****************************************
;Prevent last access time stamp from being updated on NTFS partitions
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem]
"NtfsDisableLastAccessUpdate"=dword:00000001
```

```
;*****************************************
;XP - Processor Scheduling - Adjust for best performance for Foreground Services
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\PriorityControl]
"Win32PrioritySeparation"=dword:00000026
;*****************************************
;Reset i386 Source Directory to point to Hard Drive (ie C:\i386)
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup]
"Installation Sources"=hex(7):43,00,3a,00,5c,00,00,00,00,00
"SourcePath"="C:\\"
"ServicePackSourcePath"="C:\\"
"CDInstall"=dword:00000000
;*****************************************
;Set Error Mode=2 to stabilize profiles (Q124873)
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows]
"ErrorMode"=dword:00000002
;*****************************************
;Decrease Refused Network Connections
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]
"MaxWorkItems"=dword:00004096
"MaxMpxCt"=dword:00001024
;*****************************************
;Increase Network Request Buffers (Q279282)
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]
"SizReqBuf"=dword:0000ffff
;*****************************************
;Increase PerfDisk performance counter time-out value
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PerfDisk\Performance]
"Open Timeout"=dword:0000c350
```

```
;*****************************************
;Disable Performance Monitor Counters for Remote Access Servive
;(otherwise when you disable services, errors show up in Event Log)
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Performance]
"Disable Performance Counters"=dword:00000001
;*****************************************
;Restart Print Spooler after all failures
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler]
"FailureActions"=hex:00,00,00,00,00,00,00,00,00,00,00,03,00,00,00,d0,47,13,\
  00,01,00,00,00,60,ea,00,00,01,00,00,00,60,ea,00,00,01,00,00,00,60,ea,00,00
;*****************************************
;Suppress All Print Related Event Log Messages except for errors
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers]
"EventLog"=dword:00000001
;*****************************************
;Tune TCP KeepAlives for improved performance
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"KeepAliveTime"=dword:0000ea60
"KeepAliveInterval"=dword:000003e8
;*****************************************
;Disable the Screen Saver at the logon screen (CTRL + ALT + DELETE screen)
[HKEY_USERS\.DEFAULT\Control Panel\Desktop]
"ScreenSaveActive"="1"
```

Revision: 20080129 Item: WP-053-SLN-01-01

VMware, Inc. 3145 Porter Drive Palo Alto CA 94304 USA Tel 650-475-5000 Fax 650-475-5001 www.vmware.com