Realtime publishers

Real World Considerations for Implementing Desktop Virtualization

The Essentials Series

sponsored by vmware®

David Davis

Implementing Desktop Virtualization, Step by Step 1
Consideration #1—Managing End User Applications 1
Migration vs. Fresh Install 1
Application Virtualization 1
Consideration #2—Security and Compliance 2
How VDI Helps 2
Host-Based Antivirus/Anti-Malware 2
Remote Access and Security 2
Two-Factor Authentication 2
Consideration #3—Managing the End User Experience 3
Performance Management 3
Flexible End User Access 3
Consideration #4—Shared vs. Single Disk 4
Desktop Virtualization Implementation Plan 4
Summary 5

Copyright Statement

Implementing Desktop Virtualization, Step by Step

When making the move to desktop virtualization, there are a number of considerations you need to take into account. This article starts with the top-four considerations before delving into a step-by-step implementation plan.

Consideration #1—Managing End User Applications

The first consideration when making the move to desktop virtualization is what to do about end user applications. After all, the applications are the whole reason that the end users are employing their desktops and the reason the business is funding the desktop virtualization project.

Figure 1: Consider the layers involved in VDI.

Migration vs. Fresh Install

As part of any desktop virtualization implementation, you'll need to perform application inventory. You need to find out what applications are running on your existing desktop computers. Those same applications will need to be available in the virtualized desktops.

However, you don't want to just perform a "physical to virtual" (P2V) conversion of physical desktops into virtual desktops. Although this approach might seem like a good idea at first, as it captures all the users' applications and customizations, it's the wrong approach. If you did a P2V conversion and then used that vi machine as a golden image for multiple virtual desktops, potentiall of virtual machines will include all the unnecessary configurations and applications converted from the physical desktop. For example, the desktop might include years' worth of registry changes for many applications, user customizations (which likely don't apply to others), and numerous applications that are unneeded or are just for the physical PC that the virtual machine came from. Instead, you'll want to perform fresh installations of all applications into a golden image desktop that all end user virtual desktops will be linked to.

Application Virtualization

Ideally, you'll want to virtualize these new applications when installed. Application virtualization essentially "packages" the installed applications, making them independent from the underlying operating system (OS). With virtualized applications, the underlying OS can be patched or replaced at any time without affecting applications. When selecting a desktop virtualization package, look for one that also offers application virtualization and integrated management between virtual desktops and virtual applications.

Consideration #2—Security and Compliance

Security and compliance are a concern for every company, and desktop virtualization helps to ease those processes. With traditional physical desktops, company data is downloaded across end user desktops and mobile devices. Properly securing and ensuring compliance for that data is a daunting and often futile task.

How VDI Helps

Desktop virtualization makes security and compliance easier by:

- Centralizing company data in the data center where IT can more easily secure and audit it
- Allowing IT to easily back up and provide disaster recovery for end user desktops
- Ensuring that company data isn't left on a mobile device, at a remote location, or in a window office where it can easily be lost or stolen
- Simplifying the application of security policies and updates to end user desktops (as they are all in the data center)

Host-Based Antivirus/Anti-Malware

Another way that desktop virtualization improves security is by offering the ability to utilize host-based antivirus and anti-malware. Host-based means that antivirus/anti-malware applications can run on the hypervisor host instead of on each virtual machine (end user desktop). This setup not only saves you the time of installing all those agents but also the time to maintain those agents and the processing overhead of running one agent per host instead of one agent per desktop (as you could have 50+ desktops per host). Host-based antivirus and anti-malware tools offer centralized control, efficient design, reduced resource utilization, and simplified administration.

Remote Access and Security

The centralized setup of desktop virtualization means the ability to access your desktop remotely is just part of the design. You are already using a remote display protocol to access your desktop on a daily basis. When you need to access your desktop remotely, you can easily use a software client on a laptop, desktop, or tablet device. Most VDI solutions include an Internet gateway that allows you to access your virtual desktop without the need for a virtual private network (VPN) connection; just a Web browser is required.

Two-Factor Authentication

Two-factor authentication requires two of the three formats of authentication; typically the "something you know" and "something you have" factors are used. Two-factor authentication can easily be integrated into desktop virtualization solutions to provide a higher level of security. Thus, an end user would need not only a username/password but also a password or number from a security token or security keychain fob to access their VDI instance.

Consideration #3—Managing the End User Experience

With the consolidation of end users into the data center, managing performance for the applications running in the virtual desktops is paramount. You must ensure not only that you have capacity for all the virtual desktops but also that those desktops perform as well as (or better than) the physical desktop applications.

Performance Management

The virtual infrastructure that VDI runs upon will have basic performance monitoring software. However, when implementing VDI, you really need a performance tool that understands VDI and associated applications. End user applications running inside virtual machines can periodically suffer slow performance. When that happens, you need to be able to quickly identify whether the problem is related to CPU, memory, disk I/O, or networking. A tool that can measure application response (see Figure 2) is ideal and can be employed by IT to create a service level agreement (SLA) with the business.

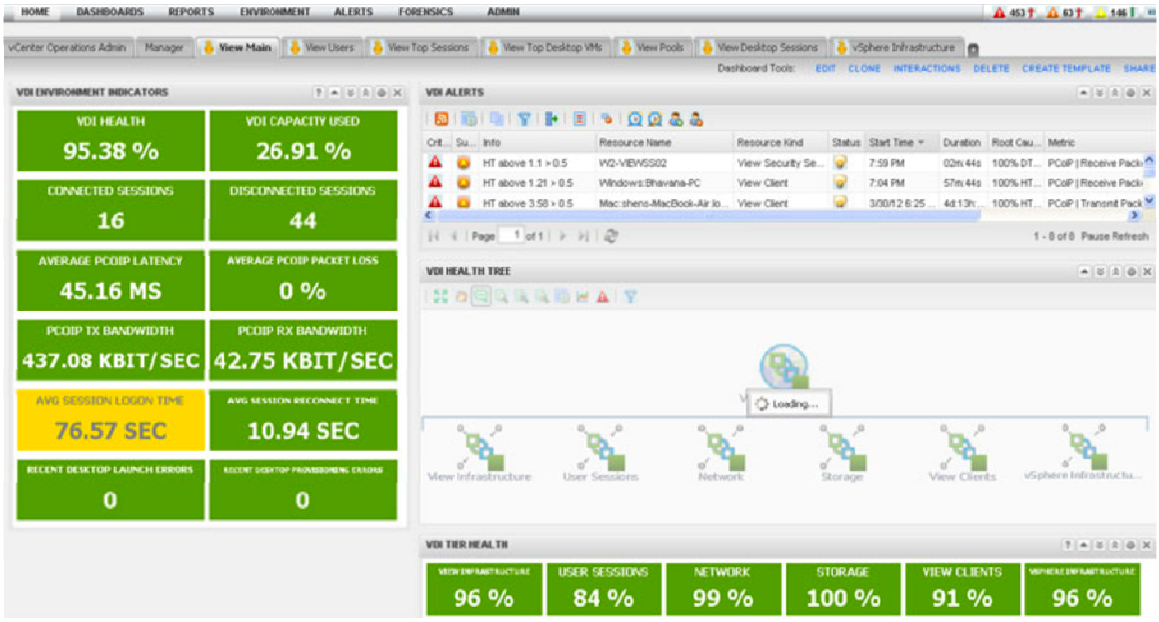

Figure 2: An example VDI performance monitoring solution interface.

Flexible End User Access

One of the core features of VDI is that it can be accessed anywhere, at any time, from just about any device. Once connected, end users will receive a consistent user experience.

Consideration #4—Shared vs. Single Disk

At first, it might seem logical to have one virtual disk for each virtual machine. However, this model just doesn't scale well. Sooner or later, you'll have way too many virtual disks, taking up way too much storage capacity; updating them will become a huge undertaking.

Creating a single golden master virtual machine template and then linking all virtual machines to it means that the changes made from the golden image are all that will be stored on the virtual desktop shared storage. By using a disk linking technology, you'll save time and tremendous disk capacity.

With persona management, user customizations are separated from the applications. This setup allows you to utilize a shared virtual disk for the OS and another for the apps, while keeping the user persona separate. This separation, with a shared OS and applications disk, allows you to not only save money on the disk capacity required but also enjoy greater administrative efficiency in terms of faster upgrades for virtual machines and many fewer virtual disks to administer.

Desktop Virtualization Implementation Plan

Desktop virtualization is a serious solution that requires methodical planning for implementation. The following steps take you from assessment to utilizing advanced features:

1. Assessment—The first step of any implementation plan should be to analyze where you are today. You'll need to find out what applications are in use, how many desktops you have, how they are used, and the best options for virtualizing them.
2. Pilot—You'll want to evaluate the desktop virtualization solutions you are considering before purchasing. This process could start with a short-term pilot utilizing free trial VDI solutions. If that is successful, you could move into a longer-term pilot for a small group of users before purchasing the VDI solution for an enterprise-wide roll out.
3. Monitor—You'll want to monitor the VDI implementation closely to ensure that users are receiving the applications they need and that those applications are performing as expected. This monitoring can be done with reporting offered by the VDI broker and third-party software.
4. Operationalize—The key to operationalizing desktop virtualization is to make it "the norm." Admins (and later, users) need to first think of a virtual desktop as being the "go to" solution for when a new desktop is needed. To make that happen, IT admins and support people need to gain experience with VDI (replace their desktops first), document the new procedures, understand how VDI works, and know that VDI is a better design. It's only by winning the hearts and minds of the IT staff and end users that desktop virtualization will be a success.

5. Report Value—This series discusses the benefits, soft dollars, hard dollars, ROI, and TCO of desktop virtualization. However, although the benefits of VDI may be evident to you (as an admin), they might escape CIOs, CEOs, and financial people (all of whom might have a strong say in whether desktop virtualization continues to be implemented across the company). For this reason, it's important to report the ongoing value and return of desktop virtualization to decision makers in the company.
6. Utilize Advanced Features—Once you have proven desktop virtualization as a success for your company, you can begin implementing advanced features. Examples of such features include 3D graphics, two factor authentication, offline desktops, and more.

Summary

When implementing desktop virtualization, there are numerous considerations, including the migration of existing applications, awareness of security features, ability to manage performance, and virtual disk storage. To ensure the best chance of success, take the process step by step and follow an implementation plan that starts with assessment and pilot. With the ever-growing popularity of desktop virtualization, you'll find excellent resources to simplify the process thanks to the virtualization community, book authors, video trainers, and vendors.