BUSINESS **SOLUTIONS**

Desktop Demystified

Server-centric client virtualization model reduces costs while improving security and flexibility.

Virtualization is transforming the data center. It's eliminating the one-to-one relationship between clients, applications and servers. Just as virtualization adds to server functionality, along comes a technology to aid in desktop manageability, security and Total Cost of Ownership (TCO).

Client virtualization or Virtual Desktop Infrastructure (VDI) is a server-centric computing model. (Note: VMware also uses this term as a brand name.) While it borrows from the classic thin-client model, it offers IT the ability to host and centrally manage Virtual Machines (VMs) while providing end users a full-desktop experience.

VDI is a hosted approach. It centralizes all the software and data components that make up the desktop environment (operating system, installed applications, user personalization settings and data) moving into the data center, computer room or other secure IT facility.

Vendors including Citrix, Microsoft and VMware are now letting IT combine the power and benefits of computer virtualization with the centralized hosting and management of thin-client infrastructures. If you haven't yet discovered the advantages of a VDI, now is the time to put yourself in command of the desktop.

The VDI Approach

In a classic thin-client architecture, users either share access to a multi-user hosted environment or are each assigned to a blade or rack-mounted server processor. On the other hand, a VDI environment provides user resources as virtual machines sharing common hardware, but with resource optimization along with privacy and reliability.

The VDI lets IT provision and maintain an infrastructure of virtual desktop machine instances for many users — tens, hundreds, thousands or even more. It also addresses growing security and compliance concerns, reduces end-user downtime and improves ITs ability to upgrade environments.

"We're seeing VDI adoption pretty much across the board," says Michael Rose, industry analyst for enterprise virtualization software at the tech research and analysis firm IDC. The driving motivations may vary, Rose notes.

"For example, with financial services and government organizations, it's security," he says. "And there are places where VDI, and desktop virtualization in general, can fill a gap not currently filled by current technology, notably call center deployments, off-shore developers, contractors and some educational institutions."

VDI Components

In addition to the desktop virtualization system software that creates, runs and manages desktop VMs, a VDI includes server hardware, operating system(s), desktop delivery protocol(s) and user access devices.

Server Hardware

Server hardware is what the VDI system software, the virtual machine images and associated management tools run on. These can include tower servers, blade servers or rack-mount servers, depending on how many concurrent users need to be supported and the application load the users will be generating.

Like virtualized servers, virtual desktops provide better utilization of the host hardware, and make it easier to allocate capacity and facilitate failover, disaster recovery and business continuity.

Operating Systems

A VDI can have up to three layers of operating systems. These can be located on the virtualization host, the "guest" operating system in each VM and the operating system in the user's desktop or thin-client device.

On the virtualization host, the hypervisor — the software managing and running the virtual machines — may need to run under a host operating system, such as Windows Server, or Linux. Some, like the VMware ESX hypervisor, may run directly on server "bare metal," with no separate host operating system required.

Each virtual user desktop — containing the user's applications and data — needs its own licensed operating system. VMware ESX can support VMs running a variety of operating systems such as different versions of Windows or Windows alongside Linux, etc.

In addition, thin-client devices, at users' desks, each run an operating system. This typically consists of Windows, Linux or Mac OS, or possibly a purpose-built OS from the thin-client device vendor, like Wyse's Thin OS.

Thin-Client Display Protocol

"Delivering a desktop" means making the user device (thin client, PC, etc.) appear, to the user, to be a desktop computer. This is in terms of the keyboard, mouse, display, access to desktop applications, access to data, ability to print, use USB ports and so on.

A virtual desktop will not be accepted by end users if it does not work as well or better than current PCs. To do this, the VM host and the thin-client device need a Thin-Client Display protocol, also known as Desktop Delivery Protocol, for input and display.

The two most common methods to "deliver" the desktop experience to a user device (thin client, PC, etc.) are the Remote Desktop Protocol (RDP) which is built into every Windows XP and Windows 2000 Server (and later) operating system and Citrix Systems' Independent Computing Architecture (ICA) Protocol.

The RDP client is now standard on every Windows operating system. It also can be downloaded for free when using an operating system older than Windows XP. RDP clients are also available for Linux and Macintosh systems, so the technology is widely available to connect Windows desktops remotely.

Citrix's ICA Protocol is slightly older than RDP. However, it delivers a much faster, richer customer experience to access devices. Until recently, ICA was only available to connect to desktops hosted on servers via Citrix XenApp (formerly Presentation Server).

Citrix XenDesktop, and its suite of products, now allows the use of ICA to connect to any Windows desktop operating system, whether it runs on a virtual or a physical machine or if it runs on a blade PC. This extends the capabilities of ICA to every possible Windows desktop operating system.

User Access Devices

Each user needs an access device that runs an operating system, supports the VDI's Desktop Delivery Protocol, and connects to the network and to the user's display, keyboard and mouse.

User access devices can be a regular desktop, notebook, tablet PC or thin-client hardware. While regular PCs can be used in a VDI, this leaves the machines at the desk vulnerable to all the traditional reliability and security risks of PCs.

By contrast, a thin-client device has no hard drive and no moving parts. In fact, it stores no data and uses far less power (and makes far less noise) than a desktop or notebook machine.

One of the leading vendors of thin-client devices — ideal for VDI (as well as for non-virtualized thin-client infrastructures) — is Wyse Technology.

"Each of the thin devices that we sell has the software built into it for the leading desktop virtualization infrastructure platforms from Citrix, VMware and Microsoft," says Jeff McNaught, chief marketing officer, Wyse Technology.

Desktop Virtualization Benefits

Virtualizing your company's desktop infrastructure offers a range of benefits that save money. It also can reduce administrative time-per-user, time-per-system and energy consumption. Furthermore, it improves security and compliance along with IT's ability to change desktop environments more rapidly.

For example, it is estimated that over a three-year period, a 500 desktop VDI would show an overall ROI of 81.5 percent, with a projected payback period of between 1.5 and two years. It will also reduce power consumption by over 200,000 kWh per year.

To help project the potential cost benefits of a VDI implementation, VMware offers an online TCO Calculator. Go to VMware.com and search "TCO Calculator."

"In most of the cost modeling that we're doing, businesses find a break-even point within six-to-eight months followed by more savings," says Calvin Hsu, director, product marketing, Desktop Delivery Group, Citrix Systems. "And that's not counting the security or other indirect benefits."

Greater Manageability

What do IT administrators like most about desktop virtualization: manageability. "With virtual desktop provisioning, a single, clean and updated operating system image is maintained for all desktop clients, says Citrix's Hsu.

"This eliminates the need to keep one operating system image for each virtual desktop," he adds. And with a centralized VDI, applications can be updated quickly and easily on the host machine, without the need to access each user's PC.

For example, VMware View Composer software lets IT managers create new virtual desktops from a master template, allowing faster deployment, according to VMware. Thousands of virtual desktops can be updated or patched simultaneously by applying changes to the master template.

Virtual desktops and virtualized applications also make migration simpler and more reliable. With virtualized applications, there are fewer conflicts between applications. And virtual desktops allow deployment to be done to multiple machines at the same time.

Thin client hardware is much simpler and more reliable than desktop PCs. It can also be less expensive. And if there is a problem, thin client devices are less costly to physically replace.

Assuming there's a spare device on hand, even a non-technical, non-IT person should be able to replace a defective machine. And if need be, a user can work at any other thin-client device, accessing their regular desktop image, data and settings.

Security and Compliance

With a desktop virtualization infrastructure, all data resides in the data center and not on the user devices. That means data security, as well as compliance with government, industry and other regulations, can be more easily adhered to.

"Instead of having data at the edge of the network, where it's vulnerable, it's centralized behind your firewall in a data center," says Jerry Chen, VMware's senior director of desktop platforms and solutions. In a sense, the enterprise network is locked down.

"While IT has a lot of processes and expertise for managing PCs, you don't want something as fundamental as your desktop infrastructure to hold back responding to business opportunities like entering markets or doing mergers, acquisitions or consolidations," says Citrix's Hsu.

"Rather than think of the desktop as hardware with something IT has to deliver, think of it as a service IT can offer," he adds. "When you do this the endpoint becomes much less of a direct concern for your management."

Energy Savings

A VDI can also be "green." By relocating user processing to centralized hardware running virtual machines and using thin-client devices, IT can significantly reduce the per-user IT energy footprint.

Where desktop PCs can use between 70 to 200 watts (not counting the display), Wyse thin-client hardware uses six to 20 watts (not counting the display), according to Wyse's McNaught. "And the total energy savings are even more significant.

"For example, we found that working with Citrix using low-power PCs ran about 70 watts per user," he adds. "Using a Citrix Presentation Server 64-bit environment, we found you could host 1,000 users on three servers, for about 11 watts per user.

"This is plus 6.6 watts per user for a Wyse thin client in full-mode user," he adds. "Or about 18 watts per user instead of 70 watts — again, not including displays."

IT Advice

In considering a DVI, there are, of course, a variety of factors to be weighed against the benefits. First, does your data center have the power, cooling and space to support the servers that will be hosting the desktop VMs? If not, do you have other computer rooms or other secure facilities available?

Second, does your network, between where the VDI servers will go and the desktop access devices, have the bandwidth to support the load? And third, have you evaluated the initial investments that will be required in hardware, licenses and time to deploy a VDI?

"If you've already got VMware for virtualized servers, doing VDI is an incremental addition," notes VMware's Chen. "You can start running pilots on the same hardware."

If you don't yet have a desktop virtualization strategy, the key is to find a population of desktop users and run a pilot on one server, perhaps for a department or a workgroup, Chen advises.

VDI Products

Some of the products used to successfully implement a virtualized desktop environment include:

- VDI Software — These include the tools to create, run and manage an infrastructure of desktop virtual machines. The leading vendors include: Citrix Systems and VMware.
- VMware View 3 — Formerly known as VMware Virtual Desktop Infrastructure, it provides a server-hosted desktop virtualization infrastructure that runs in the data center.
- VMware Infrastructure 3 — It represents VMware's virtual data center operating system and software suite for virtualizing desktops and servers.
- VMware View Manager 3 — The software provides platform management, provisioning and deployment of virtual desktops.
- VMware ThinApp — This is VMware's agent-less application virtualization software. It allows a user to run multiple versions of an application in their desktop VM (or on a desktop PC) without conflict, or run the same version of an application on multiple OSs without modification.
- Citrix Systems XenDesktop — The software offers a virtualization system for centralizing and delivering applications or entire desktops as a service to users anywhere.
- Microsoft Hyper-V — It represents a hypervisor-based virtualization system for x64 systems.

Desktop Virtualization Benefits		
Business Issues:	Requirements:	Benefits:
Productivity	Ease of use	Lowest overall TCO
Optimized ROI and TCO	Minimize application launch time	Centralized management and application deployment
		Fast boot and application launch
Security compliance	Isolated Data Center	Clients free of apps and data
		Centralized data protection
Workforce flexibility/continuity	Multiple images	Unlimited isolated virtual machines
		Eliminate PC move-add change costs

LET CDW SHOW YOU WHAT DESKTOP VIRTUALIZATION CAN DO TO SIMPLIFY MANAGEMENT OF YOUR NETWORK INFRASTRUCTURE. CALL 800.800.4CDW TO TALK TO A SPECIALIST TODAY.

090204