VIRTUAL DESKTOP INFRASTRUCTURE

Improved manageability and availability spur move to virtualize desktops

Many companies have turned to virtualization technologies for their servers and in their data centers to simplify administration and to reduce management chores and operating costs while maintaining reliability and safeguarding against disasters. Seeing the significant benefits virtualization delivers in those environments, companies are now looking to apply the same technology to their desktop computers.

Executive Summary: Virtual Desktop Infrastructure (VDI)

- VDI simplifies desktop administrative and management tasks
- Users access virtual desktops running in the data center
- Technology supports both PCs and thin clients
- Desktop security and data protection are centralized
- Access can be easily extended to remote users

The idea behind what is called a Virtual Desktop Infrastructure (VDI) is to run desktop operating systems and applications inside virtual machines that reside on servers in the data center. Desktop operating systems inside virtual machines are also referred to as virtual desktops. Users access the virtual desktops and applications from a desktop PC client or thin client using a remote display protocol and get almost the full features as if the applications were loaded on their local systems, with the difference being that the applications are centrally managed.

Similar to server virtualization, VDI offers many benefits. Specifically, desktop administrative and management tasks are significantly reduced; applications can quickly be added, deleted, upgraded, and patched; security is centralized; and data is easier to safeguard and back up.

Corporate Challenges Related to Managing Desktops

Managing desktop PCs has always been a time-consuming and challenging task. And recently, it has become ever more so as companies have had to deal with new security risks and support increasing numbers of remote and mobile users. Companies also have to support an increasing use of employee owned resources. For example, because many people already use their company computer at home for personal business, Gartner predicts that by 2008, 10 percent of all companies will ask employees to purchase their own notebook computers.

Typically in a desktop environment, the IT staff member must go to the PC to troubleshoot and fix problems when they occur. If the problem is with a computer used by a worker in a remote site or who works on the road, the user might have to wait for someone to come to the site or they might be asked to send the computer to the main office for repair.

In any of these scenarios, IT staff loses time getting to the PC and workers lose productivity sitting in front of a malfunctioning PC or waiting for their PC to be fixed. If a PC is on site, it can take an IT staffer anywhere from a couple of hours to a day to correct a problem. If the PC is in a small office with no IT staff or is used by a remote user who works from home, the user often needs to bring in or ship the PC to the office, which causes that user to be down (and unproductive) for an extended period of time.

Complicating matters further, applications on today's desktops must constantly be updated and new patches must frequently be installed on a regular basis to protect systems from new exploits.
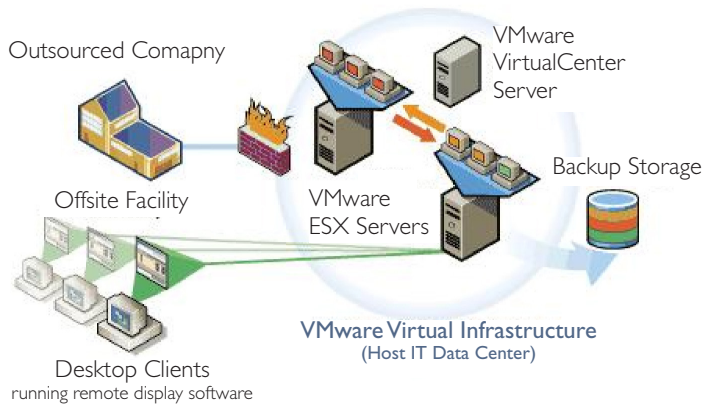
In many cases, software updates and patch installations can be automated. But frequently, the patch installations occur during non-work hours when users turn their PCs off. Users may also need help with the process, again taking up IT staff time.

Worse, some users may ignore instructions and not install the updates or patches. This can result in a desktop PC being infected with malicious software.

And this can lead to additional problems for other systems on a company's network. For example, a 2006 Baseline article noted that there has been a marked increase in hackers using exploits to install malicious remote control software that turns the infected PC into what is known as a bot. (On any given day, there are 3 to 3.5 million active bots operating around the world, according to the article.)

Example of Virtual Desktop Infrastructure

Outsourced Comapny

Offsite Facility

Desktop Clients
running remote display software

VMware
VirtualCenter
Server

Backup Storage

VMware
ESX Servers

VMware Virtual Infrastructure
(Host IT Data Center)

Hackers communicate with their bots using Internet Relay Chat (IRC) and can use the bots to launch denial of service attacks or send spam from the infected PC's e-mail account. The Baseline article noted: "Once a bot is created behind a corporate firewall, the person who controls it can mess with company applications by, for example, installing a keystroke logger on the PC to capture passwords as they are typed."

Beyond dealing with security updates and patches, the job of managing desktops is made harder as users increasingly download and install personal software such as instant messaging, peer-to-peer (P2P), and file sharing programs. Having these programs on distributed physical desktops can cause a number of problems, ranging from malware applications that interfere with other applications required to conduct business to IT not knowing that these programs are installed on a PC in a remote location and thus complicating any troubleshooting efforts.

Still another challenge in managing physical desktops is keeping unlicensed software off of company

systems. Users sometimes innocently or intentionally pass around CDs of commercial software rather than call IT. In fact, a May 2006 Global Software Piracy Study conducted by IDC for the Business Software Alliance (BSA) found that 21 percent of the software in the U.S. is unlicensed. If such software is detected on a company computer, the penalties for the company can be severe. The fine for a single violation can be $150,000 for each software title copied.

Outside of the software issues, desktop management increasingly involves data protection. For instance, many companies have extensive backup and recovery and disaster preparedness plans in place to protect data on servers and dedicated storage devices. But they do not routinely back up the data and applications on desktops.

In today's work environment, where workers can be in geographically dispersed, remote offices, the data stored on distributed desktop computers is often vital to the operation of the business. Such data could include correspondence and documentation that would be essential in protecting intellectual property. Or the data could be essential corporate records, files, or data.

Regardless of what the data is, there is generally a need to protect it from corruption and it must be backed up in case of a hard disk crash, user error, or malicious destruction.

And with regard to data protection, there is a new urgency to protect desktop data due to the new laws governing e-mail archiving and other compliance regulations such as Sarbanes-Oxley or HIPAA.

On top of all of these issues that make desktop management so challenging, there is one more point to consider: Many companies are preparing to migrate to Microsoft Vista. Before any systems can be migrated, companies will need to perform a hardware inventory on each PC to see if it has the CPU, memory, and disk space to run Vista. Companies also need to inventory peripherals in those desktop PCs to check whether they are supported in Vista. Similarly, a software inventory is required to see which programs must be run on the existing PC or be transferred to a new desktop. This inventory

also serves to check whether the programs can run under Vista.

Benefits of VDI

- Efficient use of CPU and memory resources
- Reduced desktop downtime and increased availability
- Patches and upgrades performed in data center
- New users can be up and running quickly
- Data and applications reside in secure data centers
- Centralized management reduces operational expenses

And since Vista is Microsoft's first major new desktop operating system since Windows XP was introduced in 2001, many industry experts expect there will be several new patches and upgrades over the next year or so as was the case with XP.

All of these various chores including maintaining updated software and patches, protecting and backing up data, securing the desktop, and migrating to a new operating system take time. Given all of these issues, it is easy to understand how managing desktops can sap IT resources.

Introducing an Alternative: Desktop Virtualization

To cut recurring management costs and hardware acquisition costs, companies have increasingly been adopting virtualization technology for their servers and in their data centers. Given the success of virtualization in these areas and the growing challenge to manage desktops, companies are beginning to look for ways to get similar benefits by applying the same technology to the desktop environment.

For instance, over the last few years, industry trade publications have reported on the benefits of virtualizing server applications, where applications run on virtual machines. With this approach, numerous virtual servers run on one physical server and computing resources are consumed based on each application's needs.

This approach typically allows companies to consolidate applications running on separate physical servers while improving server efficiency and maintaining application performance. The result is often significant cost savings. For example, a 2006 Baseline

magazine case study on a Welch Foods virtualization project found that the company increased its average server utilization from 5 to 10 percent before to between 50 to 60 percent after. Additionally, Welch Foods reduced total cost of ownership by 20 to 30 percent and saved more than $100,000.

Companies are also finding similar benefits when virtualizing storage. Rather than manage discrete disks or storage devices as separate systems, simpler management comes from virtualizing volumes and file systems without regard for where the data is physically stored. As a result, managers can more easily configure, share, and manage storage.

As these applications of virtualization have proven themselves, companies are looking for ways to leverage the same concept for their desktops using what is called a virtual desktop infrastructure (VDI).

The VDI approach should not be confused with another form of desktop virtualization offered by CPU vendors. Specifically, AMD and Intel are offering ways to virtualize multiple operating systems or applications running on a single or multi-core CPU within a desktop system.

In contrast, the idea with VDI is to run virtual desktop machines on servers within the data center. Users access the machines from a refurbished PC or thin client using a remote display protocol. (The technology works with a variety of thin client solutions.). The idea also helps to extend or eliminate the costly refresh cycle of corporate PCs.

Benefits of using VDI

VDI has some similarities to a shared application infrastructure architecture where user access is via a thin client. However, there are differences. For example, VDI allows companies to isolate users from each other in the case of an individual session failure. VDI also can run most applications natively with no modifications. And VDI supports applications that require a "fat" client.

This ability to support the full range of desktop types is essential since many users want the benefits, such as personal storage space, that a full blown PC offers.

ZIFF DAVIS MEDIA CUSTOM PUBLISHING

vmware

Basically, users want the features and flexibility of the traditional desktop, but without the failure issues.

From an end-user perspective, VDI gives workers close to the full functionality of their desktop operating system and applications with less hardware failure. Specifically, a 2006 Gartner study found that the annual failure rates (AFRs) of desktop computers is about 5 percent in a computer's first year and 12 percent in its fourth. Notebooks have higher AFRs; 15 percent in the first year and 22 percent by the fourth year.

Types of Virtualization

- **Server virtualization:** Multiple applications and operating systems run on virtual machines on a hosted high performance server.
- **Virtualization within a single desktop:** Multiple operating systems or applications run on a single CPU locally within a notebook or desktop computer.
- **Virtual desktop infrastructure:** Desktop operating systems and applications run on virtual machines on servers in the data center.

In contrast, virtual desktops hosted in a data center can be run on servers with high availability features including redundant and hot swappable power supplies, fans, and storage disks. Such systems can help protect against downtime.

From the corporate perspective, because the virtual machines are in the data center, they are a centrally managed resource. This means any changes such as installing a new application, upgrading an existing application, or applying a patch can be made without having to touch the user's physical PC. Scheduling and automating patching and upgrades have a greater success rate since you can start/stop desktop virtual machines in the data center for patching/upgrading. These virtual machines are hardware independent and can run on any data center server and can be accessed from any client. Additionally, the data associated with these applications can be stored in the data center, thus making it easier to back up the data and protect it from unauthorized users.

Besides making it easier to deploy and maintain applications, VDI also simplifies the resolution of problems. For example, when a user calls the helpdesk, IT staff can work on the problem in the data center and do not have to visit the desktop. Furthermore, the IT staff can manage applications and operating systems using standard desktop management tools.

VDI can also be used to provide access to applications and data to remote users who are not within the company wall firewall. This comes in handy when an IT department must support users who work from home or are in other, geographically dispersed offices. Supporting such users is often a difficult task. When problems occur, the user often needs to send their desktop or notebook to the main office for repair. With VDI, problems are easier to fix since the virtual systems are maintained in the data center where there is an IT staff.

An additional benefit of using VDI is that it enables companies to maintain security and meet compliance regulations without having to put as much focus on the PCs' security. Essentially, unmanaged PCs can still have access to applications, but the integrity of the applications and their data can be safeguarded in the data center.

Since VDI leverages the VMware Infrastructure 3, a virtual desktop can be tuned and customized to run any operating system by optimizing the resources associated with the virtual machine that runs it. For example, companies migrating to Windows Vista need not upgrade their physical PCs but can tune the virtual machines easily by allocating more CPU and memory resources. An end user experience in the virtual desktop can be completely customized and tailored based on specific performance needs regardless of the physical PC or thin client used to access a virtual desktop.

VDI reduces downtime, speeds the resolution of problems, improves manageability and control, and helps IT maintain security and data protection. The end result is higher availability and improved worker productivity.

ZIFF DAVIS MEDIA CUSTOM PUBLISHING

Real world benefits from VDI adopters

Most adopters of VDI, before investing in virtual desktop infrastructure were faced with growing support and operational costs and complex deployment situations.

For example, Bell Canada had a variety of issues that led it to VDI. It had to support 8,000 call center agents and faced rising support costs and hardware attrition issues. It had to provide workers in customer locations with secure and locked down systems. And it needed to deploy 400 desktops within a three week period.

To address all of these issues, Bell Canada selected a solution that used a VMware virtual desktop infrastructure. This enabled the company to quickly deploy new systems, centralize management, reduce total cost of ownership, and provide security even when the workers were in customer locations. Additionally, it gave Bell Canada hardware independence, so partners can choose any system as long as it runs Windows and supports the Windows XP RDP (remote desktop protocol).

Case Study: WTC Communications

WTC Communications realized several benefits including:
- Reduced thin client deployment time from hours to minutes
- Simplified and centralized desktop management
- Ensured security of sensitive company data
- Saved about $600 per PC in operational expenses

Another early adopter is Wamego Telecommunications Co. (WTC). The company provides telecommunications, Internet, telecom services over the Internet, and cable TV services in the Kansas River Valley. Going through a period of tremendous growth, the company moved to virtualized servers to cut costs. It then took a look at desktop virtualization.

It selected VMware so employees can access a Windows desktop and the company's customer billing software. VDI helped cut setup time to a point where it takes about 15 minutes to provision a desktop environment for a new employee.

As was the case with server virtualization, the adoption of VDI continues to grow as companies realize the benefits the technology delivers.

VMware as your technology partner
VDI is built on VMware Infrastructure.

In a typical implementation, desktops are hosted on VMware Infrastructure running on data center servers. To ensure high availability and suitable response times, companies can leverage features of the VMware Infrastructure suite such as Dynamic Resource Scheduler, which provides load balancing, and High Availability Services.

A complete VDI solution requires the integration of a number of third party products. To make the task of assembling a complete solution easier for its partners and customers, VMware teamed with leading technology vendors and service providers and created the VMware Virtual Desktop Infrastructure Alliance.

There are 33 members of the alliance including hardware vendors Sun, HP, IBM, Wyse, and ClearCube. The group also includes a variety of management, security, and remote access companies such as Altiris, Citrix, Check Point, LANDesk, Novell, and Platform Computing.

The purpose of the group is to make it easier for companies to move to VDI. This objective was duly noted in a 2006 eWeek article reporting the formation of the alliance. That article said: "The creation of the VDI Alliance is intended to speed the adoption of virtualized desktops by fostering interoperability among alliance members' products and generally speeding up the improvement of virtualized desktop bundles." ∎

ZIFF DAVIS MEDIA®
CUSTOM PUBLISHING