How VDI can cut costs and secure your environment

Andrew Rennie

A VIRTUAL DESKTOP infrastructure (VDI) can be extremely useful in some IT environments, offering the potential of lower costs and a secure working environment in situations where "normal" desktop PCs would be inappropriate or are not available. The term VDI is used to describe an infrastructure in which users access a full desktop operating system environment remotely. The desktop could be a normal PC, a blade PC or a virtual machine (VM). Of course, the ability to access a full desktop remotely has been available for many years via Terminal Services (TS), but VDI is different from TS.

In a TS environment, multiple users accessed a single environment. This could be customised, but resources were not dedicated to a particular user. Some applications did not run well in a TS environment, partly because of this lack of dedicated system resources. In a VDI environment each user accesses either their own centrally hosted physical PC, blade or VM, or a shared VM. VDI enables applications to be run as if they are on a local PC, so overcoming problems that arose with TS. In a VDI environment, physical CPU, memory and disk capacity can be allocated to particular users. This stops one user's actions affecting other users. VDI provides:

- An up-to-date machine when a user's local device can't the latest OS and applications.
- A secure means of working from anywhere, especially for emergency access using a non-company PC to access company resources.
- A hosted image where this would be more secure than local desktops (for offshore workers , for example).
- Up-to-date core images of OSs and applications. VDI enables these to be updated quickly and cost- efficiently. This allows companies to take advantage of new OSs and applications without the usual delays caused by cost and planning.
- A new desktop for users each time they use the system. This reduces support costs as the issues that build up with ad-hoc software installation and removal do not exist.
- Disaster recovery capabilities. Data and the VDI infrastructure can be deployed in geographically dispersed data centres, so enabling disaster recovery even for PC hardware. Many disaster recovery plans do not include hardware, so that if a disaster were to occur, the company would first need to source new hardware.

VDI applications

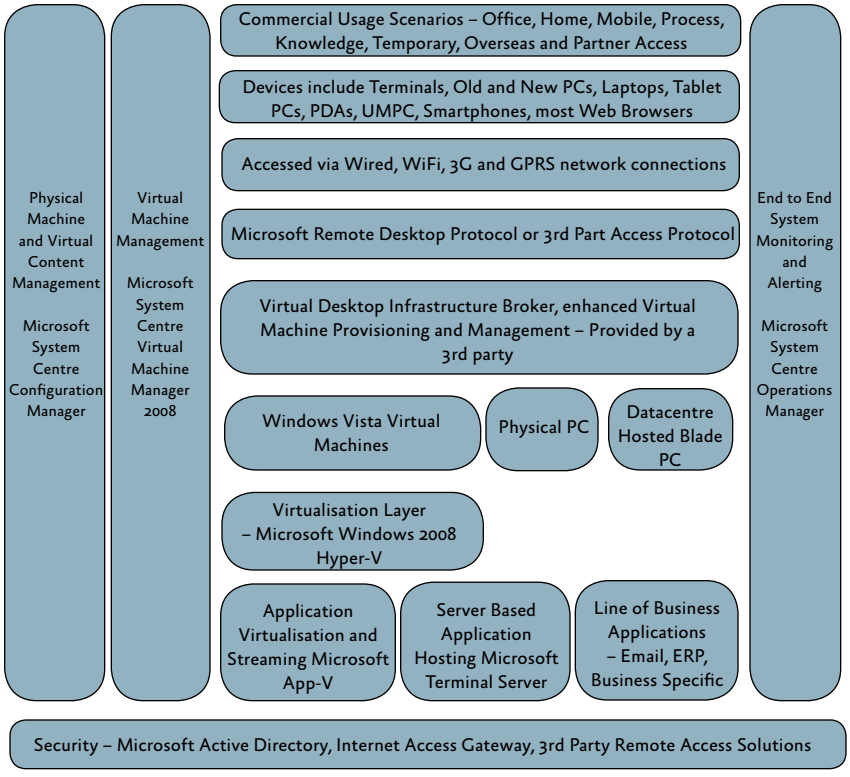
Applications can be provided to VDI machines various ways. One option is for the VDI environment to have all the software a user requires installed on it. Another is for a user's applications can be streamed on demand, or for them to access web-based or TS applications as they would using a local machine. The locally installed applications are managed using the same tools you would use to manage a local desktop machine. Broker software provides different functionality depending on the vendor, though all provide core functions including:

- Allocating users to the correct VM or physical machine depending on the permissions.
- Providing tools that allow multiple users to access a single VM and to load up and shut down VMs depending on the time of day and workload. The broker maintains the appropriate numbers of free VMs to ensure there is always adequate capacity.
- Enabling disaster recovery capability.
- Managing connections that have been accidentally dropped.
- Managing connection persistency.
- Masking the original OS except at login. For instance, suppose a user has a local Windows XP PC on which the broker's client is installed and configured to automatically start and load a Windows Vista VM. When the user logs in they see the Windows XP login screen, but this is followed by the loading of a Vista desktop so that the user never sees a Windows XP desktop. This provides a great way of deploying the latest OS and applications on hardware that would otherwise need to be upgraded or replaced because it does not meet the system requirements.

> VDI enables apps to be run as if they're on a local PC, so overcoming problems that arose with Terminal Services

A number of vendors have created their own access protocols or added enhancements to Remote Desktop

ANDREW RENNIE *is a solutions architect with Microsoft Services UK.*



VDI architecture diagram

The diagram opposite illustrates the components required in an enterprise VDI environment. Where Microsoft provides a product which fulfils the technical requirement this has been identified, though alternative products from third-party companies are also available for some elements. In the case of the VDI broker, Microsoft does not have a product, but a number of Microsoft partners provide products to suit customers' requirements.

A list of Microsoft's virtualisation partners can be found at the link below. The page allows users to filter on the type of partner product they require. Selecting desktop/VDI includes the companies that provide brokers.
http://www.microsoft.com/virtualization/partners.mspx

Protocol (RDP). These protocols and enhancements add a number of features including the following:

- Reduced bandwidth requirements per user.
- Increased responsiveness between the client and the VDI.
- Enhanced video and audio capabilities – these can increase bandwidth requirements.

Create a simple VDI environment

The apparent infrastructure requirements may deter people from experimenting with VDI but the components listed below will create a basic VDI environment. Testers can use the environment to check whether VDI can meet their business requirements. The results of this testing will enable a request for information (RFI) or request for price (RFP) to be created for the broker components. After the RFI/RFP, a fuller test environment, including the remaining architecture stack, should be created to test if a fully featured VDI environment can meet the business requirements.

This test environment could be used to compare a number of brokers to help a company choose the one they need (assuming that one is needed). If a company plans to map specific VMs to specific users and RDP provides the required performance, a broker may not be required.

A simple VDI environment consists of the following elements:

- Active Directory
- A Hyper-V server
- A number of Windows Vista VMs
- A number of PCs, which should be representative of the existing estate

This will allow testers to make RDP connections from PCs to VMs for test purposes.

Summary

VDI may be implemented for many reasons. These include enhanced security, cost savings and business enablement. Despite its potential advantages, VDI is not suitable in all situations and should be considered as an option rather than a panacea for all desktop requirements. As in all technology investments, the business requirements form the starting point and so need careful analysis. If this indicates VDI is an option, further investigation will show whether a test environment is worth implementing. Although cost savings are an obvious advantage, a business may decide to implement VDI for other reasons, such as security improvements or enhanced functionality. ■

For additional information, see the following online resources:

Windows Server 2008 Hyper-V
http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx

Virtualization TechCenter
http://technet.microsoft.com/en-gb/virtualization/default.aspx

Desktop virtualisation
http://www.microsoft.com/virtualization/solution-tech-desktop.mspx

VDI and Windows Vista Enterprise Centralized Desktop (VECD)
http://www.microsoft.com/virtualization/solution-product-vdi.mspx