Realtime publishers

The Essentials Series: Important Questions in Implementing Virtual Desktops

What Technologies are Critical for Virtual Desktop Success?

sponsored by

pano LOGIC

by Greg Shields

Copyright Statement

What Technologies Are Critical for Virtual Desktop Success?

Virtualization, orchestration, personality management, servers and storage, and the all-important endpoint—these are technologies you must integrate to create a successful virtual desktop infrastructure. The first article in this series closed with the statement that today's virtual desktops encompass no single technology. There is no shrink-wrapped box of software that you can buy to *Next, Next, Finish* your way to a virtual desktop environment. Instead, multiple technologies must be integrated in careful ways to create the necessary architecture.

But don't let this statement scare you. The multi-product approach to creating an IT infrastructure of any type isn't a new technique. Even mature technologies such as email and file services require multiple products to be successful. As an example, an email server requires the server to function but also requires the addition of anti-spam, anti-malware, proxying, and often multiple additional servers in larger environments to correctly accomplish its mission. With virtual desktops, *it is likely that you already have many of its components* or the capacity to host them in place.

What Are the Prerequisites for Virtual Desktops?

Figure 1 outlines a few of the components necessary to stand up your initial virtual desktop infrastructure. Obviously, the first necessary component is a mechanism to actually virtualize the desktops themselves. This enterprise virtualization platform should be able to support a high level of virtual machine density, enabling large numbers of virtual desktops to be hosted per configured server.

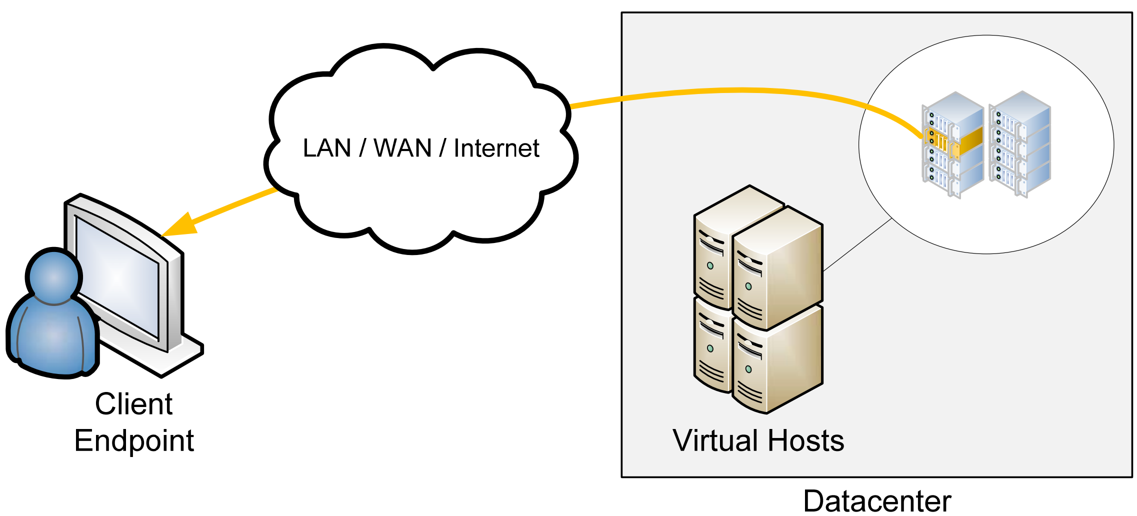

Figure 1: A virtual desktop is powered by a virtual host. It is accessed via a client endpoint through many types of network connections.

Also necessary in combination with that virtual platform are the servers that host virtual machine processing. With an enterprise-class virtualization platform and correctly configured hardware, it is not unheard of to expect between five and eight virtual desktops per server core. Each desktop can be configured with as little as 512MB of RAM for users with light workloads such as minimal Microsoft Office utilization, or as much as 1GB or more of RAM for heavier uses.

> **Note**
> Be cautious with the assignment of memory to virtual desktops, as conservation of RAM is critical to ensuring the highest level of virtual desktop density.

Disk performance in virtual environments can be a singular bottleneck when not properly planned. As virtual machine processing is highly disk-centric due to its entire configuration being on disk, the rotation speed of disks used in virtual environments is exceptionally important. High-performance SAS or FC disks with a rotation speed of 15,000RPM or greater is recommended to eliminate any disk bottlenecks, although slower drives (such as those that operate at 10,000RPM) can be used for less-demanding workloads if properly monitored. The use of high-speed disk controllers with efficient RAID is recommended to ensure that the processing of disk requests can keep up with server processing.

Also critical is the speed of the network. Although a deficiency in any physical component such as processor power or disk speed can cause a reduction in performance for the end user, a well-performing network is critical to the best user experience. Although not technically a "streaming" technology, the connection between virtual desktop and user is highly reliant on an uninterrupted and efficient stream of data. Latency either in the network or as a function of a resource bottleneck is the greatest enemy of a virtual desktop infrastructure. Any latency will be felt by users as sluggish performance and will result in a reduction in the user experience. Most high-speed business LANs should not experience this problem; however, environments that span the Internet, multiple sites, campus environments, and metro-area environments must take care to architect the proper amount of bandwidth to prevent latency effects.

As such, you must be cautious not to overload your virtual infrastructure with too many virtual desktops. Although a virtualization platform can create effectively unlimited numbers of virtual machines, the performance utilization and count of those virtual machines must be closely monitored to ensure that each user retains an experience equivalent to a local desktop.

Lastly are the personality management and orchestration components that ensure users are correctly connected to the right virtual desktop and that user state is properly injected. Orchestration components are typically made available through a virtual desktop technology's vendor, making each technology different in the mechanism by which users are connected to desktops (more on this in a minute). Personality management technologies typically leverage either Microsoft Windows Roaming Profiles or make use of a third-party application.

How Do Users Interact with Virtual Desktops?

With all these pieces, we're not quite done. It can be argued that of these components, the most important to consider relates to *the client endpoint itself*. Essentially, some technology must exist at the users' network connection in order to interact with their virtual desktops.

Figure 1 shows how the display and interaction with a virtual desktop occurs over the network. Transporting that data across the network occurs through one of many network protocols, all of which are highly-optimized for network utilization and preservation of the user experience. Different virtual desktop vendors leverage different technologies for delivering that interface to its users, and it is the selection of the right technology here that will determine the success of your virtual desktop implementation.

To explain this statement, think for a minute about the elements that must be in place for a user to access a virtual desktop. A virtual infrastructure must be in place to host that desktop. The network must contain the capacity to support the network transport of its interface. Management tools must be available for creating and administering the desktop infrastructure. And, most importantly, some component must be in place at the user's location to *receive* the desktop.

It is the selection of this client endpoint component that ultimately makes or breaks a virtual desktop deployment's ROI. Cost models associated with hosted desktops gain much of their financial benefit through the elimination of "real" desktops at the user's location. By eliminating the real desktop, the cost of maintenance and upgrade is eliminated, as is the annual cost of administering the configuration, security, and application load-out on that endpoint.

However, with virtual desktops, one cannot simply eliminate the device at the client's location. Something must be present to receive the data for the virtual desktop and convert it into a useable interface for the user. Accomplishing this task by using traditional desktop computers eliminates much of the potential benefit gained by centralizing desktop processing. Rather, needed is a specialized device that requires no configuration, retains no onboard state, and can be swapped out as easily as the user's desk or their telephone. Such a device fulfills the need for an endpoint but does so while maintaining the ROI gained through the total and complete centralization of desktop processing.

The Value of the Zero Client

Lacking any form of onboard configuration information, such a device could be considered a completely stateless client, or a "zero client." This moniker is used as a comparison with early "thin client" devices. These devices interoperated with remote application environments such as Terminal Services or XenApp. With a thin client, a minimal operating system (OS) is stored on the client device itself. Its processing was used to connect the client device to a remote access server for the deployment of applications.

Thin clients grew in popularity towards the end of the last decade. Having very few moving parts, these clients could be easily deployed and needed only minor updating—often through flash RAM updates but sometimes via small onboard hard drives. Their primary responsibility was to connect the user to their remote applications, present a user interface, and send keyboard/mouse commands back to the server.

However, over time, many found that the promise of thin clients didn't align with the reality of their administration. With many thin clients, their minimal onboard OSs still required updating, a process that consumed time and increased their cost to maintain. Further, producers of thin client OSs weren't often able to keep pace with changing technology at the server side, forcing many thin client deployments to stick with older server-side technology. Even more problematic, when needed business applications were found to not function atop Terminal Services or XenApp, businesses were often forced to revert back to traditional desktops.

Contrast this situation to the virtual desktop alternative. Here, every part of a virtual desktop's processing (and indeed all its code) is retained at the server side and within the virtual desktop itself. In this situation, the client is little more than an electrical transceiver, one that converts electrical signals from an Ethernet cable that is connected to a common TCP/IP network into useable signals for video, mouse, keyboard, and peripherals.

Such a client is entirely stateless, and as such, never needs updating, management, or replacement of onboard code. When technology changes at the server side—alternative virtualization hypervisors, new technologies in deployment, improvements in data transport protocols, and so on—there is never a need to update individual clients. Technology changes at the server side are immediately and automatically useable by clients that are deployed into the field. The only necessary step to implement new technology is in altering the server infrastructure.

Lastly, and most importantly, the virtual desktop infrastructure back in the data center retains the 1:1 mapping between users and OS instances. This means that any application that works on Microsoft Windows will work in the virtual desktop environment. Thus, it is likely that your business will never be forced to revert back to traditional desktops because of an application incompatibility.

Multiple Technologies. Agile Processing.

There are a number of technologies that are required to create a virtual desktop infrastructure. These technologies incorporate the consolidation power of virtualization with the automation flexibility gained through OS management. With the right tools in place, it is possible for users to connect to their desktops from anywhere with a network connection. At the same time, problems in the environment can be solved with very little effort. Although the initial costs of building such an environment can be high considering the technology outlay that is required, such an expense can quickly pay for itself through the reduction in operational expenditures over time.

Now that you understand the promise of virtual desktops as well as the technologies that make them a reality, your final question likely relates to the use cases where it most makes sense. Today's implementations of virtual desktops work well across a range of environments, with some gaining dramatic efficiencies. The final article in this series will tell a set of stories from industries who have benefitted from their virtual desktop implementations.