SANS Technology Institute

Joint Written Project

Is Virtual Desktop Infrastructure (VDI) Right for Me?

Tim Proffitt and Emilio Valente

June 2009

Executive Summary

As organizations seek to improve management and/or user productivity, control costs or increase information security, it is becoming clear that they must address the endpoint environment. With the combination of a mobile workforce, shrinking budget dollars, compliance requirements and the growing corporate culture of going green, organizations are seeking more efficient methods for deploying a secure desktop. Virtual Desktop Infrastructure (VDI) is a solution for server hosted, virtual desktop computing that leverages thin client architecture and centralizes endpoint images as virtual machines. By centralizing endpoint infrastructure, organizations can realize lower costs through reduction in administration tasks, hardware requirements, and endpoint compliance exceptions. VDI allows the technology staff to quickly add or patch applications, security is centralized for the endpoints, and the data can be positioned to be more effectively backed up.

Benefits of VDI

- A centralized, secured VDI environment provides a number of benefits to the organization including:
  - A virtual desktop can be saved and subsequently restored in minutes.
  - Improved management productivity
  - Corporate standards, compliance & regulatory requirements are easily met and maintained.
  - VDI offers management ease and convenience whereas it has been traditionally more difficult with physical desktop machines.
  - VDI is managed in the same way other virtual servers are at the data center. High availability and disaster recovery can be built into the process from the beginning.

- Improve user productivity
  - Users can experience improvements in responsiveness. Desktops run on faster server hardware, with reduced latency in applications due to the proximity of the core network.
  - Tools available today can ensure that a virtual desktop is only available to the user if patch requirements are met.

- Control costs
  - Desktop management costs decline by simplifying and standardizing the server hardware and client access devices.
  - Memory, process, and disk resources of a virtual machine can be modified with very little to no interruption in a user's workday.

- Increase information security
  - Patching and modifying the virtual desktop is done from within the data center and may require very little user acceptance or intervention for success.

- Vulnerabilities inherent to a desktop environment can be minimized or eliminated by moving the desktop into the data center.

Architectural Components of VDI

As with any technology, there are several components that make up the VDI infrastructure. Depending upon the organization's requirements and deployment strategy, some or all of the VDI components may be necessary.

PCs or Thin Client devices are used to access virtual desktops. There are several schools of thought on which platform to choose. Whether it be a true thin client, such as a Wyse terminal or a traditional PC, the workstation hardware requirements can be met easily.

There are obvious advantages to both. Thin clients allow for a single hardware platform to support and remove the ability for users to exploit external media. Older, out of lifecycle workstations can be repurposed due to the reduced requirements of VDI display protocols and backend processing by the host server.

Host servers are referred to the actual physical hardware that runs the virtual desktop. The host server will run multiple instances of desktops much like traditional virtual server environments. Scaling the correct hardware for the host servers is very important since it will directly impact the end user experience.

The virtual desktop manager, often called a connection broker, connects and manages sessions between client devices and virtual desktops hosted on the server. In larger infrastructures the connection broker can be valuable in properly controlling connecting client hardware to backend resources. When the goal is to deploy a highly available VDI, a connection broker will be a sought after architectural component.

The hypervisor is a piece of virtualization infrastructure that runs on the host server, at a processing level below the virtual desktops, and works to manage the images hardware and software requests.

In some cases, application and presentation virtualization services may be warranted to deliver applications to virtual desktop instances. Multimedia, streaming video, print services, VOIP, etc. are examples of services that may need special consideration when using VDI.

A network infrastructure that considers VDI will be an important architectural component. The infrastructure, that interconnects end users and other infrastructure services from inside and outside the LAN to the host server, will need to be able to deliver a presentation protocol at one end and allow quick responses between the host server and the shared storage.

Shared storage refers to the centrally located server attached disks or tapes. Shared storage is where data ultimately resides and can be locally attached, iSCSI, or an alternative SAN solution. Unlike other enterprise solutions running on backend hardware, VDI may not require speedy disks. The requirements from a virtual desktop will be quite different than the requirements from an Oracle DBMS.

Deployment Strategies

VDI can be deployed in a number of ways to address a variety of use cases. Although there may be varying deployment strategies being pushed by the Value Added Reseller (VAR) space, at a high level there are three major camps.

The first deployment strategy is individual desktop deployments. Individual desktop deployments consist of end users that have a 1:1 mapping to a specific virtual instance. Users work with and are connected to the same image day to day. Special software needs, such as legacy software, is ideal in this space. This virtual desktop instance might have previously lived on a physical PC.

Second is a non-persistent pool deployment. Non-Persistent pools are individual virtual desktop instances managed as a pool of resources. They have inherent the same hardware requirements and are created using the same provisioning template. Users or groups that are entitled to use a non-persistent pool are randomly assigned an image at login. The desktop is non-persistent from the standpoint that there is no guarantee the user will be connected with the same instance at the next connection. Any data saved locally to the desktop could be lost as the desktop may be destroyed at any time.

Third is the persistent pool deployment. Persistent pools are individual instances managed as a pool of resources. They have inherent the same hardware and domain policies and are created using the same template. Users in a persistent pool are assigned a desktop at login and are persistent from the standpoint that the user is reconnected with the same virtual desktop instance at each login.

There are some considerations that must be taken into account before deploying VDI.
There needs to be thorough testing for any users type that have a need to use graphically intense applications and those that use heavy streaming video and audio requirements.

Unless there is a strong demand or immediate need, users should be considered in later stages of deployment. There are more solutions coming to market that enable the delivery of multimedia video that are in the initial stages of release. Users or deployment scenarios that require the use of multimedia can be considered, but as a later phase of the project.

IT Challenges and Requirements Related to a Virtual Workforce

While VDI has clear benefits to the organization, it can also pose challenges to an IT organization accustomed to delivering services where most users are permanent employees located in physical offices. Reengineering existing infrastructure can result in unnecessary costs, degraded performance, and security risks; thus impacting an organization's traditional workforce without fully meeting the needs of the virtual workforce. By understanding these challenges in more detail, a comprehensive solution can be implemented, leveraging existing infrastructure investments.

VDI desktops are required to be at least as productive as traditional PCs used by existing users. As such, they should benefit from identical IT service performance and availability levels. This is often not the case due to the degradation of network performance over wide area, wireless, or residential grade networks.

Outage of services is a common complaint for both VDI workforce and existing fully installed desktops, it causes decrease in productivity. In addition, business continuity disruptions can have a greater impact with VDI, due to the number of additional infrastructure components between the worker and their applications.

The remote aspects of VDI produce difficulties for IT departments in terms of providing connectivity back to the host server. Replacing the traditional laptop with VDI can be a political challenge as well. For those roaming users who utilize a laptop while on a Trans Atlantic flight, they will not be an ideal consumer of VDI. Although the permeation of wireless Internet is stretching farther into the corners of the world, there are still common places where connection back to the host server will be difficult to obtain. Additional thought will be needed to secure VDI utilizing public connections. How will organizations ensure the integrity and confidentiality of resources transmitted this way when they do not have complete end-to-end control over the transmission?

Reduce Costs and ROI

The total cost of ownership for a traditional PC ranges significantly but, in all cases, is fairly expensive compared to VDI. These per workstation costs include:

- Hardware
- Maintenance
- Help desk support
- Change management issues
- Software distribution
- Patching
- Security policy compliance

In environments where PCs are tightly managed, these costs can range from $700 to 1,000 per PC per year. In loosely managed environments, they can balloon to several thousand dollars per PC per year. With an approximate 496 million PCs distributed across IT environments, these costs are very substantial.

The infrastructure agility provided by VDI enables flexibility for the virtual workforce, enabling IT support for all scenarios, such as corporate staff, remote office workers, mobile workers, outsourced workers, offshore workers, and contractors. VDI enables organizations to reduce the costs involved with replicating infrastructure when supporting new remote workers, building out new parts of the business, or integrating or combining business systems during initiatives such as outsourcing. VDI enables reduced cost by:

- Centralizing and optimizing existing datacenter infrastructure to reduce overall hardware, real estate, power, and cooling requirements, thus providing green IT and cost benefits.
- Easily provisioning applications and desktops, enabling the rapid expansion of remote and branch offices.
- Delivering a standard desktop environment from images in the datacenter to new users in any location. No shipping required.
- Providing a single, standard desktop to all devices.
- Lower desktop TCO by allowing organizations to use existing desktop hardware.
- Pooling of applications for use by all workers.
- Provisioning entire virtual offices without requiring IT staff to be available on site, providing response without travel costs.
- Lowering infrastructure replication and support costs by centralizing desktop lifecycle management and extending the life of PCs.
- Performing and applying company-wide updates and patches to desktops from a central location therefore reducing the support staff otherwise needed to visit each office.
- Support staff can roll back updates efficiently and quickly.
- Reusing existing infrastructure for new ventures.
- Using an optimized delivery protocol to reduce network costs and complexity.

Based on interviews with existing customers, organizations can usually construct a ROI analysis of 24 months after deployment of a typical VDI project.

Provide Business Continuity for the Desktop

Statistically, if critical data is inaccessible by a company for more than 48 hours, that company will be out of business in less than a year. In the 1993 World Trade Center bombing, 50 percent of the businesses without a disaster recovery plan were out of business within 2 years.[1] In the case of natural disaster, power failure, hardware crash, compromising systems and so on, it is vital to be able to reintegrate user desktop functionality as soon as possible.

The VDI characteristic of centralizing the use of programs and storage of current data will allow a replacement of a virtual “terminal” with minimal service disruption.

It is important to plan the time that it takes for systems administrators to get the user desktop back online and running as expected. Recovery times are based upon the VDI technology adopted by the

organization. The following are times and features of the business continuity and disaster recovery of several VDI vendors in normal deployments:

1) VMWARE View is 1 (one) hour.[2]
2) Microsoft Enterprise Desktop Virtualization (MED-V) client and server have a high rate of availability thanks to the fact that they run independently from each other. In case of a failure of the server, the workplace is still running and all client events are aggregated locally to the client until the server become available again. Redundant configurations with active and passive nodes, or servers, provide for seamless failover without interruption of services.[3]
3) Sun VDI 3 still does not support user work offline (like we have seen for Microsoft MED-V); therefore, if we have a network failure, the user can't continue his/her work.[4]

Increasing Security and Control of the Infrastructure

The centralization of the applications and data gives us an unusual "return to the past" when mainframes were dominating the market and terminals were used to connect users to the central unit where data were processed. This separation gives a high level of security; if in fact the client is corrupted or compromised, it will not affect the global application and data infrastructure.

The benefits of the session based desktop and virtual application delivery allow increase in security and control of the infrastructure not only for local users, but also for contractors that need access to corporate resources from home or on travel using corporate laptops or any wireless device. For most organizations a major defense is to make sure that remote users have in place security protection software and use VPN to log in to corporate resources. When utilizing VDI there are several options to allow a more secure access to information.
A good example of VDI at work is what the company HOB Inc. presented at the last RSA conference 2009 as a solution for an end-to-end access adopting two different versions of products. Both are deployed using SSL-encryption via a LAN (HOB- or via Internet and HOB-WSP uses a web-proxies) for secure user connections.[5]

The core of the Virtual Desktop Infrastructure are the virtual images or, from a hardware point of view, the central virtual servers. Those are the objects that the security professionals have to dedicate their attention to securely protect them from internal and external threats.

While traditionally each desktop can be a potential compromised host and each server is a possible target for an attack, in VDI the desktop becomes less of a point of failure and security vulnerability.

Data and applications run on the central servers and the security professionals have fewer attack vectors to defend against.

In most organization, system administrators are constantly fighting with users on installing software that is not licensed or does not align with the business mission. With VDI the tools are available to lock down the virtual desktop image reign in local storage, and control approved applications.

Pitfalls

According to Gardner Inc., in the next near future (2013) virtual desktop market will reach the astronomical amount of 65 billion.[6] Although this number may be ambitious, several drawbacks should be mentioned that arise during the transition period where old hardware must coexist with VDI equipment:

- Datacenter capacity (space) for large scale deployment of VDI
- Power consumption: an August 2007 report by the US Environmental Protection Agency[7] discovered that in 2006 in USA, servers and data centers used 61 billion kilowatt-hours or about 1.5% of the country's total electricity consumption, at a cost of about $4.5 billion. This was more than double the amount of energy consumed in 2000.
- The United States is in an economic recession. Typically, the adoption phase of new technology is resource intensive.
- VDI can be vendor independent. With the growing number of companies developing pieces of the Virtual Desktop Infrastructure, the need to standardize in order to avoid incompatibilities is vital.

Conclusions

While there are plenty of choices for desktop deployment, the physical, full application, data locally stored desktop PC, is the one technology that met most needs. Alternatively VDI definitely is developing into a viable technology that can provide a majority of users needs with only slight compromise. However, the advantages to VDI as pointed out in this document are clear.

Ultimately profit is what drives organizations to make technology changes. If VDI will be effective in reducing costs and ROI, as described above, it definitely will make a mark in the technology space.

This is particularly true if we consider the fact that associated with the implementation of VDI there are some special services like multimedia, streaming video, print services, VOIP, that require intense usage of bandwidth. VDI relies on bandwidth for the reasons explained above. Therefore management will need to make an evaluation.

- Is the adoption of the new technology worth it, in terms of costs, benefits, revenue and increase in productivity?

- Does the company have a network infrastructure that can support special services that require high network utilization?

It is of paramount importance for the management to answer those questions based on the specific characteristics of their computing environment. There is not a one size fits all quick fix. However, VDI can position an organization to reduce the risks associated with traditional workstations.

REFERENCES

1. http://www.plasticsbusinessmag.com/wp/?p=35 Internet, 2007

2. http://www.vmworld.com/docs/DOC-2438 Internet, 2008

3. http://www.microsoft.com/windows/enterprise/products/med-v.aspx Internet, 2009

4. http://www.itbusinessedge.com/cm/blogs/cole/sun-launches-improved-vdi- platform/?cs=31318 Internet, 2009

5. http://www.darkreading.com/security/storage/showArticle.jhtml?articleID=217000025 Internet, 2009

6. http://www.connectitnews.com/usa/story.cfm?item=3173 Internet, 2009

7. http://www.energystar.gov/ia/partners/prod_development/downloads/EPA_Datacenter_Report_Congress_Final1.pdf Internet, 2007