

CLIENT COMPUTING STRATEGIES

Virtualizing clients presents opportunities for organizations adapting to cloud computing and the proliferation of smartphones and tablet PCs.

Table of Contents

2	Executive Summary
2	Client Virtualization
4	Client Virtualization Benefits
5	Changing Roles and Responsibilities in IT
6	Client Virtualization and COOP
6	Client Virtualization and the Cloud
6	Thin Clients
7	Other Client Devices
7	Client Virtualization Support Needs

Executive Summary

The increasing interest in cloud computing over the past few years and the introduction of smartphones and new tablet PCs have motivated many IT departments to reevaluate their desktop strategies. On top of these escalating technology trends, the appointment of Vivek Kundra as the first federal CIO, and his push toward light technology and shared solutions, has reinforced the notion that it's time for IT departments to rethink client computing.

Where does the enterprise desktop model stand in this sea change that organizations are experiencing through cloud computing and the move toward IT as a service? Is client virtualization simply a shift of computing focus from desktops to data centers? How does it align with the overall move to IT as a service?

This white paper addresses these questions by outlining the basics and benefits of client virtualization and describing how the IT department's role is changing as the client computing landscape shifts. Other topics covered include a full update on thin client computing, the types of devices that are available and how IT departments can support client virtualization – all the information IT staffs need to develop a client computing strategy that is adaptable to today's changing technology landscape.

Client Virtualization

Client virtualization decouples the operating system (OS) from the applications and the user data, rendering those layers into light technologies that can migrate into private or public clouds.

By gaining a better understanding of what client virtualization encompasses, some of the benefits it offers and the number of changes introduced, IT managers can make much more informed decisions on the ultimate direction of their desktop strategy. Furthermore, grasping the relationship between client virtualization and cloud computing and the impact it has on security is vital for organizations that maintain sensitive data, yet need to share technology solutions.

How Client Virtualization Works

IT managers familiar with server virtualization might be under the impression that client virtualization is mainly about virtualizing desktops and moving them to a central data center. Yet when it comes to client virtualization the solutions vary, and some of the challenges are quite unique.

To truly understand the myriad solutions that client virtualization encompasses and what is required for a successful implementation, IT managers need to understand the multiple layers that a desktop is made of.

From an end-user perspective, those layers are transparent; the end user usually interacts only with the software applications to manipulate or generate data. Yet in its most basic form, a typical computer is composed of four layers: hardware, OS, software applications and data.

Although client virtualization solutions may vary somewhat, the notion of moving some or all functionality to the data center is fairly constant. Client virtualization software typically separates the layers and offers a multitude of solutions to deal with one or multiple layers. For example, virtual desktop infrastructure (VDI) abstracts (hides) the hardware layer, virtualizes the OS and software applications, and redirects the user and application data.

What IT managers must decide when thinking about client virtualization (besides whether to virtualize a few or all of the layers) is whether to move some or all of the layers to the data center, or use existing devices and keep the processing local, centralizing only some functions.

Based on the form of client virtualization selected, some layers might remain local (on the desktop) while others are centralized in the data center. For example, in client-hosted virtualization, the desktop runs a virtual machine that isn't in the data center.

Different Forms of Client Virtualization

There are four primary forms of client virtualization, each with its own unique benefits and drawbacks, depending on the needs of the organization.

Client-hosted virtualization: This type of virtualization lets users run multiple operating systems as virtual machines on a single client system. It is ideal for situations in which the end-user device is a high-end machine because the processing takes place locally.

Today, the most common implementation of client-hosted virtualization is using a Type 2 hypervisor or hosted hypervisor. IT managers who have deployed server virtualization are familiar with the Type 1 hypervisor, which is a layer that's installed on the server and sits between the hardware and the operating system.

A Type 2 hypervisor, on the other hand, is installed on top of an existing operating system and lets additional operating

systems run simultaneously on the same computer in an isolated environment.

Type 2 hypervisors are often now used to run Windows XP applications in a Windows 7 environment. IT departments running Macs with Intel processors might be familiar with Type 2 hypervisors, such as VMware Fusion or Parallels, that let them run different operating systems in an isolated environment while also running the Mac OS. There are some Type 1 client hypervisors, but at this point it's still a niche market.

Application virtualization: Application virtualization encapsulates an application and decouples it from the operating system. Through encapsulation, a software application becomes self-contained and does not need to be installed on a computer in the typical way.

Virtualized applications still need an underlying operating system to execute on, but they run in their own isolated environment (commonly referred to as a "bubble"). Because of this, multiple versions of the same virtualized application can run simultaneously, and regression testing can be minimized.

Additionally, based on the solution deployed, it's possible to centralize application distribution and, by doing so, collect usage information. This can be useful in making an informed decision on the number of software licenses to purchase.

Virtual desktop infrastructure: The main idea behind VDI is to abstract the existing hardware; virtualize the operating system, applications and data; and run it all on servers housed in the data center. Since VDI virtualizes the OS, the number of images maintained by IT is reduced tremendously because the image is no longer dependent on the model of the desktop or notebook.

VDI builds on the idea of server virtualization, by running a hypervisor on bare-metal servers and then running virtual machines accessible by end users remotely. A typical VDI solution uses application virtualization to manage software and maintain the separation between the OS and application layer.

With the OS virtualized, VDI is highly centralized and secure because all processing and data reside on servers in the data center. In addition, each virtual machine runs in its own isolated environment and can be pooled with other virtual desktops, or they can be assigned to and accessed by a specific user only.

Client Virtualization ROI

Although the primary benefit of implementing client virtualization may vary greatly from organization to organization, there are three value propositions that are the most common and tend to provide the quickest and best return on investment.

- **Application conflict elimination:** Client virtualization helps avoid some of the inherent problems that crop up with applications running on the same system. This can generate up to a 30 percent reduction in help desk costs. It also allows for reduced predeployment testing and greatly simplifies operating system migrations.
- **Application streaming:** Client computing enables self-service application delivery, reducing license costs and ensuring that users can access apps on any device, any time.
- **License compliance and cost optimization:** With client virtualization, because licenses are needed only for actual users and are no longer tied to a hardware base, related costs will be reduced. Reharvesting unused licenses can save up to 40 percent on software costs.

Profile virtualization: At its most basic level, profile virtualization is folder redirection and support for offline computing. Folder redirection moves designated computer folders to central storage and is transparent to the end user. When a user clicks on a redirected folder, it will appear as if the files are stored locally, when in reality they're securely located in the data center.

In addition, if a user is offline and needs to access a file, folder redirection can be set to save files locally and then sync the changes to central storage when back online. For highly secure areas, the offline mode might need to be disabled because data will be stored on the end-user device instead of remaining in the secure data center.

Each of these forms of client virtualization has a very specific purpose. When evaluating a virtualization strategy, IT managers need to consider what solutions would work best in their environment and possibly combine different solutions to solve a problem.

Client Virtualization Benefits

The need to enhance or add new features is usually one of the main drivers behind implementing any new technology. Client virtualization initiates several benefits, including

security gains; easier configuration, management and maintenance; greater mobility; increased flexibility; and reduced desktop support, to list a few.

Security gains: Although centralizing some or all aspects of the desktop infrastructure has myriad advantages, it also makes the data center a richer target for penetration and potential exploitation. Thus, a complete reassessment of data center security policies and standard operating procedures needs to be a part of any client virtualization strategy.

Client virtualization helps on the security front in several ways. By decoupling and isolating the four computing layers – hardware, OS, applications and data – client virtualization creates a seamless sandbox (that is, a security mechanism for separating programs). This also offers the IT staff the opportunity to design granular solutions that specifically target each of those layers in addition to the existing overall desktop security strategy.

Centralizing one or several desktop layers offers IT departments more control over the environment and increases the staff's ability to monitor and respond to threats. From an OS perspective, virtual desktops can be configured as stateful or stateless. In a stateful configuration, a user is assigned a specific virtual desktop that no one else has access to, and any changes that are made are sustained following a reboot.

In a stateless configuration, when the machine is rebooted, it reverts to its original configuration. This approach can be very useful for functional areas that deal with sensitive data and need that level of security. Some organizations are familiar with this configuration through the use of third-party software that returns the computer to its original configuration on reboot.

Depending on the level of security desired, a solution can be designed that makes it possible to use devices that are not able to store any data (because they don't have any memory) to access virtual desktops. In such a setup, all processing takes place on servers in the data center.

With application virtualization, centralized application delivery makes it easier to patch or update applications when security holes are found. Furthermore, access to applications can be revoked centrally without the need for uninstalling software or creating elaborate ways to disable an application from running through Group Policy.

One of the major security advantages of client virtualization takes place at the profile virtualization layer.

Focusing on People and Process Issues

The tech research firm Gartner maintains that managing hosted virtual desktops requires more than just technical know-how during implementation. Equally important are people and process skills, the ability to effectively manage changes in support and organizational structures.

Because both the availability and the performance of a hosted virtual desktop (HVD) are dependent on servers, storage and networking, multiple technical skills are needed to deliver a desktop service. The 2010 Gartner report, *Organization and Staffing Considerations When Planning for Hosted Virtual Desktops*, goes on to say that hosted virtual desktops will create more interdependencies among different IT teams, as opposed to occasional interactions.

Additionally, the broader benefits that hosted virtual desktops introduce, such as better IT security and remote computing, will require new technologies, location-independent process requirements and different approaches for dealing with software updates.

Furthermore, the report says that existing support structures will likely need to undergo changes in personnel and processes. By shifting to IT as a service, new metrics are required to measure performance.

For physical desktops, typical metrics usually include a number of successful changes (for example, software distributions) during a certain period of time. For HVDs, availability and performance metrics will be more illustrative measures of service quality.

Through profile virtualization, data is located centrally, where it is easier to secure.

By centralizing data, policies can be uniformly implemented for securing data through encryption and appropriate backup procedures. Government agencies and public sector institutions, which must comply with a variety of federal data security legislation, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA), find that through data centralization, legislative and auditing compliance is generally easier to achieve.

Easier configuration, management and maintenance:

Centralized solutions offer numerous management tools to help in configuring, managing and maintaining a virtual client environment. VDI techniques such as image provisioning and linked clones let IT departments reduce

the number of operating system images they maintain to a mere few as opposed to the several dozen they used previously.

In addition, when a new staffer is hired, the only thing that person needs to get started is a device with which to access a virtualized desktop. As long as they have an account and are in the right groups, new hires will have easy access to the software used by everyone else in their department.

Greater user mobility: In most current setups, desktops can be configured for remote access. But because of security concerns, many IT departments tend to disable that feature. However, by centralizing the desktop, the IT staff can design secure ways for granting users remote access to virtual desktops.

Staff can work from any location with an Internet connection. And depending on the network security procedures in place (for example, the requirement to use a VPN client to access a secure gateway), staffers might be able to connect using a number of devices, such as a desktop, notebook, tablet PC and even a smartphone.

Additionally, users who work at different locations would have no need for a desktop at each location because they can connect to a virtual desktop from anywhere.

Increased flexibility: At times, flexibility might introduce additional complexity to the network. The ability to do more – for example, using application virtualization to deploy a new application to all users in minutes – might require a set of new management tools. When thinking about the flexibility that client virtualization can introduce, keep in mind the added complexity of managing and maintaining the new infrastructure.

Reduced desktop support: In some implementations of client virtualization, all processing takes place on virtual machines hosted in the data center. This changes the role of desktop support, which is discussed further in the next section.

Typically, thin clients are used to connect to virtual desktops. And in many instances, these devices have no moving parts, reducing the need for hardware support at the desktop level. As for application and operating system support, the nature of the calls and problems will change. Different troubleshooting skills will need to be developed. But generally, decoupling some of the layers should reduce the number of service calls.

Changing Roles and Responsibilities in IT

The introduction of new technology is usually accompanied by internal and, at times, external changes. Standard operating procedures and workflows may need to be revisited based on the changes the new system ushers in.

New roles and responsibilities in the IT group: The introduction of new technologies naturally changes some roles and responsibilities in the IT department. Desktop support professionals will need to learn new skills and different troubleshooting methods. In addition, depending on the client virtualization solution implemented, some roles may need to be reclassified because requirements can change drastically.

Desktop professionals will need to work more closely with server, storage and network teams to gain a better understanding of the new infrastructure. This interaction will help them improve their ability to troubleshoot and identify any bottlenecks. Reciprocally, server teams will need to understand that client virtualization is not the same as server virtualization and that new skills will be needed for supporting the new infrastructure.

Last but not least, some of the changing roles and responsibilities might affect individuals outside of the IT department. For instance, after implementing application virtualization, software purchasing and licensing models (as well as standard operating procedures for ordering and publishing software) will need to be revisited.

Process changes: With client virtualization, some existing processes may need to be changed and new ones put in place. Certain forms of client virtualization tend to centralize management. In some decentralized environments, such as federal and state agencies and higher education, that kind of process change can be challenging. New workflows may need to be developed and adapted to suit the new environment.

Cultural changes, and how to manage resistance: Staff buy-in and early communication is crucial when considering client virtualization. End users need to be involved at the early stages of a client virtualization project, and expectations must be set early on.

Because client virtualization projects directly impact end users, rank-and-file staff need to participate in testing any prospective solutions, and their input and feedback should be collected and acted on. Desktop support professionals

aren't application experts; they need end users to pinpoint some of the constraints or issues introduced by client virtualization.

Depending on the environment and the type of work that the staff is involved with, some client virtualization solutions may not be suitable. Graphics-intensive or media-rich applications – for example, in a publishing environment – might not be suitable for client virtualization. By engaging end users at the early stages of evaluation and testing, an appropriate solution can be implemented that will suit the majority of the staff.

Client Virtualization and COOP

Most forms of client virtualization discussed here revolve around centralizing some or all of the layers contained in a typical computer. This means that reliance on the data center increases in most client virtualization scenarios, especially VDI, because storage and computing resides in that location. So proper security measures, including reliable power, sufficient redundancy, backups and disaster recovery need to be planned for and put in place.

Certain forms of client virtualization, VDI in particular, turn the data center into the focal point of the desktop strategy. This factor doesn't always get the attention it deserves in the planning stages. It's an important consideration because if the data center goes down, desktop operations grind to a halt.

On the flip side, decoupling and virtualizing desktop computing layers plays a tremendous role in achieving continuity of operations (COOP). Through centralizing desktop services, the IT group gains the understanding and control needed to develop emergency plans for desktop users, their applications and their data. In addition, client virtualization grants users the ability to work remotely in the event of a disaster that prevents them from traveling to their workplace.

Client Virtualization and the Cloud

Client virtualization solutions, in most cases, are about shifting resources into the data center. Application virtualization centralizes software distribution by adding application servers, database servers, the occasional web front-end and a few other components. VDI provisions images, delivers access to applications, and configures and manages virtual desktops.

Given such an architecture, the infrastructure residing in the data center behind client virtualization could be viewed

as a private cloud. Furthermore, some applications might be provided as a service by manufacturers as part of their public cloud offerings. Recently, for example, Microsoft announced agreements with 16 new government and education customers for some of its online services.

Moreover, some cloud providers are offering desktop as a service (DaaS): remote access to desktops hosted in the provider's data center, available for a monthly service fee. This precludes the need to build (and pay for) an internal client virtualization infrastructure.

Cloud offerings are rapidly evolving, so it's important that the IT staff investigate the existing options and do a cost analysis to determine what's best for their organization. And it's important to review the cloud service contract before signing to have a full understanding of service uptime, where data is stored, what data security policies are in place and standard operating procedures in the event of a security breach.

Thin Clients

Thin clients have been in existence for a few decades now. With the advent of client virtualization, IT departments have started to pay closer attention to them. Thin client manufacturers offer several different models, each with its own set of features and suitable for various setups. It's important to take the time to understand how they operate and what advantages they offer.

How thin clients work: A thin client can be thought of as a stripped down version of a desktop that has some type of operating system, such as Windows Embedded or Linux, either installed or streamed to it. The idea behind thin clients is to create a device with only enough components to let end users establish a network connection and interact with a remote session.

Many models are available with different capabilities and limitations. The type or types of thin clients required must be planned for in the overall client virtualization design. For example, certain thin clients can process graphics-intensive work locally, which reduces the load on servers and is more cost-efficient.

Thin client architectures: Similar to desktops, thin clients have a processor, RAM and a network connection, and they need an operating system to function. But that's where the similarities end.

Typically, thin clients have no moving parts such as hard drives or fans, and they are also short on peripherals (most don't have DVD drives, for example).

There are a few points to consider with a thin client architecture. One is whether to offload graphics processing on the thin client or use up server resources and render the graphics apps on the server. It's also important to know which protocols are supported by the thin client's operating system. Certain protocols perform better when using applications that are graphics intensive (as mentioned earlier).

Energy efficiency: Because thin clients are essentially stripped-down desktops, they are more energy efficient. However, this gain is offset somewhat by the power consumed by the server that manages the thin client. IT managers should keep this in mind when looking to measure cost savings from energy efficiency.

Total cost of ownership: The jury is still out on the TCO of thin clients versus traditional desktops or notebooks. The thin client itself is usually less expensive than a desktop and more energy efficient as well. But a thin client is useless without a server infrastructure, and costs associated with cooling, maintenance and support for that infrastructure must be taken into account when considering TCO.

Longer refresh cycles: Unlike desktops, which are typically on a 3- to 5-year refresh cycle, thin clients generally operate on an 8-year refresh cycle. With thin clients, the actual refresh is a lot less time-consuming because most everything touched on in a typical desktop refresh already resides in a data center and only the thin client device itself needs to be replaced. As soon as that's done, end users can go back to the last task they were working on with little disruption.

Questions to Ask About Thin Clients

Here are six areas to investigate before moving forward with a thin client deployment:

- What is the current desktop strategy, and how will client virtualization improve that strategy?
- What are the current issues that need to be resolved, and how can client virtualization help?
- How will thin clients affect the user experience?
- What is the impact of thin clients on the network infrastructure, in terms of performance and bandwidth?
- What is the impact on storage, and how scalable is that infrastructure?
- Does the current IT staff have the skills required to configure and manage a client virtualization infrastructure? If not, what type of training is needed?

Better security: Given that a thin client has few components and a stripped-down operating system, the device can play a positive role in data security. Neither personal nor application data is stored on the thin client – all of that resides in the data center. In addition, USB ports on certain thin client models can be disabled, rendering those ports unusable.

Other Client Devices

Thin clients aren't the only devices that can be used to access virtual desktops. Other client devices, such as netbooks, smartphones, tablets and zero clients, can be used as well. Also, older PCs can be repurposed and used as thin clients.

Because so many different devices can deliver a virtual desktop environment, some organizations have started Bring Your Own Computer (BYOC) programs. With BYOC, users are given a stipend to purchase a device, and that new machine is the staffer's gateway to accessing a virtual desktop. In other words, users can utilize their own computer to access a virtual work desktop and departmental resources.

Zero clients are similar to thin clients, but as the name suggests, they are even more stripped down and require less time to manage and maintain.

Client Virtualization Support Needs

Client virtualization introduces a new desktop strategy with multiple features and benefits. To maximize returns on that investment, organizations need to think carefully about the changes and challenges that a new strategy brings.

Infrastructure support: When considering client virtualization, especially VDI, organizations need to view it as a shift of resources from desktops to data centers. It's important to assess, as part of the planning phase, the potential cost and impact of housing this new infrastructure in the data center.

For example, are there enough power circuits and connections to handle the servers needed for a VDI implementation? Will the existing cooling units be able to handle the extra load, or will additional cooling be needed? Are there enough network connections, and is there sufficient bandwidth? Is there room to expand and add more servers in the near future? Those are some of the questions that need to be answered as part of the cost assessment for a VDI implementation.

There are additional concerns for organizations that have implemented server virtualization and have an existing solution for managing that virtual environment, including a hypervisor. Depending on the client virtualization solution selected, a different hypervisor might be implemented. This will introduce greater complexity to the existing infrastructure, along with the possibility of having to manage multiple hypervisors and their associated tools.

Device support: Thin clients still need to be managed and updated (though less frequently than a regular desktop). So a system needs to be in place to upgrade firmware or to patch the embedded operating system.

In addition, organizations will still need hardware support to handle faulty thin clients, failed monitors and peripherals. And depending on the solution implemented, support may be needed for older desktops used as thin clients. Security is another consideration. Support for equipment such as biometric scanners, smart-card readers and two-factor authentication tokens also needs to be in place, if needed.

Storage: Client virtualization differs from server virtualization, and existing storage will need to be tested with the new infrastructure. Recent research has shown that storage design plays an important role in virtual desktop performance.

Operating system reads and writes to disk, measured as inputs/outputs per second (IOPS), are very different for servers than for desktops. Measuring IOPS in a VDI environment and the impact that this has on existing storage is important in deciding whether changes need to be made.

Licensing: Before deploying client virtualization, be sure to study any existing contracts, available software licenses and restrictions. Licensing costs may change depending

on what's being virtualized, how it's being accessed or distributed and from where. For example, with VDI, to access a virtual machine running Windows, there's a yearly license fee associated with that model that might not be part of the Microsoft contract.

On a more positive note, client virtualization may help in cutting down on software purchases because some solutions deliver application usage reporting. For example, an organization may move to a concurrent licensing model for some software and could possibly see a reduction in its licensing costs of around 30 percent.

Invest in Infrastructure

Greater flexibility and mobility in computing environments often brings greater complexity. Certain client virtualization solutions shift costs from desks to data centers and require a significant investment in infrastructure. Through this investment, organizations can leverage the newly added benefits of their environment, such as user mobility.

But for organizations to reap the benefits of client virtualization, certain network security and protection layers must be considered. For remote users who need access to local resources, a virtual private network (VPN) appliance is required to enable secure remote access. A VPN establishes a secure and encrypted tunnel between the remote endpoint and the local network.

Additionally, in cases where the staff is using their personal unmanaged machines to access organizational resources, a network access control (NAC) appliance is highly preferred. With a NAC, the endpoint must ensure that it meets criteria set by the IT team, such as a certain patch level, an antivirus solution and its latest virus definitions, before it is allowed to access organizational resources.