SEPTEMBER 2012

CLIENT VIRTUALIZATION

Centralized management of endpoints for security, cost-efficiency and sustainability benefits

800.800.4239 | CDW.com/clientvirtguide

CDW REFERENCE GUIDE

A guide to the latest technology for people who get IT

CDW® PEOPLE WHO GET IT™

WHAT'S INSIDE:

800.800.4239 | CDW.com/clientvirtguide

Visit CDW.com/clientvirtualization for more information on client virtualization.

GET M.CDW.COM ON THE GO

m.cdw.com is now available anywhere with our new mobile-friendly website or download the CDW app for your iPhone from the App Store.

SCAN IT

Download a QR code reader on your mobile device to scan and see how CDW solved client virtualization problems.

What is a CDW Reference Guide?

At CDW, we're committed to getting you everything you need to make the right purchasing decisions — from products and services to information about the latest technology.

Our Reference Guides are designed to provide you with an in-depth look at topics that relate directly to the IT challenges you face. Consider them an extension of your account manager's knowledge and expertise. We hope you find this guide to be a useful resource.

Meeting Today's IT Needs

Addressing the growth in diversity and distribution of computing devices while reaping security, management and cost-efficiency benefits

Desktop PC management has come a long way over the years. Many younger IT administrators likely cannot recall a time when their job would have included visiting each and every workstation in the organization (usually with a sleeve of disks) to load software, upgrade applications or configure security settings. And the employees who were supposed to be working at those computers when the admins arrived? They were left biding their time until their PCs were ready to use again.

These days, most software patches upload automatically over the network; a central server hosts and pushes out applications; and the IT team can know when a virus has infected a user's system almost immediately. Client systems can be locked down so that no changes or random software installs occur; operating systems configured so that only authorized users can access client and network resources; and remote-management software makes it possible for IT workers to troubleshoot an end-user device from any location on the network.

It's a near-perfect world for IT management — except recently, technological developments have brought even more drastic change to the situation.

Endpoint Proliferation

The desktop system is no longer the only place where client computing occurs. It's often not the only system a worker uses for productivity applications, communications or accessing networked resources, such as data stores and enterprise software. Notebook PCs initiated this change; high-performance tablets, smartphones and other devices continue to move it forward.

Today, referring to "desktop PCs" to describe a client computing environment is no longer adequate. Desktops, notebooks, tablets, iPhones and Android devices — they're all endpoints now, client devices that access the enterprise network. And they all place an additional management burden on IT departments.

Regardless of how advanced an organization's desktop PC management program may have been, its IT team likely didn't plan for the diversity and wide distribution of devices now common in many computing environments. Client virtualization is the next major step in regaining control of endpoints and reaping security, management and cost-efficiency benefits.

In CDW's 2011 *Client Virtualization Straw Poll*, in which 200 IT managers were interviewed, 90 percent said they were considering a move to client virtualization. And almost 60 percent say it's as important to them as server virtualization. At the same time, nearly all the surveyed respondents say they have encountered challenges in considering and implementing client virtualization. It's clear that this is an IT initiative that requires education and analysis.

Client virtualization can deliver benefits similar to server virtualization, but the former should not be seen as an extension of the latter. Client virtualization decouples the various components of a traditional computing device — data, applications and operating systems, for instance — so that a central IT group can manage and serve them to users in a controlled, flexible manner.

The organization determines which components it wants to decouple from endpoints and how it would like users to access those components. In one form of client virtualization, an entire desktop environment is hosted on a server as a virtual machine (VM) and delivered to the user over a network.

But that's not the only form of client virtualization, nor is it the right solution for every organization. There are approaches that virtualize only applications, for example, and there are client virtualization architectures in which the VM runs on the endpoint, not on the server.

But before examining those choices, it's important to understand why client virtualization is worth investigating in the first place.

Why Consider Client Virtualization

No matter how an organization eventually architects its client virtualization solution, it first must spend the time and resources to investigate the possible options.

There are many reasons an IT department might consider client virtualization. Chief among them is that no matter how streamlined a client management system is today, it's not completely frictionless. Users can still disrupt their systems. Click the wrong Twitter link, and a user can download a virus that turns off centrally managed security software, which in turn would require a visit from the IT group to address.

Today, computing has fundamentally changed. The more time the IT team can spend on initiatives such as cloud computing, service-oriented architectures and data center consolidation, rather than on client management, the better it can support and adapt information systems to meet the organization's goals and missions.

Increased reliance on mobility, one of the fundamental changes to end-user computing in recent years, might also drive organizations toward client virtualization. Initially, notebooks were enterprise devices, managed (through considerable effort) by the same IT department that had to keep desktops, servers and network infrastructures secure and productive. But now the ownership situation has been shifting.

Notebooks, tablets and smartphones, powerful computing devices in their own right, are being purchased by people for their personal use. And many workers have begun pushing for the same mobility on the job that they enjoy in their personal lives. (This growing influence of consumer market technologies in IT innovation as opposed to business market drivers is known as the consumerization of IT.) In some cases, users even want to access enterprise resources on their personal devices — something previously considered taboo by most IT departments.

The benefits derived from bring-your-own-device (BYOD) initiatives aren't just for employees. Allowing workers to communicate, access enterprise programs and manipulate data on personal mobile devices can also be a boon to organizations.

With a BYOD program, employees are allowed to buy (sometimes with the assistance of a stipend) their own mobile devices and use them within the organizational systems infrastructure. By embracing BYOD, organizations keep their staff happy, foster productivity and avoid some of the purchase cost (and often some maintenance expenses) of the devices themselves.

On the other hand, BYOD also increases the number of endpoints that an IT department must accommodate. If every worker needs a desktop or notebook computer and a smartphone, and suppose some also want enterprise access on their personal tablet (or any combination of enterprise and BYOD computing platforms), then the tech support implications are considerable. Also consider that users might have to interact with computing resources and applications differently from device to device.

Workers may understand instinctively how to access data and apps from their desktop interface, but strip away that familiarity, and make the same data and apps available in mobile versions — the tech support calls will mount.

Through client virtualization, in addition to centrally controlling access to data and applications across multiple endpoints, the IT shop can begin to standardize the client computing experience so that the interface has a similar look and feel across all devices, thereby boosting productivity and reducing support needs.

Adoption Drivers

In light of the increasingly heterogeneous client computing environment, there is a litany of interrelated drivers that might prompt IT departments to embrace client virtualization, such as the following.

Software distribution: It can be a management challenge to ensure that software is up to date and running without conflicts or configuration issues. Getting new or upgraded software out to various mobile devices, given multiple configurations and often varying operating systems, magnifies the challenge.

Software distribution management also entails testing to make sure new software doesn't conflict with old. The more endpoints that need a particular app, the longer the process can take.

OS upgrades: One of the most challenging upgrades in IT is the operating system refresh because the OS is foundational and touches everything from apps to peripherals. It's why many organizations try to find a solid OS platform and ride it out as long as possible.

But upgrades can't be avoided forever. For example, Microsoft will cease all support of Windows XP in April 2014 (the OS having debuted in 2001), so any organization still using XP is likely planning an OS deployment. Also of note, Microsoft will be releasing Windows 8 in late 2012.

Data security: The more endpoints a computing environment has, the more likely it is that sensitive enterprise data resides somewhere exposed on a device. There are certainly solutions for managing and securing mobile devices, but for some organizations, abstracting data from a device may be the best solution. Moreover, when data is stored centrally rather than on clients, the data center can easily back it up.

Cost: Desktop systems typically cost from $1,000 to $3,000 per year to support. With IT budgets stretched thin (and in some organizations, cut severely), any opportunity to trim ongoing maintenance costs will resonate with IT leaders.

INTEREST ON THE RISE, *DESPITE CONCERNS*

In a 2012 survey of 1,300 IT decision-makers worldwide, Cisco Systems found that 79 percent of respondents plan to implement virtual desktop technology, one of several options for client virtualization *(see Chapter Three: Architecture Options)*.

Some organizations are already in the process, with 25 percent saying they currently use virtual desktops (55 percent say they plan to do so within the next three years).

But the Cisco survey also identified several barriers to adopting virtual desktops that are common to all client virtualization initiatives:

46% Cost

45% Bandwidth requirements

37% Performance issues with the WANs that virtualized clients might have to traverse

34% Integrating client virtualization with traditional client computing

33% The belief that virtualizing desktops is too complex

SOURCE: *Cisco Global Cloud Networking Survey*, 2012

And although organizations have made strides in extending the useful life of their desktop and mobile computers, equipment does eventually require an upgrade. With client virtualization, at least on the desktop, organizations can employ thin clients or zero clients, which don't have as many components as a traditional desktop or notebook and can cost as little as $200.

Sustainability: Similarly, if an organization has made green IT an operations priority, client virtualization and thin client computing can save power. Typically, their load is less, and they emit less heat. Thin clients also require fewer materials that might end up in a landfill.

Despite the potential benefits, client virtualization is far from a perfect solution. In some situations (at first glance) it might not make sense, either enterprisewide or within a group or department.

For example, environments with a significant mix of basic knowledge workers and power users may not seem to be the best candidates for client virtualization. Power users often prefer a traditional computing environment that allows them to constantly customize their systems and install their own software. They may also enjoy greater IT privileges to alter their computing systems on a regular basis based on job function, such as engineering or software development and testing.

But such environments can also benefit from client virtualization. Ironically, the most complex engineering environments (in which developers traditionally switch among multiple desktop platforms) are well-suited to a virtual desktop infrastructure (VDI), the most involved of the client virtualization architectures *(see Chapter Three: Architecture Options)*. But the best client virtualization strategy is to focus on the easiest environments first and then follow with the more complex ones.

Client virtualization is best suited to pools of users who need a standard suite of applications. A call center is often cited as an optimal candidate. It's critical to evaluate the computing that goes on within the organization. Even though the technologies that support client virtualization — servers, networks, storage and client devices — are continuously improving, certain legacy software or programs with intense graphical requirements might not function well in a virtualized environment.

Overcoming Barriers to Adoption

Of course, as with any new approach to something that's been done the same way for a long time, client virtualization presents hurdles that IT groups often struggle to surmount. While most organizations can empathize with the various drivers that push technology managers to consider client virtualization, many also have unique reasons for proceeding with caution.

Some of the reasons are legitimate, such as concerns over application compatibility, which can present challenges in a client virtualization deployment. Other skepticism is based on not being sufficiently informed, such as worries about a new technology's maturity. Although some forms of client virtualization are indeed leading edge, others have been around for decades.

The costs involved with implementing client virtualization mainly derive from the infrastructure build-out needed to support it. Those costs are not necessarily tied to the clients. In fact, once an infrastructure is in place, the cost of deploying and managing new desktop or mobile clients can be considerably less than for their traditional counterparts, both from a capital expenditure

and an operations perspective.

For example, because much of the processing and storage needed for client virtualization happens in the data center, it's less important to keep a high-performance system on the desktop — a system that likely must be replaced every three to five years. Thin clients can last for as long as six to eight years. And configuring one for a new user requires considerably less IT support because the desktop environment resides on a server, not on the client.

That being said, depending on the organization and its existing infrastructure, client virtualization may require an upfront investment in the following areas:

- Servers to run the virtualized components
- Software to manage and provision the clients
- Storage to hold everything from virtual desktops to client data
- High-speed connectivity to ensure that the client experience is the same as if all the client components were local

If an organization focuses on total cost of ownership and requires a satisfactory TCO calculation before moving forward with client virtualization, it may have to wait a few years. Client virtualization is a new way to deliver an existing IT service, and its benefits are best seen in ongoing IT operations (*see Chapter Two: The Value Proposition*).

For example, it is hard to quantify the cost benefit of virtual client upgrades (in which IT migrates operating systems from the data center instead of at the desktop) until they actually happen, and that can be several years from initial deployment.

Finally, in many organizations, the user presents a significant barrier to client virtualization adoption. In large part, this is because although the virtualization backend is largely transparent to a worker on a computing device, the computing experience may change. The extent of that change will depend on the virtualization architecture an organization adopts.

For example, when virtual desktops are run from a server, users may lose the flexibility to customize their environment or install apps themselves. If not implemented properly, with the right attention to infrastructure planning, client virtualization also can result in a slower computing experience.

Users today typically expect a rich, graphical desktop environment with streaming video. If a virtualization solution hinders that, users will be dissatisfied. Plus, whenever client computing resources are centralized (software and data, in particular), users tend to feel they're being monitored.

These barriers to adoption can be addressed, but first the organization should work on achieving a shared understanding among users of what client virtualization actually entails.

A Different Shade of Virtualization

For several years, IT departments have heard the constant refrain to virtualize, virtualize, virtualize in the data center. For that reason, many IT managers approach client virtualization with some preconceived notions.

In fact, client virtualization is a distinctly different initiative from other virtualization projects. While not a logical extension, pursuing client virtualization can boost an organization's IT efficiency more than either strategy alone.

Among the popular misconceptions about client virtualization are the following.

It's old-school technology. Yes, some forms of client virtualization have been around since Windows NT. But the modern, high-speed high-performance infrastructures that they run on have rendered them new (think terminal

CONTINUITY
AND THE *VIRTUALIZED CLIENT*

When it comes to business continuity (BC) and disaster recovery (DR), client virtualization is a two-sided coin: There's what client virtualization offers in terms of continuity and DR preparedness, and what it requires.

Of all the reasons to consider client virtualization, BC and DR may be the most compelling. For example, if a sensitive government agency can never afford a massive virus outbreak in its desktop environment, client virtualization can help it ensure uptime.

Or, as another example, if a company happens to locate its headquarters where earthquakes, tornadoes or hurricanes are common, and losing days or weeks to a natural disaster would cripple operations, then client virtualization presents a compelling, mission-critical investment.

When client computing resources are abstracted from the physical device and then moved to a central data center, those resources are accessible from a variety of endpoints and under myriad conditions. If an office closes for whatever reason, workers can access the identical computing environment from home, on the road or even from a backup office in a nearby location, equipped with cost-effective thin clients.

Client virtualization also supports BC and DR in situations where physical systems and offices are available, but computing resources are not. Not all disasters are natural disruptions; corrupt files, application conflicts and other issues can also erode an organization's productivity. So maintaining applications or entire desktop environments in virtual machines can improve uptime.

Through client virtualization, when technical issues arise that prevent desktop or mobile devices from operating effectively, IT departments can easily roll back to an earlier instance of the virtual client or provision a clean desktop image from a central server, depending on the architecture.

What's unique to client virtualization is the continuity and DR required to ensure that the virtualization architecture itself remains up and running. In a traditional desktop computing environment, if one computer goes down, the IT group can offer a backup with the same OS, applications and network resources (though with different settings and no access to what had been stored locally).

But with a client virtualization architecture, data center failures can take down an entire fleet of endpoints. The virtualized architecture itself needs a continuity and recovery plan.

services). Call them proven or mature, but they're not old school.

Existing desktop licenses will easily transfer to a new client virtualization environment. Actually, licensing can be one of the most complex pieces of a client virtualization rollout. Usually, an organization needs to renegotiate licensing. It's best to bring in an expert to help navigate the requirements.

Virtual desktop infrastructure can be deployed in a month. Although the task of deploying virtualized desktops and applications eventually will be reduced to minutes, building out the infrastructure takes time, from modeling and assessing the organization's current applications and conducting a pilot to designing and implementing the required infrastructure. Many deployments take six to 12 months, though the time frame can vary depending on the size and complexity of the environment.

There is little to no return on investment from undertaking client virtualization. Such thinking couldn't be further from the truth. Depending on an organization's size, applications, security requirements and more, there are several opportunities for realizing fast, appreciable ROI.

For example, because software licenses cover the number of actual users rather than the number of endpoints, organizations should see lower licensing costs. Moreover, because client virtualization reduces or eliminates the types of software conflicts that arise when traditional applications run on fixed OSs, organizations will experience a drop in help-desk costs.

But client virtualization isn't just about achieving ROI. It's also (maybe more) about changing the way an organization delivers desktop services in response to an evolving computing environment. For many, the benefits offered by that change make up the bulk of the business case that justifies migrating to a virtualized client environment. ■

The Value of Client Virtualization

Finding the benefits, both direct and indirect

If the IT staff never has to visit another desk to troubleshoot a problem, it will have more time to devote to strategic projects. If the IT manager never has to field complaints from workers who can't access their client computing environment from their home office, he or she will have addressed a growing enterprise requirement. And if the IT organization can enable access to enterprise applications for an increasing number of mobile computing devices while ensuring security, it will have ushered in new opportunities for productivity and service within the organization.

Client virtualization can help accomplish all of the above, and more.

Effective Endpoint Management

Perhaps the single greatest benefit of a client virtualization strategy is less complex endpoint management. Regardless of the virtualization architecture an organization chooses, centralizing one or all of its traditional client components means the IT department can exercise significantly more control over the environment, improve the shop's ability to monitor and respond to issues, and ultimately perform endpoint management tasks in the data center — not at individual workers' desks.

Endpoint management benefits manifest themselves as soon as a new hire joins an organization. Instead of configuring a desktop or notebook system and delivering it to the new hire's location, the IT group can provision a hardware device already in place using software images and computing resources that reside in the data center.

Similarly, when staff switch offices, they don't need to bring their preconfigured computing devices with them. As soon as they sit down at a new endpoint, their computing environments (OSs, user profiles, applications and data) stream to them wherever they are located.

This ability to provision clients from a central location is especially important for employees who need

/// WITH CLIENT VIRTUALIZATION, VIRUS OUTBREAKS ARE EASIER TO CONTROL AND AVOID BECAUSE OF SOFTWARE, OS AND DATA ABSTRACTION.

or want multiple computing devices (desktop, notebook, tablet). Through client virtualization, the IT department can deploy the same computing environment (with the same permissions and enterprise resources) to whichever endpoints the worker uses, without having to physically set up each device.

Once endpoints have been provisioned, client virtualization helps ease ongoing management by letting the IT team conduct routine maintenance from the data center, instead of at the endpoints. For example, when OSs or apps need to be patched, that work can be done on the central, virtualized instances of those resources.

Users won't experience any disruption. And when they next launch their endpoints, they will be running the patched environment. The same goes for more significant upgrades to productivity software or enterprise apps.

Client virtualization also lets the IT department distribute new software to users without having to touch each desktop, notebook or other device. And because the OS and other apps that new software must interact with are also located in the data center, the IT department can test them together for conflicts before pushing them out to users. Depending on the organization, this preproduction testing can be a major benefit.

For example, upgrading hundreds or even thousands of users to a new productivity suite can take months, if not longer. The software must be tested on the organization's primary OS (or in many cases, OSs) and with other programs users work with regularly.

Centralization makes it easy to identify whether a new word processor or e-mail client, for instance, interoperates with the organization's records management platform. By testing and troubleshooting client apps in the data center, then pushing an identical verified software image to each endpoint, the IT team avoids having to validate new software on individual systems, which over time may have developed their own issues and software conflicts.

On the flip side, removing virtualized applications from an endpoint, or revoking a user's access to an application or resource, can also be done centrally. There's no need for a systems technician to visit a user's desk to uninstall software.

And should a user's system become inoperable through either malware or application conflicts, the IT department can reprovision the client in minutes from an image stored in the data center. Depending on the level of client virtualization, all of the user's data is immediately accessible because it's stored virtually in the data center — not on the users' devices.

Additional Benefits

Although effective endpoint management is the greatest benefit of client virtualization, there are others, including the following.

Better security: In addition to the ability to control patch management and other endpoint security details, a client virtualization deployment enhances security in other ways. For example, if the organization decides to utilize client virtualization with thin clients, concern over computer theft becomes less of an issue because the client holds no data and generally costs less than a traditional desktop system.

Similarly, endpoints in a client virtualization environment can be configured to be "stateless," or nonpersistent. That means at the end of each computing session, the user's desktop environment is wiped clean and it restarts from the original configuration the next time a user logs in. Plus, organizations can set up endpoints so they don't store any data locally, directing it all to secure storage systems in the data center.

In addition, virus outbreaks are easier to control and avoid because of software, OS and data abstraction. With parts of the computing environment decoupled and virtualized, it's easier to isolate viruses, ensure they don't spread and ultimately remove them without affecting other users in the environment. In certain architectures, if a user accidentally downloads a virus or spyware, it is unable to propagate and will disappear when the session ends because the virtual machine is isolated.

Heightened compliance: A client virtualization solution can be especially helpful to organizations that must comply with laws or regulations written to protect data. In many client virtualization architectures, data is centralized and access is stringently controlled.

This allows organizations in government, healthcare, financial services and other industries to better protect sensitive data, such as health records or credit card information, and comply with legislation such as the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA).

Not only is the data better protected,

but because computing resources are centralized, it's easier for organizations to demonstrate and audit their compliance with regulations in a virtualized environment than if they operated traditional desktop computing platforms. The data they need for reporting resides in a single location, not on multiple local drives.

Increased flexibility and agility: Organizations can deploy new applications and capabilities more quickly than in a traditional desktop environment, making it easier for them to adapt to changes in their industries or to seasonal computational workload peaks. Moreover, applications can be configured for "self-service," meaning users can request and stream programs to their endpoints as needed.

Additionally, should the IT staff need to uninstall a program, whether enterprisewide or from a specific user, it can simply revoke the virtualized app via a management console and then move on to other IT tasks.

Greater user mobility and secure remote access: Demand for mobility is one of the biggest drivers of client virtualization. Many users don't understand that they could have remote access to their systems if the IT department allowed it. By centralizing the client environment in the data center, the IT team can feel more assured in letting users work remotely.

With client virtualization, employees can work from wherever they can access an Internet connection. Depending on the architecture and network security infrastructure, they can use a variety of devices — including their own, whether a smartphone or tablet.

By enabling secure remote access, an organization takes a significant step in its business continuity and disaster recovery planning. Should anything happen to disrupt access to an office site, workers can either work from an alternate location or from home without interruption.

Help-desk relief: The endpoint management available through client virtualization means the IT group doesn't have to visit as many locations to troubleshoot applications, settings and other desktop minutia. In addition, when thin clients are adopted to access virtualized computing environments, hardware support needs plummet.

Because thin clients have no moving parts, they are less prone to breaking than desktop systems. The help desk no longer needs to diagnose damaged hardware, and it doesn't need to arrange for potentially costly shipping and repair. It also doesn't need to keep as many spares in reserve for malfunctioning or broken systems.

Longer desktop refresh cycles: With no drives, fans or other moving parts, thin clients typically last several years longer than traditional desktop computers, and they're less expensive. So the IT department can develop a new refresh cycle that includes less costly purchases, less often — freeing up resources for other initiatives, such as maintaining the virtualized environment or creating new apps and processes to support the organization's mobile workforce.

Identifying Measurable ROI

How do the benefits of client virtualization translate into dollars and cents?

By some estimates, almost half of organizations that consider client virtualization struggle to quantify the potential return on their investments. And considering there is a cost involved with building out a client virtualization infrastructure, it's important to identify possible sources for savings. The following are six areas where organizations can expect return on investment (ROI).

Power savings: If the organization goes the thin-client route, it can realize ROI due to consuming less power. Thin and zero clients require less power to operate, and they give off less heat, so office site may require less cooling.

Capital costs: Thin client units typically cost less than traditional desktop systems. They also last longer between replacements. If timed to coincide with a preplanned desktop refresh, the move to client virtualization can have an immediate cost benefit.

In addition, a move to client virtualization should be viewed as an opportunity to extend the useful lives of existing desktop PCs (essentially turning them into thin clients), and creating a lower total cost of ownership (TCO).

Help-desk head count: Because client virtualization allows the centralization of troubleshooting and management (and therefore fewer visits to users' physical desks), fewer technicians are typically needed to support the organization's computing environments. But take note: Some organizations choose to parlay that ROI into other projects. In other words, they take idle IT staff and move them to other technology initiatives, which can potentially translate into even greater ROI.

Opportunity costs: Troubleshooting and fixing an issue with a virtualized client can take significantly less time than troubleshooting a traditional desktop environment. Because client virtualization reduces app conflicts, some groups can see help-desk costs drop as much as 30 percent. Again, those savings can help either reduce head count or reappropriate idle resources to other projects.

Break-fix costs: For a variety of reasons, client virtualization translates into lower costs for fixing damaged endpoints. To start with, thin clients last longer. They have few moving parts that can fail, and they can be easily replaced without having to reconfigure an entire PC or ship the client to a service depot for repair. Moreover, when a thin client needs to be fixed, the cost to reimage the software environment is minimal.

Unified software licensing: The move to client virtualization can also have a positive effect on an organization's licensing costs. In most situations, a software or OS license is tied to a user, not a machine. So by centralizing software licenses, an organization can identify and eliminate redundant or unused licenses.

In some instances, organizations may be able to cut licensing costs by 40 percent. To be clear, however, there may be upfront licensing costs to bring software into compliance with requirements for running some programs in virtualized environments (*see Chapter Four: Technology Requirements*).

Intangible ROI

Not all ROI from client virtualization will be immediate or easily measurable. Still, residual savings can add up over time or contribute to some of the measurable savings detailed previously. The following are four areas that typically deliver benefits but are not easy to quantify.

More efficient client management: With a minimal number of desktop images to maintain (sometimes, as few as one), deploying new clients or rolling back clients to the last problem-free configuration can take mere minutes.

More efficient patch testing and release management: With much or all of a client environment centralized, it is easier for the IT team to test new patches, software upgrades and entire applications. As a result, there is time to conduct thorough testing to ensure a rollout of computing resources that gets it right the first time, every time.

Quicker deployment of new applications: In related savings, the IT department can get new functionality out to users far faster in a virtualized environment. In some architectures, applications can be configured for self-service, allowing users to request and access programs themselves without any intervention by IT.

Greater control over desktop and application security: Needless to say, one of the most significant drags on productivity and ROI (and a major cost center) occurs when entire pools of clients can't function because of a virus outbreak or security breach. Thanks to the security benefits of client virtualization, a boost in client uptime can improve ROI from the computing environment. ■

CLIENT VIRTUALIZATION AND THE CLOUD

Client virtualization and cloud computing have a lot in common.

By decoupling client system resources and moving them to a data center, organizations are taking steps toward establishing their own private clouds. In addition, they can more easily incorporate cloud services from third parties into their virtualized environments. This includes services such as customer relationship management, e-mail or other software as a service applications. There are even cloud providers beginning to offer desktops as a service.

More immediate, however, client virtualization represents a step toward deploying a more recognizable cloud solution. These days, enterprises are exploring the cloud-based app model for their distributed workforces. Organizations can build their own app cupboards in the cloud with validated, secure software programs available for downloading to a variety of endpoints.

Architecture Options

Choosing a path to client virtualization's benefits

There are many ways for organizations to implement client virtualization. Some cover the entire client computing environment, virtualizing everything from applications to data storage on a server. Others take a piecemeal approach, choosing a combination of server-based virtualized components and local system-based components.

The different client virtualization architectures can be thought of in terms of the following:

- **Where the computing occurs physically:** in the data center or on the device
- **What the user accesses virtually:** applications, storage or both
- **How the IT team manages what each individual can access:** through individual user profiles

When it comes to selecting an architecture, the organization must decide if it wants to deliver virtualized applications or entire virtualized desktops.

Often, the answer is applications. Whether driven by mobility or IT management efforts, many organizations want to centralize their applications and let users access them as needed. But in other cases, whether driven by security concerns or unique computing environments (such as developers and engineers who have multiple computers under their desks for working on various platforms), delivering entire virtualized desktops is the better option.

Understanding what exactly should be virtualized helps in selecting the appropriate virtualization architecture.

Presentation Virtualization

When an organization determines it wants to deliver applications via client virtualization, presentation virtualization should be one of the first architectures considered (though it can be used for delivering entire virtual desktops, too).

Even if an organization is inexperienced with client virtualization, it may have some experience with presentation virtualization, also known as terminal services (now commonly referred to as remote desktop services or RDS).

Presentation virtualization has been around for more than 20 years and is often considered old-school computing. But, in fact, it is one of the most mature methods of client virtualization and is widely used today.

Terminal services technology was introduced in Windows NT 4.0 Terminal Server Edition. It's been enhanced significantly over the years, and most versions of Windows today include client applications for using virtualized services. Additionally, third-party software developers offer presentation virtualization solutions that build on Windows RDS.

With RDS, applications run on a shared Windows server in a data center. But their interfaces are presented on a remote endpoint, such as a standard desktop PC, notebook or thin client. Either individual applications or entire desktop environments can run across a network without IT staff needing to install them on the endpoint. Only keystrokes, mouse movements and screen data actually move back and forth.

Using RDS, an endpoint connects to a web portal, which can be an actual Windows RDS portal or a third-party virtualization system that runs with Windows Server. This intermediary requests virtualized application sessions and delivers them to the user.

Although presentation virtualization is most closely associated with remote applications, its support for published desktops is notable. Such virtualized desktops can appear identical to standard Windows desktops, providing users with a look and feel that is intuitive.

Because presentation virtualization has been around for so long, it's considered a proven technology. It can support almost any endpoint device and operating system, provided the device is running the supported RDS client. Among other things, presentation virtualization helps ensure that an organization is running a consistent version of a software application throughout its enterprise and makes it much easier for the IT group to provision software because application sessions initiate on demand.

Presentation virtualization is often compared with virtual desktop infrastructure (VDI) in situations where organizations want to reinvent their desktop computing environments. Because presentation virtualization shares a single instance of Windows Server among multiple sessions, each session uses fewer resources than an equivalent VDI session. This means that presentation virtualization can cost less to implement than VDI.

Organizations should make sure that the applications they want to deploy in a presentation virtualization architecture are compatible with Windows Server. And, although it may be unlikely, some software companies may not allow their applications to run on a virtualized server. If such a situation arises, VDI can usually overcome such issues.

Although it can be done, it's a challenge to deliver entire desktops using presentation virtualization. From managing changes to the environment to thoroughly testing software updates, presenting desktops via presentation virtualization can eat up IT time and resources, especially in organizations with a computing environment that frequently changes.

Virtual Desktop Infrastructure

If an organization determines it wants to manage entire desktops centrally and deliver them to users over the network, virtual desktop infrastructure is the next logical consideration in client virtualization technology. The concept behind VDI is to abstract everything. Virtualize the operating system, applications and data, and run it all on servers.

Because VDI virtualizes everything, the number of software images that the IT organization must maintain drops considerably. For example, the IT team won't need separate images for different models of desktops and notebooks.

Similar to presentation virtualization, VDI runs from the central data center. But unlike presentation virtualization (which uses a shared server OS to deliver applications or desktops), VDI involves running client OSs, such as Windows 7, as virtual machines using hypervisors.

Only one user at a time can access a VM, which enhances security in a VDI deployment. Typically, the VMs reside in the data center, although there are architectures in which they run on client endpoints *(see the Intelligent Desktop Virtualization sidebar)*.

When the VMs are centrally hosted, users need only a network connection to access their desktops. Any device may be used, as long as the VDI vendor supports it. The VM environment will have the same look and feel from any device being used to log in.

Because VDI wraps up an entire desktop computing platform (including apps and OSs) and delivers it to the user, it can offer better application compatibility. And in addition to enhanced security, VDI offers better protection against OS failure because each VM runs its own OS. (In presentation virtualization, if a Windows server goes down, it affects many users.)

VDI also offers flexibility. For example, the virtual desktops can be stateful (or persistent). The user can customize a stateful virtual desktop because there's a one-to-one relationship between the two. When the virtual desktop reboots, it looks the same as when it was shut down.

But a stateless, nonpersistent virtual desktop is wiped clean at shutdown and presents a clean startup desktop every time it's launched. Depending on the organization, the IT department may want to prevent or allow changes to the client.

In general, VDI can be more costly to deploy than presentation virtualization. Choosing one or the other requires a detailed analysis to determine which of their respective benefits

INTELLIGENT DESKTOP VIRTUALIZATION

Believe it or not, there will be situations in which deploying the reverse of a virtual desktop infrastructure makes sense. Call it client-hosted, intelligent desktop or even distributed desktop virtualization. This model of client virtualization lets users run multiple operating systems as virtual machines on a single desktop system.

In client-hosted virtualization, a Type 2 hypervisor often runs on top of an existing operating system so that other OSs can run simultaneously in their own isolated areas. (A Type 1 hypervisor runs directly on hardware, as in server virtualization, to manage the various environments.) Type 2 hypervisors are used to run Windows XP applications on a Windows 7 machine, or to run Windows on a Mac OS system.

When might an organization want to use client-hosted virtualization? A good opportunity is when it's just beginning to investigate client virtualization and wants to experiment with hypervisor and virtual machine technology. A large data center investment isn't required. Plus, because the computing environment (including the OS and apps) is local, it's not dependent on network performance or availability.

In production environments, client-hosted virtualization makes sense on powerful desktop systems supporting users who must typically work on multiple computing platforms. Programmers, engineers, IT support and other power users often run more than one desktop environment. Rather than running multiple systems, these users can work on one system where client-hosted virtualization consolidates their platforms.

Finally, there are scenarios in which client-hosted virtualization and blade PCs combine to offer the benefits of centralized management without some of the data center investment required for something such as VDI.

Blade PCs came into prominence several years ago. They are really just traditional PCs (with memory, storage, OS and applications) but stripped of their desktop chassis and installed in data center racks. Their keyboard, video and mouse (KVM) functions run over a network connection.

Organizations that have adopted blade PCs can now run virtual machines on those systems and serve up desktop environments to multiple users from the same blade. Depending on the applications and network connections, anywhere from two to four virtual desktops can run on a blade PC, effectively reducing by half — at a minimum — the number of physical clients that the IT department must manage.

an organization is seeking. In general, many enterprises find it best to adopt presentation virtualization as a first option and VDI when special circumstances dictate.

Application Virtualization and Streaming

Application virtualization and streaming are similar technologies in that they decouple apps from the underlying client. The difference between the two is where the decoupled applications reside. Both approaches can offer organizations limited client virtualization, or they may be used in conjunction with presentation virtualization or VDI.

With application virtualization, apps run locally on the client. But they are not actually installed on the endpoint in the traditional sense. Instead, the app and related data are encapsulated in a package, separate from the OS.

When executed, the app runs in a virtual layer that controls its interaction with the underlying OS. A virtualized app still needs an OS to run, but does not carry with it OS-specific dependencies, meaning it can run in a computing environment that might otherwise present conflicts.

With application steaming, the encapsulated apps reside in the data center and the package is optimized. When a user requests an app from the server, it's streamed to the endpoint. This way, users can run virtual apps in the same conflict-free, protective bubble afforded by app virtualization, but the apps come from a central location rather than residing on their local devices.

A user isn't tethered to a specific device, allowing the IT department to free up some of its own resources by enabling self-service. In addition, the tech support staff gains better visibility into app usage, helping it make better-informed decisions about licensing and upgrades.

Organizations can deploy app virtualization and streaming as part of their presentation virtualization or VDI architectures. In fact, VDI solutions often exploit app virtualization to manage software and maintain a separation between the OS and application layer.

Encapsulating apps and reducing how many of them require direct access to an OS can reduce compatibility problems and the amount of testing needed to change an environment. And once an app is packaged, it can be deployed across client virtualization platforms, so the IT team won't need to prepare it multiple times for use in different environments.

App virtualization encapsulates an app and decouples it from the OS. Through encapsulation, the software becomes self-contained and does not need to be installed on a computer in the typical manner. Virtualized apps still need an underlying OS to execute upon, but they run in their own isolated environments (commonly referred to as "bubbles"). Because of this isolation, multiple versions of the same virtualized app can run simultaneously, and regression testing can be minimized.

Profile Virtualization

Profile virtualization, also known as user virtualization, is unlike the other three architectures described previously, but it can be used in conjunction with all of them. It is particularly useful for organizations that remain committed to traditional, physical endpoint devices but still want to reap the benefits of centralized control and streamlined client provisioning.

With profile virtualization, a user's data and desktop settings are decoupled from the endpoint. This can be as simple as folder redirection, wherein a folder on the endpoint seamlessly connects to a folder in the data center in which the user's files reside.

From the user's perspective, the files appear to be stored locally. If the user is offline, folder redirection can synchronize the local files with those in the data center once the user reconnects to the network.

Beyond data, profile virtualization centralizes a user's Windows settings, permissions and configurations, which allows them to follow the user from endpoint to endpoint. In some cases, profile virtualization can also store a user's installed apps so that they follow the user, which can be useful in some cases, such as in stateless, nonpersistent VDI environments.

In a stateless environment, the virtual desktop is wiped clean after each session. (Although, with certain profile virtualization solutions, the user can run an app on a stateless system, and it will still be there when the user reboots.)

Profile virtualization ensures a consistent user experience across multiple platforms, particularly as users incorporate smartphones and tablets into their computing work. For example, a change to application preferences on one device can be pushed out across all of them, whether the user is accessing an app on a mobile device or on a conventional desktop.

But perhaps the greatest benefit of profile virtualization is its role in planned desktop infrastructure upgrades. As organizations begin to migrate from Windows XP or Vista to Windows 7, or Windows 7 to Windows 8, profile virtualization can make it significantly easier for the IT staff to move settings from one environment to another. ■

Client Virtualization Components

Putting the pieces together for a successful solution

There are many technology requirements that must be addressed to successfully deploy client virtualization.

Consider the start of a day in a traditional computing environment: Tens, hundreds, even thousands of users boot up their desktop systems — each client device hosting its own power, hard drive, memory, OS and software — at roughly the same time.

Now consider the same mass of users launching their virtual desktops at roughly the same time, or accessing virtualized applications, or launching RDS sessions. Each worker logs in to a thin client and needs to pull down the necessary computing environment from the same bank of server resources. The organization's infrastructure must be designed to support this.

Client virtualization requires investment in infrastructure. There's no way to avoid it. Migrating to a client virtualization environment is essentially moving computing resources out of the distributed desktop environment and back into the data center.

Depending on the strategy employed, the initial costs for the new infrastructure may be the same as for a traditional desktop infrastructure. But the benefits and potential ROI of client virtualization cannot be realized, or the possible reduced total cost of ownership, without having the right pieces in place.

The best way to maximize an organization's investment in a client virtualization infrastructure is to have a professional service provider work alongside the IT department to flesh out the hardware, software and security requirements.

Hardware

When shifting the clients' computing activity to a data center, the first thing an organization must do is ensure that the data center can handle the new workload. In most cases, client virtualization will require some investment in extra servers. Are there enough circuits to support them? More servers require more power and give off more heat, so it's important that the data center be equipped to handle these ancillary changes.

With the supporting infrastructure in place, the systems to support the fleet of virtualized clients to be deployed must be built. In general, a virtual desktop infrastructure (VDI), because it calls for hosting the entire client environment in a server-based virtual machine, requires the most data center resources. Other client virtualization architectures may require less hardware.

Whichever an organization chooses, shared storage and multiple server hosts will be required to support a highly available client virtualization architecture. Ensuring the highest possible network bandwidth between the data center and all possible endpoints often is the difference between a successful deployment and one that leaves users dissatisfied.

Servers

In the data center itself, the primary hardware focal areas are servers and storage. Looking at VDI, this architecture requires a high level of infrastructure

planning because the VM load per server will vary greatly depending on the servers deployed and the virtualization software chosen. Organizations should be able to support anywhere from eight to 16 users per server processor core.

Virtualization vendors lean toward the high-end figure for servers running the latest chipsets. However, many virtualization experts recommend that organizations begin in the range of six to eight users per core, taking into consideration any modestly configured servers and leaving available capacity to support demanding office applications.

Moreover, Windows 7 needs at least 1 gigabyte of memory (and more for better performance), so it makes sense to plan for 1GB to 1.5GB of RAM per active virtual machine. It's recommended to plan for enough CPU and RAM capacity to accommodate growth of 40 percent or more.

How the organization deploys the supporting servers — whether stand-alone or as blades, for example — depends on the data center itself, the organization's existing server structure and any internal initiatives to reduce space, energy and cooling. A service provider can be helpful here, analyzing the current situation and recommending hardware deployment strategies.

Storage

After servers, the storage infrastructure is the next most vital component of a client virtualization deployment. When it comes to storage, there are two guiding principles. First, the organization will need enough storage to centralize client environments and all of the data that would normally reside on end-user systems. And second, read/write performance must be good enough that users don't experience any lag in client responsiveness.

To correctly size and design the storage infrastructure, the focus must be on disk input/output, typically as it pertains to Windows environments. When planning for VDI deployments in which entire Windows environments are delivered over the network, total disk I/O throughput for traditional Windows users can range from 5 megabits per second to 7Mbps. The throughput rate will depend on how heavily a user accesses desktop resources (the bulk of that throughput is typically disk reads).

$$\frac{\text{THROUGHPUT} \times 1024}{\text{BLOCK SIZE}} = \text{IOPS}$$

To match client virtualization usage to storage solutions, organizations must translate user throughput to input/output operations per second (IOPS). This is how storage systems such as network-attached storage (NAS) and storage area networks (SANs) gauge performance. The following calculation explains IOPS:

(Block sizes may range from 4 kilobytes for early NT Files Systems to 1MB for Windows 7 disk I/O.)

Ultimately, what the organization needs to do is right-size its storage system to support the appropriate number of virtual machines. Storage solutions operate using various protocols, including Fibre Channel, iSCSI, Network File System (NFS) and 10 Gigabit Ethernet (10 Gig-E), which must be supported by the client virtualization platform.

Organizations should choose a protocol that provides the throughput and IOPS required for the number of virtualized desktops they intend to deliver. For example, with VDI, 10 Gig-E (whether over fiber or copper) can support twice the number of VMs per host (more than 2,000 in certain environments) as Fibre Channel, which can support several times the virtual machines as iSCSI or NFS.

Systems architects recommend NAS or SAN environments for storing virtual desktops. Many organizations may already have robust storage infrastructures in place. To determine whether an existing infrastructure can support the addition of client virtualization, the organization needs to know if it has enough IOPS capacity, enough storage capacity and the proper fabric (Fibre Channel, 10 Gig-E) to support the anticipated number of virtual machines and/or hosts.

Because storage access is so important to application responsiveness in client virtualization, many organizations choose to deploy caching solutions to improve performance. Others adopt solid-state drives, which use flash memory to store persistent data and make it available faster. Both should be considered to optimize storage performance.

Clients

For end-user systems, there are several options. Organizations can use existing desktops and notebooks and configure them to access virtual resources. Or they can deploy thin clients to replace aging, power-hungry PCs. Thin clients consume less power, have no moving parts, and last longer than traditional desktops.

Often, because some users are initially uncomfortable with a move to a more limited platform, an organization may opt to put some of the client virtualization-related savings toward larger, better (more energy-efficient) monitors to compensate this false sense of a downgrade.

For organizations only a few years into their current desktop cycle, there are ways to turn fully functional Windows desktops into thin clients as well. Environments that already have Software Assurance (SA) licensing (see *Before You Dive In: Software Licensing sidebar)* can use Windows Thin PC (WinTPC) to created locked-down, Windows 7 thin clients, either on Windows 7–compatible desktops or notebooks.

Software

As with the hardware requirements for client virtualization, the architecture chosen will influence the software needs. Typically, there is a software component at both the client and server ends of the equation. With presentation virtualization, for example, the client runs a Windows RDS client application while servers run Windows Server 2008 R2 with RDS and appropriate client access licenses (CALs).

Many organizations choose to run a non-Windows client virtualization environment, such as those from Citrix Systems or VMware. These platforms have their own server and client software components and run on top of RDS.

On the server side, they also may have their own data store requirements — such as specific versions of SQL Server, Oracle or some other database server. Organizations should consult with a solution architect to match virtualization platforms to software requirements.

When it comes to application virtualization, organizations must consider back-end programs such as Microsoft App-V, Citrix XenApp and VMware ThinApp. These programs run in the data center and communicate with the proper client programs to initiate sessions for app streaming.

Regardless of architecture, the trickiest part of defining the software infrastructure involves licensing. After all, a major driver for client virtualization is to let

BEFORE YOU DIVE IN: SOFTWARE LICENSING

Because so many enterprises run Microsoft Windows operating systems (on the client and in the data center), it's important to keep tabs on Microsoft's software licensing requirements as they pertain to virtualization. With Windows 8 coming soon, there is talk that Microsoft plans to make some changes to its virtualization licensing.

The crux of what needs to be known when pursuing client virtualization is that traditional Windows desktop licensing does not apply to a virtualized environment, whether it's for Windows, Microsoft Office or any other virtualization platform that the IT department chooses. In a traditional environment, software licenses are tied to devices; in a virtualized environment, they're tied to users.

For its part, Microsoft offers Software Assurance (SA), a subscription-based volume-licensing agreement that covers most endpoint devices. SA allows users to access virtual clients through licensed Windows PCs.

Organizations that currently operate a traditional desktop environment may or may not have SA, depending on how they purchased their systems. (Desktop computers shipped with OEM versions of Windows, for example, are not eligible.)

So how can users access their virtual desktops when using nonenterprise endpoints, such as personal notebooks or hotel kiosks? Along with SA, organizations can acquire Virtual Desktop Access (VDA) licensing, another subscription-based program, which lets users access their computing environments from outside the enterprise and through third-party devices.

Organizations that adopt thin clients will need VDA because these clients are not eligible for SA (because they don't run an operating system). Moreover, organizations can subscribe to VDA for current systems not covered by SA, though in some cases, the best option may be to purchase endpoints with OEM Windows and upgrade to SA.

If that isn't enough to consider, keep in mind that there is SA for the endpoint (Windows, Office, etc.) and SA for the server (Windows Server, SharePoint, etc.). When in doubt, organizations should engage a licensing expert who can spell out exactly what licenses are needed and why.

workers access programs through a variety of devices. Those programs must be licensed for access from all necessary devices. A solutions provider can help the IT department cut through the legalese and ensure the organization has its licensing requirements covered.

Security

When it comes to client virtualization, there are two important security considerations.

The first is securing the data. If an organization is adopting client virtualization, it is taking operations that used to happen between a local hard drive and a CPU and running them over a network.

And if remote access is allowed to desktops and applications, that network may include the Internet. Because of this, virtual private networks (VPNs) should be an important component of a client virtualization deployment, to encrypt clients, data and applications in transit.

Third-party virtualization platforms include many proprietary security features to protect virtual clients, applications and data from end to end. Many of these platforms meet certain security standards for particular vertical markets, such as Common Criteria certification for U.S. government agencies.

Moreover, depending on the organization and the work it does, additional planning and development may be necessary to ensure security, such as running certain virtual machines on dedicated servers to keep them isolated. This kind of consideration comes out during assessment, planning and design (see *Chapter Five: Rolling Out a Solution*).

In addition to protecting data in transit and in the data center, client virtualization raises the importance of setting policies for authorized access to data. Organizations may want to adopt fresh network access control (NAC) solutions, especially if client virtualization is being made available on a wider variety of fixed and mobile devices.

NAC not only ensures that only authorized users have access to virtual resources, it enforces policies on the endpoints that staff use. For example, a NAC policy might specify that if a device is not running a certain level of antivirus protection, it cannot access the virtual environment.

The other security consideration is protecting the infrastructure that supports the client virtualization architecture. Doing so is an exercise in business continuity planning.

With so much of a desktop infrastructure centralized in a data center, ensuring that the data center remains operational is more critical than ever. Larger organizations may choose to completely mirror their client virtualization infrastructure at a separate site. Others will build in server and storage redundancy so that if one section of the data center fails, it doesn't adversely affect thousands of virtual client users. ■

EXTENDING YOUR REACH:

MOBILE DEVICE MANAGEMENT

If greater workforce mobility is the chief driver for an organization's move to client virtualization, it makes sense to create a related strategy for supporting mobile devices.

With so many platforms out there — notebooks, ultrabooks, tablets, smartphones — mobile computing presents a new management paradigm, especially when an organization supports BYOD.

Today, mobile device management (MDM) solutions let the IT department exercise control over the mobile devices attached to its network regardless of OS, device type or ownership. MDM tools not only enable over-the-network configuration and deployment, they also force users to adhere to centrally managed policies.

For example, with MDM, the tech staff can require that all mobile devices connecting to the network are encrypted; that only approved applications are installed on the mobile device; or (in the case of BYOD) that nonwork applications must run in an isolated container (or sandbox) on the device so as not to expose enterprise data to security risks.

And the most critical MDM capability? Being able to wipe the content of a missing device. To prevent sensitive data from falling into the wrong hands, the IT department can use MDM to cripple or erase data on a notebook, tablet or smartphone if the device is reported lost or stolen, or if it fails to connect to the network within a prescribed period of time.

Rolling Out a Solution

Taking the right steps for a successful migration

How does a client virtualization project get off the ground? In some cases, an enterprise has already undertaken server virtualization, developed a unique virtualization-oriented skill set and considers virtualizing clients as a next step. But client virtualization for its own sake can prove challenging to deploy.

Ideally, top managers and IT staffs should be on the lookout for computing challenges that might lend themselves to a client virtualization strategy.

For many enterprises, one of the most obvious trigger points is the transition from Windows XP or Vista to Windows 7 or 8. With a short time to go before Microsoft officially and completely ceases to support XP (one of the most successful and widely used OSs ever), there has never been a better time to consider client virtualization. Virtualizing the computing environment now will make migrating to a new OS later a simpler proposition.

Along those lines, desktop refresh cycles also represent an excellent opportunity for client virtualization. If a significant portion of an organization's desktop or notebook fleet is due for replacement, either because of age or expiring warranties and maintenance contracts, the time may be right to virtualize some or all of those client computing environments and migrate to thin clients on the desktop and, if appropriate, tablets for mobile workers.

Finally, another prominent trigger for launching a client virtualization project is a demand for greater mobility within the organization. It's not just that notebooks and tablets have become more critical to the way organizations operate.

Telework and the rise in BYOD policies (whereby organizations allow workers to use their own smartphones, tablets and mobile PCs to do their jobs) have also increased the need to present a unified, centrally managed client environment to more endpoints. The more mobile devices and home-office systems that the IT department must oversee, the better fit a client virtualization solution may be.

Once an organization commits to client virtualization, it can follow a series of interconnected steps to ensure a successful rollout. When possible, it's worth bringing in outside expertise to help to guide the process from start to finish.

Not only does a third party offer system architects and process experts who understand client virtualization, it also doesn't have legacy ties to an organization's existing infrastructure and can offer unbiased advice as the situation dictates.

The infrastructure migration is defined by five steps.

Step 1: Define Business Goals

Before any purchase or installation work begins, it's critical to flesh out the business objectives. Documenting the answers to several simple questions can help:

- Is the organization planning a Windows 7 or 8 migration?
- Is there a need for a more secure computing environment?

- Is there motivation to reduce the cost of managing clients?
- Does the organization require a disaster recovery solution?
- Is there a drive to support internal and remote employees on various endpoints?
- Is there a complex application deployment solution in need of replacement?
- Does the organization want to replace or enhance an OS deployment or imaging solution?
- Is there a requirement to consume less energy and contribute to a sustainability initiative?
- Is there motivation to replace or enhance a terminal services solution?

In addition, when defining goals for client virtualization, an organization should specify approximately when it wants to complete implementation – six months, 12 months, more than a year? An honest assessment of the timeline – in light of other goals – can help lead the organization to the right client virtualization approach and solution.

Step 2: Assess the Environment

After deciding to deploy client virtualization, conducting a readiness assessment is the most important step in the rollout. Often, it's useful to bring in a third-party partner to help analyze the organization's existing environment.

Again, it's important to document the current environment in as much detail as possible, starting with how the organization currently handles help desk and incident management, configuration management, software distribution, and image deployment. After that, the IT staff should meet with a partner and describe the current setup.

This is just a sampling of the most basic questions to answer:

- How many desktops are in use? What brands?
- What is the typical age of the desktops?
- How many notebooks are in use? What brands?
- What is the typical age of the notebooks?
- Are there any thin clients in use? What brands?
- What operating systems run on these clients?
- What versions of Microsoft Office are running?
- What web browsers are running?
- How many and what types of servers are in the data center?
- What types of storage are associated with the servers (SCSI/SAS, SATA, SDD, SAN)?
- What networked storage is in the data center, and what protocols are running (iSCSI, Fibre Channel, Fibre Channel over Ethernet, NFS)?
- Has the organization virtualized its servers? If so, which products and exact platforms are being used?

The organization also needs to get a handle on all of the applications it runs, as well as who uses which applications and how often. This information will help determine to what extent the environment should be virtualized and whether any software licenses need to be reassessed.

Enterprise programs from companies such as Flexera Software and Lakeside Software can play a major role in assessing the readiness of the current environment and providing ongoing insight into client virtualization deployment.

Step 3: Plan and Design the Solution

Assessment and planning are tightly linked. The assessment will help drive the focus on the architectures that best fit the existing environment while achieving business goals. In planning, it is important to know the mix of users in the enterprise computing environment. These determinations could be made in the assessment stage, but it's important to know how many users, and the type of users, the organization comprises. A simple breakdown of users might include:

- **Basic or light users:** CPU utilization is very low, and they mostly use office productivity software and web browsers
- **Power office or moderate users:** CPU utilization is higher (perhaps up to 15 percent) due to client-heavy software, such as graphics programs
- **Developers or tech support users:** Using programs such as Visual Studio, AutoCAD and enterprise monitoring software that require even more computing resources

The organization also needs to know how many remote users it has (and what type of users they are), how many remote sites it must support and what connectivity it provides to those sites. All of this information (plus an understanding of the options and architectures outlined in earlier chapters) will help the organization begin the design process with a plan to deliver the right client virtualization infrastructure.

One caveat: Throughout the planning stage, it's wise to adhere to Information Technology Infrastructure Library (ITIL) practices. This will help ensure that the IT solution aligns with the organization's business needs.

Step 4: Test the Concept

For some organizations, this step might be a two-part process: a pilot followed by proof of concept. For others, the pilot will be the proof of concept.

However it is approached, client virtualization is too big of an undertaking not to roll out on a limited basis initially. Unfortunately, many organizations make the mistake of rushing into a pilot program without ever taking important steps, such as establishing goals and assessing their environment.

If the organization pursues a limited proof of concept in a controlled setting, the goal should be to test everything: virtualization options, applications, endpoints, peripherals and remote-access connections. At this point, the IT team will validate the technology and ensure that all the features and functionality required exist in the client virtualization solution.

When the organization is ready to launch a pilot, there are a few schools of thought. One approach is to target the pilot to a workgroup of mostly basic or light users, preferably in a self-contained department with a finite set of applications.

Another approach is to pilot client virtualization in departments that could best benefit from it or that include expert desktop users who might be helpful in troubleshooting the solution and assisting other users as the rollout ramps up. Developers and engineers, who often work with multiple desktop platforms, might benefit if each platform ran in a virtual machine and could offer valuable feedback on the environment's performance.

The premise behind this approach is that if client virtualization works for power users, it should be easier to roll out across more of the enterprise.

Whichever approach an organization takes to testing client virtualization, it's usually not enough to conduct just one pilot. And it's critical for the IT team to have a fallback plan in the event the pilot environment does not work as envisioned. That way, the pilot group can revert to an operational desktop computing platform if needed.

Step 5: Implement the New Environment

Implementation and rollout require their own plans, detailing when each workgroup will be migrated to the new client virtualization platform and when legacy solutions will be phased out.

During implementation, it is often necessary to transition the IT department to a new model of service and support. For example, desktop support personnel will need to adopt new roles and responsibilities, and their skills will also need to change. Troubleshooting a virtualized client computing environment is significantly different than troubleshooting a traditional one.

Most important, users must receive training as the environment rolls out across the enterprise. Though much of the change should be transparent to staff, they may still need to learn how to access their new desktops. And they should be told what to expect.

If the environment has been set up to restrict certain client functions, those changes should be balanced and explained along with the benefits users will enjoy, such as remote access to the same desktop whether at home or in the office.

Once implementation is finished and there's been a transition to full support and management of the new environment, the benefits of client virtualization will touch the entire organization. Few IT solutions today spread the wealth so broadly — from IT managers to mobile workers, from desktop support staff to power users. ■

MISTAKES TO AVOID: WHY CLIENT VIRTUALIZATION FAILS

Learn from the mistakes of others that have migrated to client virtualization. Here are the top reasons why an initiative may fail.

Poor storage design: It's not just about capacity, or the amount of storage per user. For example, in desktop virtualization, the storage infrastructure receives various requests and must load different parts of the operating system and the computing environment. A poorly designed storage infrastructure can create a significant performance bottleneck.

Not enough CPU cache: Adding more memory to a server won't solve performance problems. Ample amounts of system cache (for quick data access) can speed everything from daily computing to desktop provisioning.

Boot storms: When large groups of users log on simultaneously, it's called a boot storm. Certain client virtualization platforms include features for managing these usage spikes, such as idle modes that automatically begin to load desktops before users actually log in.

Antivirus interference: It's important to integrate antivirus software into a client virtualization strategy. But if it isn't optimized for the solution, the antivirus software can actually degrade the virtual desktop experience.

Miscalculating network impact: Regardless of the architecture, the user's computing experience suffers when latency increases and bandwidth decreases. Calculating the necessary network resources per user depends on everything from the type of work users are doing to the overall network topology. What might have been served by 20 kilobits per second per user in one scenario might require much more bandwidth in another.

This glossary serves as a quick reference to some of the essential terms touched on in this guide. Please note that acronyms are commonly used in the IT field and that variations exist.

Glossary

10 Gigabit Ethernet (10 Gig-E)
This Ethernet standard was first established in 2002. It specifies a data rate of 10 gigabits per second, which is ten times faster than its predecessor, Gigabit Ethernet.

Application self-service
In the client virtualization context, application self-service refers to the ability of end users to request and stream applications to their endpoints on an as-needed basis.

Application virtualization
A type of client virtualization, application virtualization allows applications to run as virtual services in isolation from one another and from any underlying systems.

Blade PC
A blade PC is a computer on a circuit board that shares storage and power with other blade PCs in a data center rack.

Boot storm
When large numbers of users launch client virtualization sessions at the same time — at the start of the workday, for instance — the potential run on data center resources is called a boot storm.

Bring your own device (BYOD)
BYOD is a term to describe the use of personal devices to access enterprise resources.

Business continuity (BC)
BC refers to strategies and actions taken by an organization to insure that critical operational functions are maintained for those users who need access to them at their expected level of service. This definition extends to day-to-day access rather than only to specific disaster scenarios.

Client-hosted virtualization
This form of client virtualization, also known as intelligent desktop and distributed desktop virtualization, allows users to run multiple operating systems as virtual machines on a single desktop system.

Consumerization of IT
This term refers to the growing influence of consumer market technologies in IT innovation as opposed to business market drivers.

Disaster recovery (DR)
DR encompasses the strategies, processes and procedures an organization has in place to recover or maintain access to crucial technological infrastructure in the event of natural or human-induced disaster scenarios.

Family Educational Rights and Privacy Act (FERPA)
FERPA , enacted in 1974, outlines the rights of students to access, amend and control the disclosure of information from their educational records. This covers the right of privacy regarding grades, enrollment and even billing information.

Fibre Channel
Fibre Channel is a high-speed data network technology commonly used for storage area networks within data centers. Originally developed for communications among super computers, it is capable of transfer rates of up to 10 gigabits per second.

Fibre Channel over Ethernet (FCoE)
FCoE encapsulates Fibre Channel frames so that they can travel over Ethernet networks.

Health Insurance Portability and Accountability Act (HIPAA)

Enacted in 1996, HIPAA outlines provisions (including administrative, physical and technical security controls) to ensure the protection and privacy of patient health information.

Hypervisor

This is a software program used to enable virtualization by allowing multiple operating systems and applications to run simultaneously on a single host computer.

Information Technology Infrastructure Library (ITIL)

ITIL is a globally recognized collection of best practices for IT service management.

Mobile device management (MDM)

MDM software allows organizations to monitor, manage and secure staff mobile devices across multiple service providers and operating systems.

Network access control (NAC)

NAC embeds access controls into network devices. These access controls are dynamically established, based on the identification of the user connecting to the network. Frequently, endpoint security posture checks are also done, which may affect the access controls, such as sending a user to quarantine if their antivirus software is not up to date.

Network-attached storage (NAS)

NAS is a storage technology that holds data in file formats, as opposed to blocks. NAS communicates with applications via Network File System (NFS), Common Internet File System (CIFS) protocols or Hypertext Transfer Protocol (HTTP).

Network File System (NFS)

NFS is a distributed file system protocol that allows a user on a client device to access files over a network in a manner similar to accessing local storage.

Presentation virtualization

Presentation virtualization is a client virtualization architecture that encompasses Terminal Services and Remote Desktop Services wherein applications run on a central server, but their interfaces are presented on a client endpoint.

Profile virtualization

Also known as user virtualization, this architecture allows the user's data and desktop settings to be decoupled from the endpoint. This allows the users settings to follow the user from device to device, providing desktop access across a range of endpoint options.

Remote Desktop Services (RDS)

Previously known as Terminal Services, RDS is a feature of Microsoft Windows Server 2008 R2 that lets users access desktop applications and data over a network.

Software Assurance (SA)

SA is a subscription-based Microsoft licensing agreement that forms the basis for virtualizing Microsoft operating systems and applications.

Stateful client

Also known as persistent clients, these virtual desktops maintain their configuration between sessions.

Stateless client

Also known as nonpersistent clients, these virtual desktops revert back to a default configuration between sessions.

Storage area network (SAN)

A SAN is an architecture of interconnected disk drives or other data storage devices that record data by blocks instead of files. Typically, host communication is done using SCSI (or iSCSI) or Fibre Channel (or Fibre Channel over Ethernet) protocols.

Terminal Services

Terminal Services is a Microsoft Windows Server implementation of thin-client computing in which Windows applications are made accessible to a remote client (see *Remote Desktop Services*).

Thin client

A thin client is a desktop device that provides the display component of a system or network and taps centralized storage and processing. As display devices for virtual machines, thin clients require little maintenance.

Virtual Desktop Access (VDA)

VDA is a Microsoft licensing agreement that lets users access virtual desktop environments from Software Assurance–covered PCs and from third-party devices such as personal PCs and hotel kiosks.

Virtual desktop infrastructure (VDI)

VDI is a client virtualization architecture in which an entire desktop environment, including the operating system, is hosted within a virtual machine running on a central or remote server.

Virtual machine (VM)

A VM is a software implementation of a physical computer: abstracted operating system and applications that run on top of another system's OS to be presented to users on demand.

Virtualization

Virtualization is a technique for enabling multiple instances of operating systems and applications to run on a single physical host.

Zero client

A zero client differs from a thin client in that it lacks an embedded operating system. Instead, it pulls the entire operating system from its server host, along with centrally delivered applications and data. This strategy minimizes setup, configuration and maintenance chores at the desktop. Zero clients come as a book-size device or may be integrated with a monitor.

Index

ABOUT THE CONTRIBUTOR

KATHI GRUMKE is a Solutions Manager with CDW, having joined the company in 1999 as a Project Manager on the Professional Services team. In her current role since 2007, Grumke manages technical pre-sales specialists responsible for providing core infrastructure and client virtualization solutions to customers nationally. She oversees the development and execution of solutions offerings and readiness programs for the CDW sales team and customers. She is heavily involved with channel management activities, working with key partners to drive solution growth and adoption. Grumke holds a B.B.A. degree in Information Systems from the University of Wisconsin, Madison.

LOOK INSIDE FOR MORE INFORMATION ON:

- Supporting BYOD initiatives
- Choosing the right client virtualization architecture
- Upgrading hardware, software and infrastructure
- Navigating a migration