

A New Vision for Desktop Management

Jorge Pereira and Sean Kennedy

Kennedy Consulting

December 2006

Abstract:

Desktop Management has remained largely unchanged over the past few years... The ability to manage the base image, install and distribute software to those images while maintaining some level of control over those corporate assets continues to be a challenge for small, medium and large organizations all around. What started off as a simple process of providing end-user computing capabilities to everyone within the organization, and installing applications on every computer, became a challenge to manage. The landscape was slowly transformed not only with the advent of automated software distribution tools, but also with the introduction of centralized desktop management policy technology. Below you will find a discussion of the technical challenges facing the management of the Client Computing environment. The document explains the many drawbacks of traditional application distribution, and highlights the benefits today's Software as a Service (SaaS) alternative provides. This article is intended to be part of a series of publications addressing Desktop Management – New Vision.



We understand the **power** of **teamwork**.

A New Vision for Desktop Management

By Jorge Pereira and Sean Kennedy, Kennedy Consulting -- December 2006

Desktop management has remained largely unchanged over the past few years. Application provisioning and management (delivery, installation, configuration, auditing, and updates) is at the core of the challenges associated with desktop management. In the past, in order to provide applications to users; the applications had to be installed on each and every computer manually, by allowing the users to have full admin rights to the desktop, or dispatching desktop technicians. While simple in theory, this approach is expensive, unmanageable, and unsecured. Nowadays, the IT can take its pick from several approaches to management that have evolved, each with its own set of benefits and drawbacks.

The outdated method of installing all the applications on every computer has proven to be cost-ineffective. Added complications of this approach include application conflicts, locally stored user data, security issues, applications updates to each computer and may become corrupted by its users and have no easy backup. There is also no way of knowing who has access to what programs using this method since the user has access to all applications on the PC. The complexity this leads us to, make it difficult to provide adequate service levels agreements to provision applications, in a world of increasing speed. Looking closer into the details of some of these:

- **Multiple applications:** It is difficult to deploy applications that must be updated often or to deploy a wide range of applications with conflicting versions of code components. These factors limit options available to developers.
- **Administration Rights:** Because of software provisioning lead-time, configuration requirements, staffing needs, a large percentage of users have administration rights to the machines they use, increasing the security, software compliance and other risks.
- **Multiple versions:** Transitioning to newer application versions is difficult because at times the older version may still be required. Completely removing old applications can prove difficult. Applications do not usually allow multiple versions to execute side-by-side on the same computer.
- **Locally Stored Data/Settings:** Locally stored application data, settings and profiles, make it difficult to recover desktop working environment for a user due to failure or corruption. Backup of distributed, locally stored data is expensive and usually not a feasible option for organizations.

Alternatives to addressing the desktop management challenges usually include the implementation and operation of one or more of the following alternatives:

- *Automated Software Distribution*, wherein applications are installed and updated on end users' computers via SMS, and other such tools. This approach allows for centralized management of the applications, and can help keep inventory on applications installed on each end user PC. But unfortunately it requires knowledge of how to package applications and updates, and again, the applications may become corrupted by their users and lack an easy backup. Additionally, as with the old-fashioned method, if a user has access to a particular PC, they have access to all the applications on said machine.
- *Server-Based Computing approach* in which applications are installed centrally on a terminal server and provide RDP or ICA access from the client device. This method offers centralized management, configuration, and backup. With Server-Based, connections from any device are allowed, but application access can be limited to certain clients. However, devices *must* be connected to the network to use the applications and application execution happens centrally, even when the client device is capable of doing work. Furthermore, you must learn to install applications into multi-user environments, and not all applications will work or be suited for such an environment.

- *Operating System Streaming*, where an entire disk image (OS included) is streamed to the user's device. This is achieved by redirecting physical disks in client computers to virtual disk images on the network file servers. The client computer boots to the network and is recognized by the server based on its MAC address; the server then mounts the appropriate vdisk file. When a machine is rebooted, everything is reset back to the "gold" state. Thus, any single computer can do different things each time it boots, depending on which disk image is mounted. However, once again, there must be network connectivity for it to work.
- *Bladed PC*: Windows XP is installed on a server blade and then provides 1-to-1 remote access via XP's built-in remote desktop capabilities. This method has easy security and backups and no application compatibility issues. The users also have more control over their individual desktop, and clients can run the "workstation" version of their software. As with the Operating System Streaming, however, network connectivity is a must for this to work, and management tools are also required to manage the software within each bladed PC.
- *Centralized VMware PC*, which entails building a huge VMware server and dividing it into multiple VMs, each running Windows XP. It provides remote access via XP's built-in remote desktop. This method is very similar to the Bladed PC, except here the user goes to a Windows XP session in a VM rather than their own native blade. With VMware, the sessions can be suspended and unloaded from memory and resumed later on. VMware also offers better performance and security, has central backups, but no application compatibility issues. Once again, the clients run the "workstation" version of software and users have more control over their desktop, except now users can take their sessions with them when they go offline by "checking out" their disk images and running them on a local VM. VMware, however, requires a lot of server hardware and management tools and is not possible yet in today's world.
- *VMware Clients within Terminal Server*. A server is built and terminal services and Citrix are installed. VMware Workstation or Microsoft Virtual PC is installed as a publish application in Citrix, and disk images are published for each users. The users connect to the published VM via ICA. With this option there is good security and no application compatibility issues, and VMs can be suspended and moved from server to server. Unfortunately, however, the performance of this method is questionable.

As far as web-based applications: They are able to run on multiple servers and can separate the application execution from user interface quite beautifully. They are extremely easy to update, manage and access, but their big drawback is that they can only be used online. This major negative with web applications is that all interaction with the application must pass through the server, which requires data to be sent to the server, the server to respond, and the page to be reloaded on the client with the response. Up until recently, the Application Service Provider (ASP) industry has focused in delivery specific client-server applications with HTML front-ends making difficult to make it a viable alternative to manage the desktop environment.

Application virtualization technology, which entails the delivery of application to a user's device based on proper authorization, without modifying the base desktop image, has brought the promise of Software as a Service (SaaS) closer to reality. The software can be accessed anywhere, with low maintenance costs. Unlike the terminal server-based method, application execution occurs on the client device, providing the rich client experience intended by the application, without application conflicts.

The future vision of desktop management aims to reduce costs, widen availability, increase user mobility and security, ensure compliance and licensing auditing, and adhere to regulations. Application virtualization is only one component, although a key one, to achieve these goals. In simplified terms, application virtualization provides the ability to give any application on any computer based on user access and authorization via network. The benefits of application virtualization are *plentiful*.

In summary, the first step towards attaining the new vision for desktop management is to accept software-as-a-service as the model that enables applications to be treated as services, and allows for the transformation of the entire IT organization to provide generic computing devices to the individual users, efficiently and effectively, regardless of location or device they are using. Application management is greatly simplified and TCO is significantly reduced. It is user-centric, single image, simple, managed, and secure. Easily accessible and managed and provides remote service. No application installation, no data on local drives, profiles are stored centrally, and access to hardware is policy based. As a result, your organization can provide:

- ✓ Accelerated deployment
- ✓ Maximized accessibility
- ✓ Flexible computing
- ✓ Improved diagnosis and repair
- ✓ Improved Application management
- ✓ Controlled access
- ✓ Protected data
- ✓ Easily recoverable data
- ✓ Threats easily identified
- ✓ Reduced helpdesk costs
- ✓ Real time asset management
- ✓ Enhanced interoperability
- ✓ Maximized Productivity

Future articles will discuss this new paradigm and the organizational change impact that is necessary to make the technical implementation successful.

About Kennedy Consulting:

Kennedy Consulting, LLC, is a Northwest information technology (IT) and management consulting firm that assists organizations to achieve their strategic goals and objectives. We have worked for major companies in multiple industries and government organizations across the nation and around the globe. Key differentiators of our company include:

- Holistic approach that incorporates people, process and tools
 - Success is inevitable when these three areas are aligned
 - Combine services in these areas with project and program leadership expertise to achieve results
- Bridge Strategy, Tactical and Operational
 - Seamless transition from strategic thinking to acting strategically
 - We excel in the gray areas
- Flexible Teaming for Success
 - Each problem or initiative requires a unique team
 - We partner with local and national firms to quickly build effective teams focused on our clients needs

Kennedy Consulting is a privately help company headquartered in Seattle, Washington. For more information on this and other topics, please visit www.kennedyllc.com