



Enterprise Desktop Virtualization

Introduction

For nearly a decade, IT industry thought leaders and vendor proponents have hailed the anticipated widespread adoption of “virtual display desktop” as the new end-user model, touting clear benefits over the fat-client model, represented by the traditional desktop PC loaded with enterprise and productivity applications:

- Heightened security
- Increased manageability
- Significant energy savings
- User session portability
- Reduction of idle computing

Year after year, however, this adoption has failed to materialize. Primary among the reasons for the lack of momentum behind virtual display client computing have been

- cost, of both the additional network and the end-user system infrastructure;
- complexity of designing and deploying the infrastructure;
- the IT and end user cultural shift necessary to move to virtual display clients; and
- compatibility problems associated with the migration from the physical personal desktop computer to a virtual desktop driven by the data center.

However, the recent emergence of server virtualization technologies, coupled with enterprise class multi-core processor servers, has finally put the virtual display client goal within reach, in the form of desktop virtualization. As depicted in Figure 1, below, desktop virtualization, or the virtual desktop environment, is the end result of funneling the multitude of enterprise applications through a virtual desktop infrastructure, to present a virtual desktop, with the look and feel of a traditional (physical) PC desktop, on an end-user device.

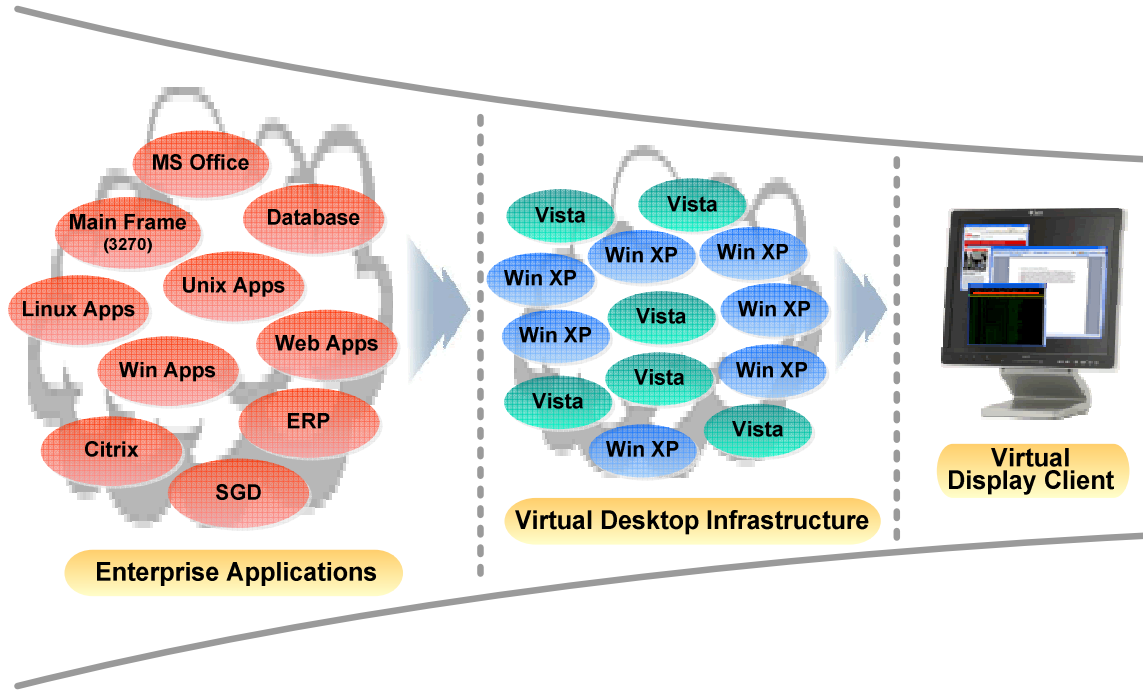


Figure 1: The Virtual Desktop Environment

One of the key goals when migrating from the physical desktop to a virtual desktop environment is to ensure that the end user’s computing experience does not change. Making this transition as seamless as possible will help mitigate end-user training costs, contain the number of help desk calls related to transitional issues, and minimize end-user resistance. In pursuit of this goal, desktop virtualization should be designed and configured to look and feel exactly like the end-user’s current desktop environment.

Another key goal in desktop virtualization is to improve upon the overall desktop security environment. Maintaining security at the desktop level is an ongoing and time consuming administrative LAN task, with many application-specific dependencies. The greater the number and variety of applications resident on end users’ PCs, the greater security challenge. Desktop virtualization moves most of these security-related issues into the data center, thus providing greater security manageability and a more tightly controlled security environment.

Virtualization Technologies

This paper focuses on two desktop virtualization technologies – Sun Microsystems’ Sun Secure Global Desktop (SGD) and VMware’s Virtual Desktop Infrastructure (VDI). These technologies will provide the user with secured access to their applications using virtual display client technology (Sun Ray).

Sun's desktop virtualization solution enables customers to leverage the value of virtual display client while at the same time minimizing the initial investment and high migration

cost that is sometimes associated with moving from a distributed fat client based environment. With SGD, IT departments can move desktop instances off physical personal computers and consolidate logical versions of same onto a server in the data center. End-users can continue to use their existing desktop operating environment of choice, whether it is Windows, Linux or Unix, because the virtual display client software can display desktop sessions or secured published application sessions from all of these platforms.

When combined with SGD, server-based applications can be published or accessed from Unix, Linux, 3270/5250 or Windows Servers to the virtual desktop instances. Once the focus is shifted from a distributed fat-client based solution, applications can strategically be selected and tested as candidates to move to application farms. Eventually, all applications, and their management, can be moved off the desktop, leaving only the user environment and a small subset of applications to be managed, thus significantly reducing desktop management cycles and operational complexity.

Another approach to desktop virtualization is to provide each end user with a unique virtual instance of a desktop operating system. VMware's VDI technology combined with enterprise servers and the virtual display client, comprises a comprehensive desktop virtualization solution. In its simplest form, VDI consolidates desktop operating system instances within the data center and presents them securely to end users through remote display protocols on a wide array of devices with network access.

With a Virtual Display Client / VMware-based virtualization solution, all services are managed from within the data center. There is no configuration, operating system or data to manage on the client device. This offers a more secure and manageable solution over both traditional PCs and thin clients that use an embedded operating system. Lower TCO/ROI can be achieved through more efficient management, optimized usability, increased productivity, reduced power and cooling, better utilization of computing resources and extended desktop lifecycles.

The remainder of the paper examines the two technologies in more detail.

Secure Global Desktop (SGD)

The SGD solution provides secure access to server-based applications running on Microsoft Windows; Solaris™, Linux and other UNIX operating systems, mainframe and midrange systems from virtual display clients, desktop PCs and mobile devices.

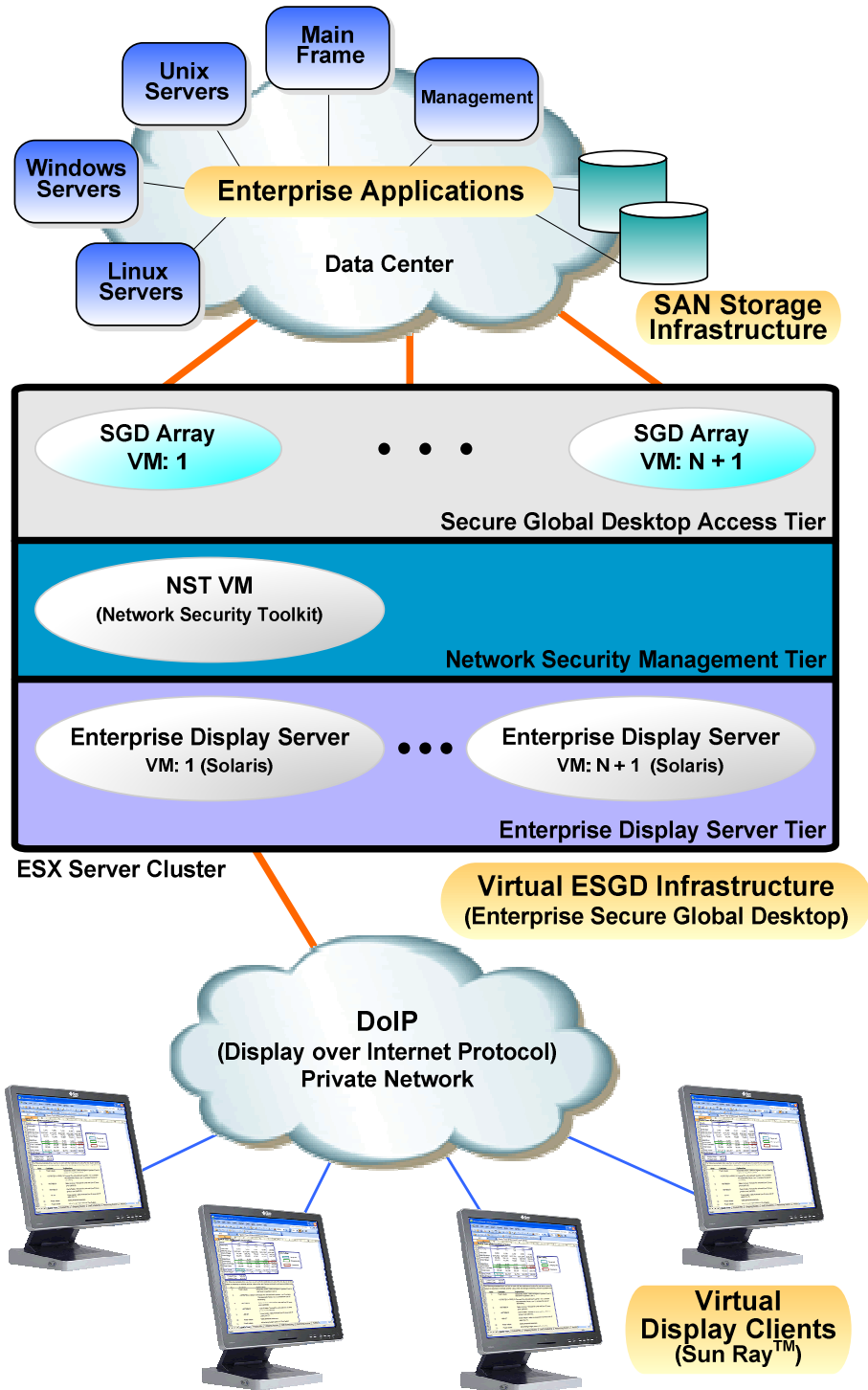


Figure 2: Sun Enterprise Secure Global Desktop (SGD)

The ESX Server Cluster depicted in Figure 2, above, is based on a multi-tiered VM architecture. Each VM tier provides a specific functional service necessary for a secure, comprehensive virtual desktop display environment. A multi-tiered approach enables higher resiliency and increases the ability to scale the infrastructure, while at the same time minimizing the effort and resources required to manage it.

Enterprise Display Server Tier (Virtual Display Client Access)

The Enterprise Display Server Tier uses Sun Enterprise Sun Ray™ Server software to provide virtual display client access, display rendering, control and management to all Sun Ray™ client devices. In a typical scenario, a Sun Ray™ server session starts, a remote display connection is made to an end user's Webtop (a web-based interface used to display the end-user applications), and the session is rendered by the associated Sun Ray™ client device. An "N + 1" enterprise display server configuration is used for high availability and load balancing.

Network Security Management Tier (Network Security Toolkit – NST)

When deploying a VM infrastructure, it is highly desirable to monitor and verify that all virtual networking resources are secure and running at optimal performance. The Network Security Toolkit (NST) is a Linux-based distribution providing easy management access to best-of-breed Open Source network security and network monitoring applications. NST is installed as a VM performing network monitoring, network packet capture, network scanning and networking/host based intrusion detection for each VM and virtual switch configured within the ESX server cluster. Management and control of the NST VM is through a web-based user interface.

Secure Global Desktop Access Tier

The Secure Global Desktop Access Tier is where end user access to virtual desktops or individual applications occurs, using a web browser. The end user is provided with a configurable Webtop session view of available applications. The SGD Array is responsible for authentication brokering, application profiling and management, backend application server connectivity, backend application server single sign on, maintaining application session state and maintaining network connections for all logged-in users. As the number of end-users increases, an "N + 1" SGD Array configuration can be designed for scalability, redundancy, high availability and load balancing. Web-based administration and management tools (Array Manager and the Object Manager) are used to configure and maintain the SGD Arrays.

Coupling SGD with the Sun Ray™ technology supports a mobile virtual desktop environment whereby end users can use a smart card to gain access to their own personal virtual desktop (Webtop) throughout the enterprise network campus (known as: hot-desking). Users' session states within each application will be securely maintained

when they move from one virtual display client to the next. Thus, users can move from desk to desk, or even building to building, essentially taking their suspended desktop sessions with them as they go.

Virtual Desktop Infrastructure (VDI)

The VDI solution provides a complete desktop environment, with the operating system, applications and configurations residing in virtual machines (VMs) running on servers virtualized by VMware ESX Enterprise Server software.

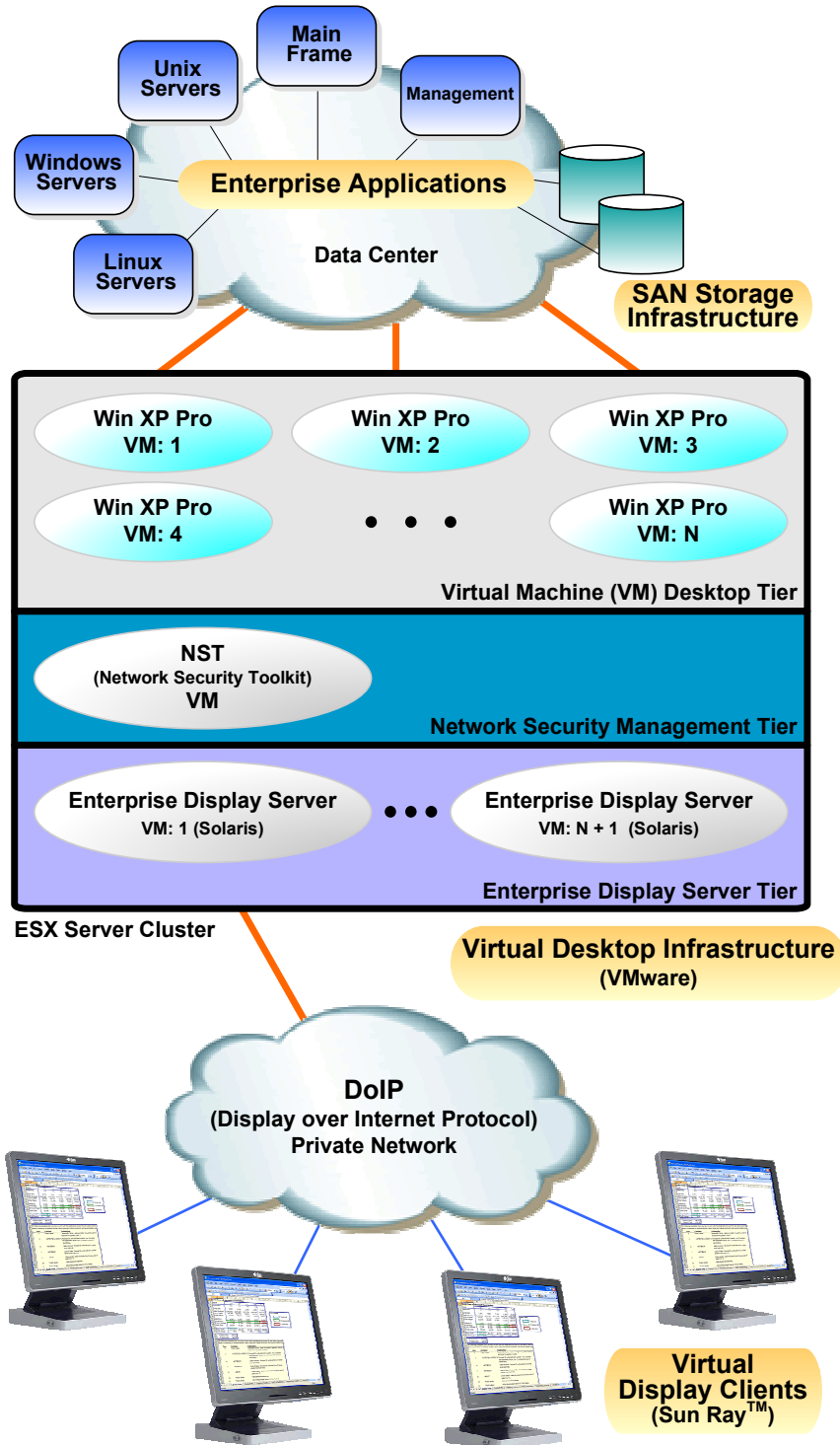


Figure 3: Virtual Desktop Infrastructure (VDI) Windows XP Desktop

The ESX Server Cluster depicted in Figure 3, above, is based on a multi-tiered VM architecture. As with SGD, each VM tier provides a functional service necessary for a secure, comprehensive virtual desktop display environment, with the same implementation and support benefits.

Administration and management of each desktop VM is accomplished using VMware VirtualCenter as a centralized data center management tool. End-users use remote display software to access their desktop environment from the preferred virtual display client (Sun Ray™), traditional PC or a thin client device.

Enterprise Display Server Tier (Virtual Display Client Access)

The Enterprise Display Server Tier uses Sun Enterprise Sun Ray™ Server software to provide virtual display client access, display rendering, control and management to all Sun Ray™ client devices. In a typical scenario, a Sun Ray™ server session starts, a remote display connection is made to an end user's VM desktop, and the session is rendered by the associated Sun Ray™ client device. An "N + 1" enterprise display server configuration is used for high availability and load balancing.

Network Security Management Tier (Network Security Toolkit – NST)

When deploying a VM infrastructure, it is highly desirable to monitor and verify that all virtual networking resources are secure and running at optimal performance. The Network Security Toolkit (NST) is a Linux-based distribution providing easy management access to best-of-breed Open Source network security and network monitoring applications. NST is installed as a VM performing network monitoring, network packet capture, network scanning and networking/host based intrusion detection for each VM and virtual switch configured within the VDI ESX server cluster. Management and control of the NST VM is through a web-based user interface.

Virtual Machine Desktop Tier

The Virtual Desktop Tier is where each instance of an end user's desktop VM is consolidated into a centralized repository within the ESX Server Cluster. Typically, the physical storage resource for each desktop VM is located in the SAN Storage Infrastructure. Base on the end user's computational resource need, different size desktop VMs are created and allocated out of the ESX Server Cluster resource pool.

Essentially, each end user can have a personal instance of a virtual desktop (desktop VM) running as their desktop computer. Access to the end-user's desktop is brokered so that availability of a given desktop will be present at each Virtual Display Client. In Figure 3, the Microsoft Windows XP Professional desktop is shown as the virtual desktop, but many other desktop operating systems, including Microsoft Windows Vista, are supported. All applications that previously ran on the end user's physical PC will run on the virtual desktop.

As with SGD, coupling VDI with the Sun Ray™ technology supports the hot-desking mobile virtual desktop environment. Using smart cards that store their unique IDs, users can move from one display device to another, resuming their suspended virtual desktop session at each stop.