Sun Desktop Virtualization Solution

Desktop Virtualization Blueprint

Warren Ponder

April 2006

Document Version: 2.8.5

Table of Contents

Introduction....4

Architecture Overview....5
- Client Tier....7
- Access Tier....7
- Virtual Desktop Tier....7
- Client Application Tier....7

Architecture Design Goals....8
- Interoperability....8
- Availability....8
- Scalability....8
- Manageability....8
- Standardization....8
- Security....8

Functional Use Cases....9
- LAN Access....9
- Secure Remote Access....10

Client and Access Tiers....10
- Virtual Display Client Access Service....10
- Virtual Display Client and Access tier - Network Protocols....11
- Secure Remote Access Service....13
- Secure Remote Access Network Protocols....13

Virtual Desktop Tier....15
- Virtual Desktop Tier Service....15
- Virtual Desktop Tier Management....17

Client Application Tier....19

Implementing Sun's Virtual Desktop Architecture....20
- Client and Access Tier planning and sizing considerations....20
- Virtual Desktop Tier Planning and Sizing Considerations....21
- Secure Remote Access Planning considerations....22
- Management and Implementation Considerations....24

Conclusion....27

Important Links....27

Acknowledgments....27

About the Author....27

Introduction

For several years, industry pundits and thin client proponents have hailed the coming of widespread adoption of “thin client” end user computing models. However, year after year, this adoption has been stalled by a number of issues. Primary among these issues were the cost, complexity and compatibility problems associated with the migration from physical private desktop computers to shared virtual client models. However, the recent emergence of server virtualization technologies has finally put this goal within reach. Sun's desktop virtualization solution combines server virtualization with Sun's stable of desktop infrastructure products to make this a complete solution.

In its simplest form, the Sun Desktop Virtualization solution consolidates desktop operating systems instances into the data center and presents them to end users through remote display protocols on a wide array of devices wherever they have network access. The solution described is specific enough to be deployed as described in this whitepaper (which is based on customer case rollouts) but the architecture is open to other products and technologies.

Sun's Desktop Virtualization solution enables customers to leverage the value of thin clients while at the same time minimizing the initial investment and high migration cost that is sometimes associated with migrating from a distributed fat client based solution. Often, customers want to move to a thin client based solution but struggle with the effort and cost of doing so. Desktop Virtualization can enable customers to leverage the value of Sun's Virtual Display Client technology by moving desktop instances off physical personal computers and consolidating logical versions of them onto a server based solution leveraging virtualization technology.

Desktop virtualization allows you to reap the benefits of thin clients without worrying about how your current and legacy desktop applications perform in a typical server based computing architecture. Customers can continue to use their existing desktop operating environment of choice whether it is Windows, Linux or Solaris™. The Sun Ray™ Software can display desktop sessions from all three platforms. When combined with Sun™ Secure Global Desktop, server based applications can be published or accessed from Unix, Linux, 3270/5250 or Windows hosts, to the virtual desktop instances. This cuts out a large portion of the functional and regression testing typically required with a full migration to a Server Based computing architecture. 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, moving these applications and their management off the desktop, leaving only the user environment and a small subset of applications to be managed.

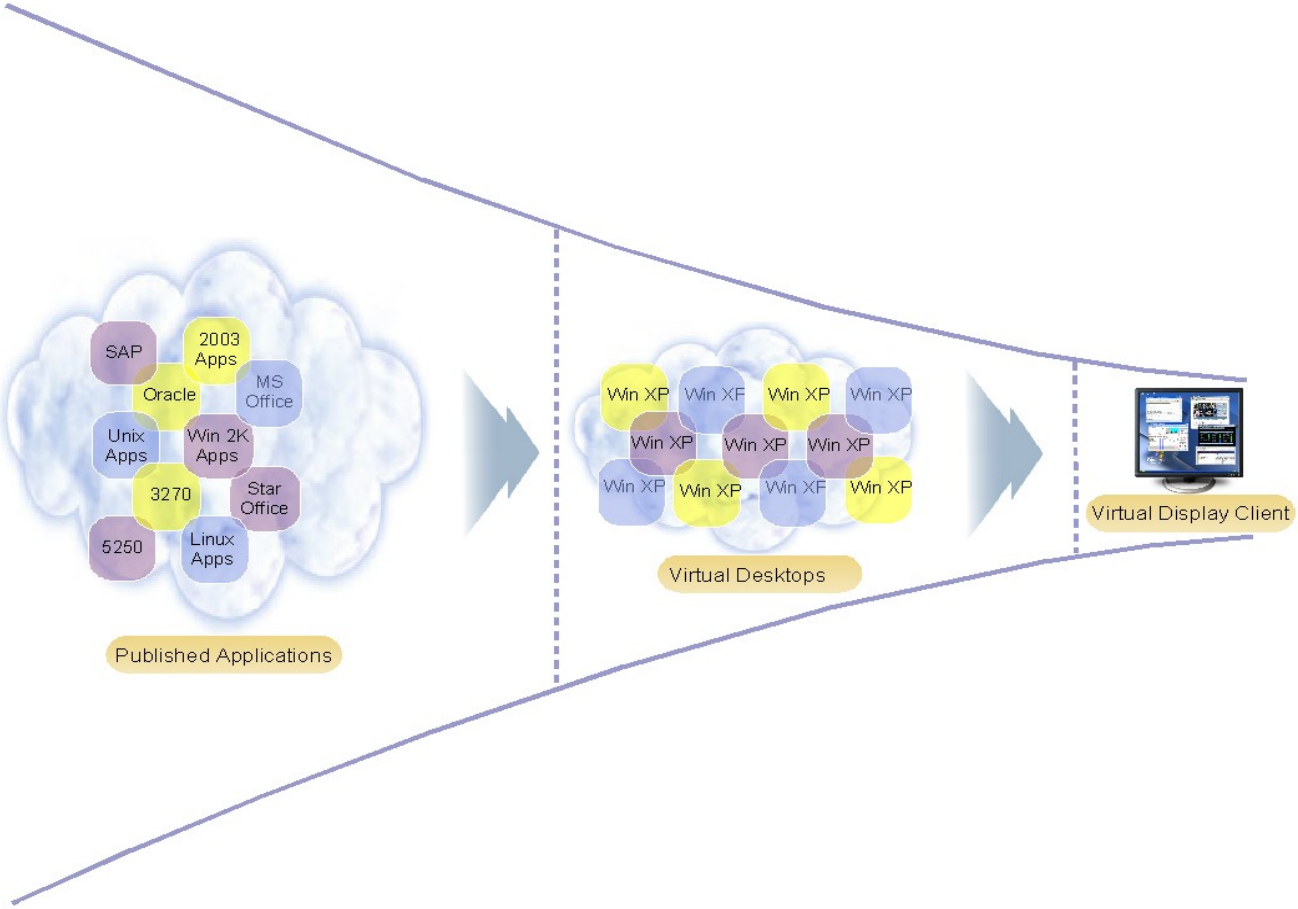

Figure 1: Virtual Desktops

With a Sun 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 traditional PC's or thin clients that use an embedded operating system. Lower TCO/ROI can be achieved through more efficient management, increased productivity, reduced power, cooling, better utilized computing resources and extended desktop lifecycle.

In this document we will outline the reference architecture and a sample implementation for the Sun Desktop Virtualization Solution. This reference architecture is an over view of the key components required to deploy the solution into your enterprise infrastructure.

Architecture Overview

The Sun Desktop Virtualization solution is a multi-tiered architecture. Each tier breaks out the functional components that enable the solution as a whole. A multi-tiered approach enables higher resiliency and increases the ability to scale the solution while at the same time minimizing the effort and resources required to manage it.

The following diagram is an overview of the end to end Sun Desktop Virtualization solution. Sun has partnered with VMware as the leading virtualization provider for the Sun Desktop Virtualization solution.

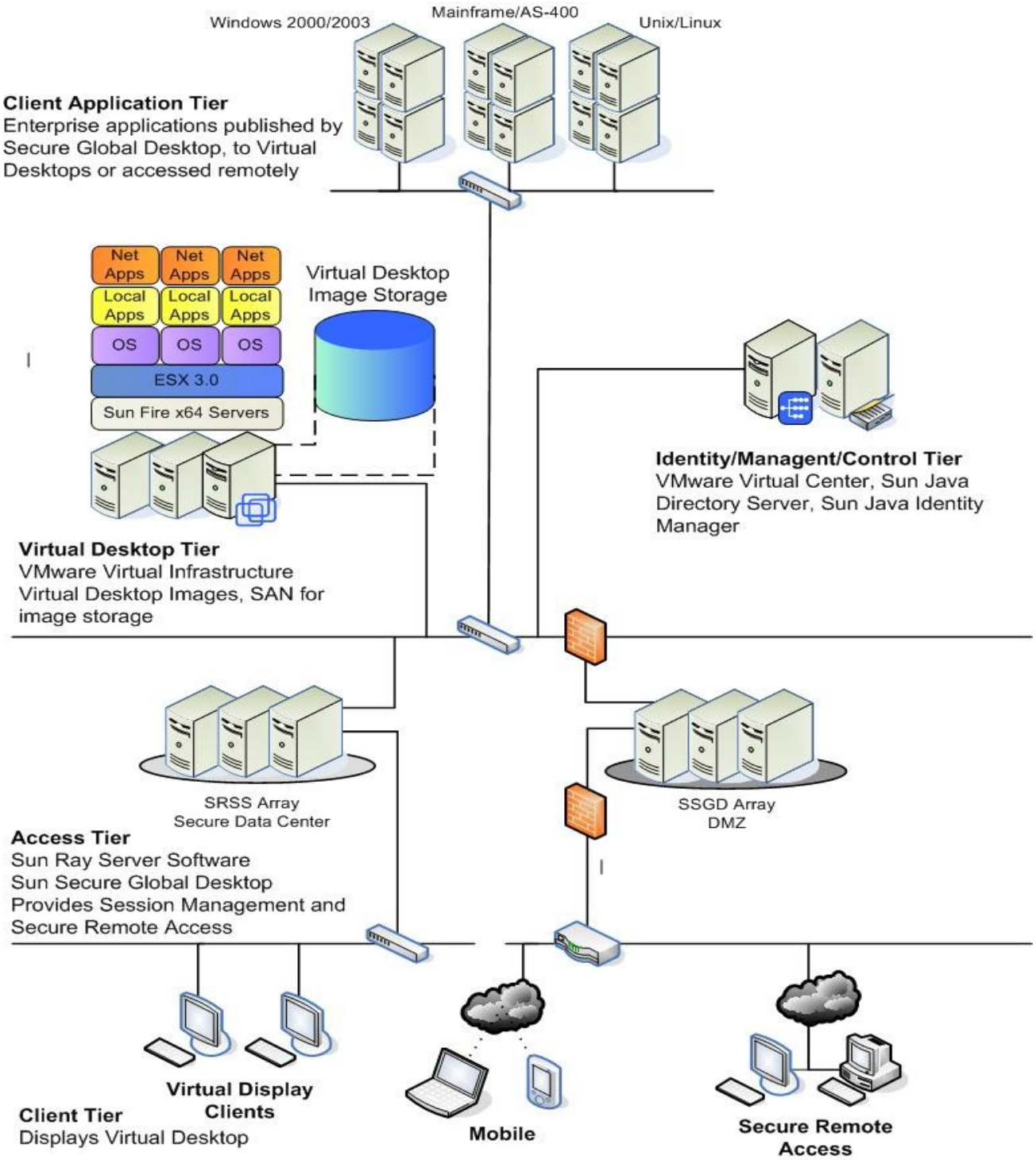

Figure 2: Sun's Virtual Desktop Architecture

Client Tier

The client tier is the access points or devices, used by end users for accessing their desktop instance within the virtual desktop tier.

Access Tier

The access tier is the infrastructure (either physical or virtual) that enables and brokers connections between the Client Tier and the Virtual Desktop Tier. It plays a critical role in the overall security and scalability of a virtual desktop solution.

Virtual Desktop Tier

The Virtual Desktop Tier is where the users desktop images are consolidated into a centralized farm of virtualization hosting servers. This also includes the storage for the virtual desktop images themselves.

Client Application Tier

The client application tier are the application farms of applications traditionally delivered to the desktop via application publishing products or display protocols such as ICA, RDP, X11, 3270 or 5250. These systems often are already in place with applications accessed via traditional personal computers.

The following is a list of functional components commonly found when designing a Sun based desktop virtualization solution. In some cases, these components might already exist. If this is the case, the Sun Desktop Virtualization solution seamlessly integrates with these existing components. In cases where these components are not already in place, they are designed into the solution.

- Clients - Thin Client Devices, Personal Computers or Laptops used to access a virtual hosted desktop
- Servers – Used to host the virtual desktop sessions, management tool or other application service
- Storage – SAN switches and Arrays used to provided connectivity to the servers and storing the virtual desktop images
- Network – Switches and routers used to provide connectivity an routing between the clients and servers
- Security – Internal and perimeter firewalls used to prevent unauthorized traffic between tiers
- Identity Management – Single source authentication for virtual desktop users
- Virtualization – Allows the hosting of virtual desktop instances
- Management – Tools that enable the day to day operation of the solution
- Secure Remote Access – Allows the users to remotely access their virtual desktop
- Provisioning – Allows new virtual desktop instances to be created and deployed in the virtual desktop tier

Architecture Design Goals

The Sun Desktop Virtualization architecture has goals similar to any other enterprise solution: interoperability, availability, scalability, manageability and security.

Interoperability

It is important the solution offer flexibility and interoperate with existing installed infrastructure and services. In most cases existing Directory, File/Print or hosted Enterprise Applications that already exist. Providing access to these existing services should be seamless and require little or no modification to the services themselves. The customer should be able to choose the desktop operating environment they prefer. Products used from multiple vendors should interoperate together using native or open protocols.

Availability

All components of the architecture should be resilient to failure. Best practices, design principles and operational procedures should all come together in order to achieve the highest level of availability mandated by the company's service level agreements.

Scalability

Each tier should be designed to accommodate growth and easily scale as users are added or removed.

Manageability

The solution should be easily managed by existing staff where possible with minimal additional training required. If possible existing tools should be able to be used or comparative alternatives. Using existing tools help during the migration and transition phases. In addition they protect the existing investment made. Operational changes should also be kept to a minimum. Because this solution proposes moving most of the components into the data center. Better operational procedures can be applied. Some of the existing desktop support procedures may need to be altered to accommodate changes in patch management, software distribution and desktop image management.

Standardization

Through the use of common components and a building block design approach. Different components throughout the architecture should be easy to standardize within an organization. This will allow for faster deployments across businesses as well as reduced cost in supporting and acquisition costs. Standard protocols and technology should be used as much as possible to increase interoperability and flexibility.

Security

Security is multi faceted design goal and can be implemented in variety of ways throughout this architecture. Each organization's security policies should easily apply to the solution. Some common

security features found in the Sun Desktop Virtualization Solution include:

- Authentication
  - LDAP based user authentication
  - Role Based Access Controls
  - Two-factor authentication compatible
- Encryption
  - ARC4 – For Sun Ray protocol traffic encryption
  - SSL encryption – For Secure Remote Access encryption
  - TLS – For Directory Server traffic encryption
  - SSH – For secure communication between systems

By design, a network delivered desktop solution is typically more secure than a distributed PC based solution because data is at less risk of loss. Encrypting the traffic between clients and the servers helps ensure connections are protected from potential compromise. Most importantly, network delivered desktops help solve the dreaded "stolen laptop" problem where confidential corporate data is lost or stolen from an employees portable computer.

Functional Use Cases

LAN Access

Access to each user's virtual desktop residing in the virtualization tier is provided by the use of Sun Ray virtual display clients controlled by Sun Ray Servers in the access tier. The process to accomplish this seamless to the end user, but contains several steps:

1. End users insert their smart card into the Sun Ray virtual display client.
2. The Sun Ray Server software operating in controlled access mode (CAM) launches the Sun Ray Windows connector script.
3. The Sun Ray Windows Connector script has two purposes: locate the end users virtual desktop instance and make a RDP connection to it. Locating the end user's desktop instance can be accomplished with a variety of methods. For example, some organization will utilize dynamic DNS naming and tie that to the user login name. Other companies will key off the inserted Java Card™ or other LDAP information. Whatever the method, the Sun Ray Windows Connector then makes a RDP connection to the newly found virtual desktop instance.
4. At this point, the end user interacts with the virtual desktop as normal. Authentication and application access is handled via the normal desktop operating system methods.

This use case can also be duplicated with stripped down PCs by creating operating system specific scripts or batch files and an RDP client. However, this may reduce savings due to the associated management, complexity and support costs. Some organizations who have a staggered personal computer depreciation schedule can use Sun Secure Global Desktop as a tool to migrate these desktops to a virtualization solution.

In this case, the physical machines are striped down to a bare OS image and configured to launch the Sun Secure Global Desktop Client at startup. These personal computers can then deliver the user's virtual desktop instance until they have been fully depreciated and replaced with a virtual display client.

Secure Remote Access

The secure remote access component provides secure access to an individual's virtual desktop from outside the network. This access could be from a customer location, Internet kiosk, a mobile laptop or an employee working from home on a PC or MAC. The process to accomplish this is slightly less seamless to the end user that the LAN scenario above. However, it is very effective in increasing the overall mobility of the users as well as helping to ensure that enterprise data is kept securely within the data center:

1. End users launch their web browser and point it to their organizations Secure Global Desktop (SGD) website address.
2. After logging in (SGD can authenticate against Windows Active Director, LDAP or Radius), the user will see their virtual desktop instance, provisioned for them in their applications side panel.
3. The SGD server has been configured to locate each users virtual desktop instance by name. When the user launches their desktop application instance. SGD makes a RDP connection to the virtual desktop instance and then proxies the user's connection securely through to the virtual desktop instance.
4. At this point, the end user interacts with the virtual desktop as normal. If the user was already logged in from another location. The desktop session is resumed as it was left. For example, if the user left the office in the middle of drafting and email. They can continue working on that message from the point where they stopped.

Client and Access Tiers

The client tier are the access points or devices used by end users for accessing their virtual desktop instance in the Desktop Virtualization Tier. Also covered is the access tier and how access is provided from inside a corporate network and how the solution can also provide secure remote access.

Virtual Display Client Access Service

Every Sun Ray Virtual Display client has a built in smart card reader. Smart cards are used in the desktop virtualization solution to establish an association between the user and their virtual desktop. In addition, this enables desktop session mobility for every user. By simply removing their card and moving from one display client to another, the user is automatically redirected to their virtual desktop. This happens without interruption to any work the user was doing prior to moving. In addition, it requires no configuration or added administration.

The access tier is comprised of Sun Ray servers for handling Virtual Display Client access and Secure Global Desktop servers for handling secure remote access connections . Sun Ray servers are deployed in a failover group, also commonly referred to as a FOG. The FOG handles load balancing to evenly distribute connections

across the pool of servers. In the event of a server failure, the client devices automatically re-establishes a session through another Sun Ray server in the virtual desktop tier. In this case, the users virtual desktop session is not interrupted and the desktop activity will resume where it left off when it disconnected.

When a new user is provisioned (or existing user migrated), they are issued a smart card. Smart cards are badge like cards that contain an embedded microprocessor and can store small amount of data. The token from this card is registered in a LDAP directory along with an assigned hostname for their virtual desktop instance. This information can reside in Active Directory or a separate directory. For smaller deployments, it is also possible to store this information on the Sun Ray servers. In Windows only deployments, the Sun Ray servers are configured in Controlled Access Mode often referred to as CAM mode. CAM allows the system administrator to configure what applications are allowed to be run on the systems. When in CAM mode, the servers are an appliance, with little or no ongoing maintenance.

When a user inserts their assigned smart card into the the Sun Ray client, the CAM application reads the token and does an LDAP search based on the card token. It searches for the users assigned virtual desktop hostname. The hostname is then used by the Sun Ray Software Windows Connector to establish a connection between the client and virtual desktop. Once the session is established, the user is presented with a Windows log in. The virtual desktops in most cases, are members of an Windows Active Directory domain. At the login, the user enters their AD user name and password and is granted access to their virtual desktop environment.

Virtual Display Client and Access tier - Network Protocols

The Sun Ray Software Windows Connector is used for communication between the Sun Ray Servers and the virtual desktop. Communication is done using the RDP protocol. RDP is a Remote Desktop Protocol that was developed by Microsoft for establishing remote desktop connections. All the RDP traffic stays with-in the datacenter network. The Sun Ray Software Windows connector is a RDP client developed and supported by Sun, using the Microsoft RDP spec.

The Sun Ray protocol is used for communication between the Sun Ray Virtual Display Client and the Sun Ray servers. The Sun Ray protocol is an adaptive protocol that has been developed to provide a high quality user experience at reduced bandwidth levels. In a LAN environment, bandwidth availability is typically less of a concern. Because of the adaptive nature of the Sun Ray protocol and its ability to perform well in low bandwidth situations. It's an attractive solution for smaller satellite offices with only a few clients and low bandwidth connections. A virtual desktop can be delivered to these remote locations without having to deploy any servers locally. This centralizes the day to day management of the desktop inside the data center with the rest of the enterprise, reducing the management cost common with managing a distributed solution. When necessary, the Sun Ray protocol can be encrypted by simply enabling encryption on each Sun Ray server.

Each virtual desktop is configured to use DHCP to obtain its network configuration information. Because each user is assigned a desktop by hostname. Dynamic DNS (DDNS) is used to handle the host name to IP address changes and updates. Typically, in a Windows-based desktop environment using Active Directory, administrators are already using DDNS to simplify their hostname management changes. This allows for a simplified migration from a PC base architecture to Desktop Virtualization. DDNS is used for establishing an association between users and their virtual desktop. When a user is provisioned or migrated to a virtualized desk top. The user is assigned a host name, managed by DDNS. This host name is used to direct the user to their assigned virtual desktop. Most deployments that have moved to a desktop virtualization architecture have only had to make minor changes if any to their existing core infrastructure when migrating.

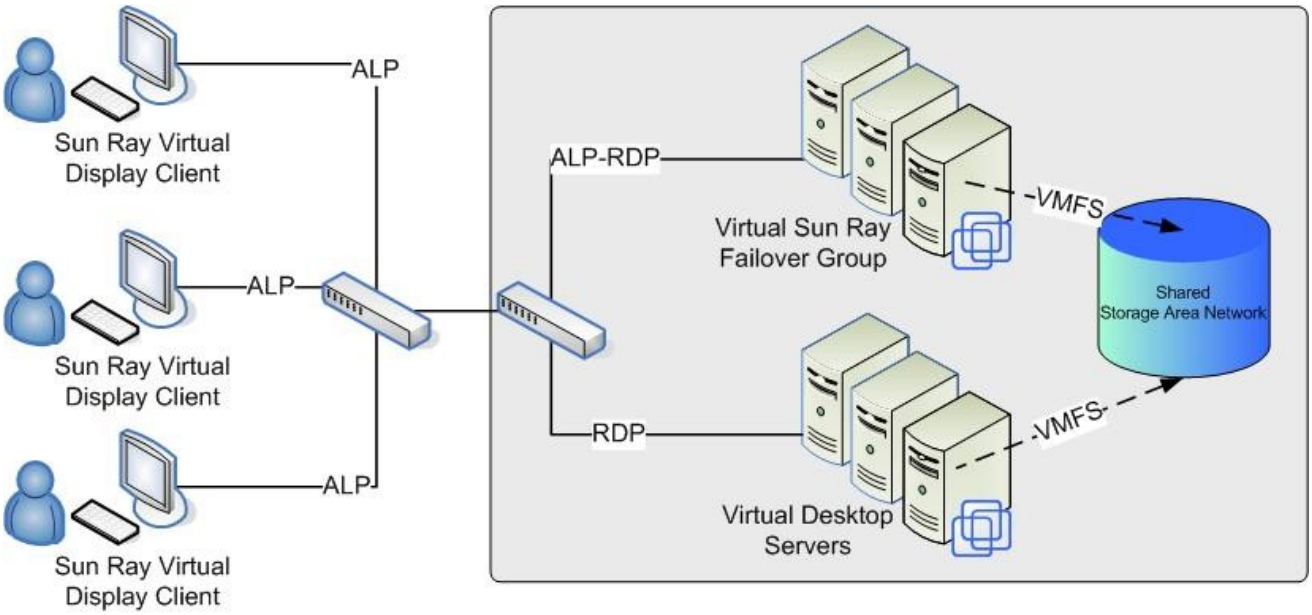

Figure 3: Virtual Display clients deployed within virtual access tier

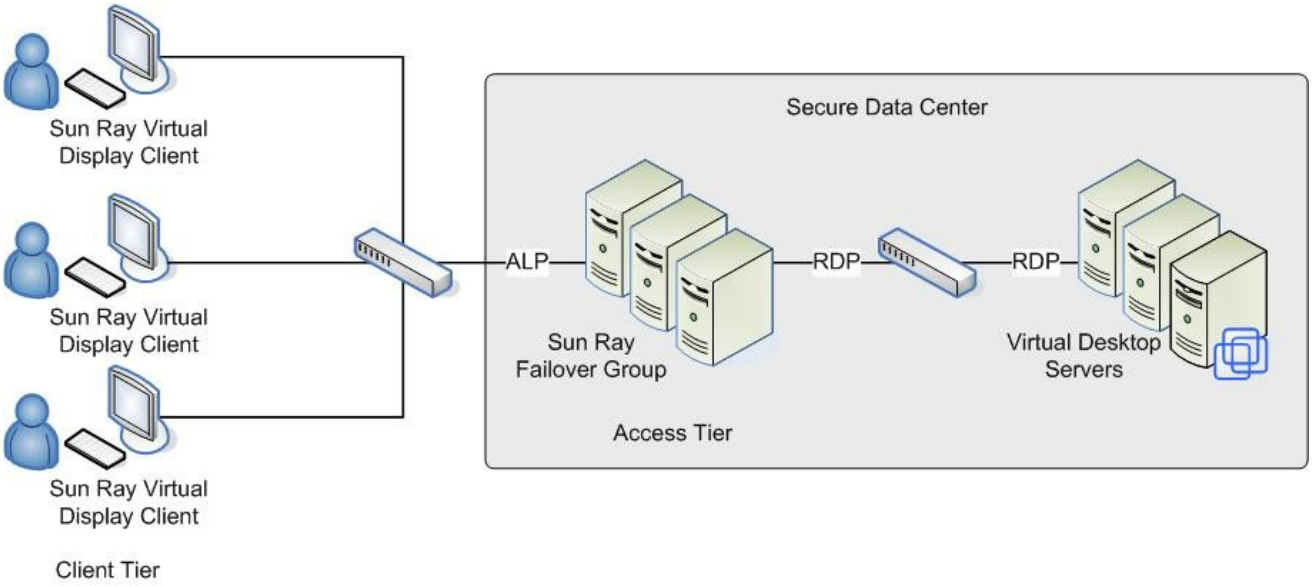

Figure 4: Virtual Display clients deployed within a physical access tier

Secure Remote Access Service

Secure remote access is provided to mobile, remote or work from home users through the use of Sun Secure Global Desktop. Remote workers can access their virtual desktop or individual applications remotely from any device using a web browser. This approach is highly secure, as the information and data being accessed is only displayed to the client. All the traffic between the client and the Secure Global Desktop servers is encrypted and the data stays in the corporate data center. No code is required to be manually installed on the end user device that is used to access the users virtual desktop. This greatly reduces the serviceability and management of the solution. Because there is no software to manually install on the client devices. The infrastructure components for secure remote access can be quickly deployed and scaled to provide additional capacity.

Secure Remote Access Network Protocols

Authorized end users access their desktops remotely by using a standard web browser. The secure remote access arrays can reside securely in the DMZ of the network. Using the virtual desktops native network display protocol (X11, RDP, TN5250, etc.) Sun Secure Global Desktop can provide access to the users desktop running on the virtual desktop servers.

Sun Secure Global Desktop uses the AIP protocol for communication between the Sun Secure Global Desktop servers and the client devices. The AIP protocol is an adaptive protocol that performs very well over a wide area networks. Because of its adaptive nature, it performs well in low bandwidth situations ensuring a high quality user experience.

SSL encryption for encrypting the remote access traffic can be handled by the Sun Secure Global Desktop Servers or via an external network appliance. The traffic between the Secure Global Desktop Server and the user's virtual desktop instance uses the desktops native protocol. In the case of connecting to a Windows XP Pro-based desktop the RDP protocol is used.

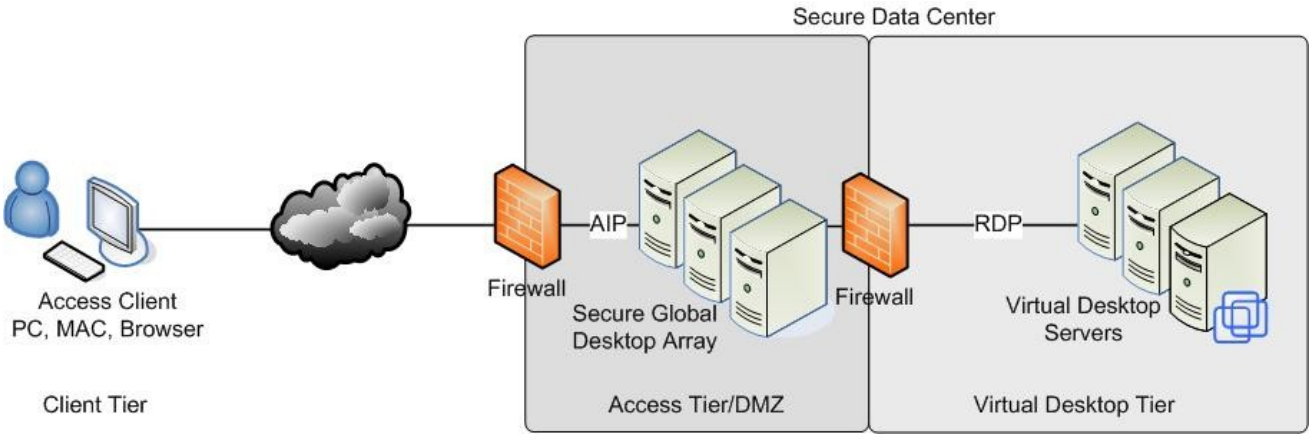

Figure 5: Secure remote access

Virtual Desktop Tier

The Virtual Desktop Tier encompasses the core of the Sun Desktop Virtualization Solution. The Desktop Virtualization Tier includes the hardware, virtualization software and storage for all the virtual desktop images. Each users individual desktop is hosted by the virtualization tier, securely within the datacenter. Each users virtual desktop instance can be accessed from within the intranet from any Sun Ray Virtual Display Client or remotely using Secure Global Desktop for secure remote access.

Virtual Desktop Tier Service

The virtual desktop solutions is comprised of three core components:

- VMware Virtual Infrastructure 3.0
- Sun Fire™ x64 Servers
- Sun StorageTek™ Storage and Software

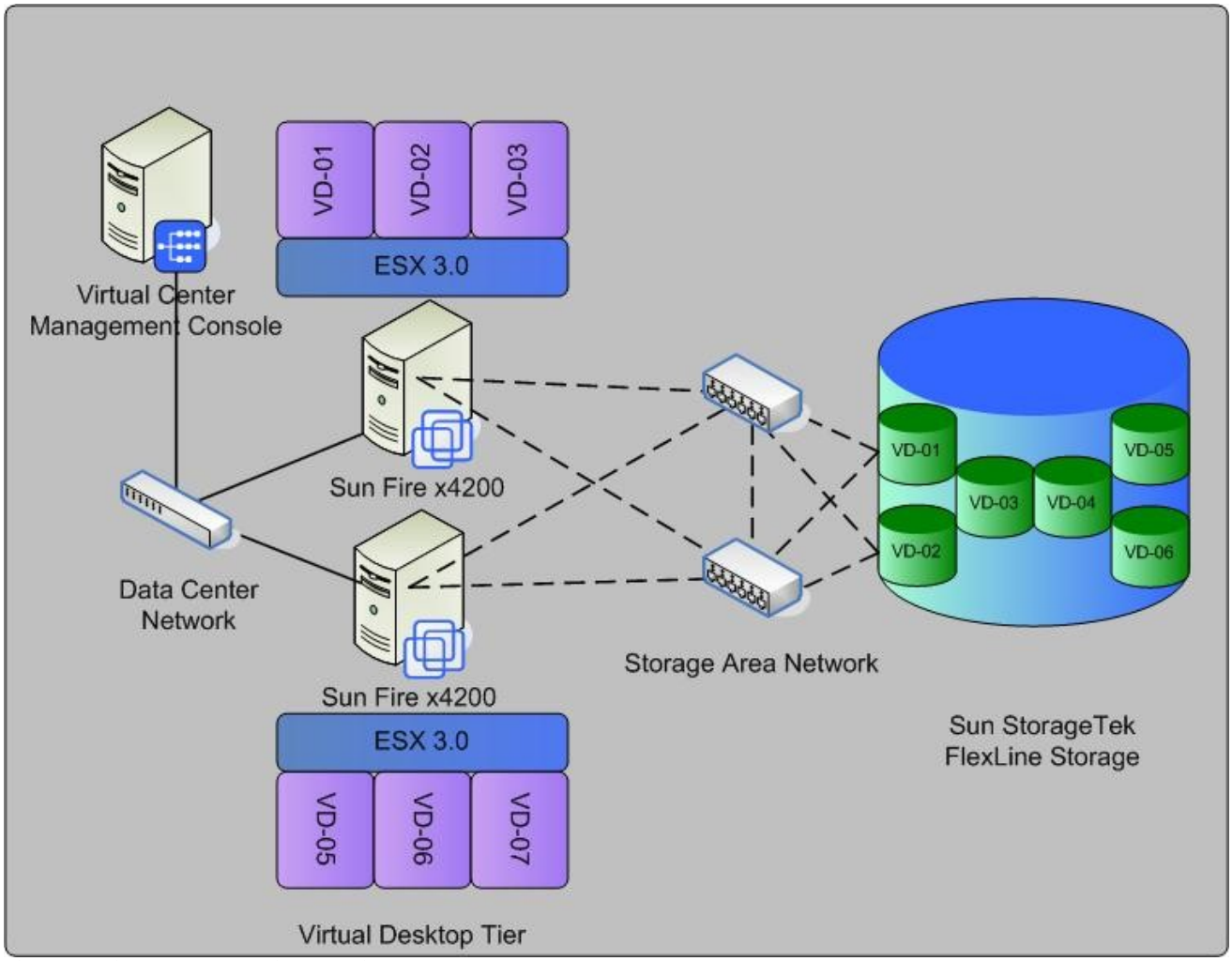

Figure 6: Virtual Desktop Tier overview

VMware Infrastructure 3.0 is used as the virtualization technology for the Sun Desktop Virtualization solution. Combined with the Sun Fire x64 servers for virtualizing the desktop instances and the StorageTek ™ Flexline series storage for storing the desktop images, we have been able to achieve significant desktop consolidation ratios as high as 40:1. This solution offers organizations a cost effective and secure way to leverage ultra thin client technology today, without having to worry about if or how, their applications will perform in a traditional server based computing model. Because each desktop instance is virtualized, the applications will function just as they did before. By adding the Sun Ray Virtual Display Client as the access device, end users can access their desktop environment with a higher level of security, increased flexibility and better productivity .

Because each desktop environment is deployed in the data center and no client devices requiring management are deployed to the desk. There is no need for desk side management or break fix. This can also help increase desktop management, software distribution and patch management success, because each desktop image is hosted inside a secure data center and controlled by the support staff. Using Virtual

Center as the control station for the virtual infrastructure, an administrator can always ensure that a desktop image is running and available either manually, automatically or using a scheduled job. With all the desktop images stored in a SAN, desktops suffering from a failure can be resumed with-in a matter of minutes Using a standby server.

Desktop roll outs and migrations are as simple as moving or deploying a new image within the virtual desktop tier. Using pre-created templates, 100's of desktop images can be deployed within minutes. This drastically reduces desktop roll outs as the average setup time for a Sun Ray Virtual display client is five minutes. All the configuration is automated in the back end, with nothing to image, deploy or configure in the client tier.

Virtual Desktop Tier Management

Virtual Center is the primary utility used for managing the Virtual Desktop Tier. Virtual center is used for resource reporting, provisioning new virtual desktop templates, template management, cloning desktop images, cold migrations and system monitoring.

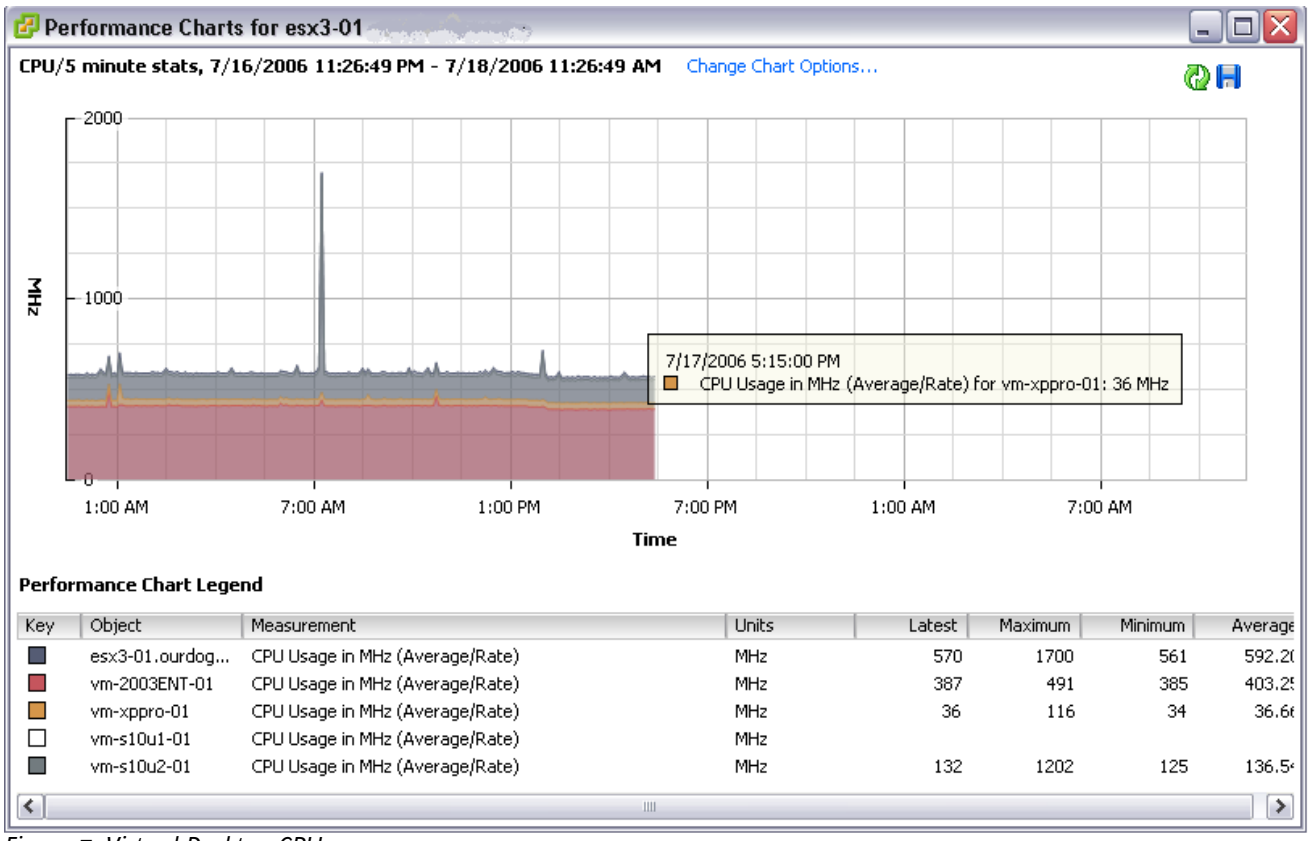

Figure 7: Virtual Desktop CPU usage

Through the use of Virtual Center reporting functions, extremely detailed trend reports can be generated showing each desktop virtualization servers utilization. These reports can be customized in order to meet the specific needs of each environment. The reporting mechanism has enough granularity for filtering out each virtual desktops resource consumption including CPU, Memory, I/O and network usage. These reports and graphs, can be used for capacity planning, future design considerations, trend analysis and troubleshooting.

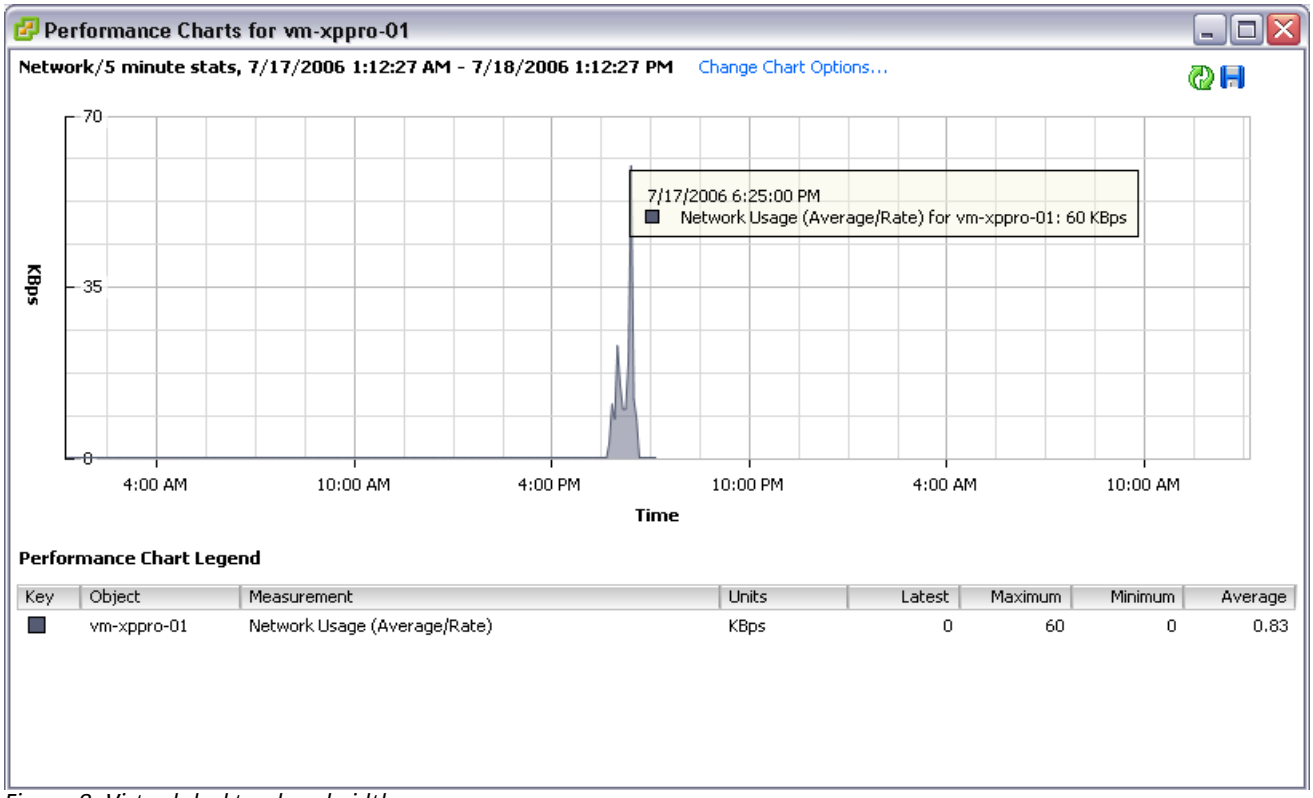

Figure 8: Virtual desktop bandwidth usage

For most organizations, only minor adjustments to standard images will be required for preparation to deploy as virtual hosted desktops. These adjustments commonly involve adding the VMware tools and any OS specific tools for changing SID's. Once these changes are made, a virtual desktop template can be created and used for easily provisioning and deploying new virtual machines. Templates reduce human error and ensure all virtualized desktops are configured the same.

Using Virtual Centers cold migration feature. Powered off virtual machines can be moved from one physical desktop virtualization server to another. This is very helpful in the event of a server problem. When a server has a problem, virtual desktops can be moved to a standby or under utilized server to minimize any loss of productivity.

For deployments needing a more dynamic desktop virtualization tier. Virtual Infrastructures Distributed Resource Scheduler (DRS) can be leveraged to dynamically provision and migrate virtual desktop machines based on resource utilization.

Servers in the desktop virtualization tier are grouped into VMware clusters. Once grouped together they are managed as single system of aggregated resources. DRS continually monitors the utilization of each server's resources within the cluster. If a server becomes resource constrained, DRS works in conjunction with VMware VMotion to migrate virtual desktops seamlessly from one system to another system within the cluster that has available resources. Virtual desktops migrated from one server within the cluster to another is done without interruption to the user. DRS also works with Virtual Center to provide a centralized view of the resources across the cluster. DRS can be configured to automatically carry out migrations and changes as they arise or configured for manual intervention where the system administrator is notified when a server is over utilized. The system administrator can then review the recommended changes and either accept or deny them.

This new capability enables the opportunity to increase the overall dynamic nature of the Sun Desktop Virtualization Solution. In addition, DRS can also greatly reduce the system management required with a more static design and configuration.

The on-going system monitoring is managed through system alerts set by the system administrator based on predetermined thresholds. If a threshold is exceeded an notification can be sent via E-Mail or standard SNMP traps to an existing network monitoring machine. In addition, these alarms can be set to run scripts for automated management. Management scripts can be created and used to ensure virtual desktops are powered on during scheduled maintenance windows for increased patch management and software distribution success.

Virtual Center uses role based access control for virtual machine and server management. It is recommend that specific groups and roles are created specific to managing the virtual desktop servers. Accessing a virtual desktop from a Sun Ray Virtual Display client is seamless and should stay that way. End Users should not have access for stopping, starting or suspending their virtual desktop.

Client Application Tier

The client application tier are the farms of applications traditionally delivered to the desktop via application publishing products or display protocols such as ICA, RDP, X11, 3270 or 5250. These systems often are already in place.

Some organizations might be delivering Windows applications to their desktop's using technology like Citrix Presentation Server. The Sun Desktop Virtualization Solution can seamlessly integrate with existing Citrix environments and Citrix can continue to be used for publishing applications to the virtual desktops. If the

customer has a need to deliver hetereogenous applications to multiple clients then they should consider standardizing on Sun Secure Global Desktop software.

A Sun Secure Global Desktop array can be deployed into the Client Application Tier and used to publish applications from existing Unix, Linux, Windows and Mainframe/AS-400 environments to the virtual desktops deployed in the desktop virtualization tier. Moving these applications off the desktop to the server allows organizations to begin focusing on application/server management more so than desktop management and software distribution.

Implementing Sun's Virtual Desktop Architecture

Client and Access Tier planning and sizing considerations

Planning of the client and access tiers is mostly comprised of policy setting and planning the failover groups in the access tiers servers. Who has access to what, how they get it and when. The bulk of the planning is around these policies, physical network design and sizing.

Because the Sun Ray Display Device is a network based device, it's best to consider a redundant network core from the wiring closets to the data center. If the Sun Ray devices will be deployed on a LAN that also has PC's. Each should be put in a separate VLAN to ensure a high quality of service.

Most organizations have existing DHCP servers. When migrating to Sun Ray devices some organizations might wish to use their existing DHCP infrastructure. This is possible and can be handled a couple of different ways. Sun Ray devices can get all their configuration information from the Sun Ray servers handling DHCP, or they can get part of their configuration information. If an organization wishes to use their existing DHCP services. Those services will need to be configured to return the IPADDRESS and AUTHSERVER information. Once a Sun Ray client has this information, it can send a second request to the Sun Ray server, requesting the rest of the information such as the server providing firmware updates. The the existing DHCP services can also be modified to provide all the necessary information. It is important to note that if the DHCP services are located on a routed network a DHCP relay agent will be required to forward the DHCP request.

Sizing considerations for the Sun Ray servers in the access tier is largely based on the desired number of concurrent sessions per server. The Sun Ray Windows connector that is used for communication with Windows based virtual desktops, is a fast, light weight client. Typical resource usage is 11M of memory and 0.2%– 0.3% CPU per user. For physical access tier deployments. A Sun Fire x64 class system with only five gigs of RAM could handle 360 concurrent connections. Common deployments to date have ranged in the 100 – 150 concurrent users per server. The Access Tier can also be consolidated into a virtual access tier leveraging virtualization technology. In this case, servers from different failover groups can strategically be placed on different virtualization servers for increased availability. Planning for this type deployment can be a little more complex. Servers should be deployed with a decent size group of users. Then, using the

reporting and monitoring features of the virtualization software. Performance data can be collected and used too make proper decisions regarding how many physical servers to consolidate into virtual servers.

Virtual Desktop Tier Planning and Sizing Considerations

When migrating to a virtual desktop solution, consolidation ratio is the single most important consideration factor. How many desktop can i get per server? This number will very from environment to environment. The job function or role and the applications used together affect the amount of resources required per virtual desktop. For example, higher consolidation is more likely is a sales office or department because the users are not always on always active doing something. They also tend to be more mobile coming and going. When in the office, they typically use low resource consuming applications like E-Mail, web Browsing and Office Productivity. Because of this usually a higher consolidation can be achieved because there is less risk resource contention will occur.

The other extreme is a Software Developer. Software developers tend to work all day heads down using applications that consume lots of resources and compiling code. This requires a higher demand from the systems and if not properly planned more likely too experience resource contention. For this type environment a better understanding of the users profile is very valuable in achieving a high consolidation without sacrificing performance and productivity. Call center environments tend to fall into this category as well. Typically a call center agent has lots of applications concurrently running, switching between applications, inputting information and call handling steadily throughout the day. They also tend to used extremely fat, rich applications.

We recommend measuring a small subset of user profiles as a test bed for establishing a water mark for consolidation. Virtual Center ha all the built in tools for reporting and tracking resource usage. Using this data you can make solid decisions regarding sizing and consolidation ratios. As a rule of thumb we recommend the following using a Sun Fire V40z with four single core AMD 254 processors and 32GB RAM.

Task/Knowledge workers : 30-40:1
Power Users/Developers : 20-30:1

Policies addressing the amount of storage per virtual desktop should be determined in the design planning phases. Now is a great opportunity to reduce the size of each desktop image and ensure desktop users store their data on a shared network drive. Storage space for templates also needs to be taken into account. In certain deployments such as developer desktop deployments. Virtual Machine snapshots can be very valuable. Developers can be given access to snapshot their machine before doing something that could cause damage their work environment.

It's also recommended when designing the desktop virtualization tier, that common workloads are grouped together when possible. For example, developers and knowledge workers should be put on separate server groups. Unless, you determine the desktop profiles are heavy in a specific resource such as I/O. In that

case, a mix of other virtual machines that are less I/O demanding will result in a higher over all utilization rate as well as being less prone too resource contention. If the Access Tier is consolidated using virtualization one approach to consider is spreading one or two access servers from a FOG across each virtual desktop server.

If you are planning to implement VMware's DRS, special consideration should be made when planning and designing the desktop virtualization tier and associated storage requirements. The virtual desktop tier servers will need shared storage on the SAN as well as a shared VMFS volumes reachable from each host.

Because DRS uses VMotion, special consideration should also be taken when selecting the servers for the virtualization tier. The servers used in the DRS clusters need to share processors from the same family. A dedicated Gigabit Ethernet network should be designed into the final architecture for virtual desktop machine migrations.

The nature of your desktop users and the resources they consume will largely contribute to what type of resource control is used. Either shares or reservations. For example, a call center might have several hundred users consistently working all day that need a certain level of committed resources. In this case it would make sense to use a reservation type allocation where each agent is guaranteed a defined amount of resources. When using reservations measuring the users and there typical resource usage is important. This prevents over allocating or under allocating resources for the virtual desktop. In an environment where there are knowledge workers or mobile workers that are attending meetings and using their virtual desktops less frequently. There is more fluctuation in the resource availability. In this case DRS shares can be more beneficial in achieving balanced resource usage and performance.

Secure Remote Access Planning considerations

Deploying Sun Secure Remote access is straight forward. Most organizations work with their security teams to determine the agreed port numbers to use for incoming traffic. Once determined, planning for firewall rule changes and updates can be made. Because the secure remote access servers reside inside the DMZ most organizations already have standard server builds and policies for configuring these servers and network devices.

Commonly, remote access users want to access their virtual desktop remotely either published full screen or as a seamless window. Full screen takes over the entire screen of the system they are accessing. However, they can toggle between their local and remote desktop. Seamless allows the user to dynamically re-size the remote desktop and still have easy access to their local desktop without the need to toggle.

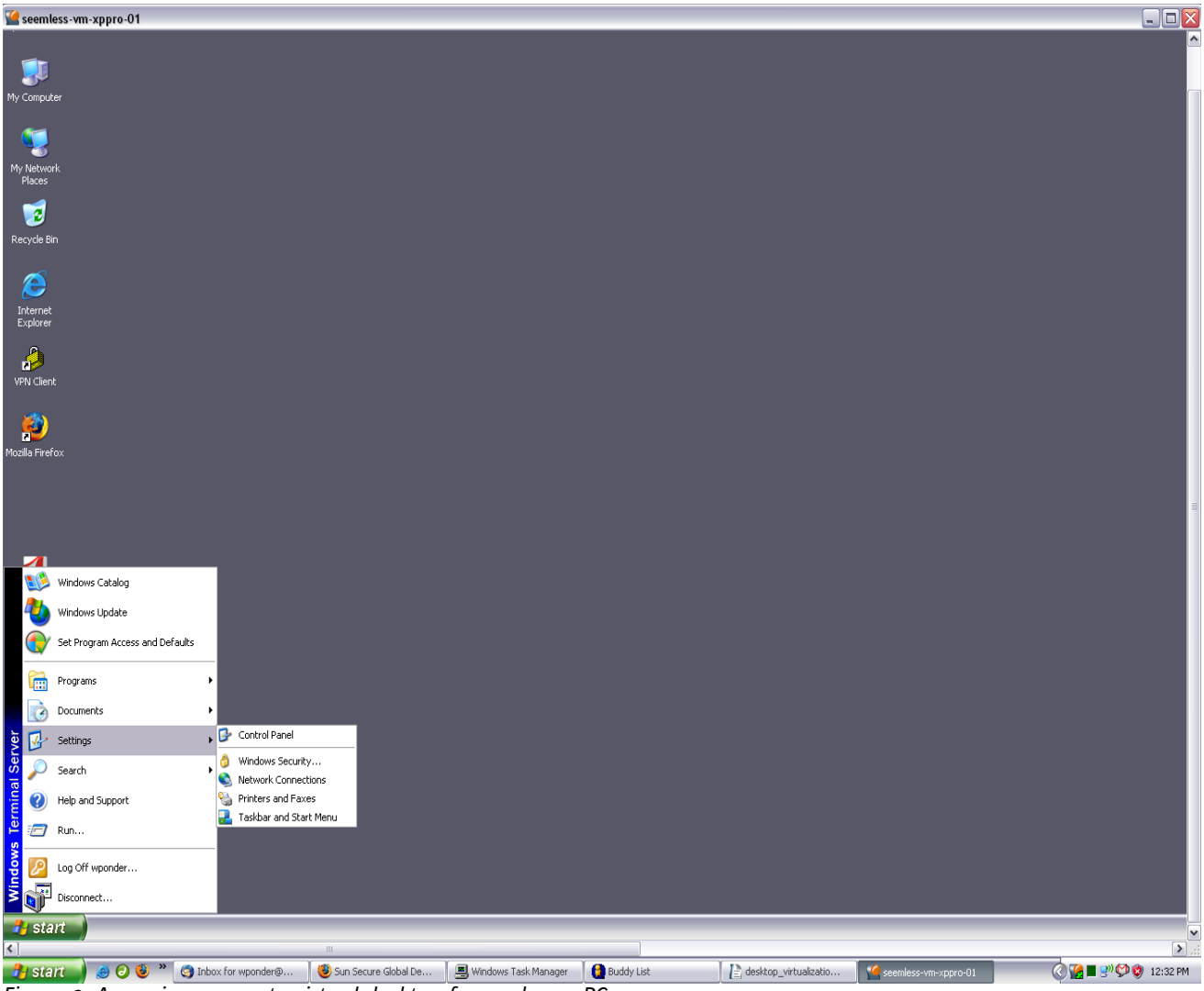

Figure 9: Accessing a remote virtual desktop from a home PC

Sizing the secure remote access component is typically based on the number of concurrent users expected per-server, while allowing for the best user experience. It's assumed the secure remote access servers will only be used for secure remote access and live within the DMZ of the corporate network. If Sun's Secure Global Desktop is also being used for application publishing. It's best practice the application publishing array is virtualized within the virtualization tier, and or, is installed on physical servers.

The following sizing can be used as a rule of thumb for remote access users accessing a full screen desktop with SSL being handled by the servers.

As a rule of thumb using a Sun Fire 4200 with two dual-core AMD Opteron processors at 2.6GHz, with 16GB of RAM. 500 concurrent user sessions per-server can be sustained.
Typically, not all users will be concurrently accessing their virtual desktops remotely at the same time. After some testing and trending of the usage patterns. A safe number of total non-concurrent users can be

determined and used for full capacity planning. An environment where users have a more flexible work environment, such as a sales office can be provisioned with higher number or total users. Because these users are coming and going and are not all concurrently using the system.

Management and Implementation Considerations

For Windows based desktop deployments, existing management tools can continue to be used for software distribution, patch management and other desktop management functions. There should be no need to immediately change these tools. Because the desktop images are moved inside the data-center and stored on a SAN, some organizations decide to backup some or all of the desktop images. The procedures are easily adapted for this environment. The introduction of the virtualization tier will require some consideration and planning regarding operational procedures such change management, admin roles for deploying, managing and controlling the virtualization servers. As well as provisioning and allocating storage for desktop images. Desktop Imaging tools in general should not be needed once existing golden images are converted to VMware templates. If required, existing PC's can be migrated to the new virtualization environment, as is, using VMware's P2V product.

The Sun Ray servers and Secure Remote access servers are easy too implement and once deployed, simple too manage. Standard imaging and deployment tools can be used to deploy standards based OS images to the servers in an automated manner. This removes the risk for human error during the configuration and implementation phases a deployment. Once the Sun Ray server software is configured, the day to day management is easy. When configured in Controlled Access Mode to deliver virtual desktop instances primarily only routine patch management is required. An configuration changes or policy settings can be configured through the web based interface included with the Sun Ray Server Software. The Secure Remote Access servers also include a web based management interface for day to day management and configuration changes. Consideration in who will manage the Sun Ray servers must be considered. In most deployments the Virtualization tier and Client Access tier are managed by the same person.

Because different technologies and software components are brought together too deliver a desktop virtualization solution. It is important the management tools and interfaces can be accessed from a single interface or console. As well as remotely in a secure manner, if needed. It is recommended that all the management tools and interfaces are accessed using Secure Global Desktop. Doing so allows you to access all the tools you need for managing all the systems and components for the Sun Desktop Virtualization solution.

Everything from SSH terminals, Microsoft Management Consoles, The Virtual Infrastructure Client, SAN management tools, network management tools etc. can all be accessed through Secure Global Desktop. Different LDAP roles and groups can and should be created to control what tools are seen and accessible by different groups such as Tier 1- 3 desktop support, Help Desk support and System Administrators.

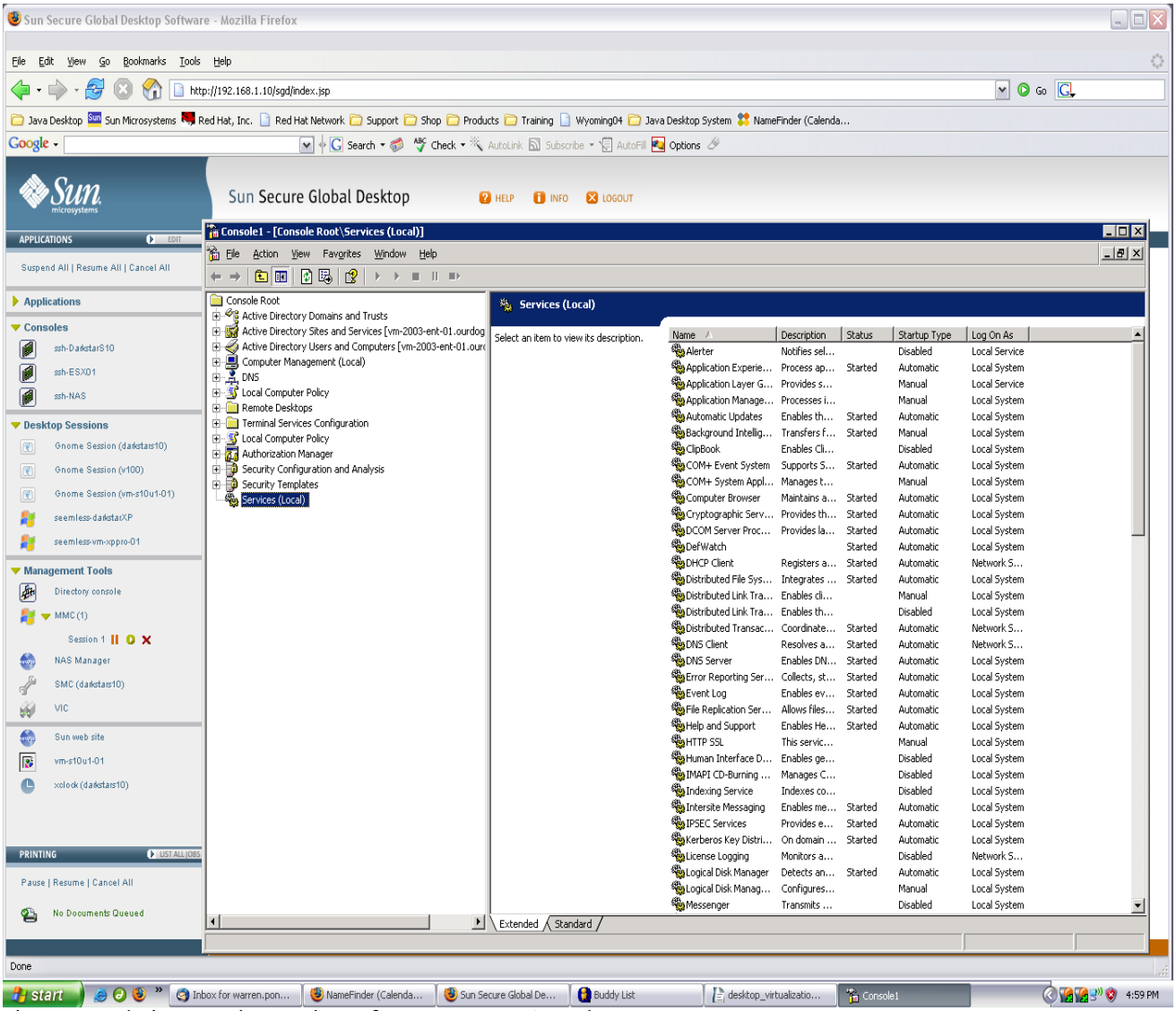

Figure 10: Admin Accessing a Microsoft Management Console

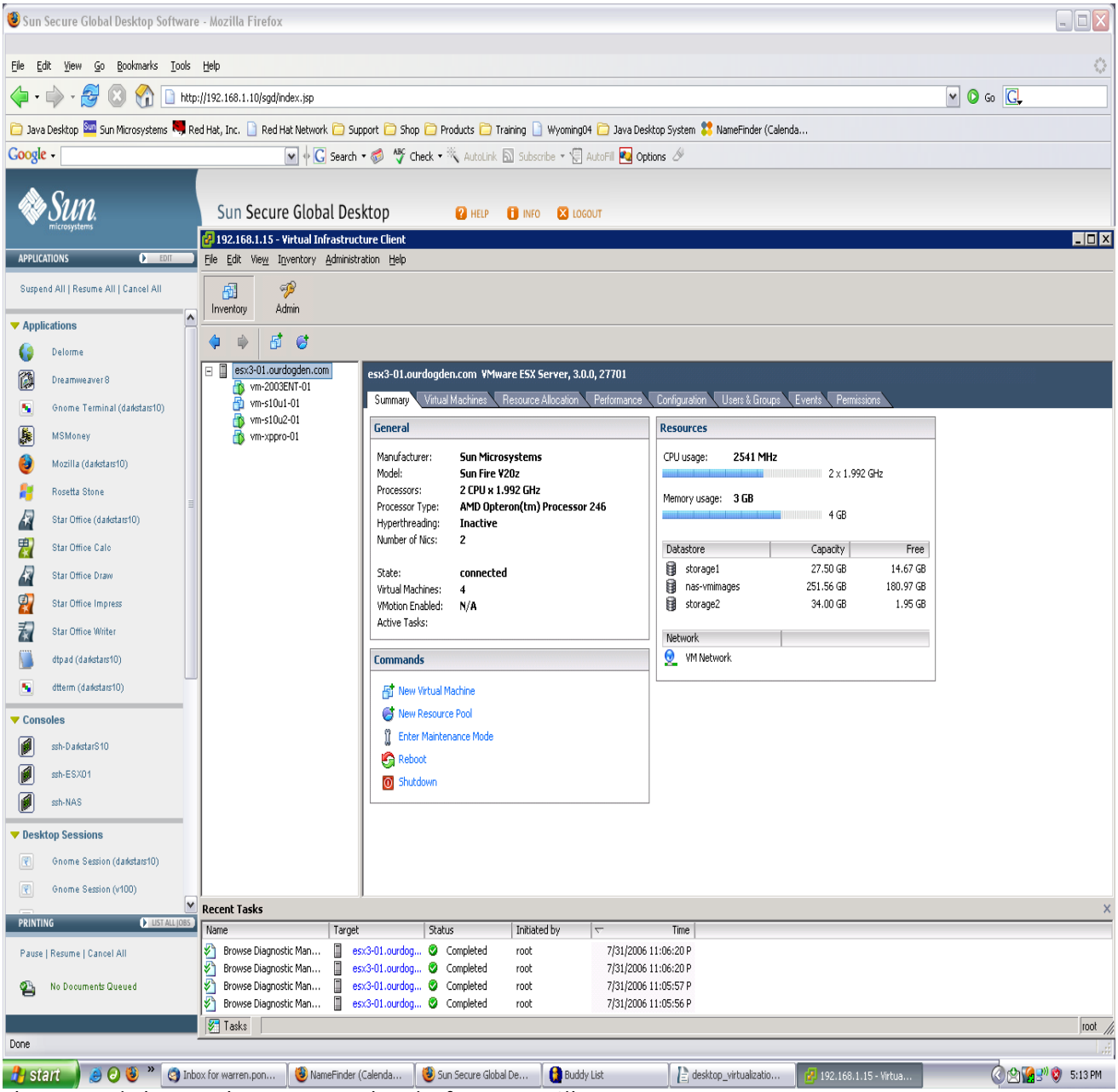

Figure 11: Admin Accessing Vmware's Virtual Infastructure Client

Conclusion

Through acquisitions and partnerships, Sun is uniquely positioned to offer an end to end desktop virtualization solution. Sun has been investing in and creating thin client technology for over six years. We currently run our own enterprise using our thin clients with over 32,000 deployed globally, within Sun. Two years ago we signed a 10 year technology development agreement with Microsoft at which time we licensed the rights to their RDP protocol. During the same time, we purchased Tarantella and their Secure Global Desktop product, a leader in application publishing and delivery through web services. We also made our largest acquisition, StorageTek™ a leading data-management company. In addition, we announced a Global OEM Alliance with VMware as a OEM and Global reseller of VMware technology. Currently, Sun is the third largest employer of VMware Certified Professionals. All this combined with the leading X64 technology and components from the Solaris enterprise system allows us to bring together the most compelling desktop virtualization solution in the market.

Important Links

- Sun Ray Software: http://www.sun.com/software/sunray/index.jsp
- Sun Ray Virtual Display Clients: http://www.sun.com/software/index.jsp?cat=Desktop&tab=3&subcat=Sun%20Ray%20Clients
- Secure Global Desktop Software: http://www.sun.com/software/products/sgd/
- VMware Infrastructure: http://www.vmware.com/products/vi/
- Sun x64 Servers: http://www.sun.com/x64/index.jsp
- Sun StorageTek Storage: http://www.sun.com/storagetek/products.jsp

Acknowledgments

This paper would not have been possible without the assistance of Ken Pepple. Thanks for providing input and mentoring during the creation of this document. I would also like to thank Michael Bartzel and Todd Dayton at VMware for their contributions and review.

About the Author

Currently, Warren Ponder is a Desktop Architect in Sun's Global Desktop Practice. In this role he works with customers to design alternative approaches to traditional desktop architectures. Warren has been with Sun for over five years. Much of this time he has focused on Thin Client computing, Windows interoperability and Linux based desktop solutions. Most recently, he has focused on, how to use Virtualization technology in solving today's desktop computing challenges.

Prior to joining Sun, Warren was an Network Architect and MCSE for several large fortune 500 companies where he helped plan, and design migration and implementation strategies. In addition, he also was responsible for standardizing the network designs and migration from legacy network platforms.