

Comprehensive Virtual Desktop Deployment with VMware and NetApp



NOVEMBER 2008

Table of Contents

Introduction.....	3
Desktop Management Challenge.....	3
Introducing VMware® View	4
How VMware® View Addresses Desktop Management Challenges.....	5
• Streamlined and Simplified Desktop Management	5
• Complete Desktop Environments for a Familiar User Experience.....	5
• Continuous Availability and Reliability.....	5
• Improved Security and Compliance	6
• Lower Total Cost of Ownership (TCO).....	6
Storage Challenges Introduced with Desktop Virtualization	6
• Increased Availability.....	6
• Storage Costs	7
• Storage Flexibility	7
• Desktop Security and Compliance	7
Introducing NetApp Storage for VMware® View.....	8
Why NetApp Storage for VMware® View?.....	8
• Provide Continuous User Access to Virtual Desktops.....	8
• Increased Agility for VMware® View.....	8
• Greater Storage Efficiency.....	9
• Desktop Security and Compliance.....	9
Conclusion	9
Further Reading References.....	10

Introduction

Over the last few years, enterprises have realized the benefits of server virtualization in their data center through consolidation and business continuity efforts. It has delivered in simplifying day-to-day administration and reducing management tasks and operating costs, while maintaining reliability and availability. Given the success of virtualization in these areas and the growing challenge to manage desktops, companies are beginning to look for ways to get similar benefits by applying the same technology to the desktop environment.

Desktop Management Challenge

Managing traditional enterprise desktops today has become increasingly difficult and costly. Some of the challenges that desktop managers face today include:

- Cost for support and maintenance
- Increasing number of remote and mobile users
- Greater use of employee owned computers
- Application version upgrade patch management
- Greater focus on the quality of the user experience
- An ever-increasing requirement for hardware and software availability
- Continuing performance and stability issues
- Security and compliance adherence
- Desktop hardware refresh
- Operating system upgrades.

Typically in a desktop environment, IT staff need to be at the computer to troubleshoot and fix problems when they occur. If the problem is with a computer used by a worker in a remote site or who is mobile, the user might have to wait for someone to come to the site or send the computer to the main office for repair.

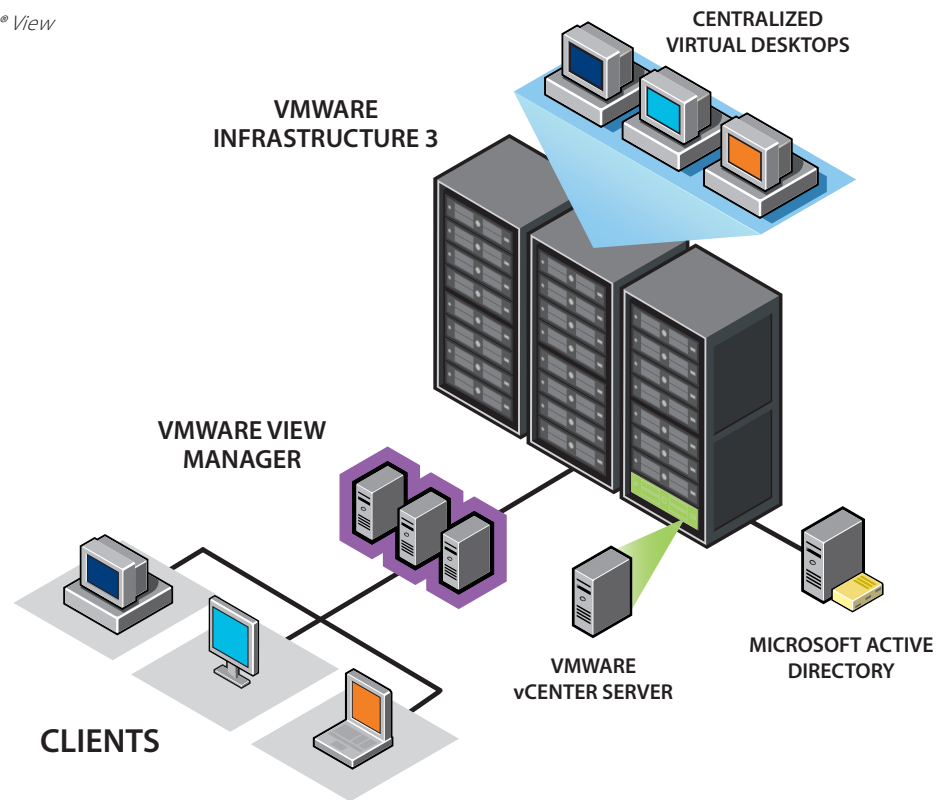
In any of these scenarios, IT staff spends time getting to the PC and workers lose productivity sitting in front of a faulty PC or waiting for their PC to be fixed. If a PC is on site, it can take an IT staffer anywhere from a couple of hours to a day to correct a problem. If the PC is in a small office with no IT staff, or is used by a remote user who works from home, the user often needs to bring in or send the PC to the office, which can result in the user being unproductive for an extended period of time.

Complicating matters further, applications on today's desktops may need updates and new patches installed on a regular basis to protect systems from new exploits. In many cases, software updates and patch installations can be automated. However, patch installations frequently occur during non-work hours when users turn their PCs off. Users may also need help with the process, again taking up IT staff time. Worse, some users may disregard instructions and not install the updates or patches. This can result in a desktop PC being noncompliant and vulnerable to being infected with malicious software.

Beyond dealing with security updates and patches, the job of managing desktops is made more difficult as users increasingly download and install personal software applications. Having these programs on distributed physical desktops can cause a number of problems, ranging from malware applications that interfere with other applications required to conduct business, to IT not knowing that these programs are installed on a PC in a remote location, and thus complicating any troubleshooting efforts. Another issue is making sure that the installed software applications are properly licensed.

Outside of the software issues, desktop management increasingly involves data protection. For instance, many companies have extensive backup, recovery, and disaster preparedness plans in place to protect data on servers and dedicated storage devices. However, they do not routinely back up the data and applications on desktops.

Figure 1: VMware® View



Introducing VMware® View

VMware offers an end-to-end solution called VMware® View, the next generation of VMware VDI, that allows organizations to provide corporate end users with access to virtual desktop machines that are hosted in a central data center. This solution enables organizations to leverage the power of VMware® Infrastructure 3 along with an enterprise-class connection broker to improve manageability and control while delivering a familiar desktop experience to end users.

VMware® View is an end-to-end solution for any company, large or small. A typical VMware® View environment encompasses the following components:

- **VMware Infrastructure 3:** The VMware® View solution leverages proven VMware Infrastructure 3 software to consolidate desktop environments onto servers in the data center.
- **VMware® View Manager:** Administrators run an enterprise desktop management server that connects remote clients to centralized desktops and manages virtual

desktop environments. VMware® View Manager is an enterprise-class desktop management server that securely connects users to virtual desktops in the data center and provides an easy to use Web-based interface to manage virtual desktop infrastructure (View) environments.

- **Clients:** Users can log into their centralized virtual desktop images from a Web browser or by using the VMware® View Client on a thick or thin client. For a complete list of supported thin client devices, visit <http://www.vmware.com/resources/techresources/1053>.

- Additionally, Microsoft® Active Directory® is required to run the VMware View Manager software.

VMware® View provides users with desktop business continuity, high availability, and disaster recovery capabilities that until now were available only for mission-critical server applications. Individual end users benefit from the ability to access their familiar corporate desktop from any location.

How VMware® View Addresses Desktop Management Challenges

VMware customers are transforming the way they manage their desktops, replacing traditional PCs with centralized virtual desktops that can be more effectively managed and controlled. VMware® View provides an array of benefits that address the common concerns of managing traditional desktop computers.

Streamlined and Simplified Desktop Management

Through VMware® View, the administrator can configure, deploy, and maintain hardware-independent desktop virtual machines from central locations for simpler management and efficient desktop provisioning. The time it takes to deploy a desktop is typically reduced to minutes, optimizing the value of IT resources and increasing end-user productivity. VMware® View is a flexible and intuitive desktop management server that enables IT administrators to quickly provision and tightly control user access. Desktops are centrally managed in a secure data center so IT staff can more easily apply patches such as virus scanning software and the other standard security policies of your company. Administrators can also lock down access to various network drives or shut users off instantly when they leave the company. VMware desktop virtualization technology lets IT staff leverage the “sandbox” capabilities of a virtual machine that is fully contained, isolated from the host operating system, and designed by desktop administrators to be a good citizen of the desktop community.

Administrators can modify memory, process, and disc resources on a virtual machine with very little interruption to a user's workday. Maximum user perception can be managed and maintained with an ease and convenience impossible with physical desktop machines.

VMware® View delivers consistent and scalable IT services that address issues remote sites face such as management complexity, inadequate infrastructure, and lack of administrative resources.

Streamlined and Simplified Desktop Management: Administrators can more easily provision, manage, and maintain desktops because they are running in the data center.

Complete Desktop Environments for a Familiar User Experience: End users get a complete, unmodified virtual desktop that behaves like a normal desktop computer.

Continuous Availability and Reliability: End users get flexible access to a personalized virtual desktop that behaves like their normal PC. Unplanned downtime is minimized and recovery is accelerated.

Improved Security and Compliance: Confidential data resides securely in centrally managed data centers.

Lower Total Cost of Ownership (TCO): By reducing desktop maintenance and support costs and extending the useful life of PCs, VMware® View delivers lower TCO.

Complete Desktop Environments for a Familiar User Experience

With VMware® View, end users get a complete, unmodified virtual desktop that behaves like a normal desktop computer. There is no change to the applications or desktop environment, no application sharing, and no retraining required. Administrators can provide end users the ability to install applications, access local devices such as printers, USB devices, and other peripherals, the ability to customize their desktop environment to suit their needs and access from anywhere, or provision desktops that are more restricted and revert to a known consistent state upon log-off. Users also get better support with VMware® View because Help Desk technicians can perform tasks in the data center that would normally require an in-person visit.

Continuous Availability and Reliability

VMware® View extends the benefits of VMware Infrastructure 3 to the desktop, so customers can benefit from reliability, data protection, and disaster recovery capabilities that have traditionally been available only for server applications. Because the desktop virtual machine is managed in the same way that other virtual workloads are managed in the data center, high availability and disaster recovery can be built in to the new design from the beginning. In many instances, servers carry 24 x 7 support, so desktops residing there benefit as a result. End users can leverage shared storage to back up their desktop data. Automated failover helps to maintain high availability for virtual desktops, while site-wide recovery

mechanisms deliver rapid restoration of service after an unplanned outage.

Once desktops are encapsulated as virtual machines, they are essentially files located on central shared storage. These files can be replicated to another location and powered on inside another set of virtual infrastructure servers in another location. This process is especially easy compared to the “zero backup” desktop scenario often seen, or the “boot and pray” disaster recovery scenarios that many environments face today.

Most disaster recovery plans address data retention and server replication, but do not have a plan for the desktops. Assuming access to a second data center, and additional servers to host virtualized desktops with storage, VMware® View (by default) includes the capability to give desktops the same level of disaster recovery that servers can have under virtualization. Much of the current interest in the virtual desktop concept is specific to high availability and disaster recovery options utilizing snapshot technology for the virtual machine, allowing live, point-of-process disk and memory roll back points. A “snapshot” or “moment in time” image of the virtual machine can be saved and subsequently restored in minutes.

Improved Security and Compliance

With VMware® View, controlling access to confidential data is easier because all virtual desktops reside in a central location. This enables stronger policy enforcement and tighter data security. Tools available today can make a virtual machine available to the user only if patch requirements are met. Integration with RSA SecurID® enables support for two-factor authentication, while strong network encryption protects data in transit. These features can help reduce the risk of data leakage and malicious code intrusion while also helping to ease regulatory compliance burdens.

Vulnerabilities inherent in the distributed desktop environment (USB, DVD, CDR drives) can be reduced or eliminated when the virtual machine is moved into the data center. Data center security is higher than that of the user PC as well. With that assurance, corporate standards and compliance and regulatory requirements are easily met and maintained.

Lower Total Cost of Ownership

Organizations use VMware® View to replace traditional PCs with virtual desktops that run on servers in the data center. Desktop management costs decline when user hardware is simplified and the technical requirement for that device is reduced.

This leads to better control and management of desktops. The approach helps to reduce the total cost of ownership for desktop infrastructure, extends the lifecycle of hardware, and helps IT staff respond more quickly to business needs.

Storage Challenges Introduced with Desktop Virtualization

Similar to server virtualization, desktop virtualization poses unique challenges to storage systems. Storage is an essential component of a virtual desktop environment and a critical factor in determining the cost, overall flexibility, and availability of the final solution. The key challenges related to storage are:

- Increased availability requirements
- Increased storage costs
- Limited storage flexibility
- Data protection and compliance

Increased Availability

When enterprises centralize desktop storage, thousands of users depend on the virtual desktop infrastructure for their daily computing needs. A system outage can affect user productivity across the organization. VMware provides robust tools to maintain availability. Those same capabilities are required at the storage layer for high availability.

Storage can affect availability in a number of ways. The key areas include reduced availability through slower system performance, poor resiliency against component failures, long restore times for missing or corrupted data, and ineffective storage failover capability after a site or regional outage.

Regarding system performance, a virtual desktop environment presents unique storage workloads that can slow performance at critical times. For example, the simultaneous log-on of hundreds of users at 8 a.m. or the reboot of thousands of virtual machines after an OS patch can overwhelm a storage system and slow user access. Traditional backup applications can also slow overall performance during the backup process by using up host CPU cycles.

Data loss due to user error or corruption is a common issue affecting availability. This data loss can be caused by a virtual machine (VM) corrupted by a virus, a user who accidentally deletes a file, or the need to roll back virtual desktops from an unstable patch. These restore operations must be fast to minimize loss of productivity and disruption to the users.

In the case of a more significant failure, such as in a data center or even a region, the storage system must be able to fail over to another functioning location that has current copies of the data. This requires data replication solutions that are cost effective to avoid doubling storage costs, and that integrate with VMware technology to automate the failover sequence.

Storage Costs

The cost of networked storage is one of the biggest hurdles to implementing a virtual desktop environment. The cost of migrating data currently stored on inexpensive PC drives to data center class storage is often overlooked and can stall a virtual desktop project. The factors leading to the increased storage costs are many. The obvious one is the higher acquisition costs. Data center storage can be as much as five times more expensive per GB than PC storage.

Once the data is migrated, it is often stored inefficiently in the central storage system. For example, the same operating system and office productivity applications are stored redundantly in each individual virtual machine. In addition, files such as documents, presentations, and spreadsheets are frequently shared between users and stored locally, creating additional data redundancy for the storage in the datacenter.

Finally, most storage systems don't have the ability to load balance capacity resources in the way that VMware is able to load balance CPU resources. Excess capacity in a storage volume cannot be used for other storage needs. This limits storage utilization levels and increases storage costs.

Storage Flexibility

Moving to a virtual desktop environment makes it easier to provision, scale, and adapt your desktop environments, but to realize the full benefits of desktop virtualization; the underlying storage requires the same level of flexibility. For example, waiting hours or days to provision the storage required for a virtual machine limits the overall effectiveness of the virtual desktop infrastructure. Compound this with the need to provision virtual desktops on a much larger scale—often hundreds of desktops at a time—and the importance of provisioning storage quickly becomes apparent.

VMware® View also places multiple requirements on storage systems. For example, a common architecture for View uses SAN connections to support the virtual machines running on VMware and uses NAS (usually CIFS) to provide the centralized storage for end-user data. This can require multiple storage systems, increasing the cost and complexity of the solution.

Desktop Security and Compliance

Storage plays a central role in securing and protecting the virtual desktop data. For example, many corporate policies require regular backups of user and desktop data. Although centralizing the data on virtual desktop infrastructure makes accessing the data much easier, traditional backups may not scale in virtual environments, and new backup strategies must be developed.

Desktop data often has requirements for security and data retention set by regulations, especially in industries such as finance and healthcare. These regulations may require data encryption to control data accessibility or require long-term, unalterable data archiving to support periodic audits. These additional items can add significantly to storage costs and overall complexity.

Introducing NetApp Storage for VMware® View

NetApp provides a combination of storage hardware, data management software, and specialized services that enable customers deploying VMware virtual desktop environments to use at least 50% less storage, provision thousands of virtual desktops in minutes, deliver continuous availability, and maintain compliant storage of end-user data.

Figure 2: NetApp Storage



Why NetApp Storage for VMware® View?

Storage for a comprehensive VMware virtualized desktop infrastructure begins with NetApp (Figure 2). You can achieve continuous availability for your desktop environment with highly available storage systems that provide best-in-class data protection. At the same time, you can maximize utilization and lower total cost of ownership by using NetApp® deduplication and thin-provisioning technologies. NetApp also helps you consolidate your storage by using the industry's broadest unified storage architecture. With NetApp you get the flexibility, high availability, and cost effectiveness you need to grow your virtual desktop environment.

Provide Continuous User Access to Virtual Desktops

NetApp helps maintain continuous availability of virtual desktops by optimizing View performance, providing highly resilient storage, enabling rapid data recovery, and delivering advanced disaster recovery capabilities.

To optimize performance in a virtual desktop environment, NetApp includes the Performance Acceleration Module (PAM) as part of a NetApp solution.

This intelligent read cache improves virtual desktop system performance by 70%¹. The NetApp PAM card improves the random read performance by caching shared blocks on high-performance solid state memory, which leads to lower read latency and improved overall I/O throughput. The advantages provided by the NetApp PAM card are enhanced when combined with shared block technologies such as NetApp deduplication or FlexClone® technology. These block-sharing technologies result in a smaller memory footprint for the data, allowing more desktops to reside in high-speed cache for even better virtual desktop performance. The PAM card is especially effective in addressing the simultaneous system boot, or "boot storm," allowing a thousand desktops to boot in under 10 minutes.

NetApp provides a highly resilient storage system that transparently recovers from common component failures. A field-measured 99.999% uptime is proof of the reliability of NetApp storage systems. A standard part of NetApp resiliency is RAID-DP®, a patented technology that provides double disk failure protection without the performance trade-off of traditional RAID 6 or the capacity penalty of RAID 10.

To protect against data loss and system or site failure, NetApp provides rapid recovery and advanced replication and failover technologies. Virtual desktops or user data can be recovered instantly from local snapshot copies.

End users can even recover their own data directly from backup. And in case of an unplanned system or site outage, you can fail over to the DR site in minutes. NetApp replication technology gives you virtually unlimited configuration options, so that you deploy the most cost-effective solution to protect all of your virtual desktop data.

Increased Agility for Virtual Desktop Infrastructure

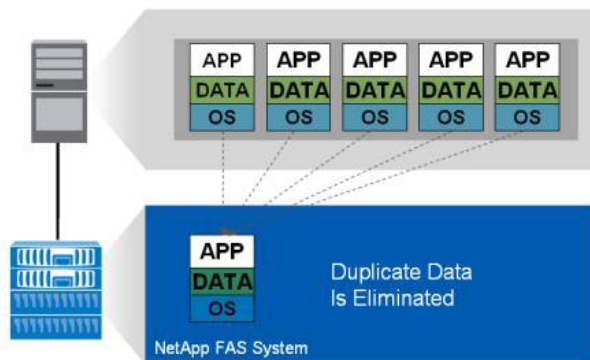
To meet the large-scale provisioning needs of a virtual desktop environment, NetApp enables you to provision thousands of virtual desktops in minutes by using nearly instantaneous, low-overhead storage cloning. Traditional solutions require each virtual desktop clone to be copied to another part of storage, taking both time and storage capacity to move the data. NetApp FlexClone technology enables instantaneous clone copies of a golden desktop image that take no additional storage capacity. This eliminates the storage provisioning bottleneck associated with most storage systems.

To meet the different storage needs of a View deployment, NetApp enables you to support both the SAN and NAS aspects of a virtual desktop environment on the same storage system with NetApp multiprotocol capabilities. In addition, the same system can be used for regulated or sensitive data that needs to be retained in tamperproof (WORM) storage to meet corporate or regulatory requirements.

Greater Storage Efficiency

NetApp can reduce the storage required for virtual desktops by as much as 80%ⁱⁱ through a combination of advanced technologies. Using NetApp's deduplication technology, you can reduce storage needs by eliminating redundant data stored across virtual desktops, user directories, and backup and DR copies (Figure 3). Deduplication can eliminate redundant data in both virtual machines and end-user storage. And when combined with the NetApp Performance Acceleration Module, deduplication actually increases overall performance.

Figure 3: Eliminating Redundant Data with NetApp Deduplication:



In addition, NetApp thin provisioning can increase average storage use above 60%ⁱⁱⁱ which is twice as high as traditional storage use. You also get the benefits of RAID 10 protection at half the disk capacity with NetApp RAID-DP. Together, these and other NetApp technologies reduce the storage costs associated with a virtual desktop deployment.

Desktop Security and Compliance

NetApp provides unique capabilities to meet both corporate policy and regulatory compliance

requirements for end-user data. To simplify and enhance comprehensive backup of end-user data, NetApp Snapshot™ technology provides a centralized backup functionality that is performed directly on the storage array. This is a more effective backup methodology because it imposes no load on the virtual desktop servers and avoids the need to create a separate backup infrastructure. Snapshot backups are also instantaneous, allowing more frequent backups throughout the day, thereby reducing potential data loss.

Snapshot backups assist in meeting corporate compliance requirements by keeping a daily history of every desktop for months or even years. Backup data is archived efficiently on inexpensive disk at a cost comparable to tape. This is made possible by deduplicating the redundant data in backups and archiving the information on low- cost disk systems.

In addition, the backup data can be archived to meet regulatory rules that require the data to be stored with a method that prevents changes or deletions. Finally, NetApp provides real-time encryption for data residing on disk to secure end-user data without compromising performance.

Conclusion

Organizations today must support a wide variety of users—local, mobile, and remote users. These users normally access sensitive information assets on a range of equipment, including desktop, laptops, and unmanaged personal computers, making it difficult to support end users in a consistent and secure manner. VMware and NetApp provide the critical components of a comprehensive virtual desktop deployment. VMware® View addresses the desktop management challenges by tightening the control of corporate assets and simplifying desktop management. This approach extends powerful VMware Infrastructure 3 capabilities such as business continuity and disaster recovery to the desktop; streamlines desktop management to reduce operations costs and increase control; and delivers complete desktop environments with greater application compatibility. NetApp provides unique capabilities that address the common storage challenges associated with virtual desktop environments, enabling organizations to realize the full potential of your VMware® View solution.

Further Reading References:

NetApp and VDI Best Practices: <http://media.netapp.com/documents/tr-3705.pdf>

Solutions for VMware and Customer Stories: <http://www.netapp.com/us/solutions/infrastructure/virtualization/vmware.html>

i NetApp Technical Report: NetApp and VMware VDI Best Practices – Oct 2008

ii NetApp Case Study – Virginia Credit Union Saves 80% Disk Utilization with NetApp – March 2008

iii NetApp Case Study: BBM Canada Protects Critical Real Time Ratings Data with NetApp – April 2008



VMware, Inc. 3401 Hillview Ave Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2007 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,961,806, 6,961,941, 6,880,022, 6,397,242, 6,496,847, 6,704,925, 6,496,847, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,944,699, 7,069,413, 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481, 7,149,843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,268,683, 7,275,136, 7,277,998, 7,277,999, 7,278,030, 7,281,102, 7,290,253; patents pending. VMware, the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

© 2008 NetApp and VMware. All rights reserved. Specifications subject to change without notice. NetApp, the NetApp logo, Go further, faster, FlexClone, RAID-DP, and Snapshot are trademarks or registered trademarks of NetApp, Inc. VMware is a registered trademark of VMware, Inc. Microsoft, Active Directory, and Windows are registered trademarks of Microsoft Corporation. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

