Enterprise Virtual Desktop Infrastructure: Design for Performance and Reliability

Abstract

This document, intended for IT architects deploying virtual desktops, explains how you can use products from VMware, Cisco, and EMC to create an end-to-end solution for VMware View 3.0. Planned correctly, the complete virtual desktop Infrastructure (VDI) provides a PC-like experience, even in bandwidth-constrained environments.

This document discusses central principles of design and architecture, including:

- Network resilience and WAN optimization
- Storage performance and sizing considerations
- Recommended deployment options for VMware View
- Interaction and dependencies between VMware View and both the storage and network infrastructure

The document concludes with a list of resources for more detailed information.

Challenge: The Desktop Dilemma

"Desktop computing" has become a misnomer. Today's users are just as likely to need application and data access from home PCs or mobile devices as they are from their office desktops. Rather than a place, the desktop has become an end-user environment that can be accessed anytime, anywhere.

The dilemma for IT departments is how to meet business needs without compromising security, control, manageability, or compliance.

The Solution: Virtualization

VMware View desktop virtualization technology meets user and IT needs, providing compelling advantages compared to traditional desktops and terminal services.

With the traditional monolithic desktop, applications, the OS, and user data are all tied to a specific piece of hardware. Virtualization breaks the physical bonds between information and hardware. IT staff can change, update, and deploy each component independently, increasing business agility and improving response time, and end users can enjoy the familiar desktop experience from almost any convenient wired or wireless device—in the office, at home, or on the road.

Unlike terminal services, VMware virtualization technology supports all applications that can be deployed on physical desktops, not just a subset. Users get a complete, standardized, and fully customizable desktop computing environment: a virtual machine. Each virtual machine is completely isolated from other virtual machines for security, and IT administrators can provision and manage the OS and application software just as they would with a traditional PC.

VMware View

A global leader in both desktop and server virtualization, VMware blends the best of its desktop and server virtualization technologies In VMware View. The next-generation VDI, VMware View builds on earlier solutions to:

- Support both server- and client-hosted virtual desktops
- Provide unified access to centralized resources
- Operate with or without a network connection

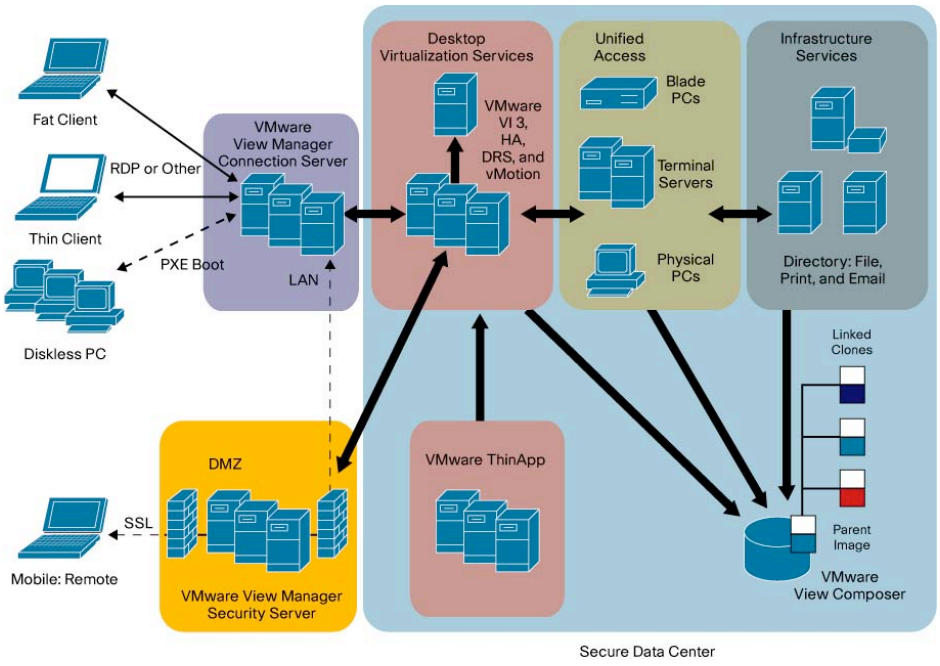
Using VMware View, IT departments can manage hardware, OS, and applications independently of each other, within a unified framework.

VMware View Benefits Summary

- Lower costs: VMware View reduces overall costs of desktop computing by up to 45 percent. Centralized management and administration decrease operational costs, and consolidating branch IT infrastructure into the data center reduces capital costs.
- Security: You can maintain all data within the data center, which helps reduce the risk of data leakage. Integrated user authentication and built-in SSL encryption provide secure tunneling to virtual desktops from unmanaged devices, protecting data in transit.
- Simplified management and control: VMware View Manager lets you centrally manage all desktops in the data center and quickly provision desktops for new users, departments, or offices. For the fastest provisioning and updating, create instant clones from a central image and maintain dynamic pools of desktops.
- Business agility: Accommodate new business needs by quickly adding new desktop users or groups of users.
- Mobility: Users can access their applications and data from any location and any device, with a consistent experience.
- Business continuity and disaster recovery: VMware View is built on industry-leading VMware Virtual Infrastructure and can automate desktop backup and recovery as a business process in the data center.
- Lower carbon footprint and energy consumption: When used in conjunction with thin-client devices, which typically use 10 percent of the power of a traditional PC, VMware View helps reduce energy costs and can decrease the carbon footprint by up to 80 percent (source: Butler Group, “Infrastructure Virtualization,” September 2007).

Figure 1 shows a typical VMware View deployment, including components from VMware and other vendors.

Figure 1. High-Level VMware View Architecture



The components of a VMware View architecture include:

- VMware View Manager virtual desktop management services: An access layer component, VMware View Manager directs authorized users to their virtual desktops. It can also act as a common access and control point for other services available to desktop users, such as Microsoft Terminal Services, blade PCs, and desktop PCs.
- VMware View Manager connection servers: Connection servers provide user authentication and direct incoming remote desktop requests to the appropriate virtual desktop. For load balancing and higher availability, you can install replicas that reference the first connection server.
- VMware View Manager security servers: Connection servers provide connections from within the company network, behind the firewall. Security servers provide a subset of functions to allow secure access to virtual desktops from the Internet. Each security server acts as a proxy host for connections inside the trusted network. This design provides an additional layer of security by shielding the connection server from the public-facing Internet and forcing all unprotected session requests through the security servers. This approach helps ensure that only authenticated users can connect to the internal network from the Internet.
- VMware View Composer: A new component of the VMware View solution, VMware View Composer uses VMware Linked Clone technology to rapidly create desktop images that share virtual disks with a master image. This approach conserves disk space and streamlines management. User data and settings are segmented from the desktop image so that you can administer them independently.
- VMware ThinApp: The application virtualization software, VMware ThinApp decouples applications from operating systems by isolating and encapsulating them into executable (.exe) or Windows installer (.msi) files. The advantages of decoupling applications from the OS are:
  - Multiple versions of applications can run on a single operating system without conflict
  - The same version of an application can run on multiple operating systems without modification.
  - Application upgrades and patches take less time. Virtual desktops need less storage space because VMware ThinApp can stream large applications from a shared network drive.
- VMware Infrastructure 3: VMware View 3 is built on VMware Infrastructure 3, which is used for hosting virtualized desktop images. Integrating the desktop infrastructure with VMware Infrastructure 3 provides the following benefits:
  - Simplifies management by providing a single management interface
  - Increases availability by grouping the servers that host virtual desktops in a redundant configuration
  - Consolidates backup for desktop virtual machines
  - Provides automated failover and recovery to keep desktops operating without interruption
  - Improves performance through dynamic load balancing of desktop computing resources

How VMware View Is Used in the Enterprise

Organizations use VMware View to meet some or all of the following business goals:

- Centralize desktop management and control: VMware View saves time, money, and resources and increases agility by allowing you to centrally manage and maintain desktops. Workforce productivity and mobility increase because users can access their personalized desktop environment, called myView, from any location and any device.
- Enable desktop backup and disaster recovery: Organizations typically protect their servers with automated backup, data protection, and disaster recovery. VMware View extends the same protection to the desktop. You can back up and restore virtual desktops remotely, using VMware View, saving the time and cost of onsite visits.
- Increase information security: VMware View enables secure, cost-effective delivery of desktop services and applications to users in remote locations, including branch offices, call centers, government offices, healthcare facilities, and schools. Security features include:
  - Physical security: You can tightly control access to confidential data and information because all virtual desktops reside in a central location.
  - Encryption: VMware View uses strong network encryption to protect data in transit.
  - Authentication: Integration with RSA SecurID supports two-factor authentication.

These features can simplify regulatory compliance and help reduce the risk of data leakage and malware infections.

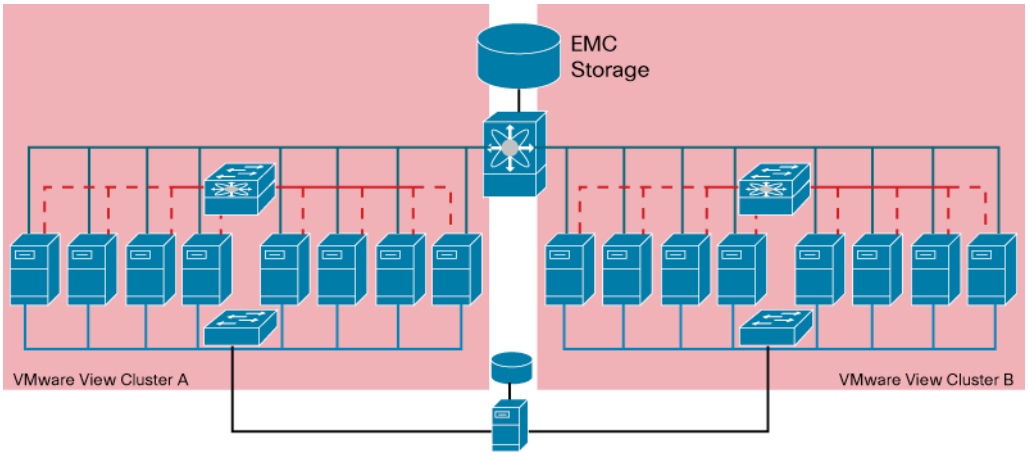
VMware View Reference Architectures

IT architects, consultants, and network administrators can save time and reduce risk by using VMware View reference architectures during the early phases of planning, design, and deployment. Built and validated by VMware and supporting partners, the reference architectures are standard, repeatable, scalable designs that you can adapt to your environment and requirements (Figure 2). They address common use cases, such as:

- Enterprise desktop replacement
- Remote access
- Business process outsourcing
- Disaster recovery

The reference architectures use common components and a standardized design to reduce implementation and management costs. All the infrastructure components used to validate the reference architecture are interchangeable. That means you can use components from your preferred vendor to add features that enhance the value of the solution for your organization.

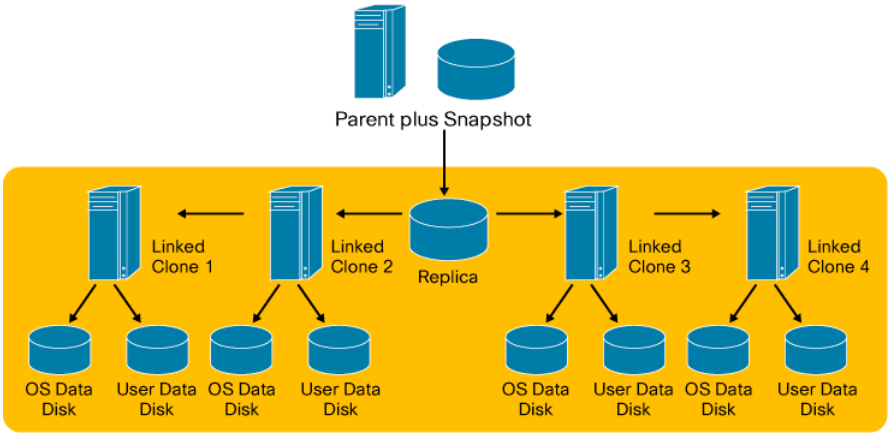
Figure 2. Reference Architecture for 1000 Virtual Desktop Users



Following are some of the main guidelines from the VMware View reference architectures:

- Client access devices: The client access device layer consists of some or all of the following: physical PCs, repurposed PCs, thin-client devices, and mobile devices. You can standardize on one type of client access device or a mix. For example, an organization might want to replace fully depreciated assets with thin clients right away and convert other assets to unmanaged endpoints. You can either use a Linux-based solution to convert the assets to clients booted from a preboot execution environment (PXE) or tightly lock down the currently installed Windows OS.
- Access infrastructure: The access infrastructure provides connectivity between client access devices and the infrastructure that hosts the virtual desktop sessions. The access infrastructure includes components that broker user connection requests to entitled desktops. An undersized access infrastructure can result in poor performance and an unsatisfactory user experience.
- Remote Desktop Protocol (RDP) considerations: Microsoft RDP is the most commonly used display protocol to access a VMware View 3 environment. The VMware View Windows XP Deployment Guide provides recommendations to optimize available network bandwidth and the user experience.
- VMware View load balancing: Load balancing optimizes performance, improves serviceability and availability, and increases scalability. Popular approaches to load balancing are round-robin Domain Name System (DNS) and network load balancers. VMware recommends a network load balancer because it increases the scalability and resiliency of VMware solutions.
- Desktop and pool management: You can create individual desktops as well as pools of virtual machine desktops, PCs, and Microsoft Terminal Services sessions.
- Desktop persistence: You can specify whether the desktops in pools are persistent or nonpersistent. A persistent desktop remains assigned to a specific user until an administrator makes a change. This choice is best for users who want to install their own applications and store local data. A nonpersistent desktop is allocated to a user only until the user logs off. At that point it becomes available for the next user. This choice is best in organizations that need a clean machine for each user session or that discourage desktop customization.
- Security: When users access virtual desktops from a remote PC or thin client, they get direct access to data and features as if the application were loaded on their local system. Integrating two-factor authentication from RSA helps ensure that users are who they claim to be, reducing the risk of improper access and distribution of sensitive information.
- Virtual disk management. With VMware View Composer, you can rapidly clone desktop images from a parent image (Figure 3). The use of linked clones reduces storage requirements. It also reduces the time needed to apply a patch or update because you apply the change just once, to the parent image, and indicate that it should also apply to all linked clones. If a problem occurs, you can revert to a snapshot of the parent image taken before the patch or update was applied.

Figure 3. Parent Image with Linked Clones



- Profile management. A single user might be entitled to access multiple back-ends, such as VMware View virtual desktops, Microsoft Terminal Services, blade PCs, and ordinary PCs. The easiest way to accomplish this is by using a robust profile management solution, such as RTO Virtual Profiles or AppSense, instead of or in conjunction with a VMware View Composer user data disk. Profile management solutions also make logging on and off faster and help ensure profile integrity.

Cisco Network Architecture

Network Architecture Considerations in a VDI Environment

The network architecture affects the user experience in a VMware View environment. To deliver the optimal user experience, consider the following aspects of the architecture:

- RDP performance: Users access the VMware View desktop remotely, so RDP performance over the WAN affects the user experience.
- Properly planned bandwidth in the data center: VDI solutions increase bandwidth requirements compared to traditional desktop environments. You need enough capacity for clients to access desktops and for the desktops to access applications. Also factor in the aggregation of multiple desktops hosted on a single server.
- CPU overhead for RDP session encryption: RDP session encryption using SSL increases CPU overhead. This increased overhead reduces the number of VMware View desktops per server, thereby increasing the number of servers required to host VMware View desktops.
- High availability: Availability becomes increasingly critical in a VDI because outages affect multiple remote users.
- Traffic segmentation: Different traffic types—VMware View desktops, VMkernel, and VMotion—must be segmented for security and traffic management.
- Storage performance: The SAN fabric must be able to handle unpredictable traffic patterns generated by the dynamic movement of virtual machines across physical servers.
- Resilience: Because multiple desktops are centrally hosted on fewer physical servers, a failure will affect many, or all, desktops.

The Cisco® VMware View Network Solution addresses these challenges.

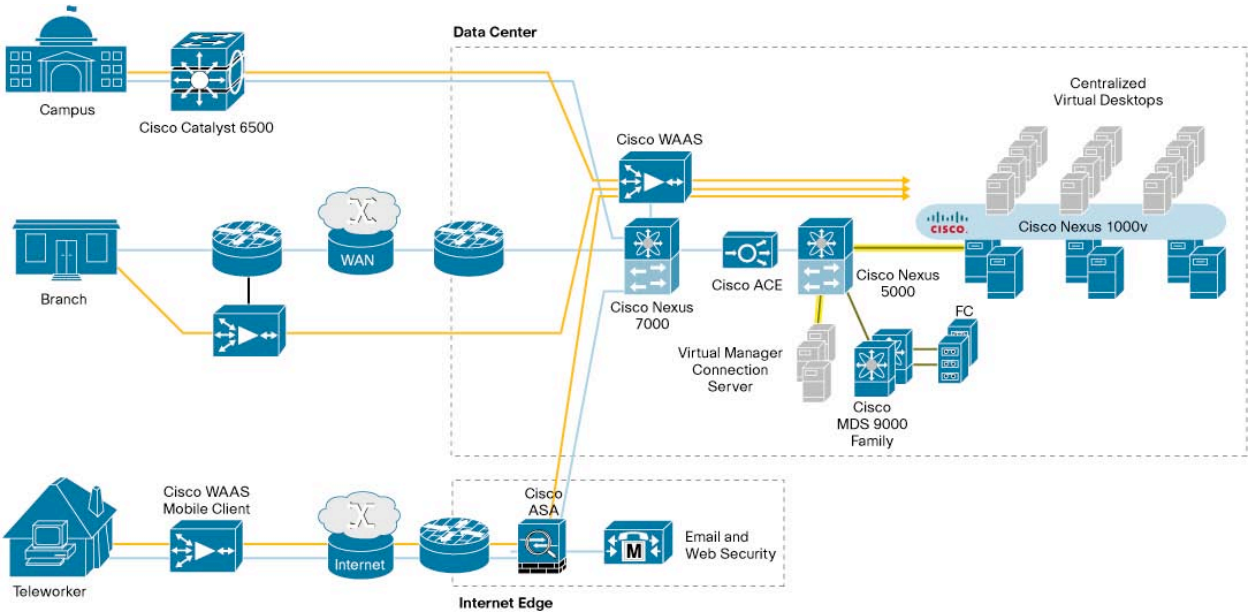
Benefits of Cisco Network Architecture

- Investment protection: The Cisco Nexus Family of switches is designed to support the entire lifecycle of the next-generation data center. Use cost-effective 10-Gigabit Ethernet or 10-Gigabit Unified Fabric today and take advantage of 40- and 100-Gigabit Ethernet and Unified Fabric in the future.
- Improved productivity: The Cisco Nexus Family provides component- and system-level operational continuity. Increased network stability and fewer service disruptions help to ensure that employees have access to the resources they need, when they need them, and that operations staff can handle problems efficiently.
- High performance: Cisco Wide-Area Application Services (WAAS) optimize VMware View performance. Cisco WAAS provides WAN optimization, traffic compression, object caching, and print optimization.
- Virtual Desktop Availability: Cisco ACE Application Control Engines can provide load-balancing services for VMware View Manager connection brokers. They continuously monitor the availability of VMware View Manager Connection Servers and efficiently route user desktop connection requests to the best available server.

Cisco Network Solution for VMware View

The Cisco VMware View Network Solution is a secure, optimized, end-to-end solution that delivers the performance, availability, and ease of management required for virtual desktop deployment (Figure 4).

Figure 4. The Cisco VMware View Network Solution Optimizes the User Experience



The Cisco VMware View Network Solution capitalizes on an organization's existing investments in Cisco network technologies, including security, quality of service (QoS), and application and virtual machine awareness. These technologies help optimize the performance of all applications, traditional or virtual.

The Cisco VDI solution optimizes VMware View scalability, availability, and performance, as described in the following sections.

WAN Optimization for Branch-Office Connections

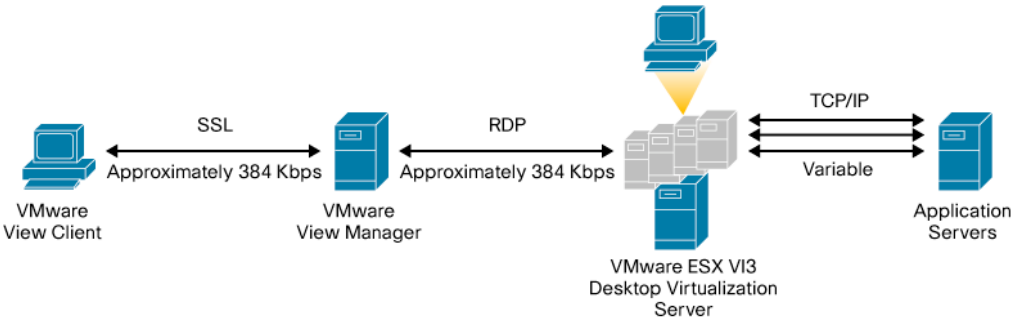
Lack of adequate WAN bandwidth to branch offices can degrade the user experience in a VMware View environment. Cisco Wide Area Application Services (WAAS) overcomes WAN bandwidth constraints by providing WAN optimization and application acceleration. As clients initiate RDP connections to the VMware View desktops, Cisco WAAS intercepts the RDP connections and uses compression and data redundancy elimination (DRE) to reduce the volume of traffic that travels over the WAN. The benefits of Cisco WAAS in a VDI environment include:

- RDP performance to provide a PC-like experience over the WAN
- Increased number of VMware View desktops that the WAN can support
- Availability of local Microsoft Windows print services to branch-office users, reducing WAN bandwidth requirements
- Optimized and accelerated backup of VMware View desktop images between data centers for disaster recovery

Load Balancing for VMware View Desktop Server Networking

The data center connection between VMware ESX servers and physical switches must be redundant, secure, and high performing. The VMware View solution consists of three elements: the VMware View client, VMware View Manager, and the View desktops that reside on the VMware ESX VI3 desktop virtualization server cluster (Figure 5). The VMware View client typically connects to the VMware View Manager, which loads the VMware View desktop onto the virtualization server cluster and brokers the remote clients' RDP session requests to the VMware View desktop. In organizations that use SSL encryption, the VMware View Manager acts a proxy between the VMware View client and the user's VMware View desktop. To achieve desired performance and redundancy, organizations typically need multiple connection brokers and multiple clustered VMware ESX servers.

Figure 5. Multiple Connection Brokers and Multiple Clustered VMware ESX Servers



To optimize the performance of the VMware View Manager connection servers, you can use the Cisco ACE Application Control Engine to load-balance RDP client connections to VMware View Manager. Cisco ACE also supports SSL encryption, so it can offload SSL encryption from VMware View Manager. This approach offers these advantages:

- Increases the number of RDP sessions that a single server can support by up to 50 percent
- Simplifies SSL certificate management
- Increases VMware View Manager availability

Resilience

To help ensure desktop availability, all components of the Cisco VMware View solution provide node, link, and path redundancy for the LAN and SAN. In conjunction with the high-availability features of the VMware and EMC solutions, the network redundancy helps ensure the continuous availability of the virtual desktop environment.

Topology and Bandwidth Considerations

In a virtual desktop environment, desktop traffic originates from the data center instead of the campus or branch office. Therefore, organizations need adequate bandwidth for the RDP session plus the traffic generated by the VMware View desktop.

To estimate total bandwidth requirements, add the bandwidth requirements for the following:

- RDP session: Cisco's tests show that an RDP session between the client and the VMware View desktop typically consumes approximately 384 Kbps.
- View desktop traffic: This amount varies by application.
- Workload processing: For example, use of a USB headset can generate 5 Mbps of traffic because all USB signals must be transmitted between the client device and VMware View desktop before they can be processed.
- Disaster recovery: Use of VMware Remote Desktop Services (RDS) increases the bandwidth needed to transfer or evacuate VMware View desktops during a disaster-recovery event.

The Cisco VMware View Network Solution uses switch virtualization technologies to provide the needed bandwidth:

- Cisco Nexus™ Virtual Port Channel (VPC)
- Cisco Catalyst® 6500 Virtual Switching System (VSS) 1440
- Cisco Catalyst Blade Switch virtual blade switch (VBS)

All these technologies aggregate multiple switch-to-server connections into a single EtherChannel interface, which simplifies server network interface card (NIC) teaming and increases cluster performance and availability. If needed, blade switches can be connected to Cisco Nexus 7000 Series Switches with 10 Gigabit Ethernet PortChannel links.

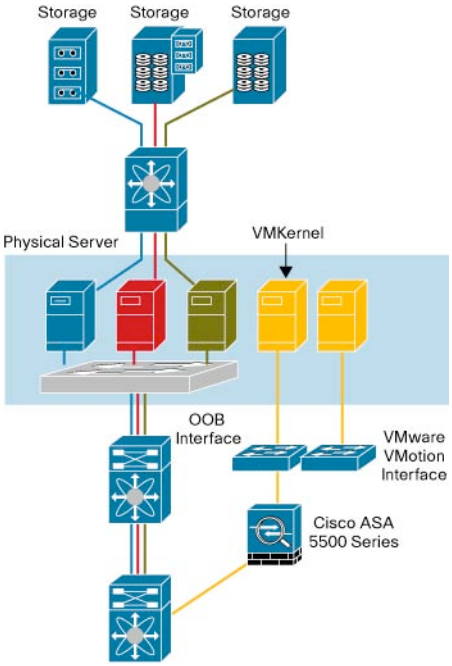
Security Considerations

Security in a VMware environment has two aspects: security of the VMware View infrastructure (VMware ESX cluster and View Manager) and security of VMware View and application traffic.

Within the VMware ESX server, a best practice Is to segment traffic types: VMware View desktop, VMotion, and Service Console. Use virtual switches (vSwitches), port groups, and VLANs to segment VMware View desktop traffic that has different security affinities.

Cisco recommends that you create two vSwitch definitions: one for management and control traffic and another for VMware View desktops (Figure 6). Although this approach requires additional server interfaces, it improves security and management. In environments with 10 Gigabit Ethernet connectivity, use port groups and associated VLANs to separate management traffic from VMware View desktop traffic. Alternatively, if a server has 10/100/1000 LAN connectivity on the motherboard, you can dedicate these interfaces to service console and VMkernel communications.

Figure 6. VMware View Desktop and ESX VI3 Traffic Isolation



You can apply different policies to the traffic traveling over each port group and VLAN. For example, you might want to secure VMware View desktop traffic using access control lists (ACLs), and secure the management VLAN using a Cisco Adaptive Security Appliance (ASA). The Cisco ASA authenticates network administrators before granting them access to the service console or VMkernel interface.

VMware View Desktop Security

VMware View uses Microsoft RDP to communicate between the remote client and virtual desktop. RDP is a multichannel protocol that transports all desktop updates—mouse, keyboard, and screen—between the client and the VMware View desktop over a single RDP session. RDP uses either HTTP port 80 or HTTPS port 443, making ACLs and firewall rules relatively simple.

The VMware View client typically connects to the VMware View Manager, which brokers the remote client's RDP session requests to the VMware View desktop. In organizations that use SSL encryption, the VMware View Manager acts a proxy between the VMware View client and the user's VMware View desktop. If you use SSL encryption, you will need a simple access control policy to allow only SSL traffic to the connection managers.

Security requirements are different if the remote client connects directly to the remote desktop. In this model, the client first establishes an HTTP or HTTPS connection to the VMware View Manager. Then the VMware View Manager redirects the client to establish a direct connection to the VMware View desktop. Organizations that implement VMware View in this way need to apply security rules that allow connectivity to both the VMware View Manager and the VMware View desktop.

The VMware View desktop has the same traffic patterns and profiles as a physical desktop. In most cases, Cisco recommends building the VMware View desktop environment on its own VMware ESX infrastructure, separate from the application environment. If you do this, you can integrate the VMware View desktop implementation without changing your existing application infrastructure and security policies.

Addressing

You need IP addresses for each VMware View desktop, client, and application server. If you do not have enough public IP addresses, you can investigate private IP addressing and Network Address Translation (NAT).

Storage Area Network

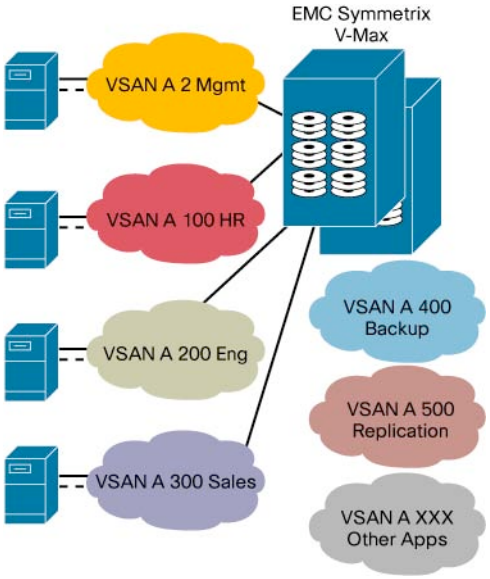
A SAN provides access to the VMware View desktop image as well as desktop data. Cisco recommends hosting the VMware View desktop images and data on a consolidated SAN so that you can load VMware View desktops onto any server in the VMware ESX cluster. The consolidated SAN also enables VMware VMotion and DRS to migrate VMware View desktops to different servers within the cluster to optimize cluster resource utilization.

The deployment of VMware View 3 is similar to the deployment of any other VMware ESX environment, with one notable difference. Instead of hosting application workloads, the VMware ESX server hosts a large number of virtual desktops with potentially highly variable workload, bandwidth, and storage access profiles.

Topology and Redundancy Considerations

The Cisco VMware View Network Solution uses two identical, fully redundant SAN fabrics, a common topology for production SANs. In Figure 7, each server connects to the Cisco MDS 9513 Multilayer Director's two SAN fabrics (A and B), for redundancy. Each storage array also connects to both fabrics, providing a fully duplicated access path to storage.

Figure 7. Redundant SAN Fabric Configuration for Vmware Deployments



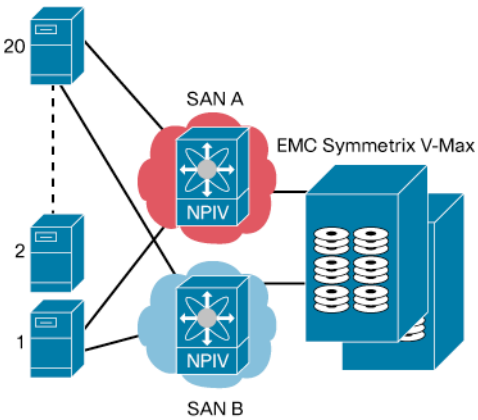
Deploying VSANs

Virtual SAN (VSAN) technology, an ANSI T11 standard, securely segments a single physical SAN fabric or switch into multiple logical SANs, or virtual SANs. Each VSAN consists of multiple interfaces that are associated with a particular set of storage resources. VSANs improve management efficiency, flexibility, and availability.

Each VSAN has independent fabric services for the zone server, name server, domain manager, and Fabric Shortest Path First (FSPF) routing services. This approach securely separates each VSAN from the others in terms of management, configuration, and protocol errors. If a zoning configuration error or a protocol violation occurs on one VSAN, it does not affect other VSANs that share the same SAN fabric.

The sample VSAN configuration shown in Figure 8 includes three VMware ESX clusters, used for the human resources (HR), engineering, and sales departments. Each cluster is assigned to its own VSAN. To ensure smooth VMware Virtual Machine File System (VMFS) operation, the corresponding storage array ports are assigned to their respective VSANs and appropriately zoned. Each core interface is assigned to the VSAN dedicated to the department that connects to a specific VMware ESX cluster. With this configuration, multiple server and storage devices can connect to any VSAN. Furthermore, the chassis can physically connect to any port on any switch. As a result, VSANs remain strictly isolated even though they share the same physical network infrastructure.

Figure 8. VSAN Configuration Example



SAN Bandwidth Considerations

In practice, 4 Gbps is usually adequate for rack-optimized and blade server connectivity to the SAN. To estimate SAN bandwidth more precisely, consider the following factors:

- Bandwidth requirements peak during the boot and login phases, when servers load desktops over the SAN. Keep in mind that although master images can reduce storage disk capacity, the entire master image travels across the SAN to load each VMware View desktop.
- Users typically do not log in at the same time, and their requests are processed across multiple servers in the VMware ESX cluster. Therefore, most organizations can safely use a 10:1 oversubscription ratio for VMware View SAN deployments.
- Bandwidth requirements after the login phase depend on how many times desktops access the hard drive. Regardless, the nominal traffic load is relatively light, and substantially lower than during the boot and login phases.

SAN Security Considerations

In a VMware environment, different departments securely share the same network and servers. The shared infrastructure must provide the same level of security and isolation as a solution based on separate networks and servers.

Cisco MDS 9500 Series Multilayer Directors provide numerous features to help prevent malicious or inadvertent data leakage. Standard SAN security features include zoning and logical unit number (LUN) masking. Advanced security features control and limit the storage arrays that a host can access.

EMC Storage Architecture for Virtual Desktop Deployments

Storage Challenges in a Virtual Desktop Deployment

Desktop virtualization requires high capacity and highly available storage for hundreds or thousands of desktop clients and their applications. When properly designed, consolidated storage can improve utilization, availability, and flexibility while reducing management burden. Organizations can also reduce costs with advanced storage technologies that reduce storage requirements, such as VMware View Composer and EMC thin provisioning and EMC data deduplication.

Benefits of an EMC Storage Architecture

- Improved storage utilization: Combining VMware View Composer inked clones with EMC storage virtual provisioning significantly reduces the amount of physical storage needed, reducing costs.
- High desktop service levels: To deliver acceptable response times to desktop users, the storage architecture must provide the capacity to meet I/O request rates for static and burst desktop demands. In an EMC storage architecture, you can meet this goal by allocating back-end storage across as many high-speed Fibre Channel and enterprise flash memory drives as needed.
- Optimized user data storage: Data deduplication and compression technology in EMC's Celerra network-attached file server reduces storage requirements for network-redirected user file data.
- Flexible protocol deployment: EMC storage supports a wide variety of storage interconnect technologies that have been tested with VMware View. These include Fibre Channel, Fibre Channel over Ethernet (FCoE), Small Computer System Interface over IP (iSCSI), and network-attached storage (NAS).

EMC Solutions for VMware View Deployments

EMC storage products can provide a VMware host or cluster with numerous logical devices connected through multiple I/O controllers. You can configure these logical devices to support different numbers and sizes of virtual machines. You can also configure them to provide needed availability levels, using RAID and more advanced capabilities, including array replication technologies for disaster recovery, such as Symmetrix Remote Data Replication (SRDF) and EMC MirrorView.

User File Data Redirection

In traditional desktop systems, the operating system, applications, and user file data are all stored on the internal hard drive. In a VMware View deployment, EMC recommends redirecting user file data to network file shares to improve management and storage utilization. You can configure the desktop for user file data redirection using Microsoft Group Policy. Separating the desktop image from the user data also simplifies the process of updating the desktop image.

Data Deduplication

Virtual desktop deployments result in many copies of identical OS and application executables. The duplication occurs on the OS boot disks created for all virtual desktops. To reduce duplicate data in the OS boot drive, use VMware View Composer linked clones for virtual desktop OS boot disks. VMware View Composer creates desktop clones from a master image, and the clones use a fraction of the storage space of the full master image. As the clone is used in production, changes from the base image are written to the clone. To reduce the growth of the clones, EMC recommends separating frequently updated data files, such as swap files, from the base OS boot disk. Also turn off unnecessary updates to file system metadata, such as file-access-time recording. When you take these two steps, most I/O to the common data will be random read access by active virtual desktop machines cloned from the base disk.

Contention for blocks on different portions of the shared base OS boot disk can affect performance. You can reduce this effect by managing the layout and caching of blocks in the storage array. EMC recommends allocating the base OS boot disk to high-performance disks and striping it across multiple spindles. This allocation helps support many concurrent read operations to different parts of the logical disk.

Deduplicating user data saves more storage space. If you redirect user file data to a network file server such as the EMC Celerra, you can use file-level deduplication at the file server to centrally eliminate duplicate files, which can reduce storage space used by approximately 50 percent. Augment data deduplication with file-server virus scanning and active archiving to provide comprehensive data management and compliance for desktop-user file data with lower overhead for virtual desktop users.

Multiple LUNs for Greater I/O Distribution

VMware View deployments include a large number of virtual desktop machines. You can use either multiple small LUNs or a single large LUN. Distributing the storage across multiple smaller LUNs reduces I/O request queuing, which improves performance. However, a single VMware ESX cluster can support only a limited number of devices. In addition, multiple LUNs increase VMFS overhead.

Therefore, EMC recommends presenting the storage for a VMware ESX cluster as metavolumes span multiple devices and their I/O request queues for higher capacity and performance. In addition, when a metavolume LUN on an EMC Symmetrix V-Max storage array nears capacity, you can expand the storage allocated to the array without taking it offline. If you configure multiple LUNs for a single VMware cluster, EMC also recommends configuring VMFS to span the multiple LUNs, to improve space utilization and performance.

Path Management for Load Balancing

To provide fault tolerance, establish multiple paths between each VMware ESX server and its EMC storage array. VMware ESX provides native channel failover when an alternative access path is available to a storage device. Although VMware ESX 3.5 does not provide native load balancing across available paths to storage, you can more evenly distribute storage I/O load by selecting separate available paths for different storage devices.

Disk Layout and Allocation Alignment

Misalignment between storage device layout and on-disk structures can severely degrade I/O response times. With EMC storage arrays, aligning the data partitions on a 64-KB boundary noticeably improves I/O response time. For optimal performance, EMC recommends aligning both the VMFS file system and its virtual disks on 64-KB track boundaries.

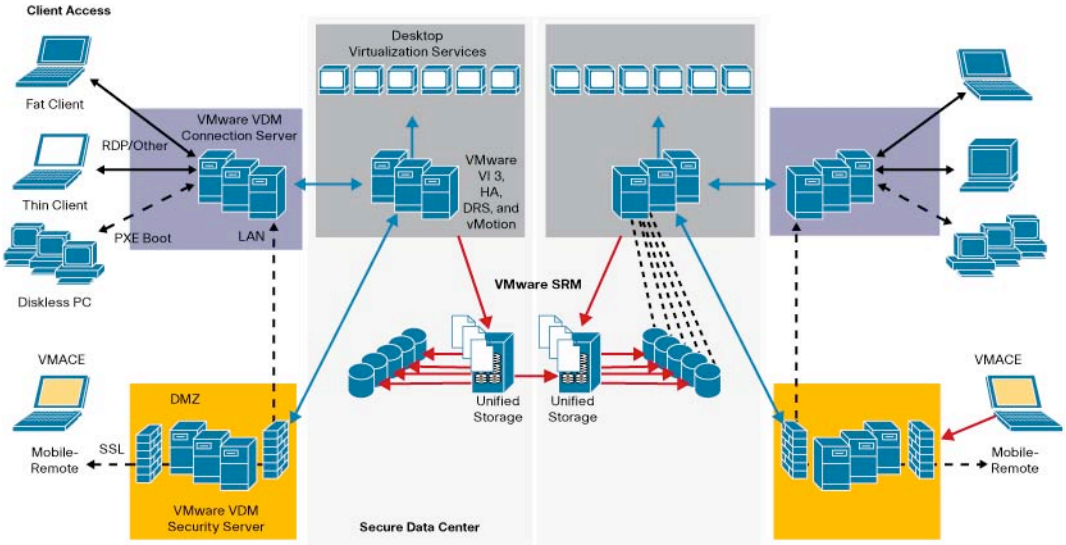
Business Continuation and Disaster Recovery

To simplify backup of user files and roaming profiles, store user files separately from the desktop OS. Storing user file data on network storage devices such as the EMC Celerra enables centralized data backup and recovery.

If you currently maintain user files on the desktop boot disks, the transition to VDI provides an opportunity to begin separating storage. You can use either VMware Consolidated Backup (VCB) or a storage system's snapshot capabilities to capture point-in-time snapshots of user data files and prepare offline backups.

The transition to VDI also provides an opportunity to manage and plan for rapid recovery from a major infrastructure failure or loss of equipment. VMware Site Recovery Manager (SRM) provides the management framework for defining, testing, and implementing a comprehensive and robust recovery plan in conjunction with the remote data replication capabilities available in EMC's storage products (Figure 9).

Figure 9. Disaster Recovery with VMware SRM



Configuring Storage for a VMware View Deployment

There are no simple formulas for determining the ideal storage configuration for a virtual desktop deployment. The VMware document VDI Server Sizing and Scaling describes an analysis procedure for this. The main steps are:

1. Measure normal use for existing desktop systems, including gigabytes used, I/O operations per second (IOPS), and throughput. You can collect statistics about the frequency and size of I/O operations in your environment using desktop OS performance monitoring tools or the VMware ESX tool, esxtop. Collect statistics for the different types of applications used in the organization. Knowing the expected IOPS and their aggregate bandwidth per second will help you provision adequate storage space and connectivity. To determine the size of the virtual disks or file shares, develop a base virtual desktop configuration.
2. Estimate the total capacity by multiplying average use by the number of users.
3. Provision storage and SAN bandwidth, adding capacity for observed fluctuations and extremes, such as concurrent logins or reboots.
4. Monitor virtual desktop storage traffic and adjust storage or SAN configurations when needed to eliminate bottlenecks.

Technologies such as VMware View Composer and EMC thin provisioning and EMC data deduplication reduce initial storage requirements.

Storage Device Layout

Consider the following factors when configuring storage devices:

- Configuring storage I/O targets as RAID LUNs across multiple spindles improves throughput and helps ensure continued availability if a spindle fails.
- The optimum RAID level for a target LUN depends on the I/O volume and how much of that volume is used for write operations.
- Higher drive rotational speed increases performance but also increases costs. To meet the I/O demands of the VDI workload with acceptable response times, store frequently accessed data on spindles with a high rotational speed.
- Providing the most frequently accessed devices on flash drives can significantly increase overall performance. An example is VMware View Composer replicas, which are the sources of many linked clones.
- The storage system should be able to dynamically reallocate a spare spindle and integrate it back into the RAID5 LUN without downtime or unacceptable overhead. EMC Symmetrix V-Max provides this capability.

Access Technology

The choice of a storage access technology in a VDI—Fibre Channel, FCoE, iSCSI, or NAS—has far-reaching effects. Factors affecting your choice should include the number of virtual desktops, experience of the IT staff, performance and availability requirements, and existing hardware. The cost of each method includes the storage, adapters, and interconnects between the storage and the VMware ESX hosts.

To reduce disruption of desktop clients by congestion or failure, choose a storage system that supports:

- Multiple paths
- Redundant data copies
- Dynamic load balancing of I/O across the available paths and copies
- Rapid reallocation of the load when a path or storage component becomes available

VMware View Storage Deployment Example

Figure 10 represents a typical enterprise VMware View deployment based on the storage configuration guidelines and best practices discussed in this document. The deployment follows the building-block model for 1000 virtual desktop users described in the VMware View Reference Architecture. In the figure, VMware View Composer linked clones created on thin-provisioned storage devices are used for the OS boot disk. User data is redirected to network file shares.

Figure 10. VMware View Storage Deployment

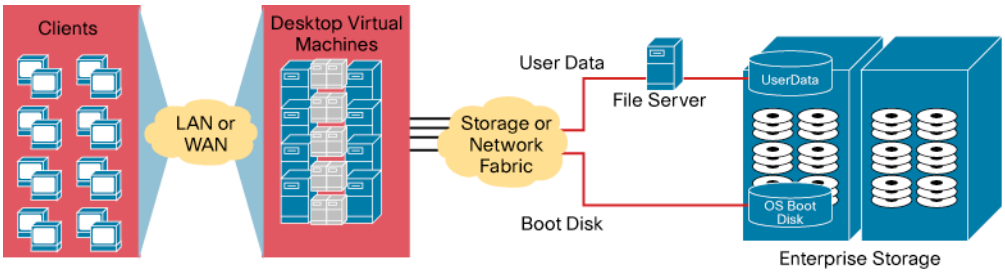
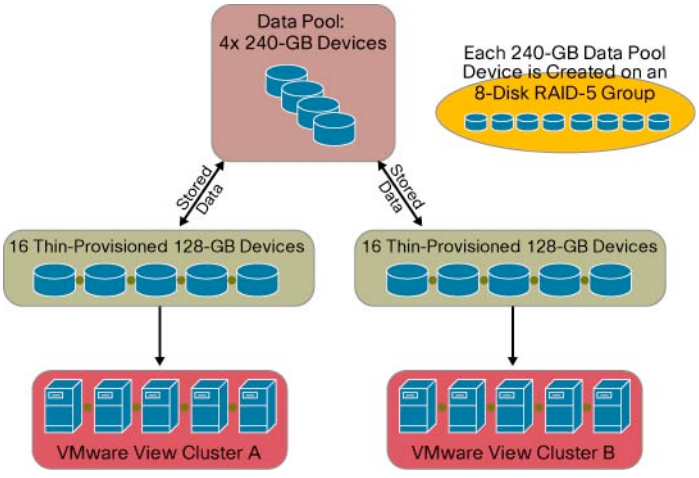


Figure 11 shows the logical view of the data stores as might be configured in an EMC Symmetrix array. Each thin-provisioned storage device is a VMware data store that contains a master replica of the golden desktop image. The replica is used to generate linked clones for the desktops. Using multiple thin-provisioned storage devices in this way distributes desktop I/O load across all the spindles in the data pool, which increases bandwidth capacity and reduces contention. Each virtual desktop is provided with a VMware View Composer–linked clone of a master boot disk image. This configuration provides a very high ratio of virtual storage space to used physical disk space. If desktop users need more space, you can add data pool devices. If more bandwidth is needed, you can configure the new data pool devices across additional physical spindles. There is a tradeoff between saving storage space and conserving storage bandwidth, and the optimal balance depends on the deployment.

Figure 11. Logical View of Storage Provided for VMware View Composer–Linked Clones



EMC provides flexible storage options for virtual desktop deployments to meet the scale and configuration requirements for a wide range of environments (Table 1). These options all offer high performance, 99.999 percent availability, and thin provisioning to allow storage consolidation and optimization.

Table 1. Storage Infrastructure Deployment Options

Business Need	Characteristics	Storage Solution
Midrange deployments	High-performance deployment using Fibre Channel or iSCSI interconnects	EMC CLARiiON CX4
Midrange deployments using unified storage for virtual desktops and redirected user file services	• High-performance deployment using Network File System (NFS) on Fibre Channel or iSCSI • Integrated file services with data deduplication and file archiving	EMC Celerra Unified Storage
Centralized enterprise-scale deployments supporting thousands of users using new or existing enterprise storage arrays in the data center	Large-scale Fibre Channel deployment using virtual storage provisioning and data center availability requirements	EMC Symmetrix V-Max EMC Symmetrix DMX

Conclusion

Virtual desktop technology reduces the daily challenges of supporting large numbers of desktops by:

- Simplifying deployment
- Lowering operational support requirements and costs
- Addressing increased requirements for information security and flexibility in a global economy

Whether an organization has tens or thousands of users, the virtual desktop deployment shares the same fundamental architecture. That is, remote clients connect to the data center over the network to access a centrally managed virtual desktop image and user data. Organizations need a strong network and storage infrastructure to support virtual desktop deployment, to meet both user expectations for capabilities and response time and IT expectations for operational simplicity.

With the introduction of VMware View, VMware is extending virtual desktop technology to address the challenges of today's mobile and global workforce. VMware View supports new capabilities to manage large numbers of desktops efficiently and securely. EMC and Cisco are actively working with VMware to build out the network and storage infrastructure to enhance the performance, resilience, and availability of the VMware View deployment. VMware, EMC, and Cisco are committed to working together to continue to provide best-in-class technologies and best practices for virtual desktop deployments.

For More Information

VMware Reference Documents

- VMware View Reference Architecture: http://www.vmware.com/resources/techresources/1084
- VDI Server Sizing and Scaling: http://www.vmware.com/files/pdf/VMware_VDI_Server_and_Storage_Sizing_120508.pdf
- Solving the Desktop Dilemma with User-Centric Desktop Virtualization for the Enterprise: http://www.vmware.com/solutions/wp/desktop-manageability.html
- VMware View 3: http://www.vmware.com/files/pdf/view_brochure.pdf

Cisco Reference Documents

- Cisco Application Networking Services for VMware Virtual Desktop Infrastructure Deployment Guide: http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/ns377/deployment_guide_c07-493981.html
- Benefits of Running VMware VI3 on Cisco MDS Optimized SAN: http://www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps5989/ps9898/white_paper_c11-506464_v2.pdf

EMC Reference Documents

- EMC Infrastructure for Deploying VDI in the Enterprise: http://www.emc.com/solutions/samples/virtualizing-information-infrastructure/virtual-desktop-infrastructure-vmware.htm
- EMC Infrastructure for Deploying VMware View in the Enterprise EMC Celerra Unified Storage Platforms: http://www.emc.com/collateral/software/solution-overview/h5986-vmware-vdi-on-celerra-solution-guide.pdf
- EMC Symmetrix V-Max and VMware Virtual Infrastructure: http://www.emc.com/collateral/hardware/white-papers/h6209-symmetrix-v-max-vmware-virtual-infrastructure-wp.pdf

- Using EMC Symmetrix Storage in VMware Virtual Infrastructure: http://www.emc.com/collateral/hardware/solution-overview/h2529-vmware-esx-svr-w-symmetrix-wp-ldv.pdf
- EMC Celerra Unified Storage: A Guide to Deploying EMC Celerra NS20 Storage with VMware View: http://www.vmware.com/resources/techresources/1084
- VMware View Deployment Guide for EMC CLARiiON Fibre Channel: http://vmware.com/files/pdf/view-deployment-emc-clariion-fc.pdf
- VMware View Deployment Guide for EMC CLARiiON Fibre Channel: http://vmware.com/files/pdf/view-deployment-emc-clariion-iscsi.pdf
- Deploying Authenticated VMware Virtual Desktop Solutions Using EMC Celerra Storage and RSA SecurID: http://powerlink.emc.com/km/live1/en_US/Offering_Technical/White_Paper/h5718-deploy-vdi-celerra-rsa-securid.pdf

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304 USA

Tel: 650-427-5000 or 877-486-9273
Fax: 650-427-5001

www.vmware.com

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134 USA

Tel: 408-526-4000 or 800-553-6387 (NETS)
Fax: 408-527-0883

www.cisco.com

EMC Corporation
176 South Street
Hopkinton, MA 01748 USA

Tel: 508-435-1000

www.emc.com