



VMware View: High-Performance, Highly Manageable Desktop Infrastructures for U.S. Federal Agencies

WHITE PAPER

Abstract

IT organizations in federal agencies are being pressured to increase systems efficiency and agility. Many factors contribute to this pressure, including the need to reduce costs, increase data security, streamline systems management, and ensure systems continuity during emergencies.

An increasing number of federal agencies are looking to Virtual Desktop Infrastructures (VDI) as an effective means of addressing these needs. VDI offers IT organizations the means to centrally manage and deliver desktops as a service. VMware View™ is the most widely deployed and trusted VDI offering, built on the industry-leading VMware vSphere™ platform.

This paper discusses the challenges faced by federal agencies and shows how VMware View helps them:

- Provide federal workers with immediate and flexible access to desktops and applications.
- Comply with security requirements and continuity of operations standards.
- Reduce the cost and complexity of desktop management.

This paper also provides a unique VDI reference architecture that was developed and tested by Force 3, a VMware Premier Partner that has served federal agencies for nearly 20 years. The reference architecture has been designed to meet federal desktop computing needs, and it has been tested with workloads that simulate real-world activities. The test results illustrate how this VDI reference architecture delivers excellent performance for the user and provides the capacity to scale the number of virtual desktops for agency-wide deployment. The architecture can serve as a guide for federal agencies as they seek to architect a VMware View deployment.

Table of Contents

Abstract	2
Overview	4
The Challenges of Providing Desktops to Federal Workers	5
Provide Anytime, Anywhere Access	5
Meet Strict Security and Compliance Requirements	5
Support Continuity of Operations Planning	5
Streamline IT Operations and Management	5
VMware View: A Comprehensive VDI Solution for U.S. Federal Agencies	6
VMware View: An Overview	7
Common Federal Use Cases for VDI	9
COOP and Emergency Preparedness	9
Training	9
Windows 7 Deployment	9
Work-at-a-Distance	9
Reference Architecture Overview	10
Goals	10
Building Block Approach	10
Key Innovation: Using Flash Memory to Optimize VDI Performance and Storage	10
Optimizing Flash Memory to Reduce Storage Costs	11
Reducing Operating System I/O Performance Impacts	11
Reference Architecture Components	12
Hardware Resources	12
Software Resources	12
Topology	13
About Violin Flash Memory Array	13
About Cisco Unified Computing System	14
About FalconStor Network Storage Server	14
Reference Architecture Performance Validation	15
Testing Tools	15
Virtual Desktop Configuration and Workload Profile	15
Test Procedures	16
Test Results	17
Conclusion	23
Acknowledgements	24
For More Information	24

Overview

IT organizations within U.S. federal agencies are under pressure to modernize and transform IT systems to be more efficient and agile. They are increasingly tasked with

- Providing federal workers with immediate and flexible access to desktops and applications.
- Complying with security requirements and Continuity of Operations (COOP) standards.
- Reducing the cost and complexity of desktop management.

Many agencies are turning to Virtual Desktop Infrastructures (VDI) to support users more effectively in a variety of environments and on a variety of computing devices.

VDI uses virtualization technology and cloud computing to provide users with virtual desktops rather than isolated, traditional desktops. This approach achieves greater desktop manageability, security, and standards compliance. VMware View™ is the most widely deployed VDI solution; it:

- Provides superior user computing experiences.
- Simplifies desktop and application deployment and management.
- Lowers total desktop management costs.

With VMware View, federal agencies can deploy large volumes of virtual desktops as easily as deploying a single desktop. This paper discusses the challenges faced by federal agencies, shows how VMware View helps them meet those challenges, and presents a unique VDI reference architecture that is tailored to and tested for federal computing environments.

The Challenges of Providing Desktops to Federal Workers

Typically, federal agencies spend nearly 70 percent of their budgets just to keep existing systems up and running. When it comes to desktop management, the situation is becoming more complex:

- Federal workers and contractors are becoming increasingly mobile.
- Security and compliance requirements are proliferating.
- The variety and overall number of computing devices is expanding rapidly.

Managing traditional desktop environments was relatively straightforward when all personnel and work resources were confined to a controlled office space. But today's dynamic federal workforce—including the military—involves field-based, office-based, remote, forward-deployed, and contractor personnel. This mix of environments, devices, and worker roles presents many new challenges for desktop management.

Provide Anytime, Anywhere Access

Wherever they are, federal workers need real-time, secure access to familiar computing resources. However, provisioning the correct operating system, security parameters, applications, and data can be difficult and expensive.

Meet Strict Security and Compliance Requirements

Agencies must meet strict computing security requirements that often involve complicated policies and procedures. Ensuring that these policies are properly enforced in a traditional desktop environment requires significant time and IT resources.

Support Continuity of Operations Planning

Since 9/11 and Hurricane Katrina, all federal agencies have committed to improving contingency planning and emergency preparedness through COOP planning. Maintaining continuity of operations requires a highly available and resilient IT infrastructure—including desktops—so that federal workers can do their jobs effectively, regardless of circumstances.

Streamline IT Operations and Management

At the same time, as federal IT organizations are being pressured to reduce expenses by streamlining operations and management, supporting and patching traditional desktop computers is becoming increasingly complex.

Meeting these challenges while streamlining operations requires a new, more efficient way to deliver applications and manage desktops.

VMware View: A Comprehensive VDI Solution for U.S. Federal Agencies

VMware View, the most widely deployed and trusted desktop virtualization solution, provides a VDI solution for federal agencies. With it, IT staff can deploy large volumes of virtual desktops as easily as deploying a single desktop while improving security and lowering operating costs. The VMware View VDI solution specifically addresses the desktop challenges faced by federal agencies:

DESKTOP CHALLENGE	VMWARE SOLUTION
Provide federal workers with immediate and flexible access to desktops and applications.	<ul style="list-style-type: none"> • Increases employee mobility and flexibility with immediate access to personalized virtual desktops and applications from any device, regardless of location. • Gives workers real-time, secure access to familiar, agency-standard resources
Comply with security requirements and continuity of operations standards.	<ul style="list-style-type: none"> • Protects user identities and data with: <ul style="list-style-type: none"> - Single sign-on (SSO) using common access card (CAC) and Personal Identity Verification (PIV) card validation. - Secure sockets layer (SSL) encryption between the server and the client. - Access control policies for USB devices. • Built-in COOP capabilities ensure desktop and application availability in the face of a catastrophic or disruptive event.
Reduce the cost and complexity of desktop management.	<ul style="list-style-type: none"> • Centralizes all desktops, data, and applications in the datacenter, which: <ul style="list-style-type: none"> - Reduces the total cost of ownership for desktop infrastructures by up to 50 percent. - Simplifies testing and deployment of updated images. - Addresses application/operating system incompatibilities. - Streamlines and guarantees patch compliance. - Makes it faster, easier, and less costly for IT staff to provision, deploy, maintain, and monitor desktop images across their entire life cycle.

VMware View also meets international and U.S. federal government security guidelines and requirements:

- It is currently in process for Federal Information Processing Standard (FIPS) 140-2 certification.

With VMware View, federal agencies can achieve the benefits of VDI architectures while complying with security, control, and efficiency requirements.

VMware View: An Overview

VMware View virtual desktops deliver a rich user experience while letting IT organizations provision thousands of virtual desktops quickly and easily. It also provides simplified management and security over the entire desktop environment.

This simplified management is possible because VMware View separates the underlying operating system from user data and applications. When a user launches his or her virtual desktop, VMware View dynamically assembles the operating system, user data, and applications and delivers a secure, unified desktop to the user's device.

Because the operating system, applications, and user data are encapsulated into isolated layers, VMware View empowers IT staff to patch, change, update, and deploy items in each layer independently—without concern that one layer will interfere with another.

VMware View consists of several layers of components, as shown in Figure 1.

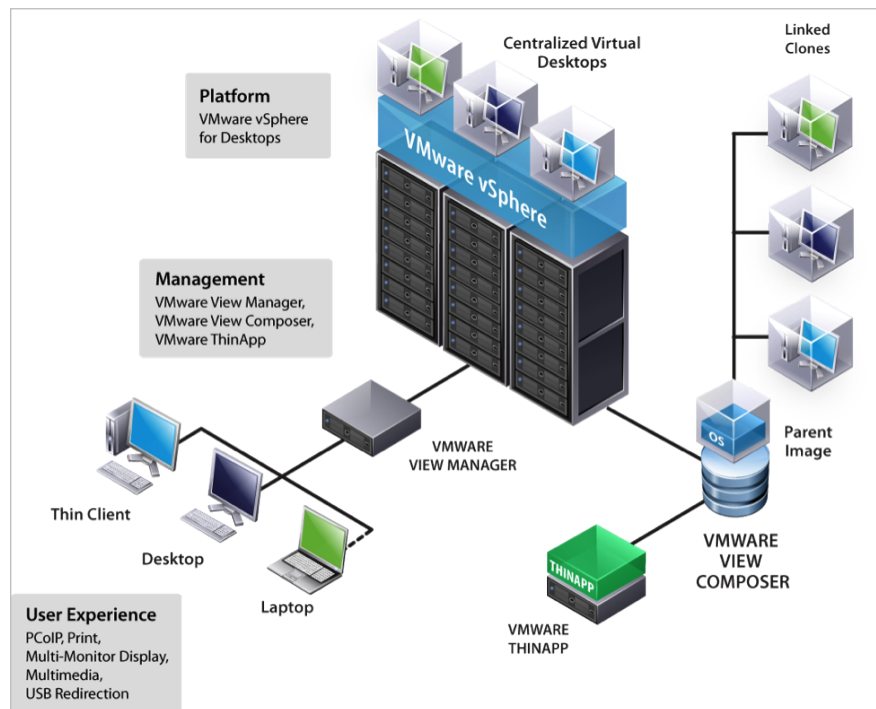


Figure 1. VMware View components

The following table contains brief descriptions of each component.

COMPONENT	DESCRIPTION
VMware vSphere™	<p>A virtual desktop management console.</p> <p>Provides tools to centrally provision, deploy, and manage thousands of virtual desktops from a single image. Makes it possible for users to connect securely and easily to VMware View desktops.</p>
VMware View Composer	<p>A flexible tool for rapidly creating desktop images that share virtual disks with a single parent image and for reducing virtual desktop storage requirements.</p> <p>Separates user data and settings from the virtual desktop's operating system, letting IT staff manage the operating systems and the data independently. Virtual desktops that are linked to the parent image can be automatically patched or updated by simply updating the parent image—without affecting user data or settings.</p>
VMware ThinApp™	<p>An agentless application virtualization solution that streamlines the delivery of applications.</p> <p>Enables IT staff to deliver and maintain applications independently from the virtual desktop's operating system. Simplifies application administration tasks and reduces virtual desktop storage needs.</p>
VMware View Client.	<p>A client application that provides access to virtual desktops from Windows-based computers, Macs, thin clients, and mobile devices.</p> <p>Local mode lets users access their virtual desktops when they are disconnected from the network. Enforces consistent security and compliance policies, such as barring access to the offline desktop after a specified period of time. If allowed by access control policies, permits users to access locally attached peripherals such as printers, scanners, and USB storage devices.</p>
PC over IP (PCoIP)	<p>A high-performance display protocol that is specifically designed to deliver a superior virtual desktop experience.</p> <p>Desktops are host-side encoded so they can be accessed from a local area network (LAN) or a wide area network (WAN). Makes it possible for users to play rich media content, choose multiple monitor configurations with pivot and mixed resolutions, and enjoy a local desktop experience without restrictions on resolution or refresh rate. Designed to meet all desktop user types, from the task worker to the designer.</p>

Together, these VMware components offer federal agencies a robust desktop virtualization solution that meets the challenges that are inherent in provisioning and managing a complicated desktop infrastructure.

Common Federal Use Cases for VDI

Federal agencies are using VDI to meet many of their desktop infrastructure needs. The most common use cases are discussed briefly below.

COOP and Emergency Preparedness

To ensure continuity of operations, IT staff must be able to rapidly provision virtual desktops to available devices. VMware View lets federal agencies provide virtual desktops to their workers as a continuously available service—even during server failures or other challenging conditions. (Note: discussing how to provide services during “smoking hole” disasters is beyond the scope of this paper.)

Training

Training requires rapid provisioning, reconfiguration, and teardown of desktops. Federal agencies can use VMware View to quickly provide secure, customized virtual desktops to workers for training purposes. When the training is done, the virtual desktops can be reconfigured or deleted.

Windows 7 Deployment

VMware View reduces the complexity of moving to the Windows 7 operating system because IT staff can create many virtual desktops based on one parent virtual machine. This makes it possible for multiple virtual desktops to use the same software installation, which reduces the number of Windows 7 configurations that have to be configured and maintained.

Work-at-a-Distance

VMware View provides remote workers with instantaneous access to a secure desktop from any location over a secure network using SSL encryption.

The reference architecture presented in this paper is designed to address the scenarios described in these use cases while also providing excellent performance for users. Test results indicate that this reference architecture provides a flexible, scalable VDI solution to the federal desktop infrastructure challenges that are represented by these use cases.

Reference Architecture Overview

To demonstrate how VMware View meets federal needs around desktop management, and to help federal agencies design their own VMware View deployment, this paper presents a VDI reference architecture with a unique design that is tailored for federal desktop infrastructure needs. This reference architecture was developed and tested in collaboration with Force 3, a VMware Premier Partner that has served federal agencies for nearly 20 years.

The architecture is designed to optimize user experiences by employing an innovative storage system that accelerates boot times, provisioning, and steady-state operation. It has been tested with workloads that simulate real-world federal computing environments. Test results using this architecture show excellent performance for users while providing the capacity to scale the number of simultaneous virtual desktops. The architecture provides a sample VMware View infrastructure that federal agencies can use as a template as they consider designing their own VMware View deployments.

Goals

This VDI reference architecture was designed to meet several goals, including the following:

1. Provide an excellent user experience around application access, data availability, and overall performance regardless of worker role, location, or device.
2. Support rapid desktop provisioning and refreshes to create flexibility and speed in maintaining the desktop environment.
3. Provide a simple and cost-effective method for rapid piloting with an ability to quickly scale up as needed.
4. Enable streamlined and comprehensive centralized desktop management, including infrastructure (for example, storage), desktop images, and desktop security.

Building Block Approach

This reference architecture represents a VDI building block: a single unit that contains all of the computing resources that are required to simultaneously power 380 VMware View virtual desktops running Windows 7. The building block includes additional storage and processing capacity for peak loads and server failure situations. In this way, the building block can maintain a consistent user experience during degraded conditions. Because it is designed as a building block, the architecture can scale easily by adding more blocks to meet desired capacity.

Key Innovation: Using Flash Memory to Optimize VDI Performance and Storage

By centralizing desktop loads, VDI combines the input/output (I/O) requirements of individual desktops into a centralized storage system. In a typical VDI deployment, storage I/O can become a major performance bottleneck, which contributes to negative user experiences.

While the I/O load for an average user can be 5 to 8 I/Os per second (IOPS), peak loads can range from 20 to 100 IOPS. With hundreds of users on centralized storage, even a small percentage near peak load can impact performance. To keep performance high during peak I/O load times, such as morning login and evening logoff, the storage system should be able to:

- Handle the peak load for all users at the same time.
- Produce little to no negative performance effects for users.

This reference architecture separates VDI storage from other enterprise storage to streamline management and to ensure high performance. It solves the storage I/O issue by using a dedicated flash memory array rather than standard hard drives to store desktop images. A flash memory array can offer very high IOPS with low latency. And even under heavy load, a flash array provides consistent performance characteristics. In contrast, standard hard drives that use spinning disks exhibit exponential performance degradation under heavy load.

The flash array used in this reference architecture can provide up to 200,000 IOPS and 20 terabytes (TB) of signaling link code (SLC) NAND memory storage in a 3U rack or cabinet. For this architecture, flash storage capacity was calculated by allowing up to 3 gigabytes (GB) of growth space plus 1 GB for the Windows 7 paging file per virtual desktop. Also, to reduce the delays caused by queuing other operations while a small computer system interface (SCSI) lock is active, 10 flash array datastores were created, with 40 virtual desktops placed in each datastore.

Optimizing Flash Memory to Reduce Storage Costs

One drawback with flash arrays is that they are currently more expensive than traditional hard disks. This reference architecture employs several mechanisms to reduce flash array space requirements:

- **Using VMware View Composer linked clones:** A linked clone is a copy of a virtual machine that shares virtual disks with the parent virtual machine in an ongoing manner. This conserves disk space and lets multiple virtual machines use the same software installation. VMware View-linked clones use writable snapshot technology to reduce the space requirement for a virtual machine deployment. Only changes to the master desktop image are stored on the linked clone storage.
- **Placing permanent user data on network storage via folder redirection and persistent virtual disk:** The architecture reduces flash array storage requirements by placing persistent virtual disk and virtual machine swap files on non-flash array storage and using folder redirection to send user data to the appropriate storage location. (This approach is a best practice for desktop data management in a physical desktop environment as well.)
- **Regularly refreshing the desktop:** A high-performance flash array backend enables fast desktop refreshes. Regular desktop refreshes return the linked clone desktops to a pristine, streamlined state, eliminating any configuration data or settings that are accumulated by user or application activities.
- **Disabling virtual machine suspension:** Disabling virtual machine suspension removes the need for a suspend file for each virtual machine in the flash array storage.

These approaches reduce the VDI solution cost by reducing flash storage size while optimizing virtual machine performance and storage.

Reducing Operating System I/O Performance Impacts

The Windows desktop I/O has a strong impact on storage system performance. Therefore, separating the desktop operating system I/O from the rest of the enterprise storage can reduce the negative impact on critical enterprise application performance. This reference architecture segregates the desktop I/O to the flash memory storage, while keeping the valuable persistent user data in an enterprise network-attached storage (NAS) or storage area network (SAN) via

folder redirection and persistent disk. This approach can optimize the storage performance against data value and overall system cost by shifting intensive Windows I/O to a higher-performing flash memory array.

Reference Architecture Components

The reference architecture is composed of the following hardware and software resources.

Hardware Resources

ITEM	QUANTITY	CONFIGURATION
Cisco Unified Computing System	1	(1) Cisco UCS 5100 Chassis with FC Expansion (2) Cisco UCS 6100XP Fabric Interconnect (8) B200 M1 Blades, each with (2) Intel Xeon 5570 processors @ 2.93 Ghz, 48 GB RAM, M71KR-Q Converged Network Adaptor
FalconStor® Network Storage Server (NSS) Gateway Appliance	1	Dual Quad-Core Intel Xeon E5520 processors @ 2.27 Ghz 16 GB RAM (2) Qlogic 2462 4 Gb FC adaptors
Violin Memory Systems 3200 Flash Memory Array	1	2.6 TB raw capacity 1.7 TB usable capacity
Enterprise Network Switch	One for this deployment (two are recommended for redundancy)	Gigabit Ethernet Switch with 32 ports Nexus 5K, 10 Gb switch

Software Resources

ITEM	UPDATE VERSION
Desktop image with applications from the Army Gold Master to simulate a typical federal workload	Built using Windows 7 Enterprise 32-bit operating system
FalconStor NSS Enterprise	6.15 (6164)
VMware View 4	4.5 Build 293049
VMware vSphere	ESXi Installable 4.1.0 Build 260247 VMware vCenter™ Management Server 4.1.0, Build 259021

Topology

The network topology for the reference architecture presented in this paper is shown in Figure 2. The tested configuration has a cluster of eight hosts. Four hosts have 47 virtual machines each, and the other four hosts have 48 virtual machines each, for a total of 380 virtual machines in the eight-host cluster.

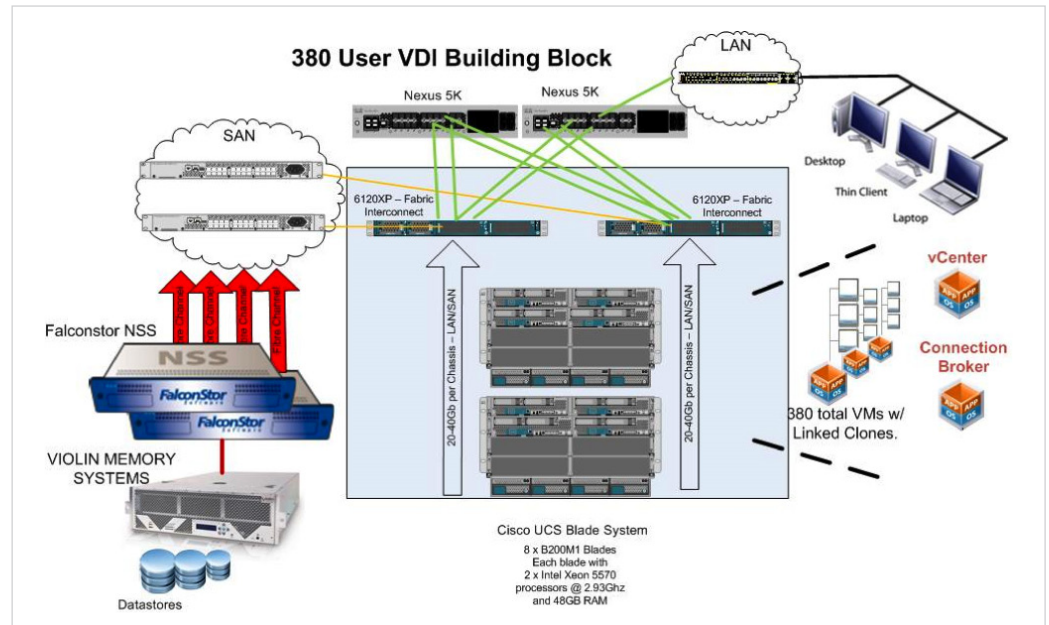


Figure 2. VDI reference architecture topology

About Violin Flash Memory Array

The flash memory array is the most critical hardware component in the reference architecture. Using a standard SAN with traditional hard disks will not achieve the same performance as the flash memory array. The Violin 3200 is a redundant, modular 3U memory array that scales from 1.3 to 10 TB SLC NAND flash memory and provides the industry's best price/performance attributes. It can scale to more than 140 TB in a rack with performance over 2 million IOPS. The enterprise-grade Violin 3200 includes hardware-based flash RAID across hot-swappable memory modules to provide robust data protection and spike-free latency of less than 100 microseconds (ms).

The key technology components of the Violin 3200 include:

- **Non-blocking flash RAID:** Flash blocks can fail, and bit error rates are much higher than on hard disk drive technology. While error checking and correction (ECC) algorithms provide sufficient data integrity for short term testing, RAID is required for long-term data integrity and retention. Violin's flash RAID guarantees that a flash memory erase, which requires 2 to 10 ms, will never impact a read or a write, providing significantly more predictable response time in an intermixed read/write workload than any other flash-based solution. While some flash storage solutions market their products as RAID-protected, several use RAID within a module, not across modules. RAID across modules is essential to prevent any single point of failure from causing data loss.
- **Distributed flash management:** In other flash memory products, garbage collection is performed by a processor. However, that processor may already be overworked by applications or other duties, such as RAID protection. Violin has implemented distributed garbage collection in hardware. This enables the system to achieve over 200 K sustained write IOPS with low latency. In comparison, most solid-state devices have a sustained write performance of between 1 K and 5 K IOPS.

About Cisco Unified Computing System

Cisco Unified Computing System (UCS) is a next-generation computing platform that unifies compute, network, and storage access. Optimized for virtual environments, UCS integrates a low-latency, lossless 10 Gb unified network fabric that combines network communication and storage data traffic into a single unified fabric.

Cisco UCS Manager

In the UCS platform, all resources participate in a unified management domain. The Cisco UCS Manager can manage up to 320 servers with thousands of virtual machines in a single domain. The combination of unified management with the simplicity of a unified fabric accelerates the delivery of new services simply, reliably, and securely.

Cisco Unified Fabric

In addition to simplified management, Cisco Unified Fabric supports a reduced cost model for VDI architectures that require high-speed network communication and Fibre Channel (FC) access. Traditional blade servers require chassis-based 10 Gb Ethernet and FC switches for every chassis. Because the management and interface mechanism is at the UCS Fabric Interconnect level, UCS does not require chassis-based switches, which reduces hardware costs.

About FalconStor Network Storage Server

The FalconStor Network Storage Server intelligent storage virtualization platform is built on an open architecture. It offers native support for high-speed FC access and 10Gb iSCSI connectivity, providing superior data throughput and IOPS. The FalconStor NSS architecture is designed for end-to-end performance. The hardware platform uses a Serial Attached SCSI (SAS) channel as the data exchange link between the controller and storage, providing data switching bandwidth of up to 72 gigabits per second (Gbps) for greatly increased transmission bandwidth, efficiency, and reliability. Features such as controller redundancy and intelligent load balancing further enhance the overall performance of the system and greatly increase link reliability.

Optimized for VMware Environments

FalconStor NSS technology is optimized for efficient VMware virtualization. It integrates with VMware infrastructure technology to provide optimal data services and continuous data and application availability. FalconStor snapshot agents create snapshots that are 100 percent transactionally consistent, providing instant recovery with complete data integrity. Support for VMware Site Recovery Manager facilitates automated failover of VMware environments between sites and simplifies VMware disaster recovery deployments. Physical-to-virtual recovery is also supported, meaning that physical systems can be recovered or re-created as virtual machines for multiple purposes, such as testing or development work.

Reference Architecture Performance Validation

Reference architecture testing focused on the following areas of virtual machine performance: boot time, provisioning time, and steady-state operation.

Testing Tools

The following tools were used to test performance of the reference architecture:

TOOL	DESCRIPTION
VMware Desktop Reference Architecture Workload Simulator (RAWC), version 1.1.3	This workload simulator has a set of randomly executed functions that perform operations on the master image and a variety of applications. For this testing, the RAWC was configured to launch applications every five seconds. Simulated tasks included typing 10 words per second with up to 400 words in a Microsoft Office Word document and browsing through 15 pages in an Adobe Portable Document Format (PDF) file, among others.
Fabric switches	Two fabric switches were used to test the reference architecture: <ul style="list-style-type: none">• Cisco MDS 9124 with 8x4 Gb ports• Brocade 300E with 8x8 Gb ports

Virtual Desktop Configuration and Workload Profile

Each virtual desktop was configured to simulate the requirements of a typical office productivity user in a federal agency. The virtual desktops were configured as follows:

- Windows 7 Enterprise 32-bit operating system
- 1 GB RAM
- 1 virtual CPU
- Folder redirection of My Documents, Desktop, App Data, and Favorites
- Authentication through Windows 2008 Active Directory

The following set of applications made up the workload used in the testing:

- 7zip
- Adobe Flash Player 10
- Adobe Reader 9.3.3
- Java 6, update 22
- Windows Internet Explorer 8
- Windows Media Player 11

- Microsoft Office Professional Plus 2007 (Excel, PowerPoint, and Word)
- VMware Tools
- VMware View Agent

For this testing, all remote access was turned off and the workload simulator was configured to log each user off after the testing was completed.

Test Procedures

Boot Time for 380 Virtual Machines

The boot time testing measured how long it took for a virtual machine to register as available in the VMware Connection Broker—meaning that the machine was ready to be used. The exact measurement started when the power-on command was sent for all virtual machines and ended when the last virtual machine was marked as available in the Connection Broker. The primary question was how long does it take for all 380 virtual machines to boot?

This boot testing was also designed to answer several performance questions about a single host with 48 virtual machines when all 48 machines are booting at the same time (a boot storm):

- What does host CPU utilization look like during a boot storm?
- What does host memory use look like during a boot storm?
- How much load is placed on the storage system during a boot storm?

Provisioning Time for 380 Virtual Machines

Provisioning time was measured from when the virtual machine pool was created to when the last virtual machine was marked as available in VMware View. The primary question for this testing was:

- How long does it take to provision 380 virtual machines using the design specified in the reference architecture?

This testing also provided performance data for CPU, memory, and storage system use on a single host when all 48 virtual machines are being provisioned at the same time.

Steady-State Operation

The steady-state operation testing measured performance of the following system components:

- Flash memory I/O throughput
- Active memory use
- CPU utilization

Test time was one hour, during which all 380 virtual machines logged in and performed various operations designed to simulate a typical user during the work day, including the following:

- Opening, editing, saving, and closing several Microsoft Office Word documents.
- Opening, editing, saving, and closing a Microsoft Office Excel spreadsheet.
- Opening and closing a Microsoft Office PowerPoint presentation.
- Opening and closing Windows Internet Explorer.
- Opening and closing Windows Media Player.
- Opening and browsing through an Adobe Acrobat PDF document.
- Compressing a set of files.
- Compiling a Java application.

This testing was designed to answer the following performance questions for a host with 48 virtual machines during steady-state operation:

- What is the average CPU utilization?
- What is the average memory use?
- How much load is placed on flash memory array?

It also answered the following questions about overall cluster performance during steady-state operation:

- What does CPU utilization look like for an eight-node cluster?
- How much memory is used on an eight-node cluster?

Test Results

Boot Time Test Results

It took only nine minutes to boot all 380 virtual machines from power on to available in the VMware Connection Broker.

Testing showed the following host performance characteristics during the nine-minute boot storm:

- CPU utilization hovered between 25 and 75 percent with several spikes to 100 percent. As soon as the boot storm passed, utilization dropped to below 25 percent.
- Active memory use never exceeded 35 GB. Total available memory was 48 GB.
- Flash memory storage I/O latency stayed between 1 and 17 milliseconds for the majority of the time, with several spikes up to 35 milliseconds.
- Storage throughput (the host communicating with the host bus adapter (HBA) stayed below 50,000 kilobytes per second (KBps), with a few spikes between 51,000 and 100,000 KBps and one spike between 101,000 and 150,000 KBps.

Overall, host performance during the boot storm showed plenty of headroom for other traffic.

Provisioning Time Test Results

It took two hours and eight minutes to provision all 380 virtual machines, or just over 190 virtual machines per hour.

In terms of host performance, testing showed the following performance characteristics while all 380 machines were being provisioned:

- CPU utilization hovered between 5 and 25 percent with several spikes between 26 and 65 percent.
- Active memory use never exceeded 2.1 GB. Total available memory was 48 GB.
- Flash memory storage I/O latency stayed between 0 and 5 milliseconds for the majority of the time, with several jumps to 9 milliseconds.
- Storage throughput (the host communicating with the HBA adapter) stayed below 15,000 KBps, with a few spikes between 16,000 and 25,000 KBps.

These results show that even while provisioning 48 virtual machines, the host had plenty of bandwidth for other tasks.

Steady-State Operation Test Results

Testing revealed that the reference architecture performs very well during steady-state operation while leaving plenty of headroom for peak loads and server failure. The following table summarizes average and maximum activity for the areas tested (storage I/O throughput, memory use, and CPU use for one host and the cluster).

AREA TESTED	AVERAGE	MAXIMUM	AVAILABLE
Flash memory storage array I/O throughput	48,000 KBps	151,000 KBps	200,000+ KBps
Host active memory use	15 GB	29 GB	48 GB
Host CPU utilization	41 percent	82 percent	100 percent
Cluster active memory use	285 GB	342 GB	384 GB
Cluster CPU utilization	52 percent	91 percent	100 percent

Flash Memory Storage Array I/O Performance

Testing showed that the steady-state activity did not put a significant load on the flash memory array, and the virtual machines experienced no performance degradation. In fact, the I/O rates never came close to the flash memory array’s upper limit of over 200,000 sustained write IOPS. As shown in Figure 3, I/O activity stayed consistently in the 25,000 to 50,000 KBps range for a host with 48 virtual machines. The peak shown here during steady state operation was primarily the result of the virtual machines launching video around the same time.

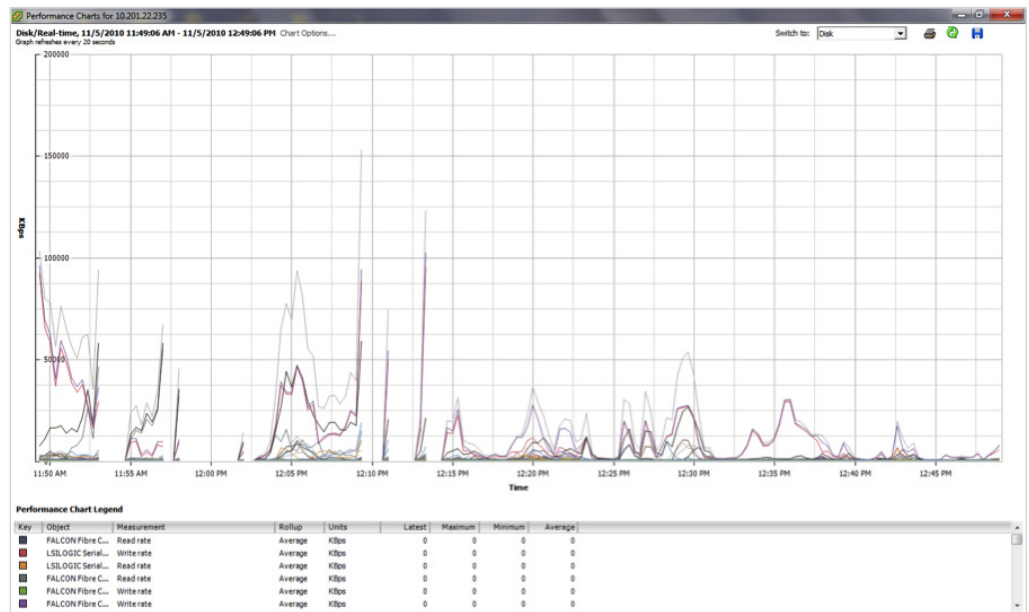


Figure 3. Flash memory array performance for a host with 48 virtual machines during one hour of steady-state operation

These findings indicate that it is possible to use the same flash memory array for three to four reference architecture building blocks without saturating the array. In other words, the flash memory array included in the architecture could reasonably support from 1,140 to 1,520 virtual machines. This scalability bodes well for federal agencies that want to move toward a VDI solution while keeping storage costs low.

Host Active Memory Performance

The host with 48 virtual machines showed no problems with memory use during the testing. Memory load was quite low, with most use ranging from 15 to 20 GB (Figure 4). This left over half of the total memory free.

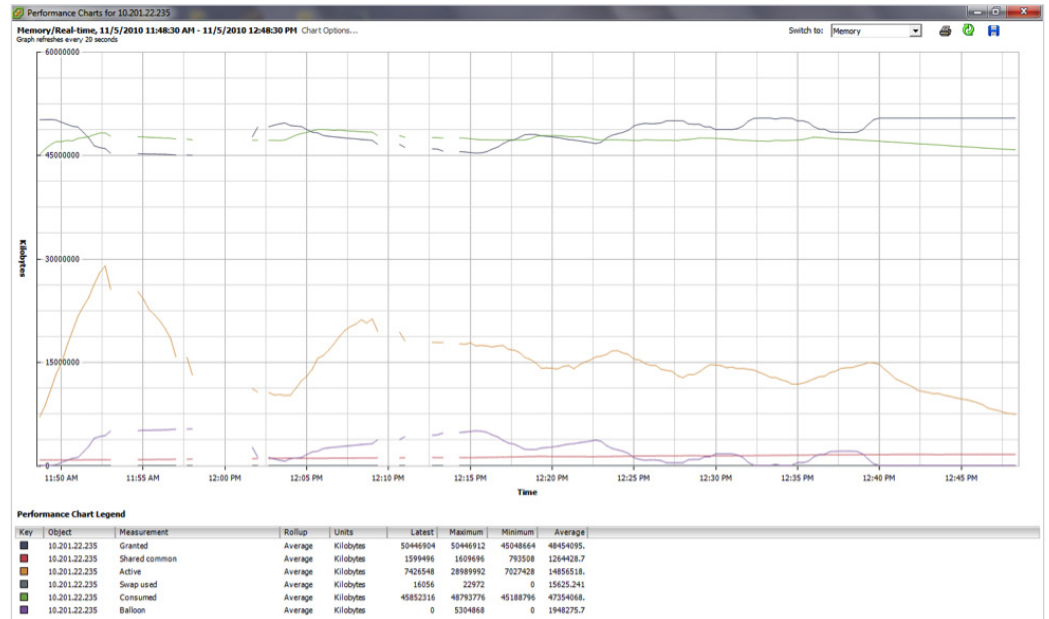


Figure 4. Memory performance for a host with 48 virtual machines during one hour of steady-state operation

These results show that the VDI architecture has ample memory to handle peak loads or memory-intensive activities. Federal workers who use virtual desktops based on this reference architecture can count on crisp, responsive applications.

Host CPU Performance

As with the disk and memory use, host CPU utilization was relatively low during the steady-state testing. Utilization fluctuated between 25 and 50 percent for most of the test period (Figure 5). This utilization pattern left plenty of headroom available for peak load or failover from another host.

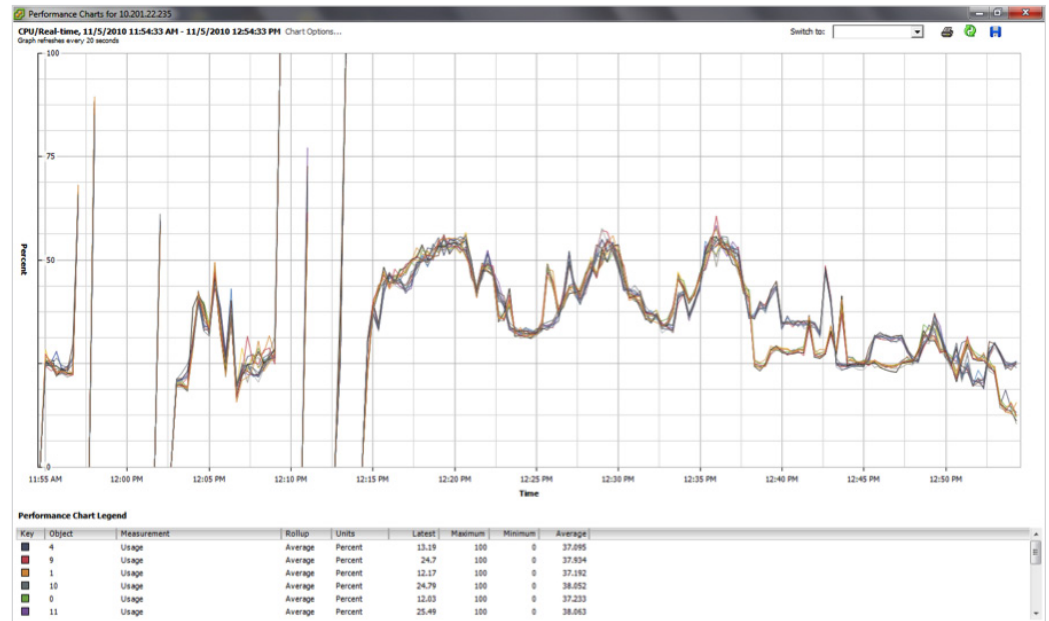


Figure 5. CPU performance for a host with 48 virtual machines during one hour of steady-state operation

In fact, two peak loads occurred during testing. As shown in Figure 5, host CPU utilization spiked to 100 percent twice during the hour-long test. These spikes occurred when the virtual machines were compiling a Java application, opening a large PDF, and compressing files. While these tasks are not as common for VDI environments, the host executed these peak loads without any degradation in performance across all 48 virtual machines.

Cluster CPU Performance

Overall CPU utilization for the cluster during steady-state operation averaged 52 percent. As shown in Figure 6, utilization never spiked to 100 percent, and for about half of the test period, it stayed at or below 50 percent. As with the host CPU utilization, the cluster maintained more than enough headroom to handle peak loads or failover situations.

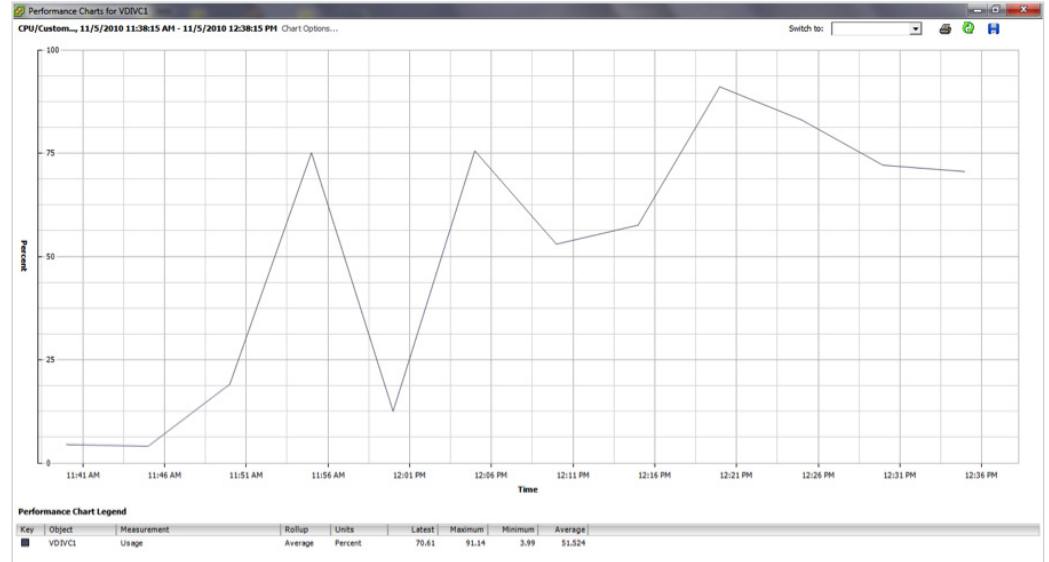


Figure 6. Cluster CPU utilization during one-hour steady-state operation testing

These results clearly demonstrate that the standard workload for 380 virtual machines did not put a significant load on the cluster’s CPU. In fact, the virtual machines experienced no performance degradation. For federal agencies, these findings indicate that a VDI environment configured like this one can easily provide virtual desktops to federal workers as a continuously available service.

Cluster Memory Performance

Overall memory performance showed no problems across the cluster. Average use was 285 GB, or 74 percent of total available memory. Use did not exceed 342 GB, or 89% of available memory. Also, as shown in Figure 7, memory use decreased significantly after about 45 minutes. This was because three of the most memory-intensive activities (Java compile, compress files, and open PDF) ended at about that time.

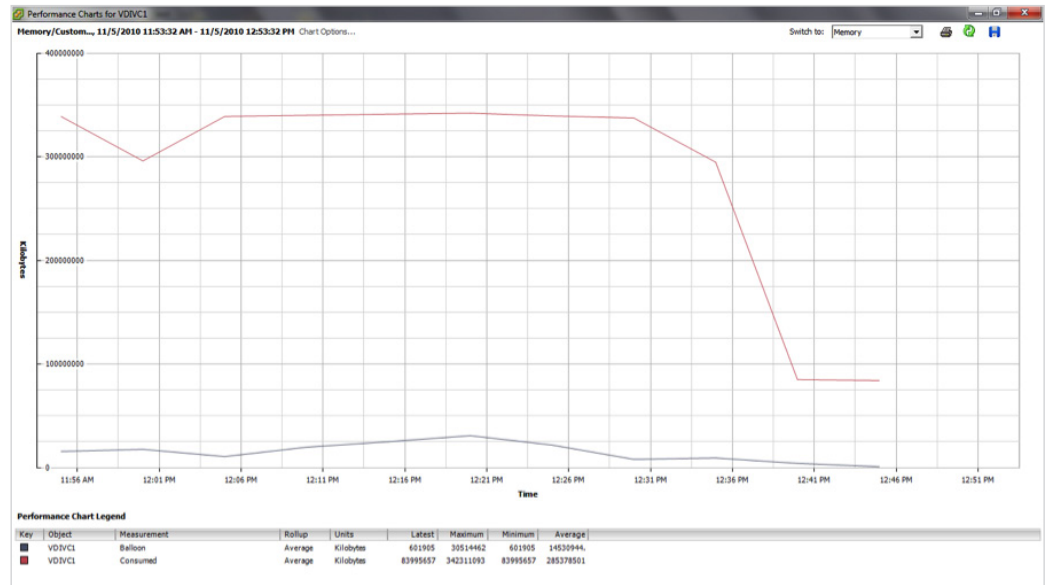


Figure 7. Cluster memory use during one-hour steady-state operation testing

Conclusion

The reference architecture presented in this paper offers federal agencies a flexible VDI solution that can satisfy the most common use cases for virtual desktops:

- For COOP and emergency preparedness, this VDI environment can easily provide virtual desktops to federal workers as a continuously available service. The flash memory storage capacity and building block approach lets IT departments cost-effectively scale the environment as needs expand. The CPU utilization pattern shown in the testing provides plenty of headroom for peak loads or server failure situations without performance degradation. And boot time testing confirms that even a boot storm, with hundreds of VMs coming up at the same time, did not stress the architecture or degrade performance.
- For training purposes, virtual machines can be quickly provisioned, used, and then deleted. The reference architecture has plenty of headroom for other tasks, even while hundreds of virtual machines are being provisioned, so provisioning and deleting machines for training purposes should not create a negative performance impact on other machines on the same host. Also, because training can be done using virtual desktops, federal agencies can reuse existing hardware. Both of these advantages bring cost savings in terms of time and money.
- For Windows 7 deployment, virtual machines can be used to rapidly pilot and test different configurations that comply with government IT directives. After the configuration is locked down, virtual desktops with Windows 7 can be easily deployed to federal workers.
- For work-at-a-distance scenarios, the memory performance shown in this VDI environment supports delivering virtual desktops across LAN and WAN links with excellent response times. Workers experience crisp application performance—even in degraded conditions.

VMware View is a trusted platform that provides a proven solution to the challenge of deploying and managing large numbers of user desktops while maintaining strict data security. With VMware View and this reference architecture, federal agencies can reduce IT costs, improve worker mobility and productivity, and comply with federal directives and guidelines.

Acknowledgements

VMware would like to acknowledge the Force 3 Customer Innovation Center for its contributions to this paper, help with the test setup, analysis, and lab infrastructure, and for building the joint solution.

The Force 3 Customer Innovation Center is a hands-on, multi-technology lab environment where a team of Force 3 engineers, collaborating with different vendor and customer partners, develops and rigorously tests solutions that are designed to meet an organization's specific objectives and goals. The Customer Innovation Center was used in the testing phase of this VDI solution to verify the criteria and benchmarks that are set forth in the reference architecture. Force 3 also provides a robust set of design and implementation services for VDI solutions based on VMware View.

For More Information

VMware View

<http://www.vmware.com/products/view/>

VMware vSphere

<http://www.vmware.com/products/vsphere/>

vmware®



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

Copyright © 2011 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark 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. Item No: VMW_11Q1_WP_FEDMKTSOLUTION_USLET_EN