VMware View

A Guide to Large-scale Enterprise VMware View 3 and VMware View 4 Deployments

REFERENCE ARCHITECTURE

vmware®

Contents

Overview

VMware® View is a robust desktop virtualization solution that allows IT organizations to reap the benefits of traditional server-based computing without the challenges that often accompany server-based solutions. By leveraging the benefits and advantages of VMware View, IT organizations can take the first steps toward transitioning away from the era of distributed PC computing toward Cloud Computing and the delivery of user desktops as a service.

Built on VMware's industry-leading virtualization platform, VMware View 3 is a Universal Client solution that lets you manage operating systems, hardware, applications and users independently of each other, wherever they may reside. VMware View streamlines desktop and application management, reduces costs and increases data security through centralization, resulting in greater user flexibility and IT control. VMware View enables customers to extend the value of VMware Infrastructure and virtual desktop infrastructure (VDI) environments to encompass not only desktops in the datacenter but also applications and the delivery of these environments securely to remote clients, online or off, anywhere.

VMware View integrates with almost every system and infrastructure component of an organizations environment. Implementing a standardized solution drives down the total cost of ownership (TCO) and helps minimize the complexity and unpredictability of a customized solution. By implementing a standardized solution that integrates with existing established IT processes and procedures requiring minimal change. IT organizations can build the foundation on which they can easily and affectively adapt to changing user requirements and technology trends.

VMware View Reference Architectures

VMware View reference architectures are built and validated by VMware and supporting partners. They are designed to address common use cases, such as enterprise desktop replacement, remote access, business process outsourcing, and disaster recovery, among others. Each reference architecture describes in detail the environment and workload used to simulate realistic usage.

The guides are intended to help customers—IT architects, consultants, and administrators—involved in the early phases of planning, design, and deployment of VMware View-based solutions. The intention is to provide a standard, repeatable, scalable design that easily can be adapted to specific environments and customer requirements.

This reference architecture's building block approach uses common components to minimize support costs and deployment risks during the planning of large-scale VMware View Manager 3 based deployments. It is based on collected information and experiences from some of the largest VMware View deployments in production today, drawing on existing best practices and deployment guides pertinent to many of the individual specific components, tested and validated in the field and described in detail. Some key features that can help an organization get started quickly with a solution that integrates easily into existing IT processes and procedures include:

- *Standardized, validated, repeatable components.*
- *Scalable designs that allow room for future growth.*

- ***Validated and tested designs that reduce implementation and operational risks.***
- ***Quick implementation, reduced costs, and minimized risk.***

Goal

This reference architecture provides IT architects, consultants, and partners a proven and tested architecture for enterprise desktop deployments. The goal was to design and validate a standardized building block, consisting of components capable of supporting at least 1,000 virtual desktops. The overall design also included the infrastructure components needed to integrate five building blocks, to support a 5,000-user VMware View pod that can be managed as a single entity.

The architecture uses common components and a standardized design to reduce the overall cost of implementation and management. All the infrastructure components used to validate the reference architecture are interchangeable, so anyone can use components from their vendor of choice to incorporate unique features that enhance the value of the overall solution.

The VMware View reference architecture addresses the following commonly required aspects of an enterprise class solution.

Standardization

By using a building block approach and common components, the VMware View Reference Architecture offers IT organizations the ability to implement a predictable, familiar solution.

Repeatability

The building block approach is designed to be repeatable across lines of business and departments.

Scalability

The building block approach allows organizations to scale out to meet growing demand for thousands of users predictably.

Availability

Each layer of the VMware View Reference Architecture is designed to offer the highest level of availability and resiliency.

Security

VMware View Reference Architecture takes security into account in each layer to offer a secure solution.

Integration

The VMware View Reference Architecture addresses the integration with components commonly found in today's enterprise.

This VMware View Reference Architecture also references and includes several deployment guides that provide detailed instructions on deploying several of the components used to validate the architecture.

Design Approach

Each VMware View reference architecture leverages basic design principles and best practices. Using a building block approach allows for the flexibility of creating a comprehensive virtual desktop infrastructure that performs or exceeds desired goals and functionality while maintaining a logical, straightforward architecture..

The VMware View reference architecture begins with the Client Access Devices layer and continues through the Session Management layer (see Figure 1). This approach provides a clear definition of services necessary to allow each functional area to be defined independently from the others, while still providing a cohesive structure for addressing the interdependency of all solution components.

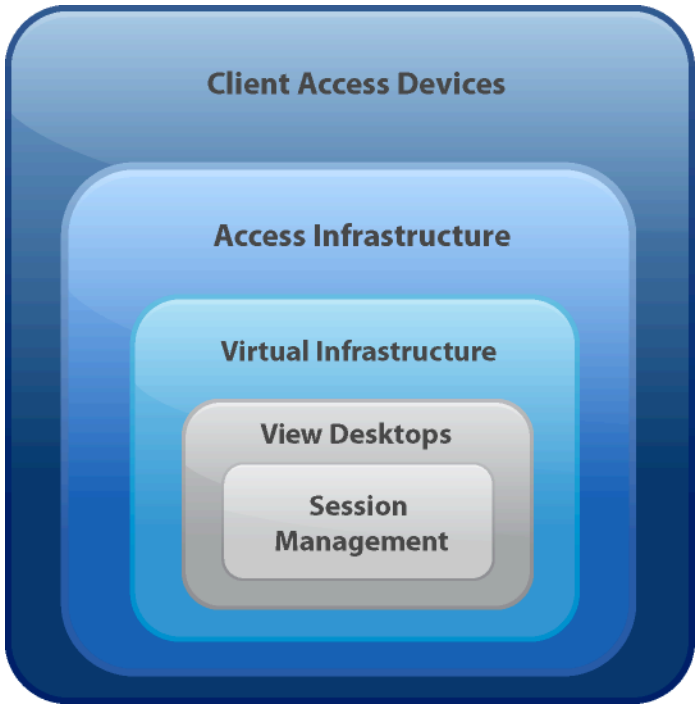


Figure 1. Layered VMware View Architecture

VMware View Components

Client Access Devices

This layer includes the physical devices that provide users access to their virtual desktop. Sub-layers include:

- *Client device*
- *Client software*
- *Peripheral support*

Access Infrastructure

Networking and connectivity components designed to facilitate client communication are addressed here. Sub-layers include:

- *Local and wide area networking*
- *VMware View Manager*
- *Network load balancing and optimization*

Virtual Infrastructure

This layer defines the components and technology used to host the virtual desktop operating systems and supporting VMware View Infrastructure. Sub-layers include:

- *Host infrastructure*
- *Virtual and physical network infrastructure*
- *Storage infrastructure*

View Desktops

This layer defines the components and configuration of the virtual machines assigned to and accessed by users. Sub-layers include:

- *Virtual hardware configuration*
- *Virtual desktop guest operating system*
- *Application deployment methodology*
- *View Composer configurations*

Session Management

This layer defines the deployment and management of a large number of virtual desktops to an end-user community. It also includes the integration with existing desktop infrastructure services, such as Active Directory, for maintaining user and computer accounts. Components and sub-layers here control user authentication, virtual desktop provisioning, and deployment as well as user entitlement to desktop resource. Sub-layers include:

- *Desktop provisioning and pool management*
- *Session monitoring*
- *Active Directory integration*
- *Virtual printing*

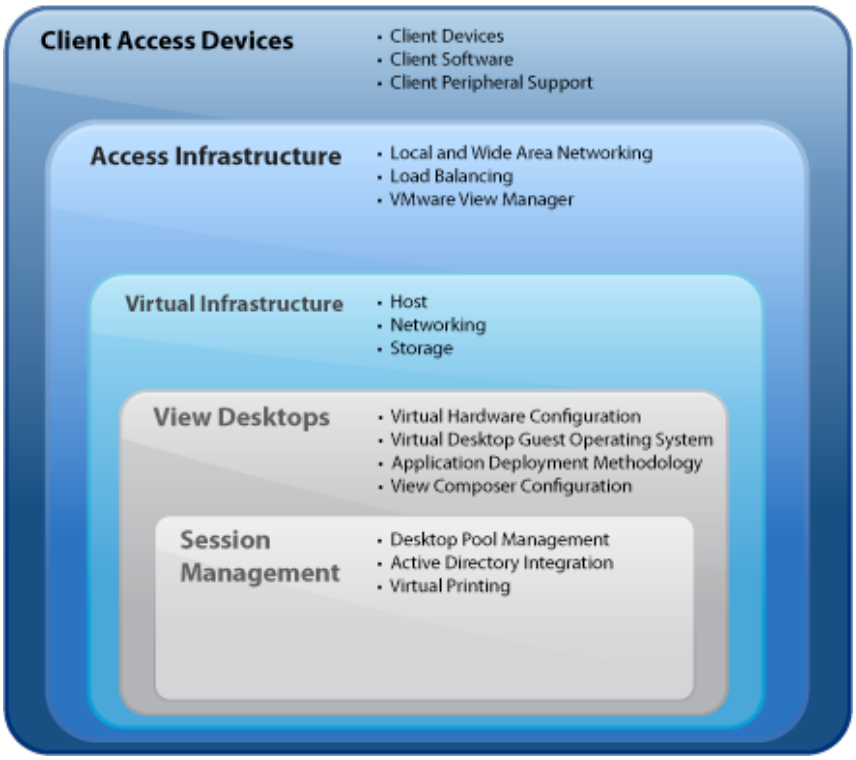


Figure 2. VMware View Component Sub-layers

VMware View Reference Architecture Components

Client Access Devices

The client access device layer is comprised of the hardware and software components needed to deliver a PC-like experience. The process for choosing the appropriate client device varies from deployment to deployment; mixed client environments are common in VMware View deployments. In most cases, users are segmented based on their needs and requirements during the planning and design phases, and business requirements and goals are also taken into consideration and mapped to the needs of the user segments.

For example, an organization might have PCs that are on a staggered depreciation schedule. Depreciated assets can be replaced by thin client devices right away, but assets that have not fully depreciated are often converted into unmanaged end-points, typically by converting them to PXE-booted clients using a Linux-based solution. An alternative would be to tightly lock down the currently installed Windows OS and repurpose them as-is. Either approach can offer the flexibility to gain the highest return on PC hardware investment. Some key considerations for an IT organization during this process are:

- ***Will the client end point fulfill user requirements?***
- ***Do reduced management benefits balance the effort to convert existing PCs to repurposed PCs?***
- ***Are there any licensing benefits to keeping the current client end points?***

VMware View supports a wide range of client end point devices. This offers IT organizations a great deal of flexibility and deployment options when rolling out a VMware View-based solution. Typical client devices include:

Physical PCs

Using the VMware View Client, users can easily access their virtual desktop from any standard Windows-based PC from within the enterprise network or, if given access, from a home PC.

Repurposed PCs

It is not uncommon for an IT organization to repurpose PCs as VMware View Universal Clients. In some cases, the existing Windows OS is tightly locked down, so only the VMware View Client for Windows can be run to access a virtual desktop. Some organizations convert the PCs into PXE boot clients that use a minimal version of Linux and VMware View Web Access to access the virtual desktop instances.

Thin Clients

VMware View supports a wide array of Thin Client devices. The most currently qualified devices are listed in the VMware View Thin Client Compatibility Guide.

Mobile User Devices

Mobile users typically have laptops as their client devices, and they often have limited or no network connectivity. VMware View offers a unique way to address such users, with an experimental feature called Offline Desktop. Using Offline Desktop, an entitled user can check a VMware View virtual desktop out to the laptop device and use it offline. Once network connectivity is restored, the Offline Desktop synchronizes the changes in the background. Alternatively, the user can initiate a check-in that synchronizes the virtual desktop with the virtual datacenter.

Access Infrastructure

The access infrastructure provides network connectivity between client access devices and the virtual infrastructure that hosts the virtual desktop sessions, including the components that manage, or broker, user connection requests to entitled desktops. This is a critical layer with respect to the overall user experience: A properly designed, sized, and functioning access infrastructure is vital to a successful VMware View implementation. Undersized or underperforming access infrastructures can result in poor performance and a less than satisfactory user experience.

Local and Wide Area Networking

Due to its reliance on network communication, a VMware View session is affected by the capabilities of the underlying network infrastructure more than a traditional PC. The solution covered here focuses on large-scale, LAN-based deployments.

Remote Desktop Protocol Considerations

The display protocol most commonly used to access a VMware View 3 environment is the Microsoft Remote Desktop Protocol (RDP). As a starting point, to maximize use of available

network bandwidth and enhance each user's experience, IT organizations should follow the recommendations in the VMware View Windows XP Deployment Guide.

The VMware View Client also allows a large number of customized settings. These settings can be centrally controlled and managed through the use of Microsoft group policy objects, and are covered in detail in the VMware publication, VMware View Manager Installation and Administration Guide, under "VMware View Client Advanced Active Directory RDP Settings".

In addition to RDP, VMware View also supports protocols provided by thin client manufacturers, such as the Sun Microsystems Appliance Link Protocol™ (ALP) used in Sun Ray™ thin client implementations, and Pano Logic's Console Direct.

Network Layer Performance Recommendations

To achieve a user experience similar to that of a traditional PC, the VMware® View Manager 3 environment requires an optimal network infrastructure, so both network bandwidth and latency should be taken into consideration in the design phase. Studies have shown that the minimum bandwidth for a useable RDP Session is approximately 30Kbps. Streaming multimedia content using multimedia redirection increases bandwidth requirements.

The amount of bandwidth needed per virtual desktop user varies, depending on the user workload and how active the use is. As a starting point, 100–150Kbps is a good rule of thumb to use until environment-specific usage patterns can be determined. This range helps account for the peak usage of a typical VMware View user. As noted above, multimedia usage increases the amount of bandwidth needed, but it is content-specific and typically not needed on a regular basis.

Even more critical than bandwidth is network latency, an expression of how much time it takes for a packet of data to get from one designated point to another. It is unavoidable in a network environment, especially at long distances. Transmission and equipment delays typically create latencies that may be as low as 1 ms on Local Area Networks (LAN), and are typically 50–100 ms for US domestic links on Wide Area Networks (WAN). For international links, latencies can range from 100-200 ms, sometimes higher, while multi-hop satellite links can produce delays of over 2,000 ms.

High network latency can contribute to a slow refresh of the desktop session and have an adverse impact on the user experience. For simple tasks such as typing, cursor motion, and mouse selection, response time should be less than 150 ms with Microsoft RDP. As latency approaches 200 ms, the user experience is often impacted even further. It is often difficult to categorize how remote offices or users will experience a VMware View desktop under these conditions. Third-party solutions, such as Sun Microsystems Sun Ray thin clients and WAN Optimization solutions from Cisco Systems, have been used successfully in combination with Microsoft RDP to overcome limitations on high-latency networks. Both these solutions integrate tightly with a VMware View solution. VMware recommends careful monitoring of both local and wide area connectivity during and after VMware View implementations.

From the VMware ESX server, it is also important to consider that, in addition to the display traffic, each virtual desktop also needs adequate speed for typical data traffic as well as for e-mail, file transfers and web browsing.

Virtual Desktop Management Services

VMware View Manager is a primary component of VMware View. The main service that View Manager provides for the access layer is brokering incoming client requests to virtual desktop instances; that is, it helps to direct entitled users to their virtual desktops. In addition, VMware View Manager can also provide a common access and control point for other services that are available to desktop users, such as Microsoft Terminal Services, Blade PCs, and Desktop PCs.

VMware View Manager includes advanced functions for provisioning and managing both new and existing virtual machines. These include workflow controls for provisioning new desktops and power control policies that can suspend and resume virtual desktops as desired. A large-scale implementation of VMware View requires such policy-based controls to reclaim unused memory and CPU resources when virtual desktop sessions are terminated or idle for long periods of time.

VMware View Manager also:

- *Validates the user name and provides a connection for that user.*
- *Provides the ability for the user to access multiple virtual desktop pools. If the user is permitted to access a variety of pools, the desktop manager prompts the user to select a pool at login time.*
- *Monitors the activity level of a given virtual machine and set status to active or inactive.*
- *Automatically provisions new virtual desktops to maintain availability levels.*
- *Handles reassignment of a virtual desktop when a user disconnects.*

VMware View Manager

The VMware View Manager integrates seamlessly with VMware Infrastructure and Microsoft Active Directory. VMware View Manger works in conjunction with VMware vCenter to provide advanced virtual desktop management capabilities, such as automatic suspend and resume of virtual desktops and the ability to deploy persistent and non-persistent desktop pools.

The VMware View installation and configuration consists of the following components:

VMware View Connection Server

The View Connection Server is a full-featured connection broker.

VMware View Security Server

The Security Server provides secure access to VMware View sessions over unsecured WAN- and Internet-based networks.

VMware View Agent

This program runs on each virtual machine and is used for session management and single sign-on purposes.

VMware View Client

This program runs on a Windows PC (acting as a client device) as a native application and allows users to connect to their virtual desktops through the VMware View Connection Server.

VMware View Portal

This component provides a web browser user interface similar to the View Client.

VMware View Components

Typical VMware View deployments consist of five common components, illustrated in Figure 3, which represents a typical architecture. It includes VMware View components as well as other components commonly integrated with VMware View.

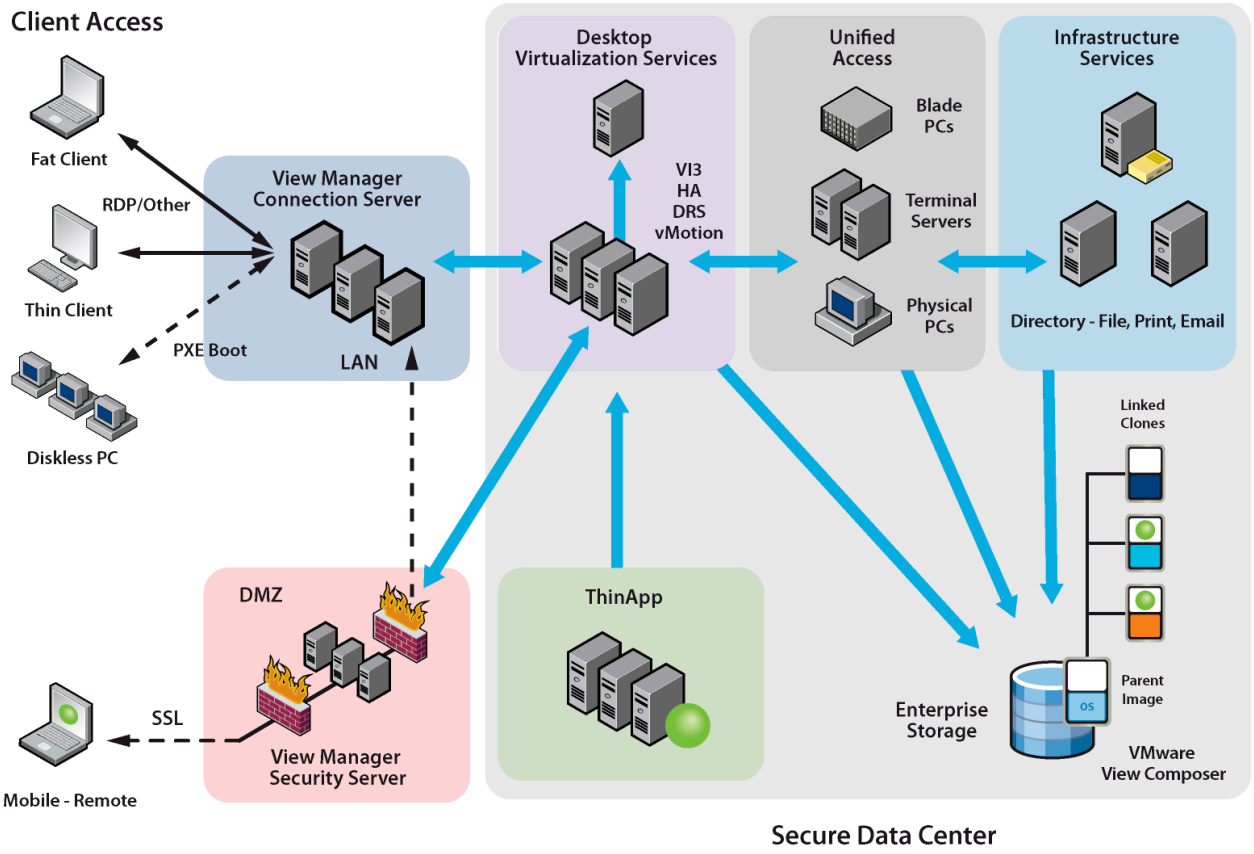


Figure 3. High-level VMware View Architecture

VMware View Manager Connection Servers

The Connection Servers act as desktop managers, providing user authentication for virtual desktops and directing incoming remote desktop requests to the appropriate virtual desktop. They are installed either as standalone servers or as replicas: the first deployed Connection Server is the standalone, all others act as replicas. Replicas, used for scaling and load balancing, reference the first connection server to replicate the Active Directory for Application Mode (ADAM) information. Both standalone and replica instances operate as fully functional VMware View Manager Connection Servers, but load balancing and higher availability through replication help them to optimize utilization resource. In addition, each system runs the VMware View Manager administrator web service, the primary mechanism for

configuring VMware View Manager, managing user entitlements, and provisioning virtual desktops. These systems are configured to manage internal connection requests only.

VMware View Manager Security Servers

VMware View Manager Security Servers run a subset of the VMware View Manager connection server functions deployed within the DMZ to allow secure access to virtual desktops from the Internet. Each system acts as a proxy host for connections inside the trusted network. This design provides an additional layer of security by shielding the connection broker server from the public-facing Internet and forcing all unprotected session requests through the security servers. This ensures that only authenticated users can connect to the internal network from the Internet.

This architecture also requires a few ports to be opened on the outer firewall to allow for connectivity between external clients and VMware View Manager security servers inside the DMZ. Specific firewall rules also require a minimal number of ports from the inner firewall allow for communication between the VMware View Manager Security Servers and the VMware View Connection Servers in the internal network.

VMware View Load Balancing

The primary purpose of load balancing in a VMware View architecture is to optimize performance by distributing desktop sessions evenly across all available VMware View Manager connection servers. It also improves serviceability and availability by directing requests away from servers that are unavailable, improves scalability by distributing connection requests automatically to new resources as they are added to the VMware View environment.

Several approaches are available. For example, round-robin DNS, while technically the simplest load balancing solution to implement, has a significant disadvantage from a failover perspective: if a server fails, it must be removed from the DNS list of records corresponding to the load-balanced domain name. Another issue with a round-robin DNS approach arises in the remote-access use case, where VMware View clients are accessing their virtual desktops across the Internet through VMware View Security Servers. In this case, the responses of the master DNS server are cached in upstream DNS servers, and it can take several hours for a DNS name deletion to replicate to all Internet DNS servers. When a server is out of service, client connections can fail if they are directed to it during the time it takes for the cached record to expire across the Internet DNS servers.

Support for a redundancy and failover mechanism, typically at the network level, prevents the load balancer from becoming a single point of failure. For example, the Virtual Router Redundancy Protocol (VRRP) communicates with the load balancer to add redundancy and failover capability. If the main load balancer fails, another load balancer in the group automatically starts handling connections.

To provide fault tolerance, a load balancing solution must be able to remove failed VMware View server nodes from the load balancing group. How failed nodes are detected may vary, but regardless of the method used to remove or blacklist an unresponsive server, the solution must ensure that new, incoming sessions are not directed to the unresponsive server. If a VMware View server fails or becomes unresponsive during an active session, users do not lose data. Instead, desktop states are preserved in the virtual desktop so that, when users reconnect to a

different VMware View connection server in the group, their desktop sessions resume from where they were when the failure occurred. For more information and examples, the VMware View Load Balancing Guide.

Session Management

The last layer in the design consists of infrastructure components that provide a flexible, dynamic environment for managing access, user sessions, and desktops. This layer supports:

- *Desktop and Pool Management*
- *Session Monitoring*
- *Active Directory Integration*

Desktop and Pool Management

Virtual Desktops are created and deployed as needed through the use of Desktop Pools. These pools are managed through VMware View Manager, which provides integrated individual and desktop pool management capabilities for the following types of desktops and pools:

Individual Desktops

Virtual machines, Personal Computers, or Blade PCs available through VMware View Manager. The pool manager can control the power state of these virtual desktops. Users with the proper entitlements can check their virtual desktops out for offline desktop use.

Automated Desktop Pools

Automated desktop pools are virtual machine-based desktops that are automatically provisioned and customized by VMware View Manager. They can be deployed to be persistent or non-persistent. Advanced settings are also available to allow you to create a much more dynamic desktop environment by giving the desktop administrator more granular control over the pool. These settings include:

- *Minimum*

  The minimum number of virtual desktops to be created when the pool is first created. The pool manager continues to create virtual desktops until the minimum number has been reached. This process ensures that a pool is appropriately sized when a user population is moved to VMware View Manager.

- *Maximum*

  The maximum number of virtual desktops that can exist in the pool. Use this parameter to limit the number of virtual desktops in the pool to avoid overusing available resources.

- *Available*

  The number of virtual desktops that are available for immediate use. For persistent pools (described below), this parameter relates only to the unassigned virtual desktops, to ensure that the pool manager creates enough virtual desktops in advance to handle demand. The number should be higher for more dynamic environments. When a pool does not contain enough virtual desktops, the manager provisions new virtual desktops from the designated template. These virtual desktops are automatically customized, named, and become joined to the Active Directory.

Manual Desktop Pools

Manual desktop pools are pools created from existing Virtual Machines, PCs blade PCs. Virtual machines can be managed by vCenter or not managed. Properly entitled users may also check their virtual machine-based desktops out for offline use.

Microsoft Terminal Services Desktop Pool

With this type of pool, Terminal Services sessions can be managed by VMware View Manager and provided to VMware View users.

Desktop Persistence

Automated and manual desktop pools support two types of desktop persistence. Persistent desktops are assigned to individual users and the desktop stays assigned to that user until an administrator makes a change. Properly entitled users may also check their desktops out for offline use. This type of pool is best for users who want to customize their desktops by installing additional applications and storing local data. Non-persistent desktops are allocated to users temporarily and used only for the current session. Once the user has logged off, the desktop goes back into the pool and becomes available for the next user. This type of pool should be used where a clean machine is needed for each user session or in highly controlled environments where there is no requirement for customization to be stored on the virtual desktop.

VMware View Manager also provides a set of power management polices that can be leveraged to further increase the dynamic nature of a VMware View solution. This gives administrators more control over the virtual machine behavior. Virtual machines that are idle and still consuming resources can be put into a suspended or powered off state, freeing up resources for active users. Power control polices can be applied to virtual machine-based Individual desktops, automated desktop pools and manual desktop pools with the following power polices:

- *Remain on*

  Once started, VMware View Manager will not power the machine down. If a virtual desktop is powered down; for example using the VMware vCenter client, VMware View Manager automatically starts it when needed.

- *Always powered on*

  VMware View Manager ensures that any virtual desktop with this policy applied is powered on all the time. If a virtual desktop is powered down, VMware View Manager immediately powers it up again.

- *Suspend when not in use*

  If a virtual desktop is not required, it is suspended. This policy is applied to individual and assigned persistent virtual desktops when the user logs off. It is also applied to non-persistent virtual desktops when there are too many available virtual desktops. For example, this can be triggered by a virtual desktop being returned to the pool when a user has logged off.

- *Power off when not in use*

  If a virtual desktop is not required, it is powered off. This is just like the "Suspend when not in use" policy, except that the virtual desktop is completely powered off.

Virtual Disk Management

VMware View introduces a new paradigm for managing virtual disks in large-scale environments. VMware View Composer provides the capability to create desktop images rapidly from a parent, or standard, virtual machine image. In addition to providing the capability of creating desktop images rapidly, VMware View Composer also reduces the total amount of storage required to deploy virtual desktop images (see Figure 4). By leveraging linked clones, it introduces a streamlined process for upgrading patches across multiple desktops by simply applying the patch to the parent image and recomposing the linked clones.

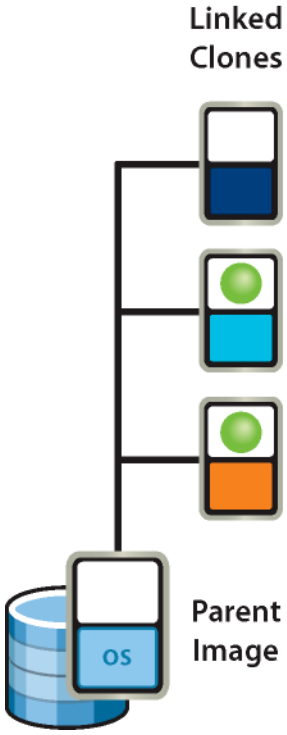


Figure 4: Parent Image with Linked Clones

VMware View Composer also provides the ability to separate user data and profile settings, which allows software updates and patches to be applied to the parent image and inherited by the linked clones (see Figure 5). After a linked clone has been updated, the user's personal settings from the user data disk are also applied to the updated image.

Existing images can be recomposed on an individual basis or all at once, instantly making the new updates available. VMware View Composer also supports taking additional snap shots of the parent image before applying new patches or software updates. This provides a fall-back mechanism in case a problem occurs. Administrators can instantly redirect users back to the previous working snapshot.

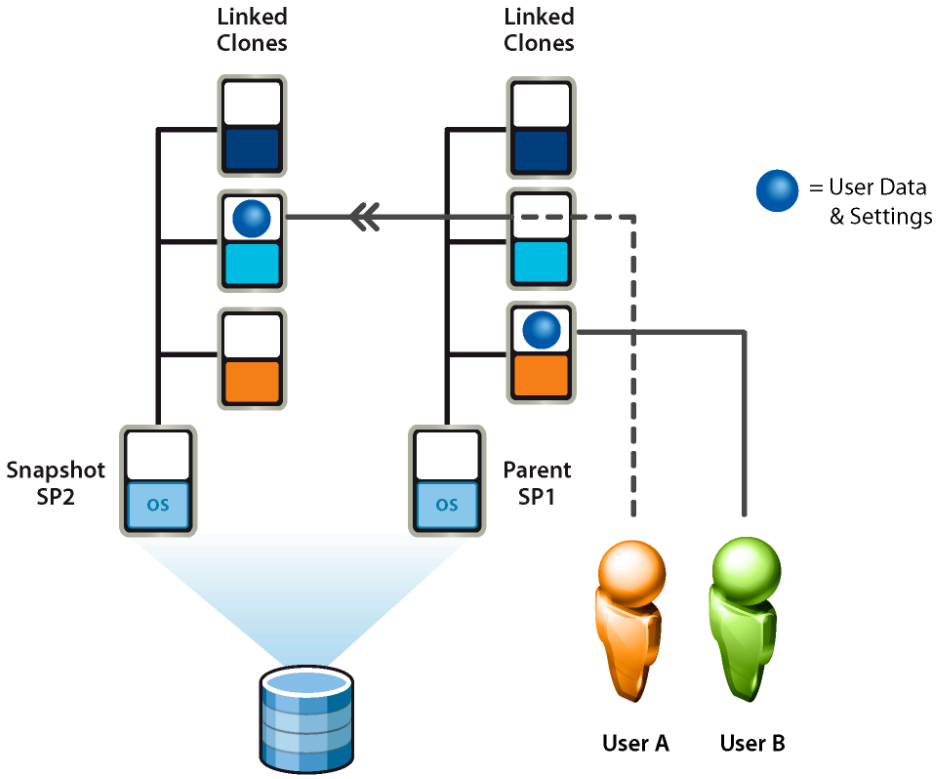
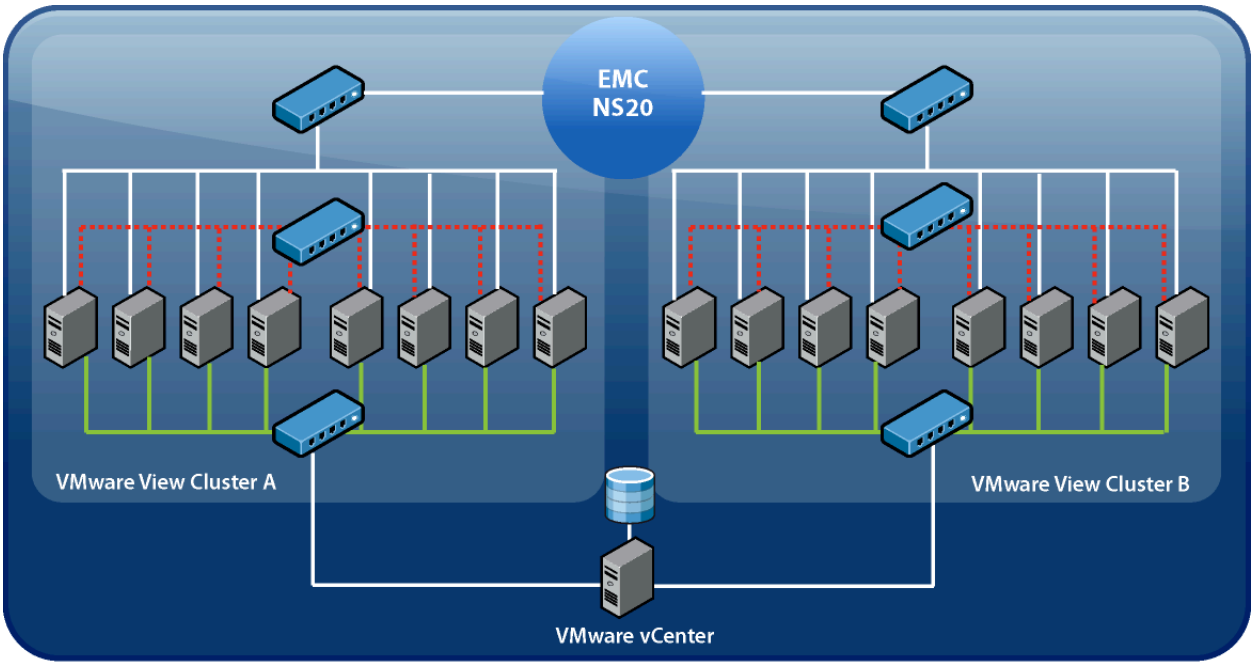


Figure 5: Upgrading from SP1 to SP2

Because VMware View Manager supports a variety of back ends, such as VMware View virtual desktops, Microsoft Terminal Services, Blade PCs, and ordinary PCs, it is recommended that a robust profile management solution be implemented. Profile management solutions such as RTO Virtual Profiles or Appsense can work in place of, or in conjunction with, a VMware View Composer user data disk. Profile management helps to ensure that personal settings will always be available to users who are entitled to multiple back-end resources, regardless of the system they are accessing. Profile management solutions also help to reduce logon and logoff times and to ensure profile integrity.

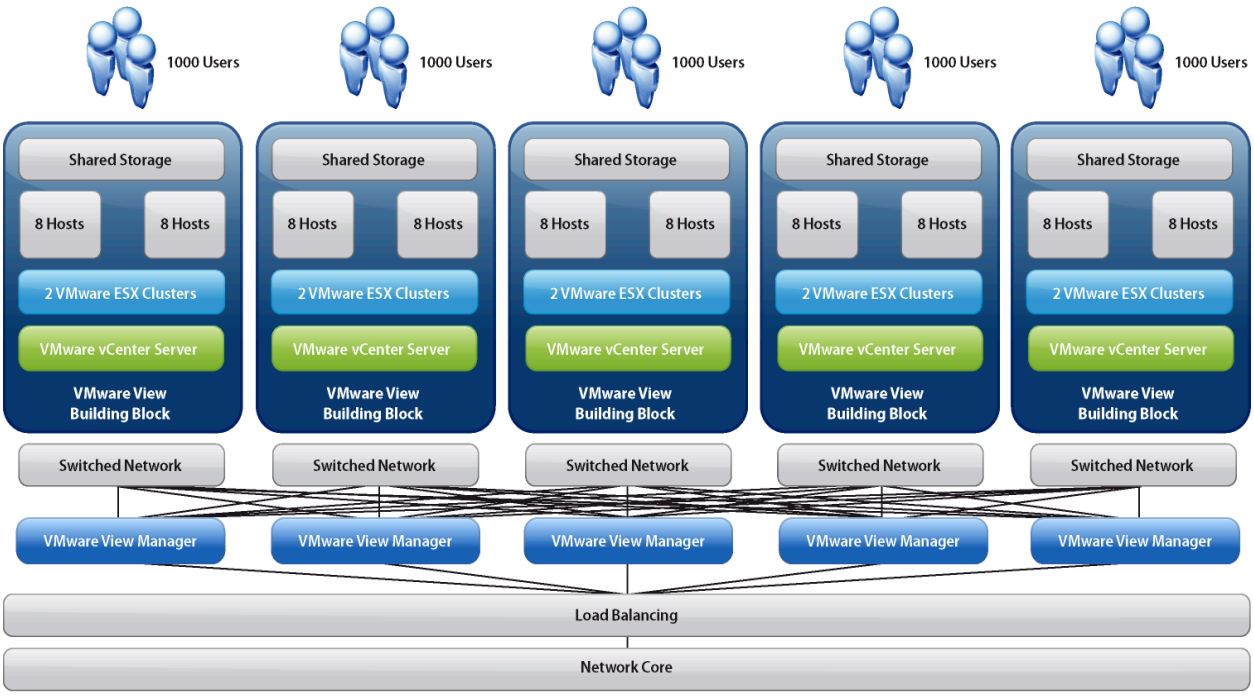
VMware View Reference Architecture Design

For this reference architecture, we designed and tested a standardized, building block-based solution capable of supporting at least 1,000 virtual desktops (see Figure 6), including the typical infrastructure components needed to integrate five building blocks of 1,000 virtual desktops each into a 5,000-user POD that can be managed as a single entity (see Figures 6 and 7). This architecture uses common components and a standardized design across the building blocks to reduce the overall cost of implementing and managing the solution. All the physical infrastructure components used to validate this reference architecture are interchangeable. This means customers can use their vendor of choice for any physical component of the architecture, including the network, storage, and server components. Various vendors might offer or include unique features that further enhance the value of the overall VMware View offering for a particular enterprise.



VMware View Building Block

Figure 6: VMware View 1,000-user Building Block



VMware View 5000 User Pod

Figure 7: VMware View 5,000 User Pod

This reference architecture focuses on enterprise desktop environments and targets larger desktop deployments commonly found in campus environments. It is intended to be a general guide that addresses common design questions and should be used as a starting point or reference when designing a particular VMware View solution. The design is general enough that it can easily be adapted to meet the specific needs and requirements of a wide range of IT organizations.

Validation Methodology

When validating VMware View reference architecture designs, it is important to simulate a real world environment as closely as possible. For this validation, we built and validated each component of the virtual infrastructure needed for one 1,000-user building block using a simulated workload. We also implemented the networking and load balancing components of the access infrastructure needed to support a 5,000-user VMware View POD. Figure 8 provides a high-level overview of the components used during this validation.

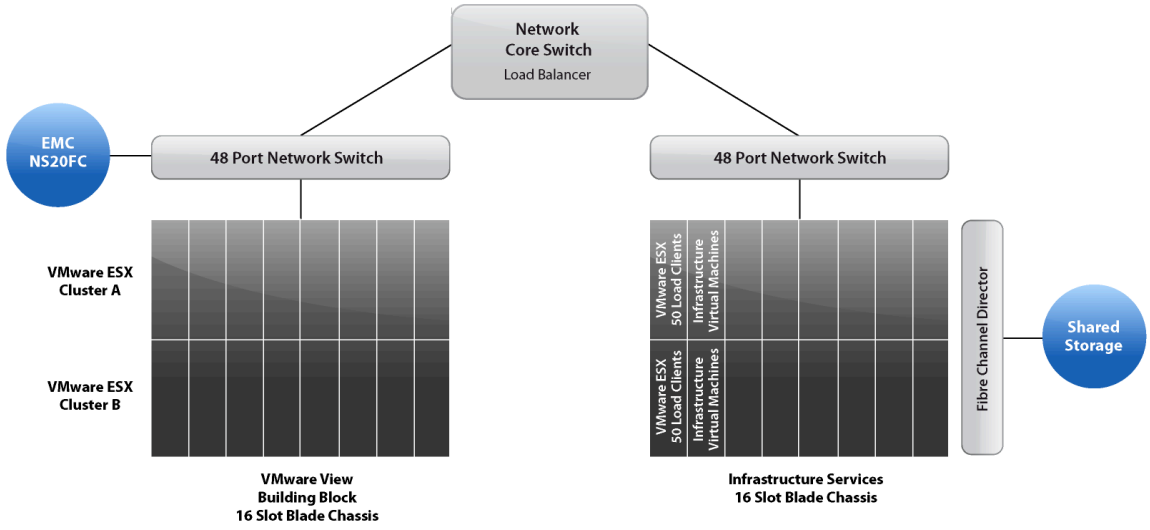


Figure 8: VMware View Reference Architecture Lab Overview

Testing was conducted in two phases. In the first phase, desktop pools were created provisioning the virtual machines. Each pool was created manually, just as it typically would be created in a normal environment. During this phase, the time to provision each pool was measured to provide a sample of the average time to deploy pools using different types of virtual disk management tools.

We used several different types of pools and clones and aligned this with how a typical enterprise might also segment their user population. For example, Cluster A primarily catered more to back office type workers, tend to be less active overall as they are more mobile, on flexible work schedules, or are coming and going from meetings. These users also might warrant a more caution regarding sensitivity to data or present other requirements that could justify a more static virtual desktop. Cluster B catered more toward task-oriented workers, who follow a more predictable work schedule and tend to be more consistent in the total amount of time spent actively using their virtual desktops.

The second phase of the validation included session establishment, logon, and execution of a workload. This phase was conducted by manually powering on load clients randomly. Each client established individual VMware View session connections to assigned View Desktops using the VMware View Client. Once a session was established, a randomized workload was run to simulate typical user activity.

Each session was allowed to remain established for 14 hours, during which time the overall system statistics were collected from several components of the architecture.

The following sections explain in more detail how each layer was implemented and used as part of the validation and how the workload was implemented.

Workload Description

Each virtual machine is equipped to run a workload that simulates typical user behavior, using an application set commonly found and used across a broad array of desktop environments. The workload has a set of randomly executed functions that perform operations on a variety of applications. Several other factors can be implemented to increase the load or adjust the user behavior, such as the number of words per minute that are typed and the delay between applications being launched.

The workload configuration used for this validation included Microsoft Word, Excel, PowerPoint, and Internet Explorer, Adobe Acrobat, McAfee Virus Scan, and Pkzip. During the execution of the workload, multiple applications were opened at the same time and windows were minimized and maximized as the workload progressed, randomly switching between each application. Individual application operations that were randomly performed included:

- *Microsoft Word*

  Open/minimize/close, write random words/numbers, save modifications.
- *Microsoft Excel*

  Open/minimize/close, write random numbers, insert/delete columns/rows, copy/paste formulas, save modifications.
- *Microsoft PowerPoint*

  Open/minimize/close, conduct a slide show presentation.
- *Adobe Acrobat Reader*

  Open/minimize/close, browse pages in PDF document.
- *Internet Explorer*

  Open/minimize/close, browse page.
- *McAfee Anti-virus*

  Real time scanning.
- *Pkzip*

  Open/Close, compress a large file.

Based on the think time and words per minute used for this validation, this workload could be compared to that of a high-end task worker or lower-end knowledge worker.

With this workload, we were able to validate that 1,000 users can easily be maintained by this architecture using the provided server, network, storage resources, and configuration. In

addition to being able to sustain 1,000 users with fast application response time, the necessary resources were also available to accommodate a host failure within each cluster, as well as to accommodate a moderate amount of growth or unpredicted increase or change in user workload. Depending on your specific environment, additional changes or features implemented, and the workload characteristics of your users, you may be able to accommodate more or fewer users.

Client Access Devices

To test and validate each layer of the architecture, we deployed simulated client access devices that simulate a real world environment where users connect from a client access device through the supporting infrastructure and establish network-based sessions with their View Desktops. The client access devices were implemented separately from the actual building blocks and other infrastructure components, typical of a virtual desktop deployment, such as Active Directory, DNS, DHCP, and file and print services.

Each client access device was implemented using Windows XP SP2 running the VMware View Client. 100 client access devices were deployed, and each was used to establish ten unique VMware View sessions. Each session was established using a unique individual user account that was entitled to use one of several pools. During the tests, virtual clients were powered on at random intervals until all the virtual clients had been powered on. Each simulated client's 10 sessions were automatically started after being powered on, with a 10-second delay implemented between sessions.

Access Infrastructure

The physical networking was implemented with a network core and redundant 10 Gigabit uplinks to 48 port switches supporting the building block's connectivity. The network core also load balanced incoming requests across VMware View Manager Connection Servers, where user requests were routed to the appropriate building block for each virtual desktop session.

Two VMware View Manager Connection Servers were implemented with load balancing validated to provide redundancy for the building block. For a 5,000-user Pod, five VMware View Connection Servers should be deployed to support added capacity and provide the highest level of performance and redundancy.

The settings for each VMware View Manager Connection server were configured as follows:

- *VMware vCenter Servers*

  Maximum Number of Provisioning Operations = 5

  Maximum Number of Concurrent Power Operations = 3
- *View Servers*

  Direct connection to desktop = Enable
- *Global Settings*

  Require SSL for client connections = Disable

VMware View Pod Details

5,000-user VMware View Pod	
QTY	Description
5	VMware View Manager Connection Servers
5	VMware View Building Blocks
1	VMware View Pod Network Core Components

VMware View Building Block Details

1,000 User VMware View Building Block	
QTY	Description
1	Building Block Network Component
1	VMware vCenter Server 2.5 U3 – View Composer Capable
1	Microsoft 2005 SQL server or Oracle DB
2	VMware ESX 3.5 U2 Clusters
8	VMware ESX 3.5 U2 Hosts
1	Shared Storage Component

Physical Network Details

VMware View Pod Core Networking Components	
QTY	Description
1	Modular Core Networking Switch
1	10 Gigabit Ethernet Modules
1	Load Balancing Module
Building Block Network Components	
1	48 Port Network Switch
VLAN Configuration	
VLAN ID	Description
16	Vmware View Desktops – Infrastructure -802.11q Tagged
20	Management – 802.11q Tagged
23	Storage – iSCSI – 802.11q Tagged

24	*vMotion – 802.11q Tagged*

Virtual Infrastructure

The virtual infrastructure at the core of each building block is comprised of physical servers and VMware Virtual Infrastructure 3. It is designed and validated to support 1,000 users. Depending on the environment and desktop workload, these results may vary.

The blade server chassis used for this validation were each capable of supporting 16 blade servers at full capacity; however, any type of server with the same hardware specification can also be used. One consideration when using blades is the port consolidation of each blade server-to-uplink module. Port consolidation is a common factor when leveraging blade servers. In most cases, it presents no problem if adequate bandwidth is provided. At the time of this validation 10 Gigabit uplink modules were not readily available, so Gigabit uplink modules were used. Although no adverse affects were observed, this should be monitored closely because differences introduced in specific environments could introduce the need for higher bandwidth. Each building block is configured as two 8-node VMware ESX 3.5 U2 clusters. Each 8-node cluster is designed to host 500 virtual desktops. Both clusters were configured as HA clusters and managed by a single VMware Virtual Center 2.5 U3 server.

A separate blade chassis was used to host the common infrastructure components needed for an enterprise desktop environment, such as Active Directory, DNS, DHCP, and VMware View Manager. Each desktop infrastructure service was implemented as a virtual machine running Windows 2003 SP3. The infrastructure blade chassis also hosted our load clients.

Each building block is designed to be supported by a single VMware vCenter 2.5 U2 server. Our VMware vCenter server database was hosted on a single Microsoft SQL 2005 server. Both VMware vCenter and our Microsoft SQL server were implemented as virtual machines. The VMware ESX hosts running these virtual machines were part of an HA cluster to protect them from any physical server failures. This is a common approach for hosting desktop infrastructure services that helps provide the highest level of availability.

Although each building block is designed with a dedicated VMware vCenter server that includes its own dedicated database server, it might be desirable to consolidate the database servers into only one or a few larger database servers. However, database consolidation is not covered as part of this validation effort. The details of each VMware View building block are listed below.

Physical Server Configuration

Infrastructure Servers	
QTY	***Description***
1	*16 Slot Blade Chassis*
4	*Blade Servers - ESX 3.5 Update 2* *2 – Infrastructure Services* *2 – Load Clients*
2	*Quad Core 2.66 GHz Processors*

32GB	*RAM*
1	*x 56GB SAS Drive*
4	*Broadcom Gigabit Ethernet Adapters*
4	*4 Port Gigabit Uplink Modules*
1	*VMware vCenter Virtual Machine* *Windows 2003 Server SP3* *2 – vCPU* *4GB - RAM* *20GB Virtual Disk*
1	*Microsoft SQL 2005 Server* *Windows 2003 Server SP3* *2 – vCPU* *4GB - RAM* *20GB Virtual Disk*
1	*Windows 2003 Server SP3* *2 – vCPU* *4GB – RAM* *20GB Virtual Disk* *Active Directory* *DNS* *DHCP*
VMware View Desktop Building Block A	
QTY	***Description***
1	*16 Slot Chassis – Cluster A/B*
8	*Blade Servers - ESX 3.5 Update 2*
2	*Quad Core 2.66 GHz Processors*
32GB	*RAM*
1	*x 56GB SAS Drive*
6	*Broadcom Gigabit Ethernet Adapters*
6	*4 Port Gigabit Uplink Modules*
VMware View Desktop Building Block B	
QTY	***Description***
8	*Blade Servers - ESX 3.5 Update 2*

2	*Quad Core 2.66 GHz Processors*

32GB	*RAM*
1	*56GB SAS Drive*
6	*Broadcom Gigabit Ethernet Adapters*
6	*4 Port Gigabit Uplink Modules*

***NOTE:** Two Mirrored 56GB drives are recommended for production.*

Storage Configuration

EMC NS20FC Storage Configuration	
QTY / Version	***Description***
1	*Celerra NS20FC with a CLARiiON CX3-10F backend array*
5.6 Maintenance Update 4 (5.6.40.3)	*NAS/DART File Server Software*
Release 26 (3.26.10.5.020)	*CLARiiON Flare Array Software*
259 MB	*CLARiiON Write Cache*
2	*X-Blade 20 configurations*
2	*2.8 GHz Pentium IV CPUs*
4	*Double Data Rate RAM (266 MHz)*
2	*Fibre Channel ports for back-end storage connectivity*
4	*10/100/1000 BaseT Ethernet ports*
Release 3.58	*BIOS*
Release 1.50	*POST*
30	*300 GB /15K 2/4 GB Fibre Channel disks*

View Desktop Configuration

Virtual Machine Configuration	
QTY	***Description***
1,000	*Windows XP SP2 - Virtual Machines*
512GB	*RAM*
8GB	*Virtual Disk*

Session Management

Desktop Pools were configured to closely match what a typical deployment might look like. A sample variety of desktop user types was implemented to reflect commonly found use cases in a typical deployment. Individual user accounts were created in Active Directory and assigned to specific groups. Each Group was also entitled to a VMware View Manager desktop pool.

Desktop Pool Configurations

View Manager Pool Configurations				
QTY	**Unique ID**	**Desktop Persistence**	**Image Type**	**Cluster Assignment**
10	eStaff	Persistence	Full Clone	Cluster A
15	Human Resources	Persistence	Full Clone	Cluster A
25	Finance	Persistent	Linked Clone	Cluster A
100	Sales	Persistent	Linked Clone	Cluster A
100	Marketing	Persistent	Linked Clone	Cluster A
50	Support Staff	Non-Persistent	Linked Clone	Cluster A
500	Contact Center	Non-Persistent	Linked Clone	Cluster B
200	Contractors	Non-Persistent	Linked Clone	Cluster A

Active Directory Groups

View Manager Active Directory Groups	
Group Name	**Number of Users**
eStaff	10
Human Resources	15
Finance	25
Sales	100
Marketing	100
Support Staff	50
Contact Center	500
Contractors	200

Validation Results

In this section we will cover several of the results and observations that were concluded during this validation. The results are aligned and specific to the two phases of testing that was conducted. The first phase being virtual desktop provisioning and phase two virtual desktop runtime.

Pool Creation and Provisioning

The results of the pool creation and provisioning are the time that it took from the time a pool creation job was submitted to the time it took to complete the creation of the final virtual machine.

Time to Provision Virtual Machines			
Pool Name	**QTY**	**Type**	**Minutes**
eStaff	10	Full Clone	23
Human Resources	15	Full Clone	58
Finance	25	Linked Clone	49
Sales	100	Linked Clone	27
Marketing	100	Linked Clone	27
Support Staff	50	Linked Clone	14
Contact Center	500	Linked Clone	161
Contractors	200	Linked Clone	63

NOTE: *The provisioning time for linked clones is significantly faster than full clones. This behavior is expected considering each virtual machine is a full copy or clone of the template that it was created from. Using linked clones this is not the case. One important consideration about the provisioning time related to linked clones is the approach that is taken.*

In most cases, large-scale VMware View deployments use several data stores for storing the virtual machines. For this validation, a ratio of 64 VM to one data store or LUN resulted in seven data stores per cluster. All of the linked clones were created from the same parent virtual machine.

Comparing the provisioning time of the Finance pool of 25 virtual machines to the Sales pool of 100 virtual machines, the time to deploy the Finance pool (with fewer virtual machines) is significantly higher. In our configuration, both pools were assigned to Cluster A, with seven data stores. Because VMware View Composer is aware of the available storage resources, it clones a replica of the parent image to each data store for use by the pool. Because of its size, it takes more time to create the first copy than to create the linked clones. Once the replica has been copied to each data store, it does not have to be copied again for the same pool or any future pools based on the same parent. For example, the Human Resources pool was the first

linked clone-based pool created on Cluster A. The creation of this pool initiated a full copy to each data store. After the Human Resources pool was created, the sales pool was created, based on the same parent virtual machine as the Human Resources pool. Because a full replica already existed in the data store, only the linked clones needed to be created for the Sales pool, resulting in a much faster provisioning time.

VMware View Building Block System Utilization

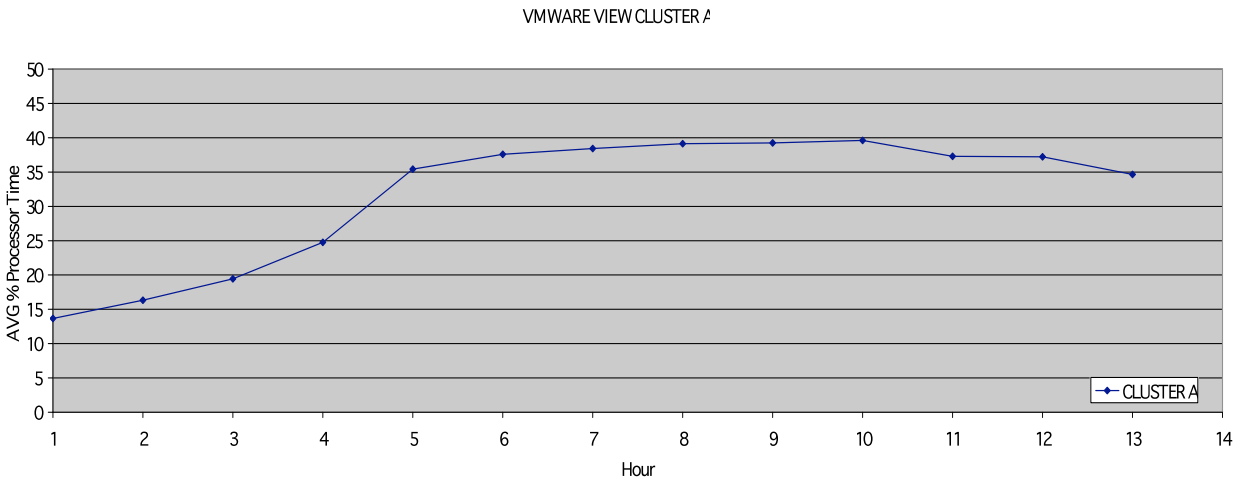


Figure 9: AVERAGE % CPU Utilization Cluster A

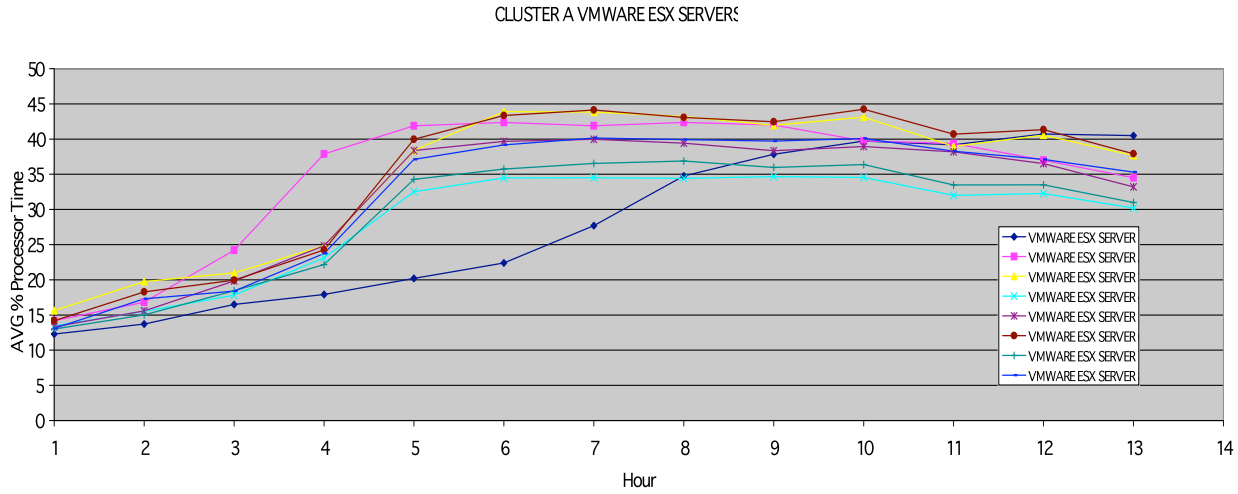


Figure 10: AVERAGE % CPU Utilization Cluster A VMware ESX Servers

Figures 9 and 10 above represent the average CPU utilization of Cluster A as a whole and the CPU utilization of the individual servers that are part of Cluster A. Two servers, Server 1 and server 2 show higher and lower CPU utilization than the rest of the servers in the cluster. This is the affect of server 2 having more virtual machines than server 1 and server 1 having more sessions that begin the workload later in the test cycle. Cluster A hosts more pools of back

office workers; these users are typically more mobile and less active overall than task-oriented workers.

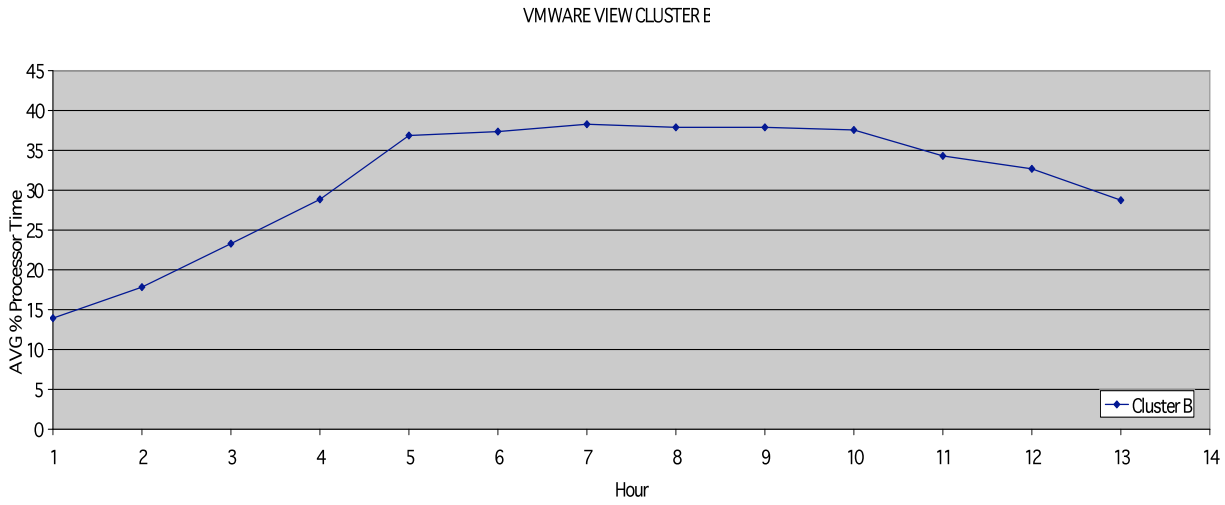


Figure 11: AVERAGE % CPU Utilization Cluster B

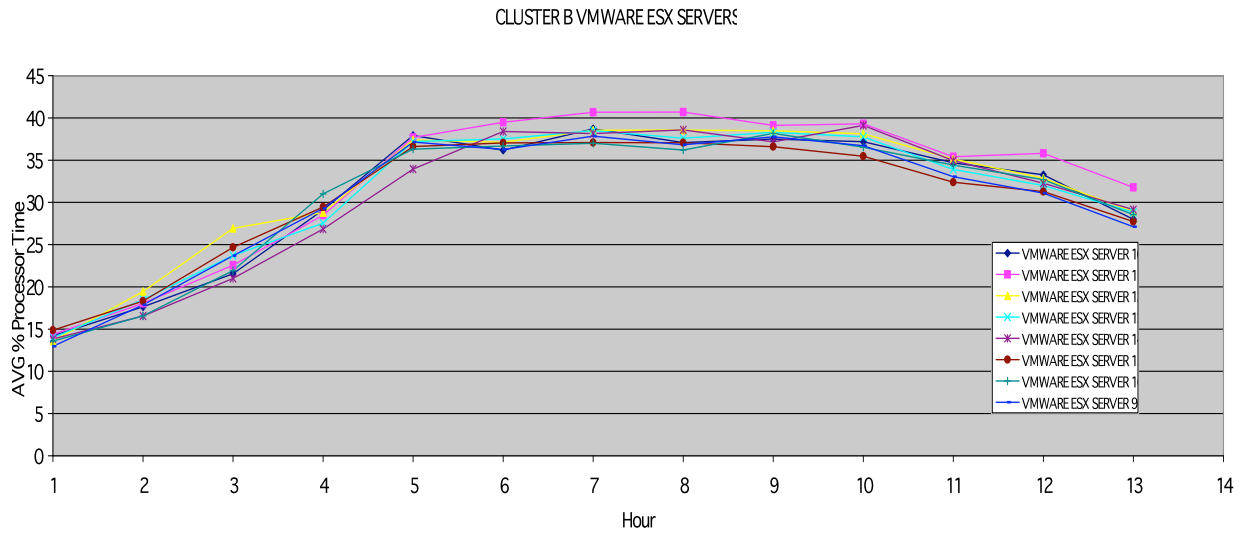


Figure 12: Average % CPU Utilization Cluster B VMware ESX Servers

Figures 11 and 12 represent the average CPU utilization of Cluster B as a whole and the CPU utilization of the individual servers that are part of Cluster B. This cluster is our Contact Center cluster where less delay is implemented. This is representative of users that are typically more consistent in their virtual desktop utilization, going to and from meetings less, resulting in less overall idle time of their virtual desktops. Two servers Server 1 and server 2 show higher and lower CPU utilization. This is the affect of server 2 having more virtual machines than server 1 and server 1 having more sessions that begin the workload later in the test cycle.

Infrastructure Systems Utilization

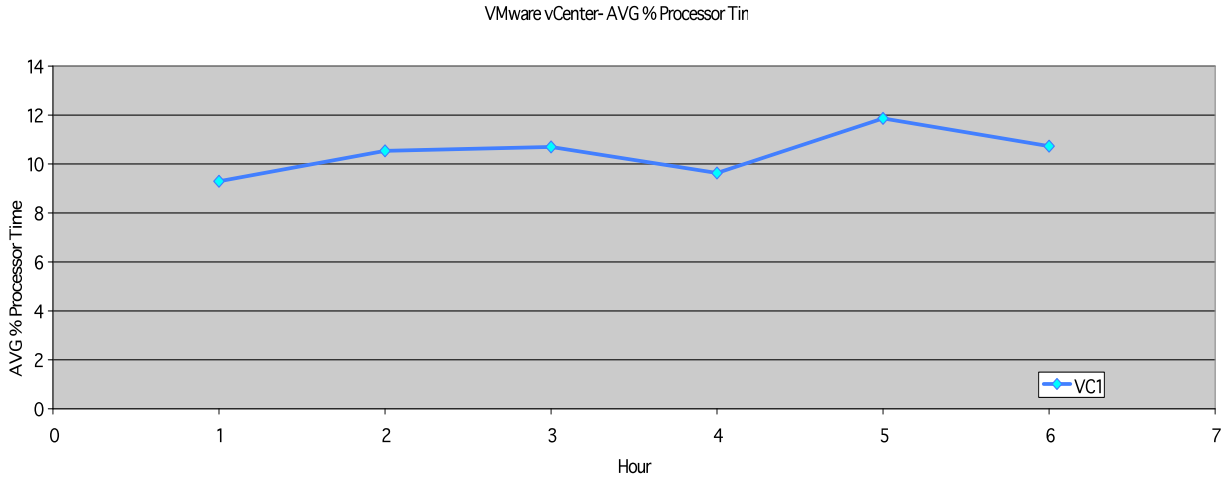


Figure 13: Average CPU Utilization of VMware vCenter

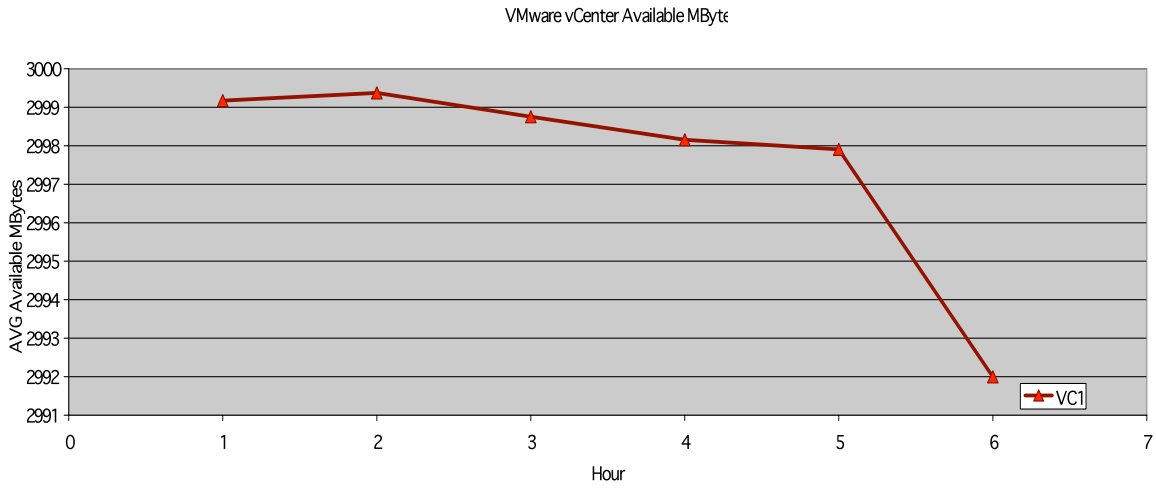


Figure 14: VMware vCenter Average Available Memory in MBytes

Figures 13 and 14 represent the average CPU utilization and average available memory in MBytes of our VMware vCenter server that was used to manage both Cluster A and Cluster B. The sample represents the progression of sessions being established and the leveling off of virtual machines running their workload. This representative of the most active portion of this validation run and demonstrates that our VMware vCenter server had sufficient resources to handle the management of the 1,000-user building block.

Figure 15: Average CPU Utilization of VMware vCenter SQL Server

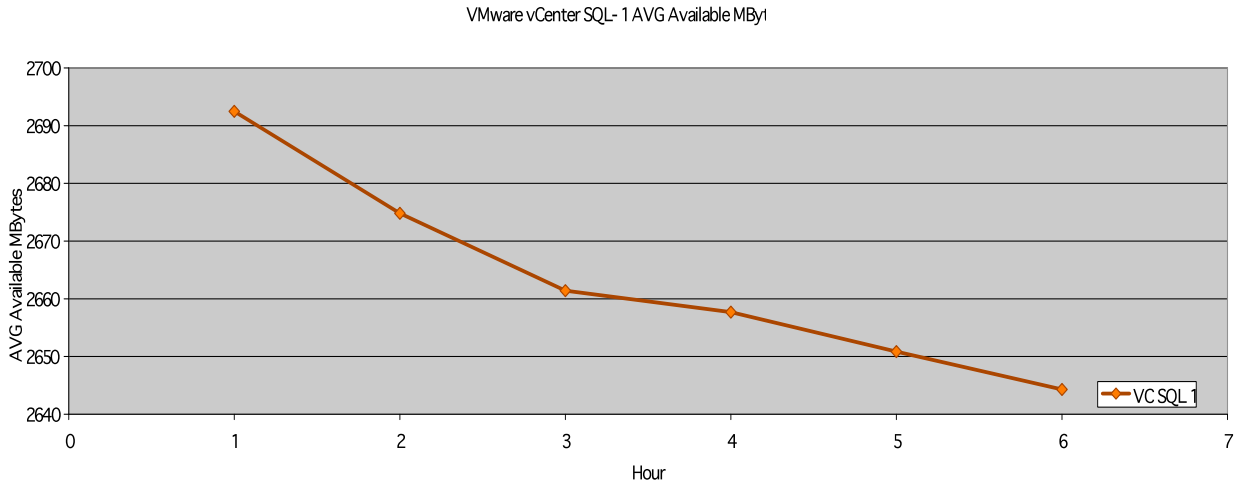


Figure 16: Average Available MBytes of VMware vCenter SQL Server

Figures 15 and 16 represent the average CPU utilization and average available memory in MBytes of our VMware vCenter SQL server that served as the database for our VMware vCenter server. The sample represents the progression of sessions being established and the leveling off of virtual machines running their workload. This is representative of the most active portion of this validation run and demonstrates that our VMware vCenter SQL server had sufficient resources to handle the management of the 1,000-user building block.

Storage System Utilization

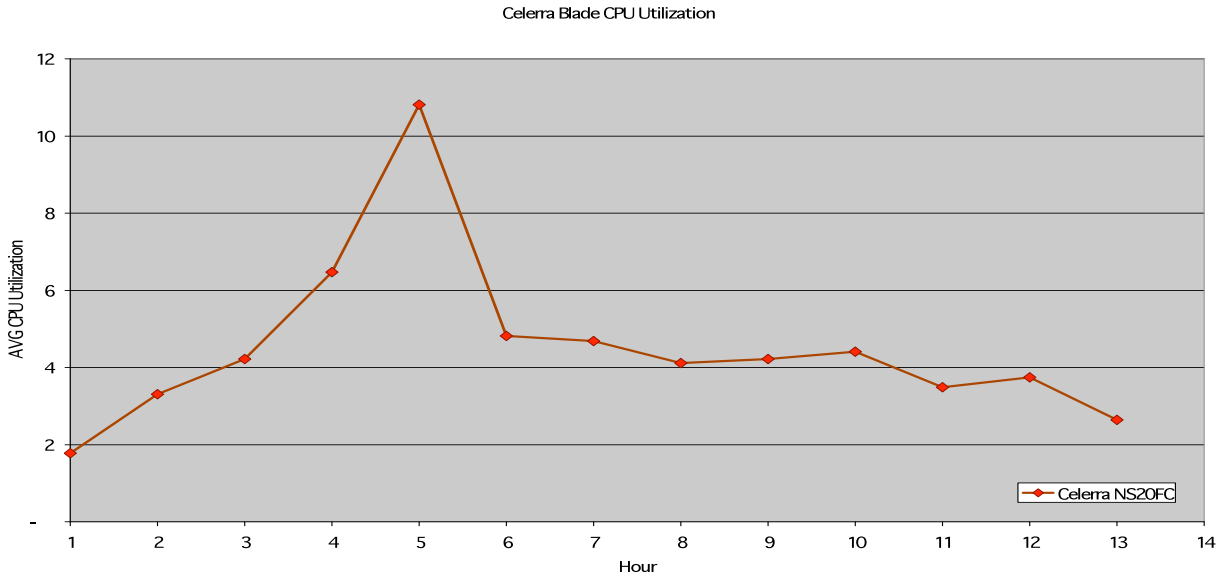


Figure 17: Celerra NS20FC Average CPU Utilization

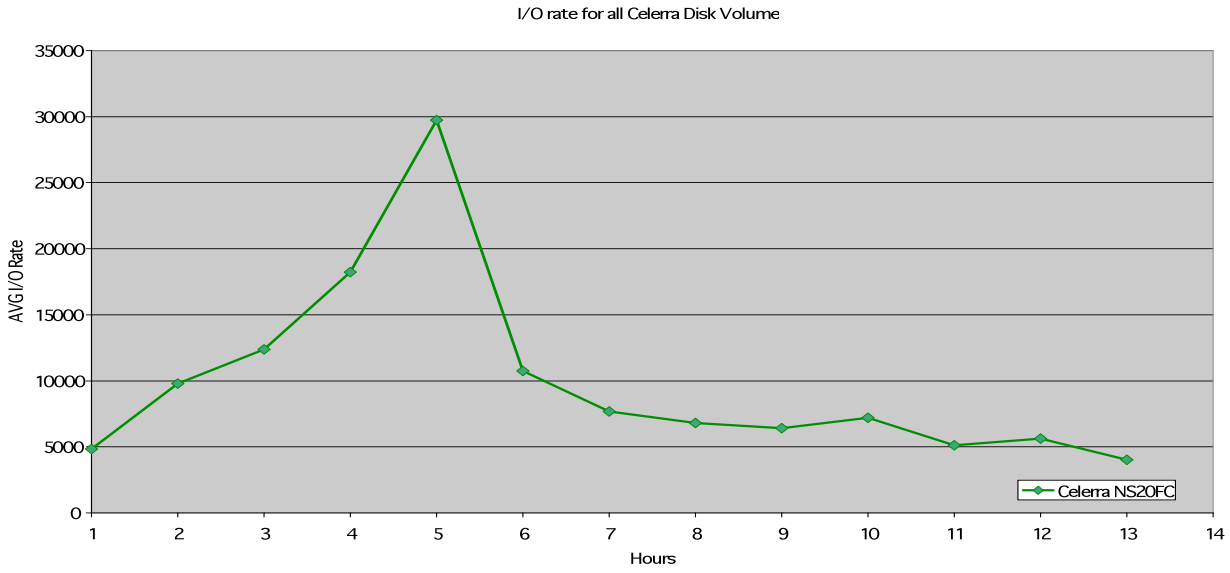


Figure 18: EMC Celerra NS20FC Average I/O Rate For All Disk Volumes

Figures 17 and 18 represent the average CPU utilization of the EMC Celerra NS20FC data movers. Also shown is the average I/O rate for all the EMC Celerra disk volumes representing plenty of capacity for handling the needed capacity of each building block.

Application Response Time

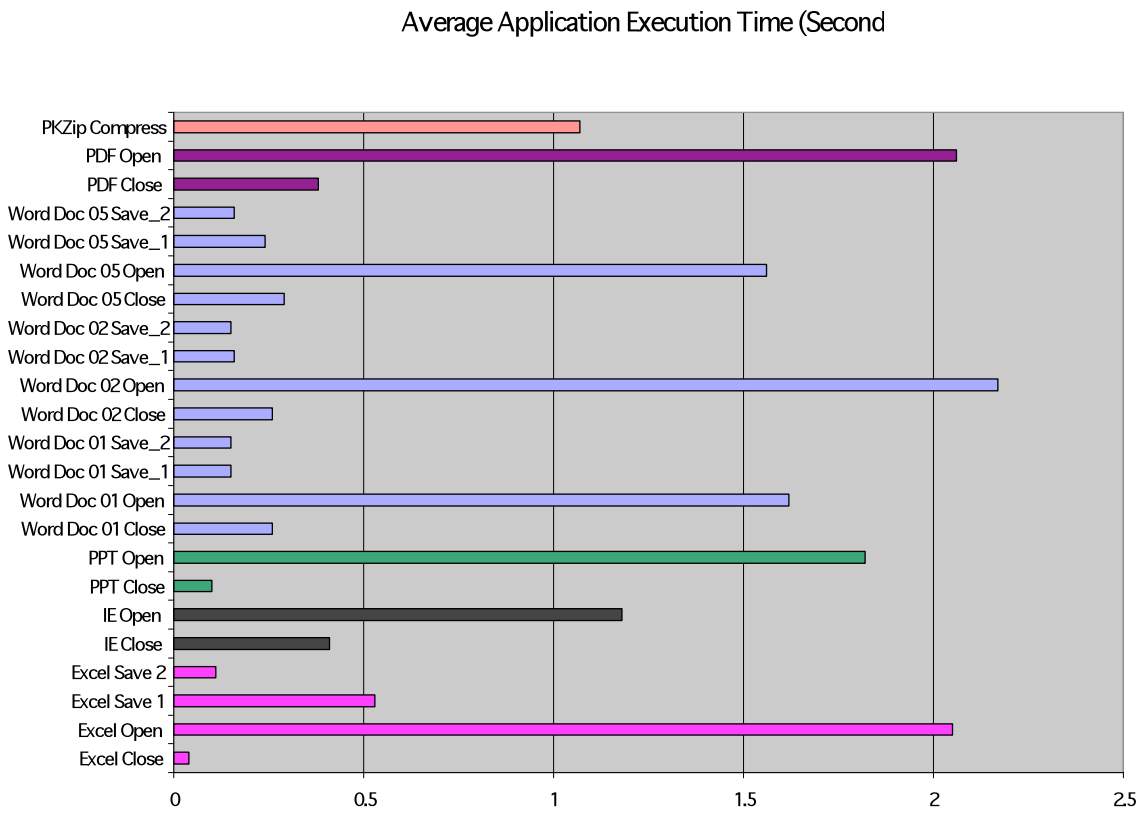


Figure 19: Average Application Execution Time In Seconds

Figure 19 reflects the average application execution time from all virtual desktops in both Cluster A and Cluster B. These application times represent the amount of time it took to open, close or save a document that was created. This does not represent the amount of time an application is minimized or being worked on. Because of the random nature of the workload, applications being minimized not simply opened, worked on and closed. The randomized workload might start out creating a Microsoft Word document, work on this document, minimize the document and then use Microsoft Internet Explorer. Later the workload will return to the minimized Microsoft Word document work on it some more and close it.

Conclusion

Using this validation methodology and design approach, we are able to verify that this building block design can support the target of 1,000 users. By combining five 1,000-user building blocks, 5,000-user pods can be created that can more easily be managed as a larger set of standardized resources. This can serve as a starting point for customers looking to scale their VMware View deployments in a predictable, standardize manner. With a standard, validated design or starting point, customers can adapt each VMware View reference architecture to meet their specific needs and requirements.

The following aspects of our validation methodology offered us the ability to implement the virtual infrastructure and to simulate real world user behavior and the affects these can have on different uses cases and solution designs.

- ***Complex, randomized workload that can be adjusted to increase load based on user type***
- ***Complex, randomized workload that minimizes and maximizes applications that more closely simulates real world user behavior***
- ***Testing with Individual unique user accounts***
- ***Testing with individual sessions end to end from the client to the virtual desktop***
- ***Designing, testing and validating the solution end-to-end***

By taking this approach, we can hope to help customers and partners better to understand in advance the different aspects of a solution or architecture and the effects they will have in their environment. This should help reduce some of the upfront risk often taken on by IT organizations as well as help them to realize more consistency, reliability, serviceability, scalability, and predictability.

About the Authors

***Warren Ponder** is a Sr. Technical Marketing Engineer at VMware. In this role, he works as part of the product marketing team, developing alternative approaches to traditional desktop architectures and solutions. Much of his time is spent speaking, writing white papers, and developing technical content focused on thin client computing, Windows interoperability, and virtual desktop solutions.*

***Fred Schimscheimer** is a Senior Technical Marketing Engineer at VMware. In this role, he works as part of the product marketing team as an expert in storage and workloads for virtual desktop solutions .*

***John Dodge** is a VCP, MCSE, CCNA, and Services Architect responsible for developing new service offerings in the VMware Practice Development 's enterprise desktop space. John joined VMware through the acquisition of Foedus Group, LLC, where he was a principal and managing partner. John's time is spent primarily designing and improving implementation services for VMware products. With over twenty years' technical and management experience in IT infrastructure, he is also a highly regarded subject matter expert for Pharmaceutical Virtual Infrastructure qualification.*

Acknowledgements

We would like to acknowledge the following individuals for their contributions and leadership, Greg Smith, Pak-Shun Lei, Todd Brune, Brian Martin, Chad Sakac, Asifiqbal Pathan, Sunil Satnur, Rishi Bidarkar, Fred Schimscheimer, Puneet Chawla, Amit Patel, Mason Uyeda, Vikram Makhija, Kaushik Banerjee, Lee McColgan, Bala Ganeshan, Vikas Singh, Ashish Hanwadikar, Radhakrishnan Manga, Mark Benson, and Anthony Wilkinson.

References

- *VMware View Manager 3 Deployment Guide*
- *VMware View Composer Deployment Guide*
- *VMware View XP Deployment Guide*
- *VMware View Profile Virtualization Information Guide*
- *VMware View Manager Administrator Guide*
- *EMC Celerra Unified Storage Deployment Guide*
- *VMware Infrastructure 3 Documentation*
- *VMware infrastructure 3 in a Cisco Networking Environment*
- *ESX Performance Tuning Best Practices*
- *iSCSI Design Considerations and Deployment Guide*
- *VMware HA: Concepts and Best Practices*
- *VMware Virtual Networking Concepts*
- *VMware ESX Performance Counters*

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