Reference Architecture for 1,000 Users with VMware Horizon (with View), Tintri VMstore and Cisco UCS

VMware® Horizon™ 6 (with View™)

TECHNICAL WHITE PAPER

vmware®

Table of Contents

Executive Summary

This reference architecture is based on real-world test scenarios, user workloads, and infrastructure system configurations. It combines the technologies of the Tintri VMstore (running the newest Tintri OS 3.0) with VMware® ESXi™ 5.5, and Horizon 6 (with View) software to produce a highly efficient, robust, and scalable virtual desktop infrastructure (VDI) for a hosted virtual desktop deployment for 1,000 users.

A virtual desktop deployment places high performance demands on compute (CPU and memory), network, and storage systems. The number of I/O operations and the resources required for servicing the operating system boot, login, logout, and workload of a large number of desktops can stress the entire infrastructure.

The solution offers:

- Single storage platform (Tintri VMstore T650)
- High performance, easy to manage, highly dense compute platform (Cisco UCS B-series Blades)
- Highly available and resilient design providing fault tolerance for the 1,000 virtual desktop system
- End-to-end virtualization, with all Windows 7 SP1 virtual desktops and supporting infrastructure components, including VMware vCenter™, Active Directory, profile servers, SQL Servers, and View components
- View with PCoIP display protocol to deliver a high-performance desktop experience with host-rendered flash video and other demanding applications

All the configuration outlined in this Reference Architecture is performed on the vSphere and Horizon (with View) software; there is almost zero configuration required in the Tintri VMstore – the product is fully tuned and ready to use the moment it gets an IP address.

This paper includes the results of a series of storage I/O performance tests, generated by LoginVSI 4.1 -- the industry-standard VDI performance testing tool -- on one test pool consisting of 1,000 users, and provides storage sizing guidance and best practices based on those results for designing and deploying View virtual desktops on a Tintri VMstore T650.

All 1,000 users running an office worker workload completed successfully for the test pool, without pegging CPUs, exhausting memory, or overloading storage systems.

TEST POOL	VSI RESPONSE TIME (VSIMAX V4.1 THRESHOLD = 2066)
1,000 dedicated desktops, linked clones	1153 (@ 200 Sessions) to 1683 (@ 1,000 sessions)

TEST	DEDICATED LINKED CLONES
1,000 desktops provisioned	1 hours 37 minutes
1,000 desktops recomposed	1 hour 52 minutes
1,000 desktops refreshed	36 minutes
Pool deleted	27 minutes

Table 1. Test Results

VDI Fundamentals

A successful VDI project ultimately depends on three key characteristics:

- ***Simplicity***: Administrators responsible for initially configuring and managing an environment are the most obvious beneficiaries of management simplicity. At the risk of seeming hard-hearted, however, financially motivated executives care surprisingly little how hard someone has to work to perform their job. What they do care about, however, is the success or failure of new projects, how quickly they can be rolled out, and how costly they will be to manage. Keeping things simple is the surest way to ensure quick and continued success.
- ***Low cost***: While it's generally a mistake to think that virtual desktops can ever be less costly than physical desktops, VDI projects are unlikely to reach even the pilot stage unless costs are kept within reason. Storage costs alone can often undermine a new VDI project (because of the surprising IO demands). Just as an enterprise storage array is more costly than the collection of individual hard disk drives it contains, the enterprise-grade hardware infrastructure required host virtual desktops will always be more costly than an equivalent number of physical desktops. The former provides additional security, availability, and data management benefits that simply don't come for free. Nonetheless, the financial justification for these benefits isn't possible if the basic hardware infrastructure costs aren't kept within reason.
- ***Performance:*** Put simply, users won't be happy unless their virtual desktops provide at least the performance and overall user experience that they received from a physical desktop. The bar is continually being raised: these days users expect their desktops to perform like an SSD-enabled ultrabook, not the hard-disk based PCs of a few years ago.

Few would argue that hard-disk-drive (HDD) based storage arrays are incapable of balancing these requirements for a VDI project—the random IO performance demands from virtual desktops completely overwhelm the cost and complexity of the design. With an HDD-based array it becomes: "Simplicity, low cost, or performance: pick any one."

Used correctly, however, fl ash storage easily satisfies the performance demands of virtual desktops. The trick is to keep it simple and reasonably priced. Simply throwing a flash cache in front of an HDD-based array does not suffice. Invariably, a simple cache actually increases complexity and costs. Even sizing the cache correctly is a difficult and complex topic.

As the rest of this document will show, the Tintri VMstore T650 storage system provides an extremely simple and low cost storage system with sufficient performance for any VDI project with hundreds of simultaneously active desktops.

Solution Overview

With an application-aware architecture, Tintri VMstore provides a simple to manage, cost-effective VDI storage platform that meets the performance demands of thousands of VMs. The result is a predictable and efficient environment that is capable of handling all of your virtualized applications and desktops, and an IT team that is free to focus on innovation.

This solution uses Cisco UCS B-Series blades, Tintri VMstore Storage, and the VMware vSphere® 5.5U1 software suite to provide a platform for a View environment running Windows 7 virtual desktops provisioned by VMware View Composer™.

Hardware Components

Server

For this Reference Architecture, we used Cisco UCS B-Series blades, running on a Cisco UCS 5108 Chassis as the computing platform. We performed all tests while running UCS-M version 2.2(1d).

The Cisco Unified Computing System can deliver the following benefits:

- Reduce total cost of ownership at the platform, site, and organizational levels
- Increase IT staff productivity and business agility through just-in-time provisioning and mobility support for both virtualized and non-virtualized environments
- Help enable scalability through a design for up to 160 discrete servers in a single highly available management domain, or thousands of servers in a multi-domain environment
- Use industry standards supported by a partner ecosystem of innovative, trusted industry leaders

Delivering performance, versatility, and density without compromise, the Cisco UCS B200 M3 Blade Server addresses the broadest set of workloads, from IT and web infrastructure through distributed database.

Network

The Cisco UCS 6248UP 48-Port Fabric Interconnect is a core part of the Cisco Unified Computing System. Typically deployed in redundant pairs (as we did in this Reference Architecture), the Cisco UCS 6248UP Fabric Interconnects provide uniform access to both networks and storage.

Benefits include:

- Bandwidth up to 960 Gbps
- Higher port density: Up to 48 ports in one rack unit (1RU) including one expansion module with 16 unified ports
- High-performance, flexible, unified ports capable of line-rate, low-latency, lossless 1/10 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE), and 4/2/1 and 8/4/2 Fibre Channel
- Reduced port-to-port latency from 3.2 microseconds to 2 microseconds
- Centralized unified management with Cisco UCS Manager
- Efficient cooling and serviceability: Front-to-back cooling, redundant front-plug fans and power supplies, and rear cabling

Storage

The Tintri VMstore T650, running Tintri OS 3.0, provides a predictable and efficient environment that is capable of handling all of your virtualized applications and desktops, and an IT team that is free to focus on innovation. Smart Storage that sees, learns and adapts to your VM environment:

- Set-up in minutes: No complex storage configuration or tuning required by only dealing with auto-aligned VMs and vDisks and not LUNs and volumes.
- Predictable performance: The Tintri VMstore delivers consistent performance for all VMs with the economics of high capacity HDD with Tintri FlashFirst™ design delivering 99% of IO from flash.
- High VM density: Serve thousands of different type of VMs from a single VMstore with VM-level QoS and performance isolation.
- Instant performance bottleneck visualization: Real-time VM and vDisk-level insight on IO, throughput, end-to-end latency and other key metrics enables rapid VDI performance diagnosis.

Tintri storage sees into the complete virtualization infrastructure so you can too:

- Get a global view of all VMs stored and identify performance and capacity trends without dealing with underlying storage.
- Instantly identify performance hot spots at the hypervisor, network and storage level with comprehensive performance visualization.

With the Tintri OS 3.0, the VMstore T650 can support up to 2,000 View Desktops, with and without VCAI integration through extremely efficient native snapshots.

Tintri OS 3.0 is fully integrated into the VMware ecosystem; VMstore is one of the few storage products that is VCAI certified (http://kb.vmware.com/kb/2061611) and that is fully integrated with the vSphere Web Client, as can be seen in Figure 1.

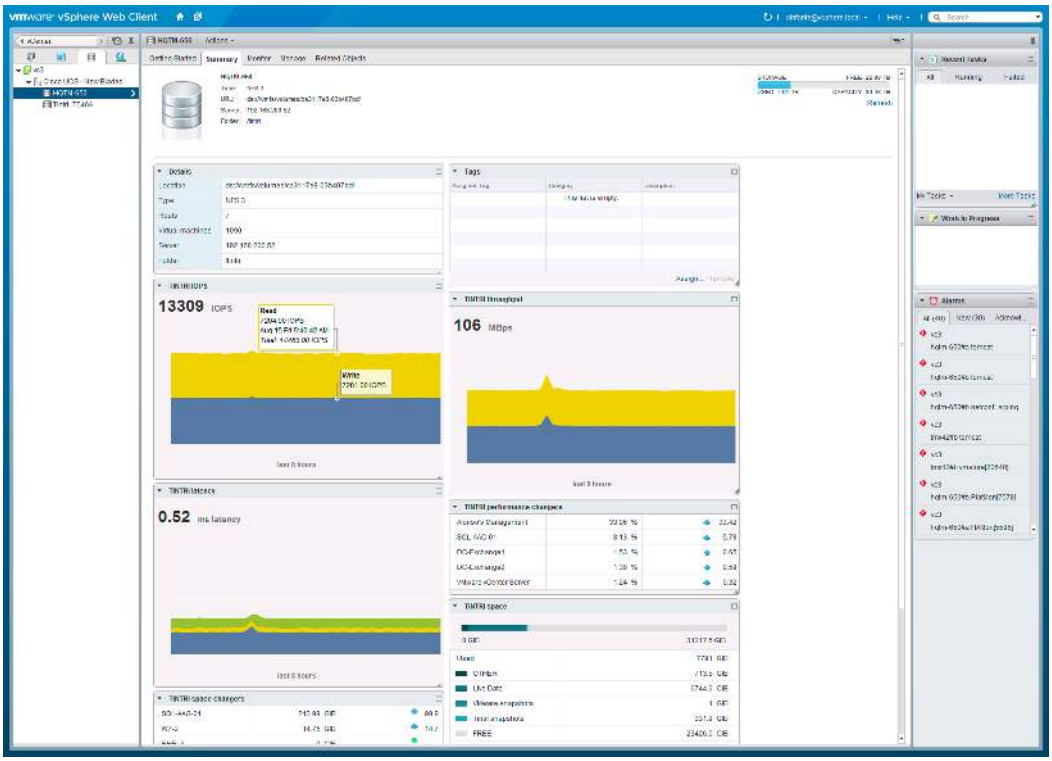


Figure 1. Tintri VMstore vSphere Web Client Plugin

Software Components

VMware vSphere

vSphere is the industry-leading virtualization platform for building cloud infrastructures. It enables users to run business-critical applications with confidence and respond quickly to business needs. VMware vSphere accelerates the shift to cloud computing for existing data centers and underpins compatible public cloud offerings, forming the foundation for the industry's best hybrid cloud model.

View

The View component of VMware Horizon 6 brings the agility of cloud computing to the desktop and revolutionizes desktops into highly available and agile services delivered from your cloud. It enables a level of availability, scalability, and reliability for virtual desktops that is unmatched by other end-user computing solutions. Horizon 6 is available in three editions, Standard, Advanced, and Enterprise, all of which include View as a component.

View delivers virtual sessions that follow end users across devices and locations. It enables fast, secure access to corporate data across a wide range of devices, including Mac OS, Windows, and Linux machines and iOS and Android tablets.

You can use View with VMware vCenter Server™ to create desktops from virtual machines that are running on ESXi hosts and to deploy these desktops to end users. In addition, View uses your existing Active Directory infrastructure for user authentication and management.

After you create a desktop, authorized end users can use Web-based or locally installed client software to connect securely to centralized virtual desktops, back-end physical systems, or terminal servers.

Figure 2 shows all available View software components from VMware; as we're going to cover later, in this Reference architecture we deployed most, but not all of these components.

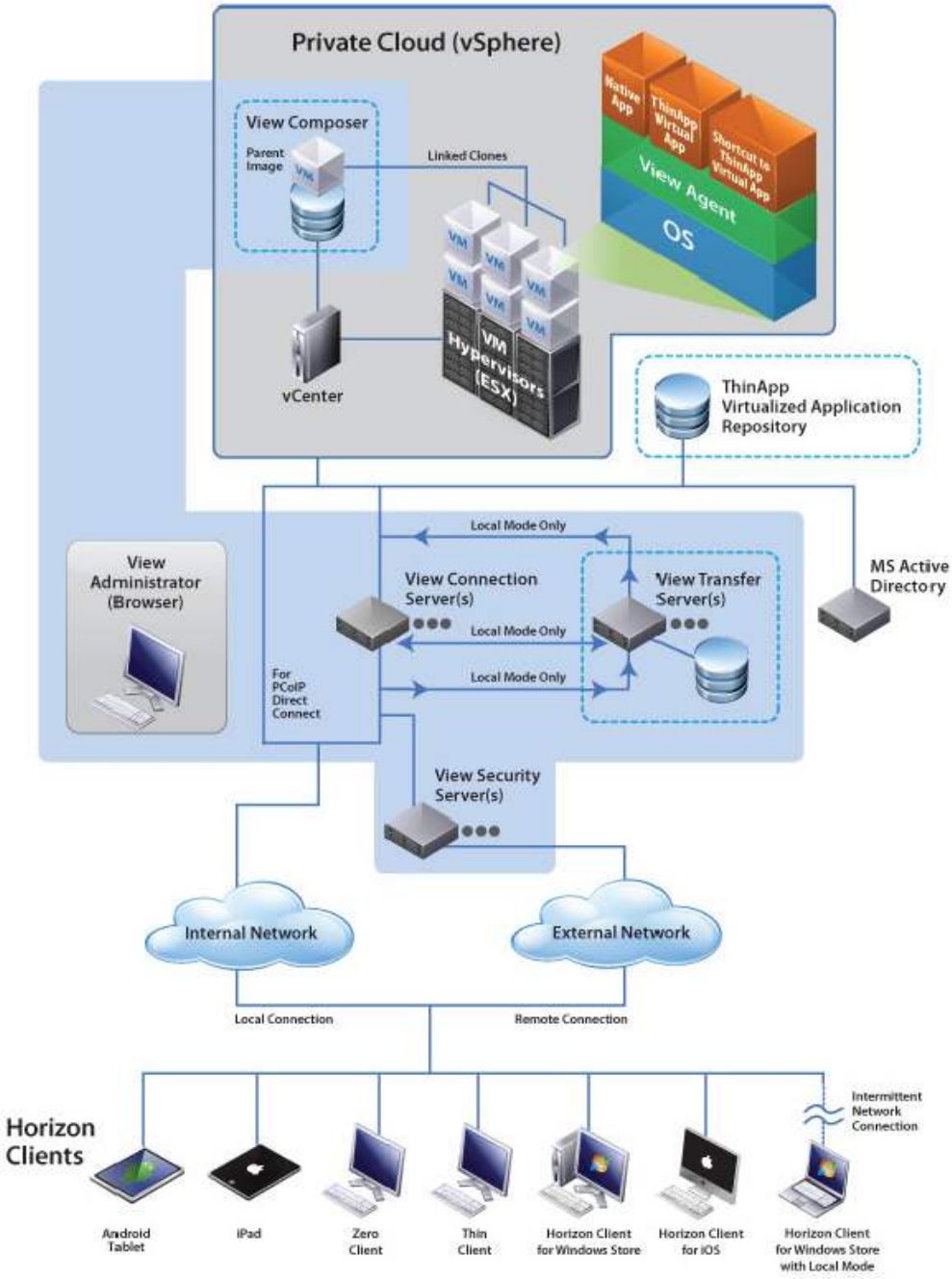


Figure 2. All available Horizon 6 (with View) Components

Testing Summary

During the course of the testing we validated the following:

General

- 1000 desktops (full clone or linked clone) easily fit and perform well on a single Tintri VMstore T650.
- The 5 host and one T650 architecture is a scalable unit for any number of virtual desktops (a half rack of equipment for each 1,000 desktops).
- All management, monitoring, infrastructure servers can be housed on a single Tintri VMstore T650
- Achieved excellent LoginVSI benchmark results for delivering low application latency (and thus good user experience).

Simplicity

- Simple architecture, excellent documentation.
- 8 minutes until first VM deployed.
- No tuning or special optimization required.
- Innovative per-VM management and monitoring Interface

Performance

- Fast desktop pool deployments, refresh, and recomposing
- Predictable performance and low storage latency even during workload bursts (including deploy or re-compose operations).

Cost-Effective

- No complicated sizing exercises required.
- Simple, intuitive administration (no need for training or specialized skills).
- Modest acquisition costs.

Detailed Results

Desktop Configuration

One type of virtual desktops was validated for this configuration:

- Dedicated desktops using linked clones

We chose this type of virtual desktops for this Reference Architecture because they offer the best user experience, while taking advantage of the Tintri VMstore's capabilities to remain extremely storage space and performance efficient.

This configuration (with a Tintri VMstore) does however support any type of virtual desktops (Floating, Stateless or Full Clones) that the customer may prefer.

The desktops were tested under a typical office workload and for standard View operations.

Workload Testing – Login Virtual Session Indexer (LoginVSI) 4.1

LoginVSI 4.1 simulates application workloads for various user types—in this case, an office worker—by running applications typically used in a Windows desktop environment. During the execution of a workload, applications are randomly called to perform common desktop user operations. Our pool passed the LoginVSI Office Worker test workload comfortably.

TEST POOL	VSI RESPONSE TIME (VSIMAX V4.1 THRESHOLD = 2066)
1,000 dedicated desktops, linked clones	1153 (@ 200 Sessions) to 1683 (@ 1,000 sessions)

Table 2. LoginVSI Workload Results

Operations Testing – View

TEST	DEDICATED LINKED CLONES
1,000 desktops provisioned	1 hours 37 minutes
1,000 desktops recomposed	1 hour 52 minutes
1,000 desktops refreshed	36 minutes
Pool deleted	27 minutes

Table 3. View Operations Results

Resiliency Testing – View

TEST	OUTCOME	DEDICATED LINKED CLONE POOL
Simulated view desktop block – ESX host failure	Success	LoginVSI Test Workload Pass
Simulated network switch failure	Success	LoginVSI Test Workload Pass
Simulated storage array controller failure	Success	LoginVSI Test Workload Pass
Simulated storage array disk failure	Success	LoginVSI Test Workload Pass

Table 4. Resiliency Results

Appendix A: Architecture Design

The core of the logical VMware View® Manager™ architecture design is the View pod, which consists of the following components.

View Connection Server – For this Reference Architecture, given the number of desktops being below 2,000, we chose to go with one View Connection Server, actively brokering and possibly tunneling connections.

Security Server – This design has one security server, paired with the View Connection Server.

View Block – The Block is sized for 1,000 virtual machines with N+1 for host capacity. Every host is estimated to carry the same number of virtual machines.

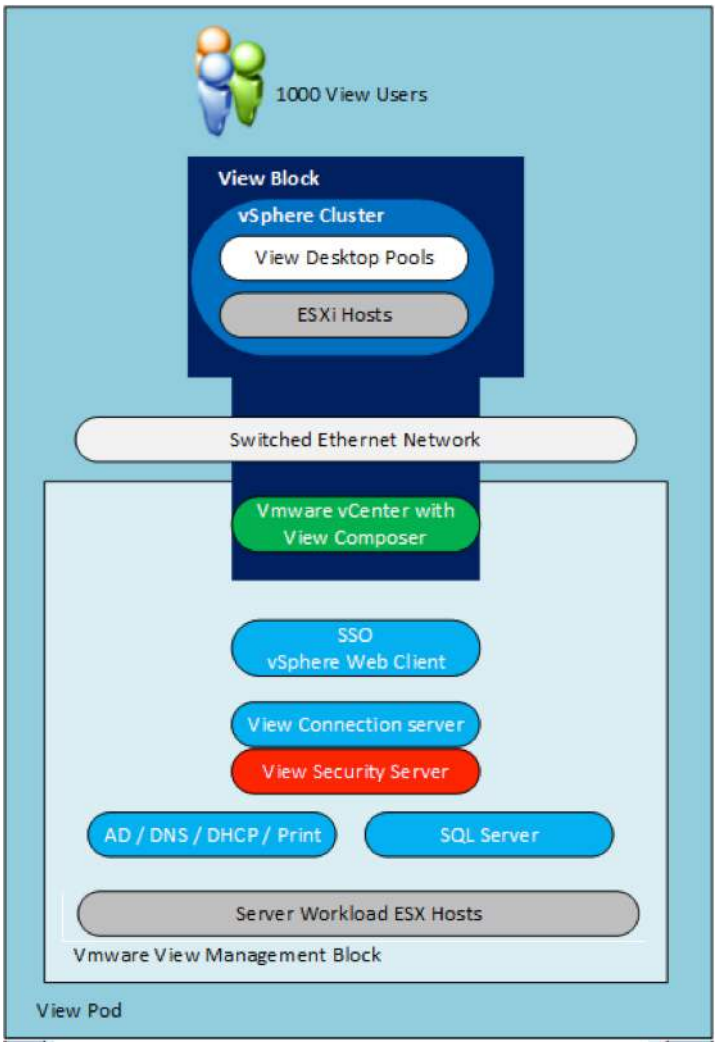


Figure 3. View Pod Logical Design

View Block

The following tables and figures describe the details of the architecture's storage requirements and logical infrastructure design. Note that one of Tintri's unique benefits is that you do not need to split each array into multiple datastores; Tintri will look at each VM individually and allocate the resources and space it needs, *so the traditional best practice of splitting the shared storage into multiple datastores to improve performance and/or space utilization is* ***not*** *necessary at all with Tintri.*

TEST POOL	NUMBER OF DESKTOPS	NUMBER OF DATASTORES (REPLICA AND CLONE)	REPLICA AND CLONE DATASTORE SIZE
Dedicated desktops, linked clone	1,000	1	30.48 TiB (of which less than 2 TiB are used)

Table 5. Test Pools

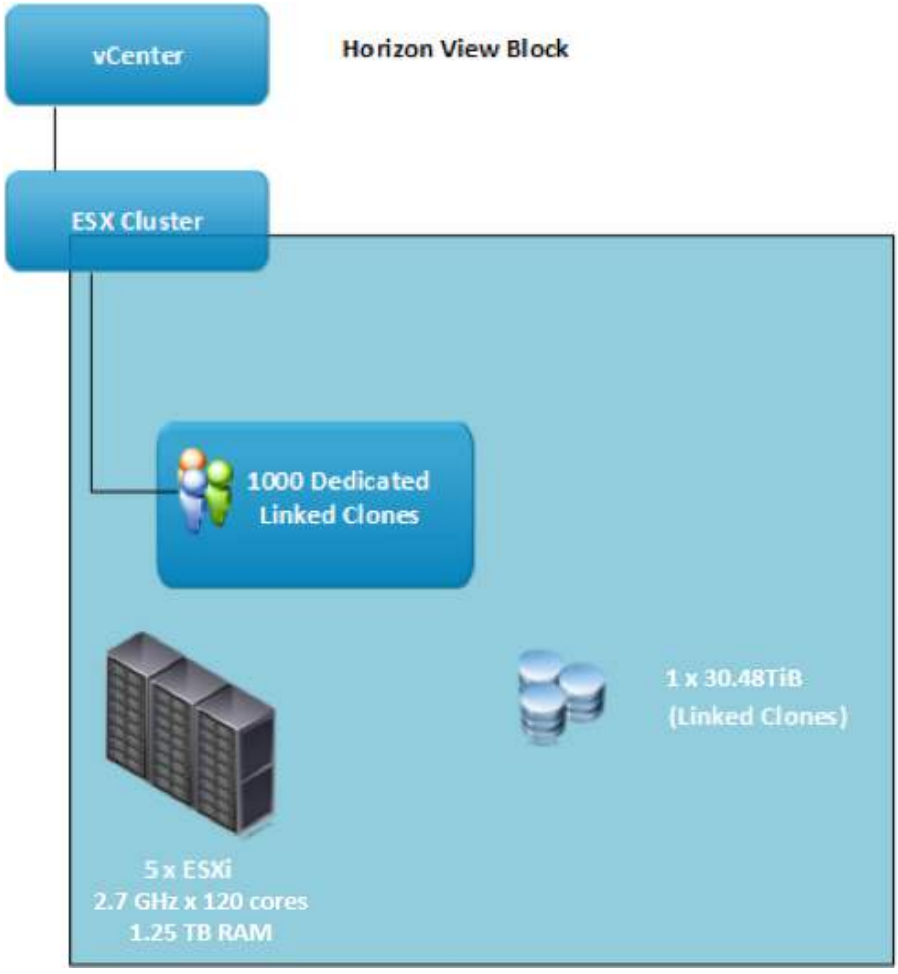


Figure 4. Pool 2 (Dedicated Linked Clones) – View Block Logical Infrastructure Design

View Management Block

A common View management block is used throughout all testing. The management block has its own dedicated ESX host, however, to take advantage of Tintri's "one datastore to rule them all" philosophy, leverages the same shared storage as the View Block, as shown in Figure 5.

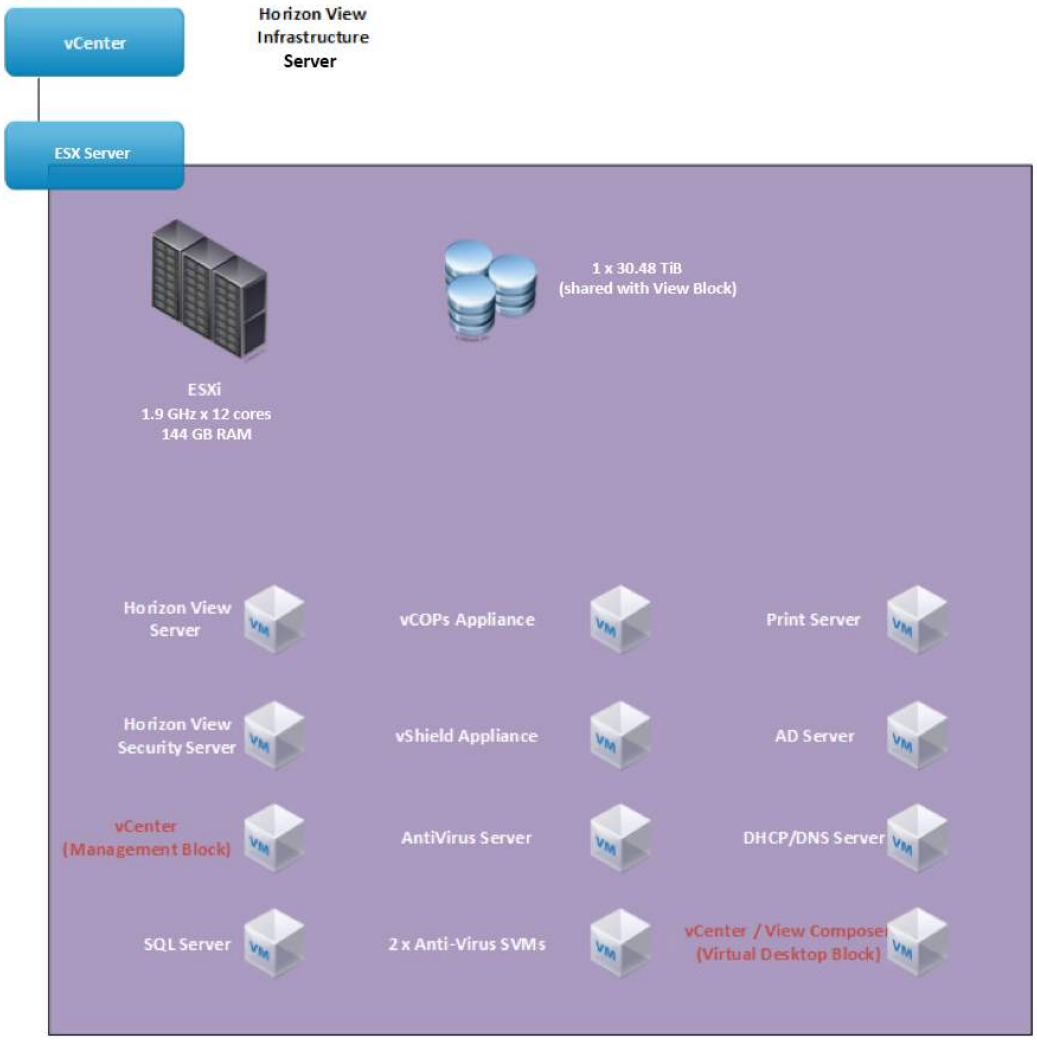


Figure 5. View Management Block

Logical Storage Design

We leveraged a Tintri VMstore T650 as the single datastore for all components of this Reference Architecture. VMstore T650 can support up to 2,000 Virtual Desktops and has dual (redundant) controllers, each with 2 x 10GbE connections that were connected to the dual (also redundant) Cisco Fiber Interconnect switches. The two controllers in the T650 were directly connected to 2+2 ports on the Cisco UCS 6248UP FIs, configured as appliance ports and trunked (i.e. leveraging Cisco's Appliance Port Channeling feature).

Logical Network Design

Traditionally, a vSphere implementation uses three types of network connections: virtual machine, management network, and VMkernel. Each type connects to a virtual switch that has one or more physical adapters (a minimum of two adapters is required for resilience) to provide connectivity to the physical networks.

In this Reference Architecture, however, in order to take full advantage of Cisco's UCS architecture, we chose to go with Distributed Virtual Switches, a sophisticated vSphere feature for network configuration that offers flexibility.

Distributed Virtual Switch Infrastructure

A vNetwork distributed switch (dvSwitch) acts as a single vSwitch across all associated hosts in a data center. This setup allows virtual machines to maintain a consistent network configuration as they migrate across multiple hosts. The dvSwitch uses two 10GbE adapters per host.

The dvSwitch features can benefit virtual machines, such as the ability to preserve the port state when a virtual machine is migrated to another ESXi server host, which facilitates the use of intrusion detection and prevention systems. Furthermore, the system supports PVLANs. For these reasons, all virtual machine network and ESXi management connections, including vMotion, use a dvSwitch. Table 6, Table 7, and Figure 6 define the standard dvSwitch that is created and configured.

VIRTUAL SWITCH	FUNCTION	NUMBER OF ADAPTERS PER HOST
dvSwitch0	All virtual machines vMotion	Two 10GbE

Table 6. dvSwitch Configuration

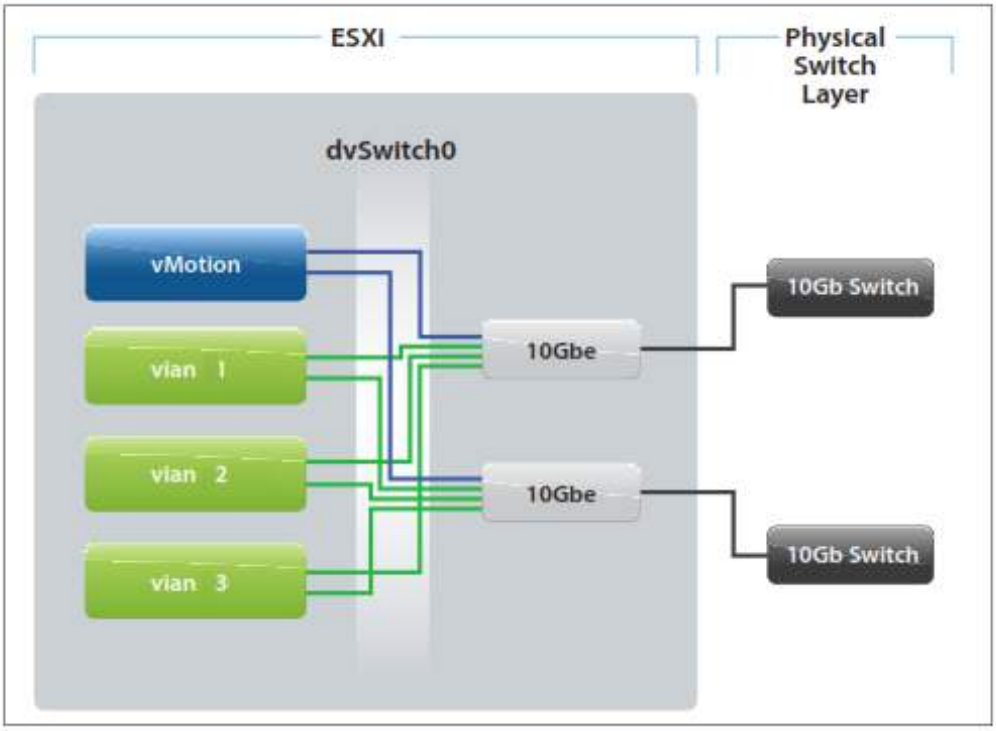


Figure 6. dvSwitch Network Diagram

PROPERTY	SETTING	DEFAULT	REVISED
Security	Promiscuous mode	Reject	Reject (unchanged)
	MAC address changes	Accept	Reject
	Forged transmits	Accept	Reject
Traffic Shaping	Status	Disabled	Disabled (unchanged)
NIC Teaming	Load balancing	Route based on the originating virtual port ID	Route based on physical NIC load
	Failover detection	Caution Link Status only	Caution Link Status only (unchanged)
	Notify switches	Yes	Yes (unchanged)
MTU Size	Failback	Yes	Yes (unchanged)

Table 7. Port Group Properties – dvSwitch

Network Physical Design Specification

The virtual machine NICs are all connected to the network backbone infrastructure using 10GbE connectivity. The network adapters assigned to the virtual switches must be connected to a minimum of two physical switches for resiliency.

Network Optimization for PCoIP

For optimal PC-over-IP (PCoIP) performance, it is recommended to do the following. Note that these are VMware's recommendations for optimizing PCoIP and are not specific to deploying VDI on Tintri VMstore systems.

- Minimize network router and switch buffers
- Set buffers to absorb 50ms to 100ms of PCoIP traffic. Large buffers can increase tail-drops, which are bad for PCoIP sessions and often cause session disconnects and disruptions. When there is congestion on the network devices, packets are dropped until the congestion is eliminated and the queue is no longer full. Uncontrolled packet loss might indicate congestion, causing PCoIP to drop to the minimum image quality, degrading the user experience.
- Set congestion avoidance to WRED
- Weighted random early detection (WRED) drops packets in a controlled way. PCoIP reacts better to WRED and goes into a build-to-lossless phase. WRED drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. Thus, higher priority traffic is delivered with a higher probability than lower priority traffic.

Load Balancing

Each View Connection Server is capable of supporting up to 2,000 users. *A load balancer is not required for less than this number, and therefore we only implemented one in this Reference Architecture.* However, in environments that mandate it, it is possible to deploy multiple View Connection brokers by using a load balancer to serve them. A load balancer can balance the number of sessions across View Connection servers, monitor their health, perform SSL offloading, and provide other useful functions.

Many different available hardware and software load balancing solutions have been validated with View. Consult with your load balancer vendor on system settings and recommended best practices for deployment with View.

Business Continuity

The system is designed to be resilient in the event of a component system failure. This design does not cover a disaster recovery scenario in which the entire site is lost, but it does cover component failures.

Two View Connection Servers are installed to provide scalability and availability. If a connection server fails, the other server is capable of taking on the extra load.

FAILURE POINT	REDUNDANCY
View desktop	If a desktop fails, the user must report it to support. A new desktop can be provisioned if the current desktop cannot be fixed. Users might lose work in this scenario.
VMware vCenter Server	If vCenter Server fails, View is not affected. Virtual desktops can still be connected; however, new desktops cannot be provisioned. Workloads are not balanced across clustered hosts. Desktops cannot be powered on or off.
VMware ESXi host	If a virtual desktop host fails, the user loses connection to the desktop. The desktop is migrated to another host in the cluster and started. The user can connect to the desktop within minutes. Users might lose work in this scenario.
Horizon View Infrastructure Server	**The virtual desktops are powered off, and deltas are lost. If a View Manager Server host fails, the user's session is disconnected. A user can log back in, and no work on the virtual desktop is lost. It is recommended to not place all View Manager Servers in the same instance on a single host. Anti-affinity rules for two View Connection Servers are recommended.** If all View Manager Servers hosts in a VMware cluster lose connectivity or fail, availability is lost. Users who are connected do not get disconnected, but users trying to authenticate to the View Servers at time of failure cannot succeed.
View desktop cluster failure	If all hosts in a View desktop cluster lose connectivity or fail, users assigned to the desktop pools hosted on the affected cluster cannot access a virtual desktop until the cluster is restored.

Table 8. Potential Failure Points and Redundancy

Appendix B: Technical Design Specifications

The technical design specifications are described here in the order of construction.

View Management Block

A View Connection Server provides user authentication and redirects incoming remote desktop requests to the appropriate View desktop. View Connection Servers within the same pod are replicas of each other and can be used for scaling and load balancing purposes. They also share a single Active Directory for Application Mode (ADAM) database. Each View Connection Server system runs the View Administrator that is the primary mechanism for View configuration and administration. The View Connection Servers must be part of the Active Directory forest.

View Connection Server

The View Connection Server is a VMware virtual machine with the specifications listed in Table 9.

ATTRIBUTE	SPECIFICATION
Number of Connection Servers	1
Physical or virtual machine	Virtual machine – VMware Virtual Hardware 8
Number of processors	8 vCPUs
Memory	32GB
Number of NICs and speed	3x VMXNET 3 adapters at 10GbE
Total storage	80GB
Operating system	Windows Server 2008 R2 Enterprise SP1 (64-bit)
View Connection Server	View
SSL certificate	Each View Connection Server requires an SSL certificate for client machines to connect using SSL. See "Configuring SSL Certificates for View Servers" in *View Installation*.

Table 9. View Connection Server Virtual Machine Specifications

If a View Connection Server fails or becomes nonresponsive while an active, established, and tunneled session exists, the desktop state is preserved in the virtual desktop instance. When the user reconnects, the desktop session continues where it left off when the failure occurred.

In the case of direct connections, users are unaffected by any View Connection Server disruption, because their session is established directly with the View desktop. If the connection between the client device and the View desktop is broken, the desktop state is also preserved, and the session continues when the client reconnects.

Global Policies

All pools are governed by a global policy, outlined in Table 10. The global policy is used to deny or allow access to certain View Manager features. For instance, USB devices are allowed to connect to virtual desktop sessions, and multimedia redirection is allowed to enhance video and audio playback in user sessions where possible.

A pool policy set at the pool level can override a global policy. Alternatively, the policy can be set at a user level.

POLICY FEATURE	SETTING
USB access	Allow
Multimedia redirection (MMR)	Allow
Remote Mode	Allow
PCoIP hardware acceleration	Allow – medium priority

Table 10. View Global Policies

Active Directory Integration

The design employs an organizational unit (OU) created specifically for View desktops. An OU is a subdivision in Active Directory that contains users, groups, computers, or other OUs.

By creating a dedicated OU for View Desktop, View–specific policies tare applied via Group Policy Objects (GPO) to all machines created dynamically by View Manager during operation without knowing the actual workstation account name.

View Manager includes administrative templates for managing View virtual machines. Administrators can import these templates and apply them via a GPO to the respective OUs. This method provides a straightforward and consistent way to manage policies specific to View virtual machines and users.

View Client GPO Template

Table 11 identifies the GPO properties available to use with the View Client GPO template (vdm_client.adm).

PROPERTY	UPDATED	REMARKS
Scripting Definitions	No	
Server URL	Yes	
Default value of the Log in as Current User checkbox		Disabled This setting does not allow current user credentials for authentication to View. You can override this setting at the command line using the switch LogInAsCurrentUser false | true Alternatively, you can set a registry entry (REG_DWORD): Key = \Software\Policies\VMware, Inc.\VMware VDM\Client\Security\ Name = LogInAsCurrentUser Value = 0 | 1 You can set this at the HKLM or HKCU registry level.
RDP Settings (optional) **Desktop Background** **Enable Persistent** **Bitmap Caching** **Redirect Drives** **Redirect Printers**	Yes	 Disabled Enabled Disabled Disabled

Table 11. GPO Configuration for View Client

View Server GPO Template

Table 12 identifies the GPO properties available to use with the View Server GPO template (vdm_server.adm). Table 13 lists the properties for vdm_common.adm.

PROPERTY	UPDATED	REMARKS
Recursive enumerationof trusted domains	Yes	Enabled

Table 12. GPO Configuration for View Server Template

PROPERTY	UPDATED	REMARKS
Log Configuration	Yes	
Days to keep		7 days
Maximum Number		10 logs
Maximum Size		100MB

Table 13. GPO Configuration for View Server Common Components

PROPERTY	UPDATED	REMARKS
Enforce removal of Remote Desktop Wallpaper	Yes	Set to Enable
Limit maximum color depth	Yes	Fixed to 16-bit
Remote Windows Security Item from Start Menu	Yes	Set to Enable
Remove Disconnect option from shut down dialog	Yes	Set to Enable

Table 14. GPO Configuration for View Desktop Common Components

View Agent GPO Template

Table 15 and Table 16 identify the GPO properties available to use with the View Agent GPO template (vdm_agent.adm).

PROPERTY	UPDATED	REMARKS
Always wait for network at computer startup	Yes	Enabled Avoids inaccessible user profile and data during the login process

Table 15. GPO Configuration for View Desktops

PROPERTY	UPDATED	REMARKS
Recursive enumeration of trusted domains	Yes	Disabled Only directly trusted domains are enumerated and connection to remote domain controllers does not take place.
AllowDirectRDP	Yes	Disabled Does not allow users to RDP to desktop outside of View control.

Table 16. GPO Computer Configuration for View Agent

PCoIP GPO Template

Table 17 identifies the GPO properties available with the use of the PCoIP GPO template (pcoip.adm).

PROPERTY	UPDATED	REMARKS
Minimum image quality	No	50 (default)
Maximum initial image quality	Yes	Set to 70 (default is 90)
Frame rate limit	Yes	Set to 12 (default is 30 frames per second)
MTU size	Yes	Set to equal to or less than the lowest MTU size of the endpoints (default is 1400)
Maximum link rate	Yes	

Table 17. GPO Computer Configuration for PCoIP

View Security Server

The following tables list information about the security server specifications. For more information, see *VMware vCenter Server 5.1 Database Performance Improvements* and *Best Practices for Large-Scale Environments*.

ATTRIBUTE	SPECIFICATION
Number of security servers	1
Physical or virtual machine	Virtual machine – VMware Virtual Hardware 8
Number of processors	4 vCPUs
Memory	10GB
Number of NICs and speed	1 VMXNET3 adapter at 10GbE
Total storage	80GB
Operating system	Windows Server 2008 R2 Enterprise SP1 (64-bit)
View Connection Server	View

Table 18. View Security Server Virtual Machine Specifications

ATTRIBUTE	SPECIFICATION
VM Hardware	VMware Virtual Hardware version 8
OS	Windows Server 2008 R2 Enterprise SP1
vCPU	4
vMemory	10GB
Number of NICs and speed	1 VMXNET3 adapter at 10GbE
Virtual SCSI controller 0	LSI Logic SAS
Total storage	80GB

Table 19. SQL Server Virtual Machine Specifications

ATTRIBUTE	SPECIFICATION
Vendor and version	Microsoft SQL Server 2008R2
Authentication method	SQL Authentication
Recovery method	Simple
Database autogrowth	Enabled in 1MB increments
Transaction log autogrowth	In 10% increments. Restricted to 2GB maximum
Database size	5GB

Table 20: View Composer Database Specifications

The managed database service resides on a Microsoft SQL Server 2008 platform. Table 21 summarizes the configuration requirements for the View Events database.

ATTRIBUTE	SPECIFICATION
Vendor and version	Microsoft SQL Server 2008
Authentication method	SQL Authentication
Recovery method	Simple
Database autogrowth	Enabled in 1MB increments
Transaction log autogrowth	In 10% increments; restricted to 2GB maximum
Database size	5GB

Table 21. View Events Database Specification

vCenter Operations

VMware vCenter Operations Manager™ 5.8.2 was deployed as a vApp with two virtual appliances: a Web UI server and an analytics engine. A virtual adapter is also installed on View Connection Server to allow access to information about the virtual desktops.

ATTRIBUTE	WEB UI APPLIANCE	ANALYTICS APPLIANCE
OS	CentOS	CentOS
vCPU	4 vCPUs	4 vCPUs
vRAM	11GB	14GB
Storage	143GB	226GB

Table 22. vCenter Operations Manager Virtual Machine Specifications

Kaspersky Antivirus

The requirement we had for this Reference Architecture was that rather than running an AV agent in each VM (which is inefficient and causes severe performance issues through AV storms), we needed to leverage vShield Endpoint. The fact that licenses for vShield Endpoint are included with View licenses proves that is essentially the default.

Currently there are many Endpoint AV vendors that support vShield Endpoint, with similar architectures and performance. The full list of vendors is covered in this document from VMware:

http://www.vmware.com/files/pdf/products/vcns/vmware-integrated-partner-solutions-for-networking-and-security.pdf

For this Reference Architecture, we **randomly** chose Kaspersky's Security for Virtualization. More information about this product can be found here:
http://www.kaspersky.com/products/business/applications/security-virtualization

Given the choice was random, our use of Kaspersky in this Reference Architecture should not be interpreted as an endorsement of this particular product; any of the other vendors with vShield Endpoint solutions (including, but not limited to, McAfee, Sophos and Trend Micro) can be substituted for Kaspersky.

These are the specifications of the centralized AV management VM:

ATTRIBUTE	SPECIFICATION
Version	Kaspersky Security Center Administration Server 10.0.3361
VM Hardware	VMware Virtual Hardware version 9
OS	Windows Server 2008 R2 Enterprise SP1
vCPU	2
vMemory	8GB
vNICs	2
Virtual network adapter 1	VMXNet3 Adapter
Virtual SCSI controller 0	LSI Logic SAS
Virtual disk – VMDK	100GB
Virtual floppy drive 1	Removed
Virtual CD/DVD drive 1	Removed

Table 23. Kaspersky Security Center Specifications

With vShield Endpoint, an additional secure virtual machine runs on each ESXi host to scan the desktop virtual machines:

ATTRIBUTE	SPECIFICATION
Version	Kaspersky Security for Virtualization 2.0.0.34
VM Hardware	VMware Virtual Hardware version 7
OS	SUSE Linux Enterprise 11 64-bit
vCPU	2
vMemory	1024MB
vNICs	2
Virtual network adapter 1	VMXNet3 Adapter
Virtual SCSI controller 0	LSI Logic Parallel
Virtual disk – VMDK	30GB
Virtual floppy drive 1	Removed
Virtual CD/DVD drive 1	Removed

Table 24. Kaspersky Secure Virtual Machine Specifications

VMware vShield Manager™

To complete the vShield Endpoint solution, another VMware Management VM is necessary:

ATTRIBUTE	SPECIFICATION
Version	vShield Manager 5.1
vCPU	2
vMemory	8GB allocated, 3GB reserved
vNICs	1
Virtual network adapter 1	VMXNet3 Adapter
Virtual SCSI controller 0	LSI Logic Parallel
Virtual disk – VMDK	60GB

Table 25. vShield Manager Virtual Machine Specifications

Active Directory Domain Controller

ATTRIBUTE	SPECIFICATION
VM Hardware	VMware Virtual Hardware version 9
OS	Windows Server 2008 R2 Enterprise SP1
vCPU	2
vMemory	4GB
vNICs	1
Virtual network adapter 1	VMXNet3 Adapter
Virtual SCSI controller 0	LSI Logic Parallel
Virtual disk – VMDK	40GB Windows System

Table 26. Active Directory Domain Controller Virtual Machine Specifications

Sizing (per Microsoft Solution Accelerator Infrastructure Planning and Design document):

- 500MB for Active Directory DS transaction logs
- 500MB for the drive containing the SYSVOL share
- 1.5–2GB for the Windows Server 2008 operating system files
- 0.4GB of storage for every 1,000 users in the directory for the NTDS.dit drive

VMware ThinApp® Repository (OPTIONAL)

ATTRIBUTE	SPECIFICATION
VM Hardware	VMware Virtual Hardware version 9
OS	Windows Server 2008 R2 Enterprise SP1
vCPU	2
vMemory	4GB
vNICs	1
Virtual network adapter 1	VMXNet3 Adapter
Virtual SCSI controller 0	LSI Logic Parallel
Virtual disk – VMDK	40GB Windows System 100GB CIFs Share with ThinApp

Table 27. Thinapp Virtual Machine Specifications

Windows Print Server

ATTRIBUTE	SPECIFICATION
VM Hardware	VMware Virtual Hardware version 9
OS	Windows Server 2008 R2 Enterprise SP1
vCPU	2
vMemory	6GB
vNICs	1
Virtual network adapter 1	VMXNet3 Adapter
Virtual SCSI controller 0	LSI Logic Parallel
Virtual disk – VMDK	50GB Windows System

Table 28. Windows Print Server Virtual Machine Specifications

Windows DHCP or DNS Server

ATTRIBUTE	SPECIFICATION
VM Hardware	VMware Virtual Hardware version 9
OS	Windows Server 2008 R2 Enterprise SP1
vCPU	2
vMemory	4GB
vNICs	1
Virtual network adapter 1	VMXNet3 Adapter
Virtual SCSI controller 0	LSI Logic Parallel
Virtual disk – VMDK	40GB Windows System

Table 29. Windows DHCP or DNS Virtual Machine Specifications

View Pod

You configure View Manager with the Web-based View Administrator console. The console lets you configure each View Manager Server, including the connection mode (direct or tunneled), tags (for specifying pool types to be accessed), authentication methods, and View Manager database backup (ADAM backup, not SQL Server). Apply the configuration settings in Table 30 to each View Manager Server.

ATTRIBUTE	SPECIFICATION
Tags	Blank
Direct Connect Mode	Unchecked
Smartcard Authentication	Unchecked
RSA Authentication	Unchecked
View Manager Automatic Backup	
Backup frequency	Every day
Backup time	12 midnight
Maximum number of backups	10
Folder Location	C:\ProgramData\VMware\VDM\backups
View Administrators	AD Group for users with administrative rights to the View Administrator console. By default, all local administrator users on the View Manager Server can log in to the View Administrator console.

Table 30. View Manager Server Configuration

View Manager – Global Settings Configuration

The View Pod hosts a single instance of View Manager. Each View Manager server shares a common group configuration, also known as global settings. Global settings specify connection, security, and local mode operation settings. Table 31 lists the global settings for this design.

Session timeout specifies how long a user can remain connected to a desktop session. The timeout feature provides security and session management if a user forgets to disconnect or log out of a session at the end of a work shift. SSL is used for client connections to provide secure authentication between the View Client and View Connection Server.

View offers the ability to warn users if a forced logout is necessary. By setting this warning, administrators can ensure that users are given enough time to save their work and log out.

ATTRIBUTE	SPECIFICATION
Session timeout	600 (10 hours)
View Administrator Session Timeout	120 minutes
Auto Update	Disabled
Display pre-login message	No
Display warning before logout	Yes
Reauthenticate secure tunnel connections after network interruption	No
Enable IPSec for security server pairing	Yes
Message security mode	Mixed
Disable Single Sign-On for Local Mode Operations	No

Table 31. View Manager Global Settings

View Manager – vCenter Server Configuration

View Connection Servers use vCenter Server to provision and manage View desktops. vCenter Server is configured in the View Manager.

ATTRIBUTE	SPECIFICATION
Description	View vCenter Server for Desktops
Connect using SSL	Yes
vCenter Port	443
View Composer Port	18443
Enable View Composer	Yes
Advanced Settings:	
Maximum Concurrent vCenter Provisioning Operations	30
Maximum Concurrent Power Operations	30
Maximum Concurrent View Composer Maintenance Operations	30
Maximum Concurrent View Composer Provisioning Operations	30

Table 32. vCenter Server Configuration

View Block

The design specifications and connections for the View block components are listed in the following sections.

View Composer

View Composer can be installed on the same machine as the vCenter Server, however in our testing we installed it on a separate VM, in order to better monitor and manage the performance of the infrastructure. View Composer requires a database, which must be created (see Table 20). Table 33 summarizes the View Composer virtual machine specifications.

ATTRIBUTE	SPECIFICATION
Number of vCenter Servers	1
Physical or virtual machine	Virtual machine – VMware Virtual Hardware 9
Number of processors	4 vCPUs
Memory	10GB
Number of NICs and speed	2x VMXNET3 adapters at 10GbE
Total storage	80 gb
Operating system	Windows Server 2008 R2 Enterprise SP1 (64-bit)

Table 33. View Composer Virtual Machine Specifications

Database Connections

DATABASE NAME	ACCOUNT NAME	DATABASE RIGHTS
Db_view_comp	view_comp	Dbowner

Table 34. View Composer Database Connection

DATA SOURCE	SERVER	ODBC DRIVER	AUTHENTICATION	ACCOUNT
Sql_vc_ODBC	Sql-view-prod	SQL Native Client 10.0	SQL	Sql_vc

Table 35. vCenter SQL ODBC Connection

ATTRIBUTE	SPECIFICATION
Database Server	Sql-view-prod
Database Type	Microsoft SQL Server
Port	1433
Database Name	Sql-viewevents
Username	Sql_ve
Table Prefix	VE

Table 36. View Events Database Connection

Virtual Machine Image Build

A single master OS image was used to provision desktop sessions in the View environment. Use a fresh installation of the guest OS so that the correct versions of the HAL, drivers (including the optimized network and SCSI driver), and OS components are installed. A fresh install also avoids performance issues with legacy applications or configurations of the desktop virtual machine.

The Windows 7 Golden Image was deployed with the attributes listed in Table 37. The image was optimized in accordance with the *View Optimization Guide for Windows 7 and Windows 8*. The VMware OS Optimization Tool (available from https://labs.vmware.com/flings/vmware-os-optimization-tool) was used to make the changes: all of the ones recommended by the tool **except** disabling the Windows Firewall. The Windows Firewall **must be left enabled** for the View 6 agent to run.

ATTRIBUTE	SPECIFICATION
Desktop OS	Windows 7 Enterprise SP1 (32-bit)
Hardware	VMware Virtual Hardware version 10
CPU	1
Memory	1024MB
Memory Reserved	0MB
Video RAM	8MB
3D Graphics	Off
NICs	1
Virtual network adapter 1	VMXNET 3 Adapter
Virtual SCSI controller 0	LSI Logic SAS
Virtual disk – VMDK	30GB
Virtual floppy drive 1	Removed
Virtual CD/DVD drive 1	Removed

Table 37. Windows 7 Gold Image Virtual Machine Specifications

Sizing VMware ESXi Hosts

CPU Sizing

DESKTOP PERFORMANCE METRIC	RECORDED VALUE
Average number of CPUs per physical desktop system	1
Average CPU utilization per physical desktop system	185MHz
vCPU Overhead	10%

Table 38. Total Virtual Machine CPU Requirements

ATTRIBUTE	SPECIFICATION
Number of CPUs (sockets) per host	2
Number of cores per CPU	12
GHz per CPU core	2.7GHz
Total CPU GHz per CPU	32.4GHz
Total CPU GHz per host	64.8GHz
Proposed maximum host CPU utilization	80%
Available CPU GHz per host	51.84GHz
VMs per Host	255
Total ESX Hosts Required	5 (4+1)

Table 39. ESXi Host CPU Requirements

Memory Sizing

ATTRIBUTE	SPECIFICATION
Proposed maximum host memory utilization	80%
Total amount of RAM per virtual machine	1024MB
Anticipated transparent memory sharing (TPS) saving	30%
Memory Overhead	118MB
3D	–
Total amount of RAM per host	256GB TPS

Table 40. ESX Host Memory Requirements – Desktop Virtual Machines

ATTRIBUTE	SPECIFICATION
Antivirus SVM (1 per ESX)	1GB

Table 41. ESX Host Memory Requirements – AV Virtual Machines

Storage Sizing – Dedicated Linked Clones

ATTRIBUTE	SPECIFICATION
Desktop OS	Windows 7 Enterprise SP1 (32-bit)
Hardware	VMware Virtual Hardware version 10
CPU	1
Memory	1024MB
Video RAM	8MB
3D Graphics	Off
NICs	1
Virtual network adapter 1	VMXNet3 Adapter
Virtual SCSI controller 0	LSI Logic SAS
Virtual disk – VMDK	30GB (25.59GB thin)
Virtual floppy drive 1	Removed
Virtual CD/DVD drive 1	Removed

Table 42. Dedicated Linked Clones Virtual Desktop Template Specifications

ATTRIBUTE	SPECIFICATION
Type of Pool	Automated
User Assignment	Dedicated
Automatic Assignment	Enable Automatic Assignment
VM Type	View Composer Linked Clone
Delete or refresh on logout	Refresh at logout at 10% Disk Utilization
Persistent Disk	Do not redirect
Disposable Files Redirection	Do not redirect – with Tintri there is no need for or performance benefit to redirecting disposable files
Select different datastores for replica and OS	No (one datastore for everything) – with Tintri, there is no need to (no performance benefit) split replica and OS into different datastores
Use View Storage Accelerator	No (unchecked) – with Tintri, there is no need for or performance benefit to VSA
Use native NFS snapshots (VAAI)	Yes (checked)
Guest Customization	Use QuickPrep

Table 43. Dedicated Linked Clones View Pool Configuration

FULL CLONE (MB)	DELTA (MB)	MEMORY VSWAP (MB)	VIDEO VSWAP (MB)	VM STORAGE (MB)	MEMORY OVERHEAD (MB)	TOTAL VM STORAGE (TB)	TOTAL VM MEMORY (MB)
0	2457	1024	8	3515	118	3.35	1,142

Table 44. Dedicated Linked Clones Virtual Machine Requirements

NUMBER OF VIRTUAL MACHINES	PARENT CAPACITY (TB)	REPLICA CAPACITY (TB)	CLONE CAPACITY (TB)	TOTAL CAPACITY REQUIRED (TB)
1	0.02	0.02	0.0	0.04
1000	0.02	0.02	3.69	3.73

Table 45. Dedicated Linked Clones Capacity Requirements

NUMBER OF VIRTUAL MACHINES	REPLICA FRONT-END IOPS	CLONE FRONT-END IOPS	TOTAL FRONT-END IOPS
1	2520	45	2565
1000	2520	45000	47520

*40 IOPS per desktop, about 20/80 Read/Write

Table 46. Dedicated Linked Clones IOPS Requirements

Appendix C: Validation

The desktops were tested under load (LoginVSI Office Worker workload) and for standard View operations.

Workload Testing

Login Virtual Session Indexer (Login VSI) is the industry standard load testing tool for virtualized desktop environments. Login VSI can be used to test the performance and scalability of VMware Horizon View, Citrix XenDesktop and XenApp, Microsoft Remote Desktop Services (Terminal Services) or any other Windows based virtual desktop solution.

Login VSI was designed by experienced VDI and SBC specialists, who created a tool that was easy to implement, easy to use and very cost-effective. Because Login VSI can be deployed very quickly it allows you to profit from the benefits of testing in every phase of your VDI project.

Login VSI allows you to measure the maximum capacity of your current infrastructure in a quick and easy way. The simulated users work with the same applications as your average employee such as Word, Excel, Outlook and Internet Explorer.

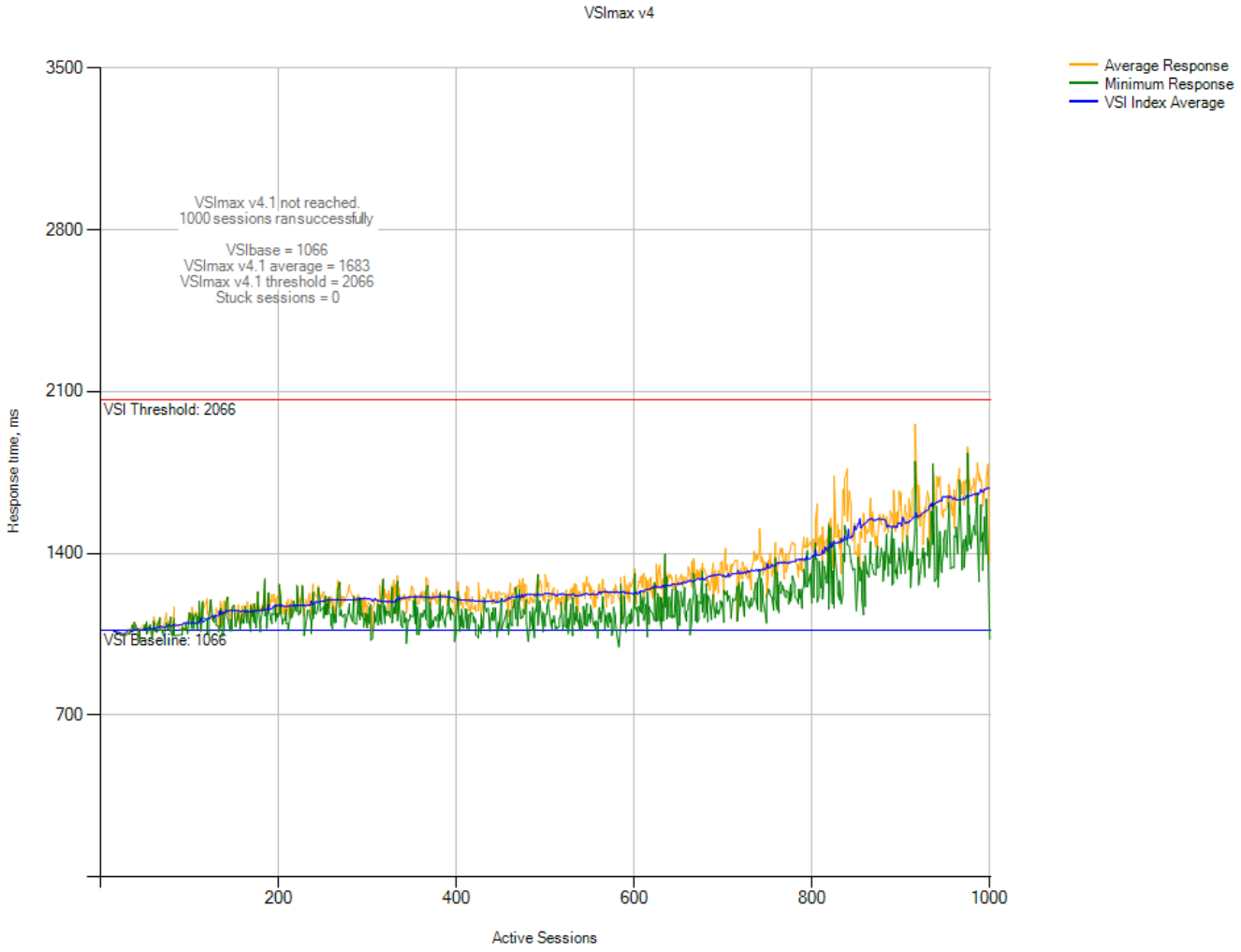
Test Results

VSImax v4	1000 Sessions & Baseline 1066 ms
VSI Threshold reached?	NO
VSIbaseline average response time (ms)	1066
VSImax average response time threshold (ms)	2066
VSImax threshold was reached at sessions	WAS NOT REACHED
VSI response time threshold headroom	1983
Sessions not responding	0
Corrected VSImax is	1000
Total Sessions configured	1000
Total Sessions successfully launched	0
Total Timeframe of test in seconds	2880
Average session launch interval in seconds	2.88
Amount of active launchers during test	50
Average session capacity per launcher	20

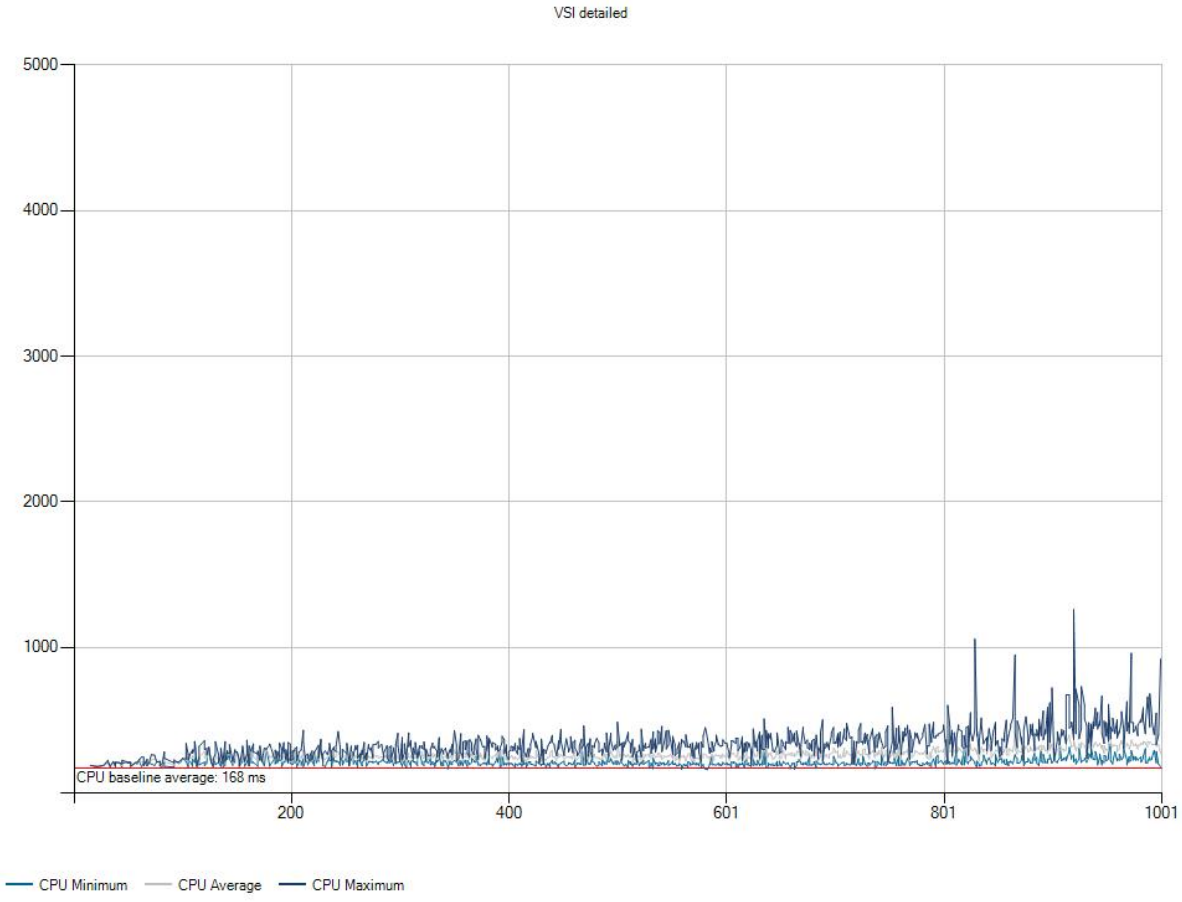
VSI response time overview (ms)

VSI response time @ 50 Sessions	1069
VSI response time @ 100 Sessions	1093
VSI response time @ 150 Sessions	1137
VSI response time @ 200 Sessions	1153
VSI response time @ 250 Sessions	1177
VSI response time @ 300 Sessions	1199
VSI response time @ 350 Sessions	1196
VSI response time @ 400 Sessions	1214
VSI response time @ 450 Sessions	1200
VSI response time @ 500 Sessions	1200
VSI response time @ 550 Sessions	1221
VSI response time @ 600 Sessions	1220
VSI response time @ 650 Sessions	1234
VSI response time @ 700 Sessions	1254
VSI response time @ 750 Sessions	1290
VSI response time @ 800 Sessions	1315
VSI response time @ 850 Sessions	1358
VSI response time @ 900 Sessions	1396
VSI response time @ 950 Sessions	1511

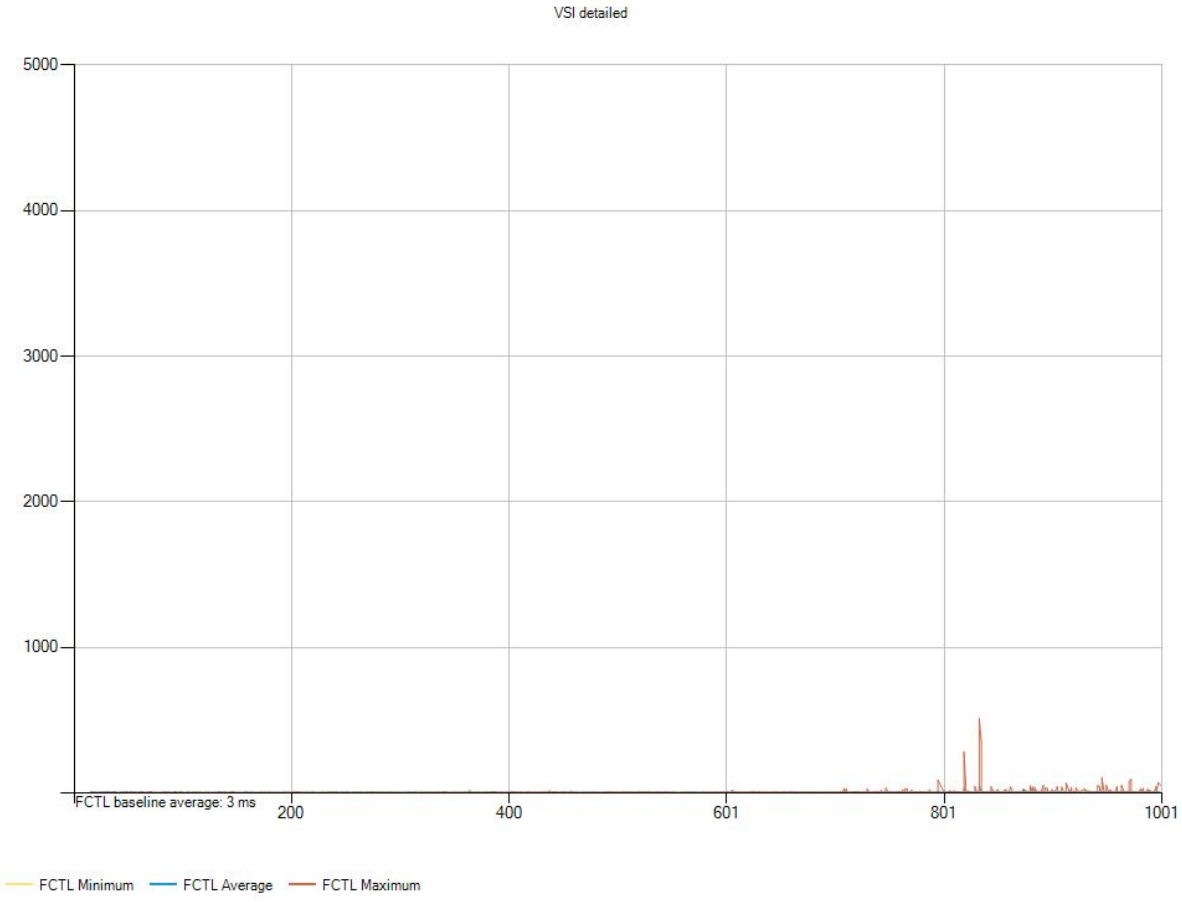
VSImax Overview



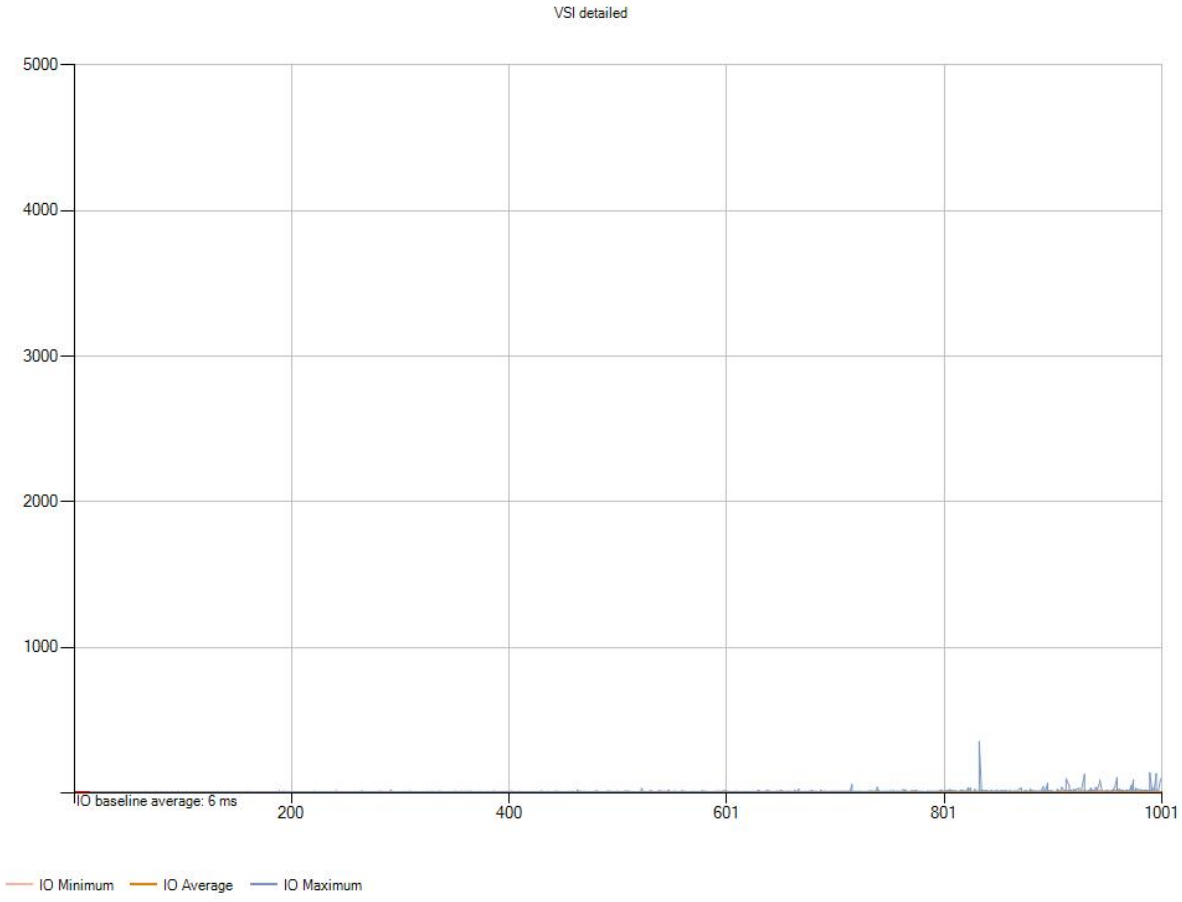
Word Load overview (WSLD)



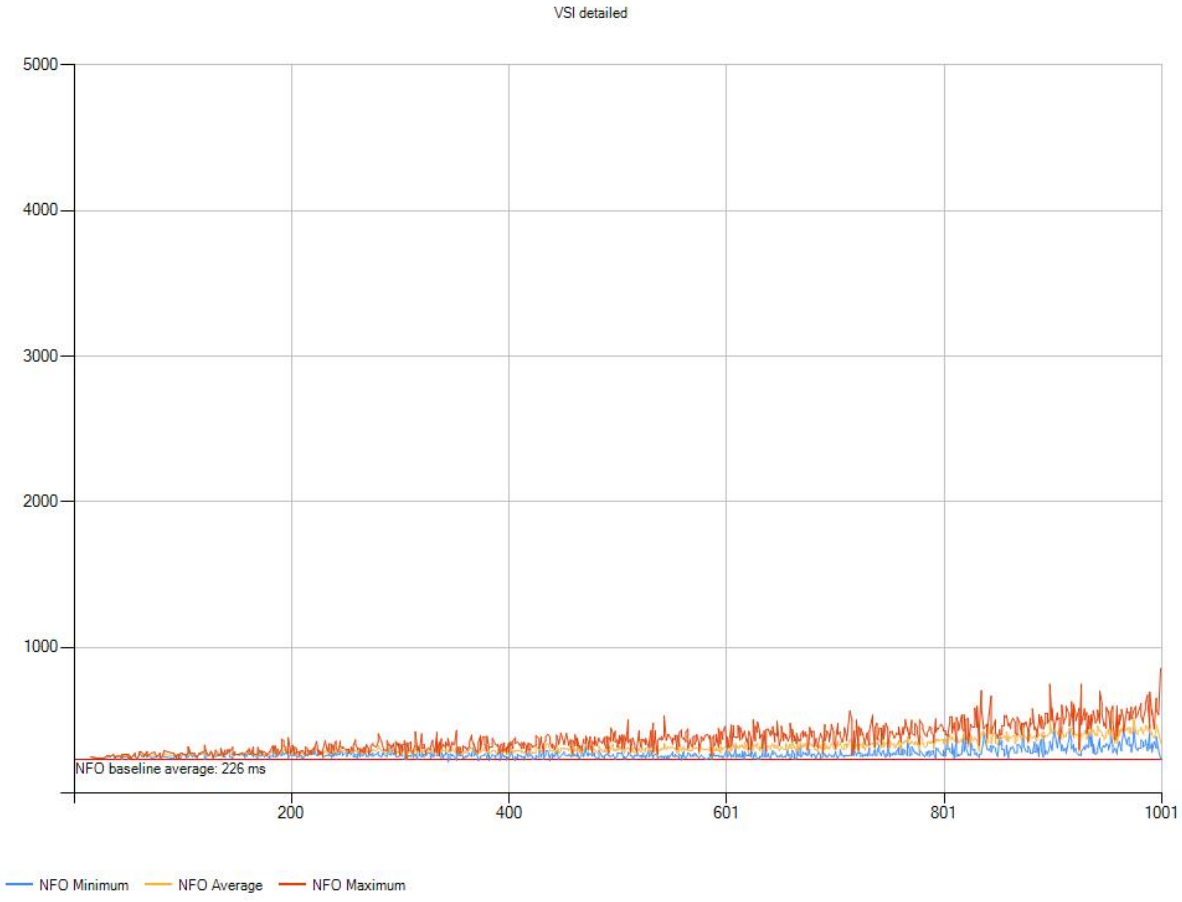
Notepad Load overview (NSLD)



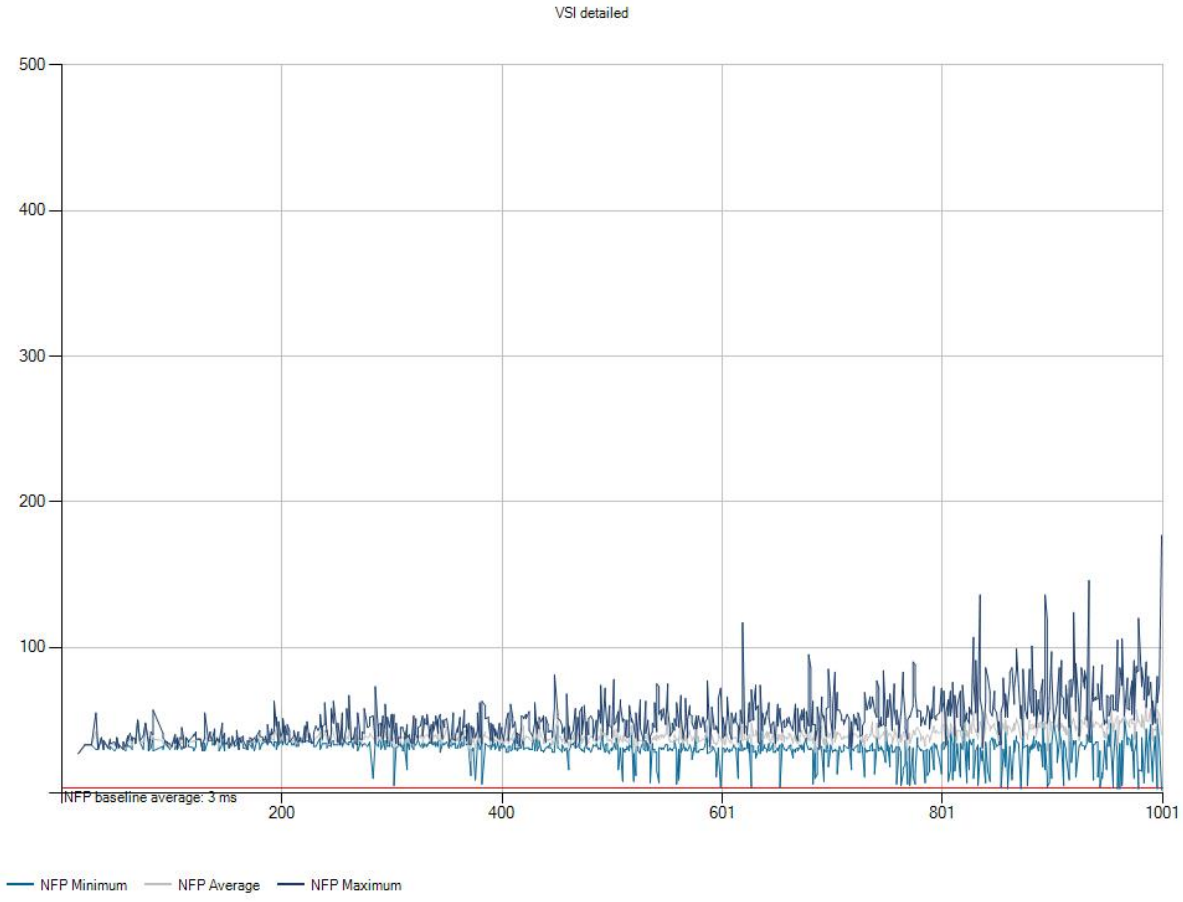
Print Dialogue overview (NFP)



Zip High Compression (ZHC)



Zip No Compression (ZNC)



Tintri OS 3.0 Dashboard

The two below charts show the load on the Tintri VMstore during the entire duration of the LoginVSI Office Workload test.

IOPS

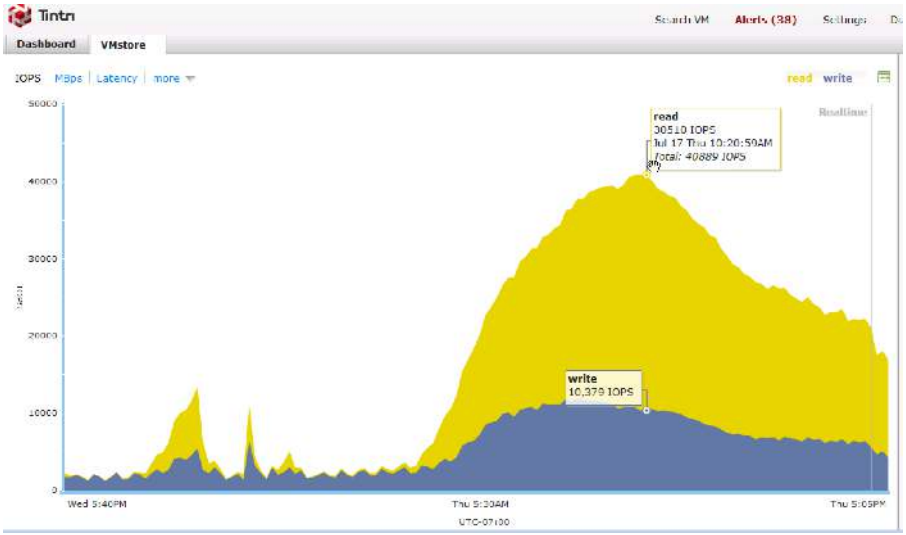


Figure 7. IOPS Chart during LoginVSI Office Workload testing

MBps

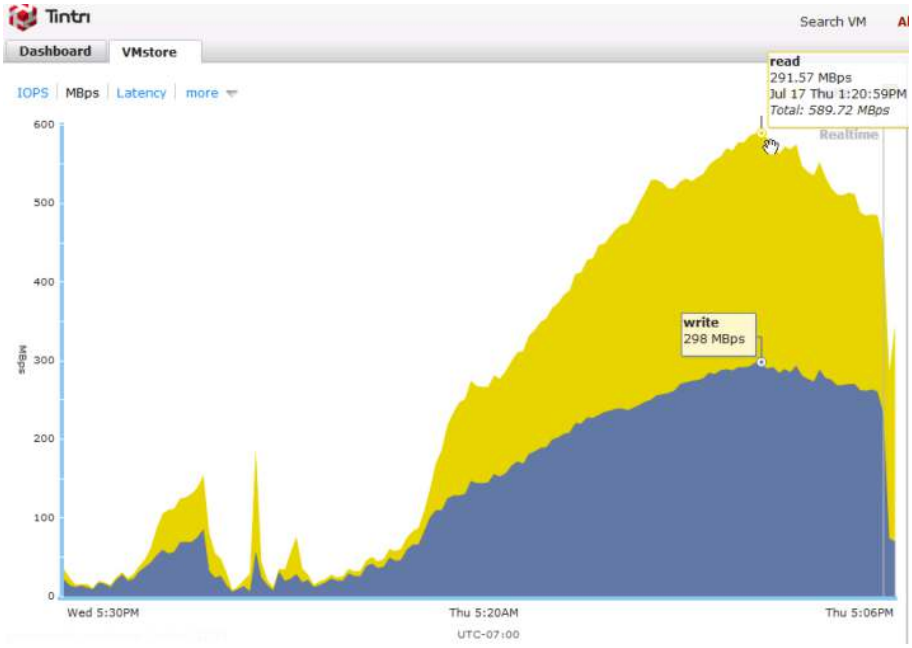


Figure 8. MBps Chart during LoginVSI Office Workload testing

Operations Testing

The common View pool maintenance operations listed in Table 47 were exercised to test system performance under load. Note that although View Composer has also the "Rebalance" operation – which evenly redistributes linked clones among available logical drives – the use of a Tintri VMstore – which presents itself as a single datastore – makes that operation unnecessary.

OPERATION	DESCRIPTION	SUCCESSFUL OUTCOME
Provision pool	Pool of desktops is created from the master image.	Desktop pool provisioned without errors.
Desktop recompose	Parent image is updated and a new snapshot created. All linked clones in the pool anchored to the old snapshot or image are updated to the new image. (In production, this operation should take place outside of business hours).	All desktops recomposed to new image without errors.
Desktop pool refresh	Restores the OS disk of each linked clone to its original state and size, reducing storage costs.	All desktops refreshed to original image successfully.
Desktop pool deletion	Desktop pool is deleted, and the associated virtual desktops and replicas are destroyed.	Pool and all associated desktops are cleanly removed, without errors.

Table 47. Validation: Operations Testing

TEST	DEDICATED LINKED CLONES
1,000 desktops provisioned	1 hours 37 minutes
1,000 desktops recomposed	1 hour 52 minutes
1,000 desktops refreshed	36 minutes
Pool deleted	27 minutes

Table 48. Results: Operations Testing

Appendix D: Bill of Materials

The test configuration bill of materials is summarized in Table 49.

AREA	COMPONENT	QUANTITY
Server	Cisco UCS 5108 Chassis	1
	Cisco UCS B200 M3 Blades (2 x Intel E5 2697 v2 @ 2.7 GHz, 12-Core, 256GB RAM)	5
	Cisco UCS B22 M3 Blade (2 x Intel E5 2420 @ 1.9 GHz, 6-Core, 144GB RAM)	1
Storage	Tintri VMstore T650	1
Network	Cisco UCS 6248UP Fabric Interconnects	2
Software	VMware ESXi	6
	VMware vCenter	1
	View	4 [1000 users total]
	VMware vCOPs for View	1 [1100 machines]
	VMware vShield	1 [Manager/Endpoint]
	Kaspersky Security Server	1 [Licenses for 1100 VMs]
	Kaspersky SVM	6
	Microsoft Windows 2008 R2	9
	Microsoft SQL Server 2008 R2	1

Table 49. Test Configuration Bill of Materials

References

Tintri

Tintri VMstore T600 Series Data Sheet

VMstore Overview White Paper

Tintri Scaling Virtual Environments White Paper

Tintri VMstore: Zero Management Storage for Virtualization and Cloud

VDI with VMware Horizon View

VMware

VMware Product Page

http://www.vmware.com/products

View Documentation

https://www.vmware.com/support/pubs/view_pubs.html

View Technical Resources

http://www.vmware.com/products/desktop_virtualization/view/technical-resources.html

VMware End-User Computing Solutions

http://www.vmware.com/end-user-computing.html

View Optimization Guide for Windows 7 and Windows 8

http://www.vmware.com/resources/techresources/10157

Antivirus Best Practices for Horizon View 5.x

http://www.vmware.com/resources/techresources/10258

VMware vCenter Database Performance Improvements + Best Practice for Large-Scale Environments

http://www.vmware.com/files/pdf/techpaper/VMware-vCenter-DBPerfBestPractices.pdf

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