Streamlined and scalable:

Virtual desktops with QoS and simplified management

Cisco® UCS™ Manager, Cisco UCS B230 M2 Blade Server with M81KR Virtual Interface Card, VMware® vSphere® Auto Deploy & host profiles, VMware View™ 5

Implementing a new virtual desktop infrastructure or expanding your current environment can present unwanted long-term challenges to your IT staff, including scalability problems, rapid provisioning issues, policy management concerns, and lack of network visibility into the infrastructure. With the right solution, however, deploying and managing new compute resources can be an easy process that is both automated and repeatable.

VMware View 5 running on VMware vSphere 5 and Cisco Unified Computing System (UCS) Manager provides such a solution. Cisco UCS Manager makes it possible to quickly add server blades to your existing server chassis with UCS Service Profiles, in a completely automated process. VMware vCenter then fully installs and configures a stateless vSphere server installation on the blade and adds it to your existing virtual desktop cluster.

In addition, Cisco VM-FEX brings management benefits like QoS and network visibility into the VDI environment. VM-FEX allows you to govern individual VMs and critical VMkernel interfaces with QoS and throttling policies, ensuring that functions such as vMotion traffic will not affect network latency and that VOIP, or other sensitive traffic, has priority over less critical data. Moreover, it enables debugging, monitoring, and fault management for a virtual desktop or the hosted shared environment. The automated deployment process of the Cisco UCS Manager with VMware vCenter Auto Deploy and the management features enabled by VM-FEX help minimize the complexity and administrative costs of your VMware View 5 environment.

March 2012

A PRINCIPLED TECHNOLOGIES TEST REPORT

Commissioned by Cisco Systems, Inc.

SIMPLE DEPLOYMENT, GRANULAR MANAGEMENT

Whether for a new or growing VDI deployment, you must adapt your physical infrastructure to meet the simplicity and scalability requirements of your virtual desktop infrastructure. When selecting data center infrastructure to meet this demand, choosing hardware and software with automatic deployment capabilities that scale on demand saves time, reduces cost, and reduces the risk of human error. Infrastructures with built-in management capabilities, such as Cisco UCS Manager and VMware vCenter, continue to deliver operational benefits after deployment.

We tested the effectiveness of Cisco UCS Manager, VM-FEX, and associated technologies in our labs, and found that they made it simple to add a Cisco UCS B230 M2 Blade Server to a Cisco UCS 5108 Blade Server Chassis. We needed only to unbox the server, install the physical blade, and configure an answer file in vCenter. UCS Manager and vCenter handled the remaining steps, including fully configuring and adding the blade to the virtual desktop cluster. VMware vSphere Distributed Resource Scheduler (DRS) moved View 5 virtual desktops onto the new host. We then used the Cisco UCS Manager to view network statistics directly from the VM interfaces. (See Figure 1.) This process is automated and repeatable.

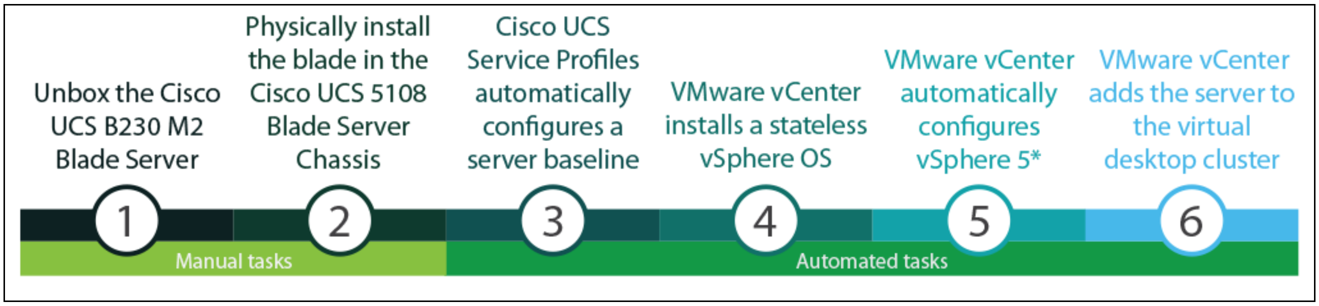

Unbox the Cisco UCS B230 M2 Blade Server
Physically install the blade in the Cisco UCS 5108 Blade Server Chassis
Cisco UCS Service Profiles automatically configures a server baseline
VMware vCenter installs a stateless vSphere OS
VMware vCenter automatically configures vSphere 5*
VMware vCenter adds the server to the virtual desktop cluster
1
2
3
4
5
6
Manual tasks
Automated tasks

Figure 1: How Cisco UCS and VMware vCenter almost fully automate virtual desktop server deployment.
*Note that we manually applied an answer file for VMware Auto Deploy.

Once the new server was up and running, Cisco Virtual Machine Fabric Extender (VM-FEX) technology also allowed us to configure per-port Quality of Service (QoS) policies to virtual machines, or VMkernel interfaces. This allowed us to manage constrained networks by giving priority to a particular VM or group of VMs, or to prioritize on storage traffic such as iSCSI or NFS, as well as to throttle on other network intensive functions such as vMotion. We were also able to view individual -port network statistics from the Cisco UCS Manager.

Cisco UCS Manager and UCS Service Profiles make blade deployment and management easy

When we created the Cisco UCS Service Profile template for our blade deployment the Cisco UCS Manager allowed us to create a custom hardware baseline for the type of virtual desktop workload for as many servers as we wanted. (See Figure 2).

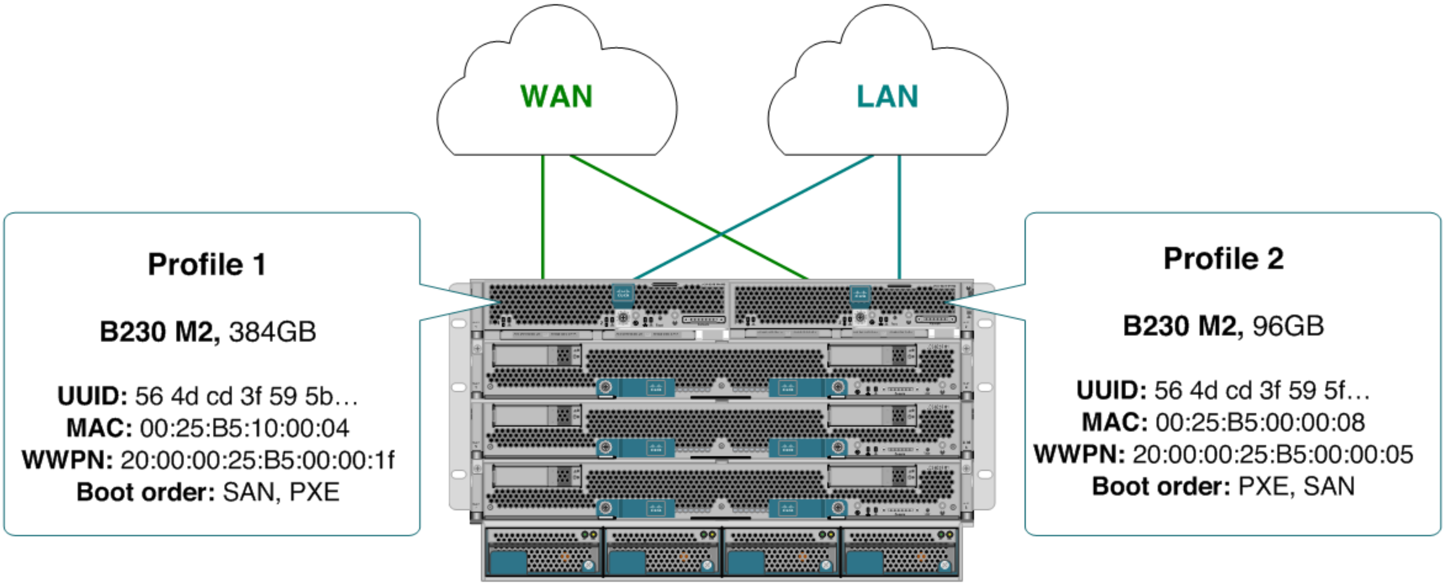


Figure 2: Cisco UCS Service Profiles.

On the service profile templates, we could define firmware policies, enable BIOS settings such as hyper-threading and Virtualization Technology, configure the local disk array, configure memory speed, and select a boot sequence. Once created, these templates can be deployed to as many blades as you require.

When we powered on the Cisco UCS B230 M2, VMware Auto Deploy used our PXE boot infrastructure and vSphere host profiles to provision and customize the new server. Because Auto Deploy stores the vSphere 5 OS in memory only, the server is stateless, so no local disk or boot from SAN configuration is required for operation. Stateless servers are preferred from a security point of view because when powered off no persistent data remains on the server. Because there is no configuration on the server, stateless servers are easy to replace.

When the vCenter Server system was fully loaded, Auto Deploy added the blade to our virtual desktop cluster. Once added, vCenter Server configured the network, storage, firewall, and advanced features like Cisco VM-FEX.

Cisco UCS Service Profiles and VMware Auto Deploy made blade deployment a stateless, scalable, and fully automated process. Figure 3 compares this approach to a traditional blade deployment.

Comparison of blade deployment steps	
Traditional blade deployment	**Cisco UCS + VMware Auto Deploy**
1. Unbox the server	1. Unbox the server
2. Physically install blade	2. Physically install blade
3. Firmware install: system (requires media + reboot)	3. Configure an answer file in vCenter
4. Firmware install: management controller (requires media + reboot)	Stateless and fully automated—no further steps required.
5. Firmware install: NIC/HBA (requires media + reboot)	
6. Firmware install: array controller (requires media + reboot)	
7. Configure internal disk array	
8. Configure out-of-band KVM	
9. Configure BIOS features (requires reboot)	
10. Set boot order/device	
11. ESXi install: boot from media	
12. ESXi install: accept EULA, keyboard layout, root password	
13. ESXi install: specify disk, requires persistent disk space, or BFS	
14. Configure additional ESXi packages and drivers	
15. Add ESXi to a virtual desktop cluster	
16. Configure management network	
17. Enable SSH and SSH shell	
18. Configure VMkernel networks	
19. Configure traditional networks and DVS	
20. Apply ESX updates (requires reboot)	
21. Configure DNS	
22. Configure NTP	
23. Configure NFS or iSCSI	
24. Configure firewall	
25. Configure licensing	
26. Troubleshooting	

Figure 3: Cisco UCS and VMware auto deployment compared to traditional blade deployment.

VM-FEX management tools improve quality of service

VM-FEX also allows data center administrators to provision, configure, manage, monitor, and diagnose VM network traffic, extending the benefit of the remote fabric extender to the VM. The VM bypasses the vSwitch, allowing for improved performance while offloading some CPU overhead from the vSphere server. VM-FEX allows you to govern individual VMs and critical VMkernel interfaces with QoS and throttling policies, ensuring that functions like vMotion traffic will not affect network latency and that sensitive traffic has priority over other data.

Figure 4 illustrates how VM-FEX enables VMware Direct I/O to the virtual desktop offering bare-metal speed with per-port manageability features like QoS, statistics, and diagnosing capabilities.

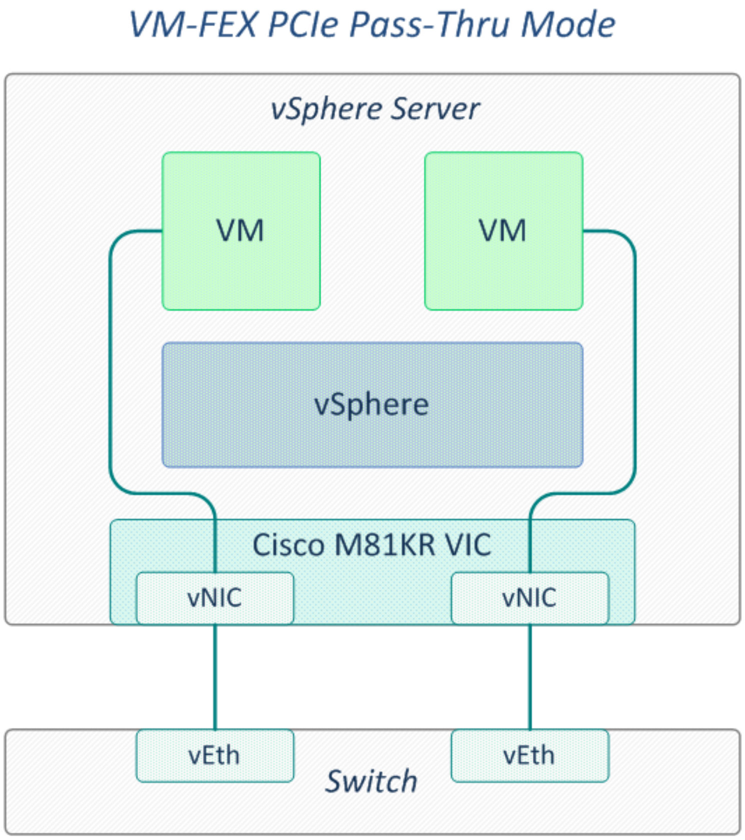


Figure 4: VM-FEX provided us with extensive management options, helping to improve QoS.

It is essential that high-priority, latency-sensitive traffic, such as VoIP, and power users, such as stock traders, are unaffected by peaks in network usage. VM-FEX allows QoS policies to be applied directly to the VM and VMkernel interfaces, giving network administrators granular controls to prioritize traffic from user groups and VMkernel interfaces that facilitate NFS, iSCSI, or vMotion traffic.

In our scenario, we were able to demonstrate the value of QoS in a VMware View virtual desktop environment. Specifically, we enabled platinum, bronze, and best effort QoS system classes and applied QoS policies to vMotion and three other virtual desktop users to simulate a diversity of service levels governed by the systems classes. We defined our service levels as low, medium and high, and we configured a QoS policy to cap the vMotion traffic at 1 Gbps. To simulate network contention between service classes, we ran JPerf and instructed all virtual desktop users to contend for available network bandwidth, while simultaneously instructing vCenter to migrate 30 virtual desktops across the same network via vMotion.

Figure 5 shows network throughput of low-, medium-, and high-priority data, as well as vMotion data, without QoS policies applied. Bandwidth to high-, medium-, and low-priority users was severely constrained when virtual desktops were migrating. When the 30 virtual desktops completed the migration via vMotion, more bandwidth was available, but users contended for bandwidth equally over the remainder of the test, with high-priority users receiving no advantage over other classes.

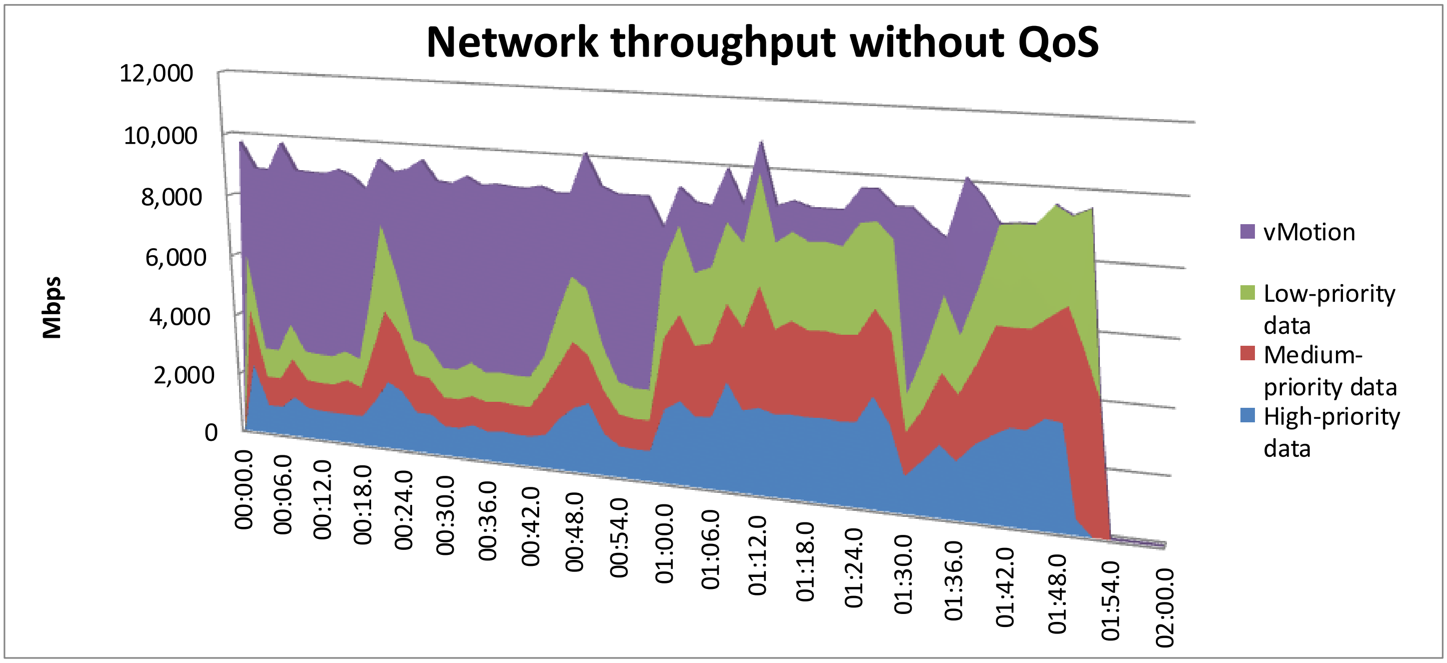


Figure 5: Network throughput results without QoS policies applied. Greater Mbps for high-priority data is better.

Figure 6 shows the same scenario with QoS policies applied to low-, medium-, and high-priority data, as well as a 1Gbps cap to vMotion data. The QoS policies ensured that high-priority data received more bandwidth than other classes of data, and that bandwidth-intensive functions like vMotion did not disrupt users from working.

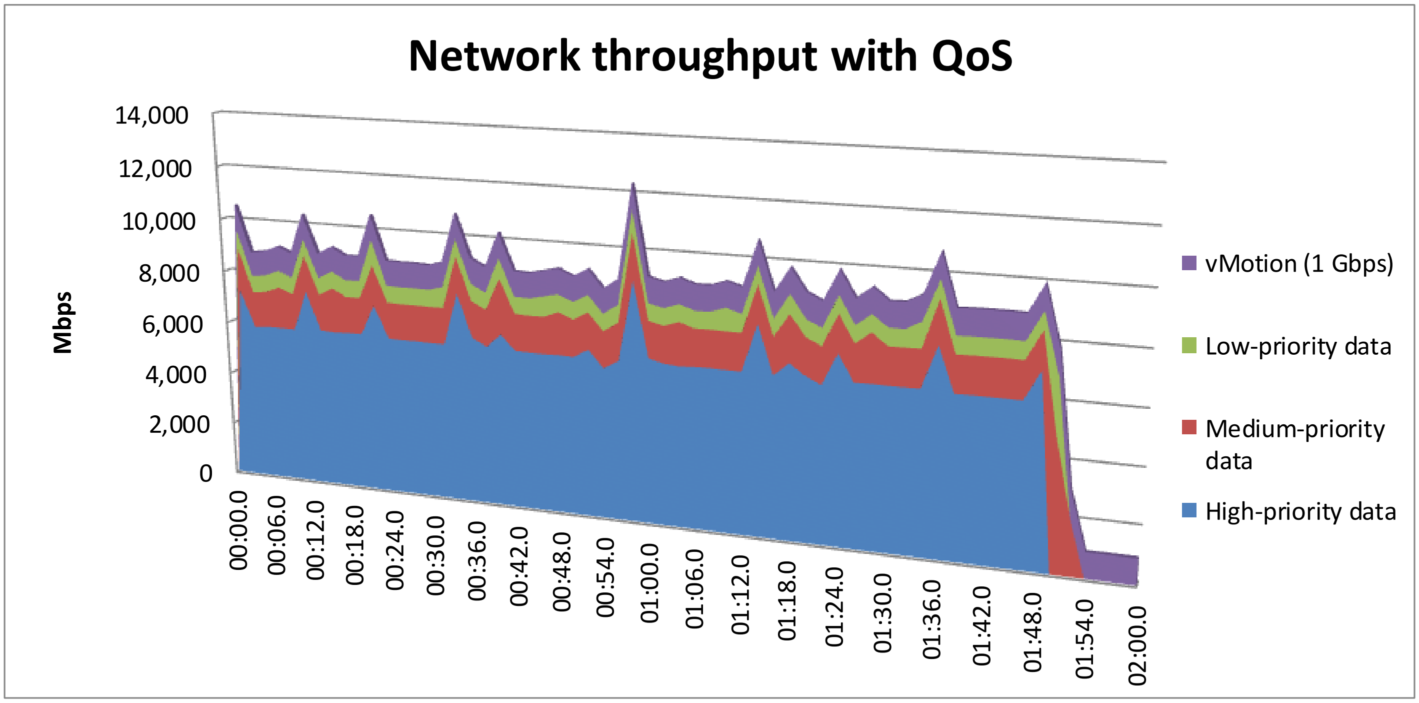


Figure 6: Network throughput results with a QoS profile. Greater Mbps for high-priority data is better.

Figure 7 shows the total data transferred in each scenario, with and without QoS policies.

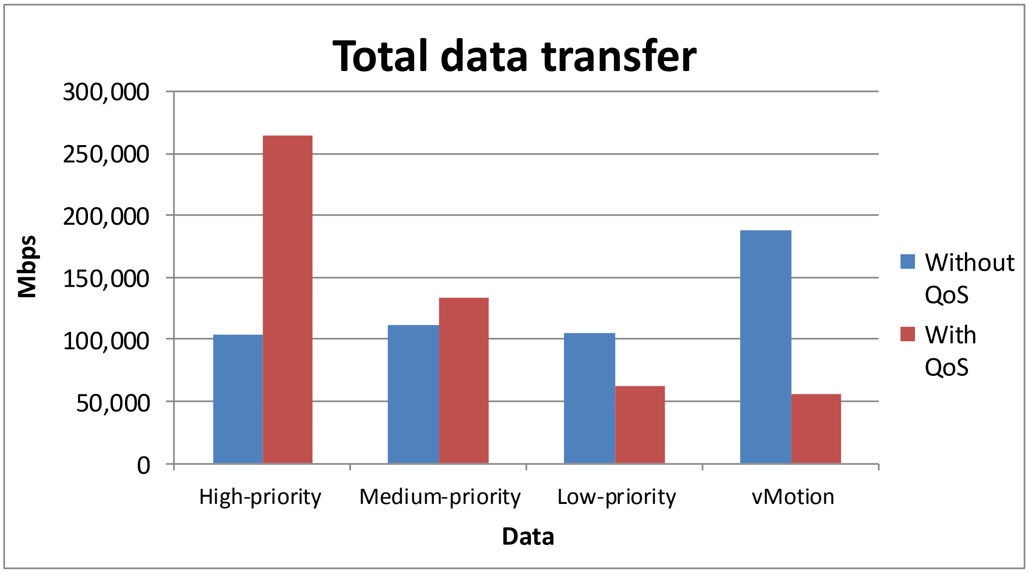
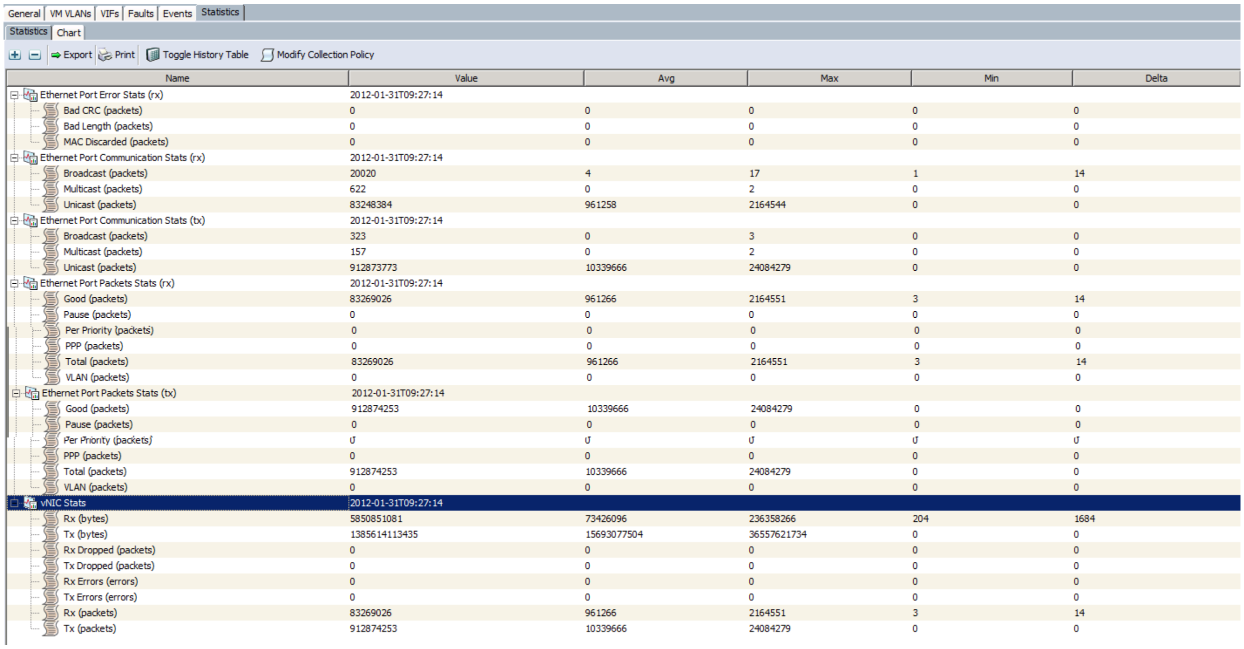


Figure 7: Total data transfer. Greater Mbps for high-priority data are better.

VM-FEX allows visibility into the network, directly from the UCS Manager. A network admin can view historical statistics to isolate and detect rogue users, infected desktops, or general misappropriation in the event of a reported network issue. Figure 8 shows a sample screenshot from the VM-FEX statistics-gathering screen.



Name	Value	Avg	Max	Min	Delta
Ethernet Port Error Stats (rx)	2012-01-31T09:27:14				
Bad CRC (packets)	0	0	0	0	0
Bad Length (packets)	0	0	0	0	0
MAC Discarded (packets)	0	0	0	0	0
Ethernet Port Communication Stats (rx)	2012-01-31T09:27:14				
Broadcast (packets)	20020	4	17	1	14
Multicast (packets)	622	0	2	0	0
Unicast (packets)	83248384	961258	2164544	0	0
Ethernet Port Communication Stats (tx)	2012-01-31T09:27:14				
Broadcast (packets)	323	0	3	0	0
Multicast (packets)	157	0	2	0	0
Unicast (packets)	912873773	10339666	24084279	0	0
Ethernet Port Packets Stats (rx)	2012-01-31T09:27:14				
Good (packets)	83269026	961266	2164551	3	14
Pause (packets)	0	0	0	0	0
Per Priority (packets)	0	0	0	0	0
PPP (packets)	0	0	0	0	0
Total (packets)	83269026	961266	2164551	3	14
VLAN (packets)	0	0	0	0	0
Ethernet Port Packets Stats (tx)	2012-01-31T09:27:14				
Good (packets)	912874253	10339666	24084279	0	0
Pause (packets)	0	0	0	0	0
Per Priority (packets)	0	0	0	0	0
PPP (packets)	0	0	0	0	0
Total (packets)	912874253	10339666	24084279	0	0
VLAN (packets)	0	0	0	0	0
vNIC Stats	2012-01-31T09:27:14				
Rx (bytes)	5850851081	73426096	236358266	204	1684
Tx (bytes)	1385614113435	15693077504	36557621734	0	0
Rx Dropped (packets)	0	0	0	0	0
Tx Dropped (packets)	0	0	0	0	0
Rx Errors (errors)	0	0	0	0	0
Tx Errors (errors)	0	0	0	0	0
Rx (packets)	83269026	961266	2164551	3	14
Tx (packets)	912874253	10339666	24084279	0	0

Figure 8: VM-FEX statistics-gathering function for virtual desktops and VMkernel interfaces.

UCS Manager can plot network data on demand for individual virtual desktops and VMkernel interfaces, which allows network administrators to see visual trends for network usage and errors. This is a level of visibility not available on host performance monitors like Microsoft Windows Performance Monitor or VMware esxtop (see Figure 9).

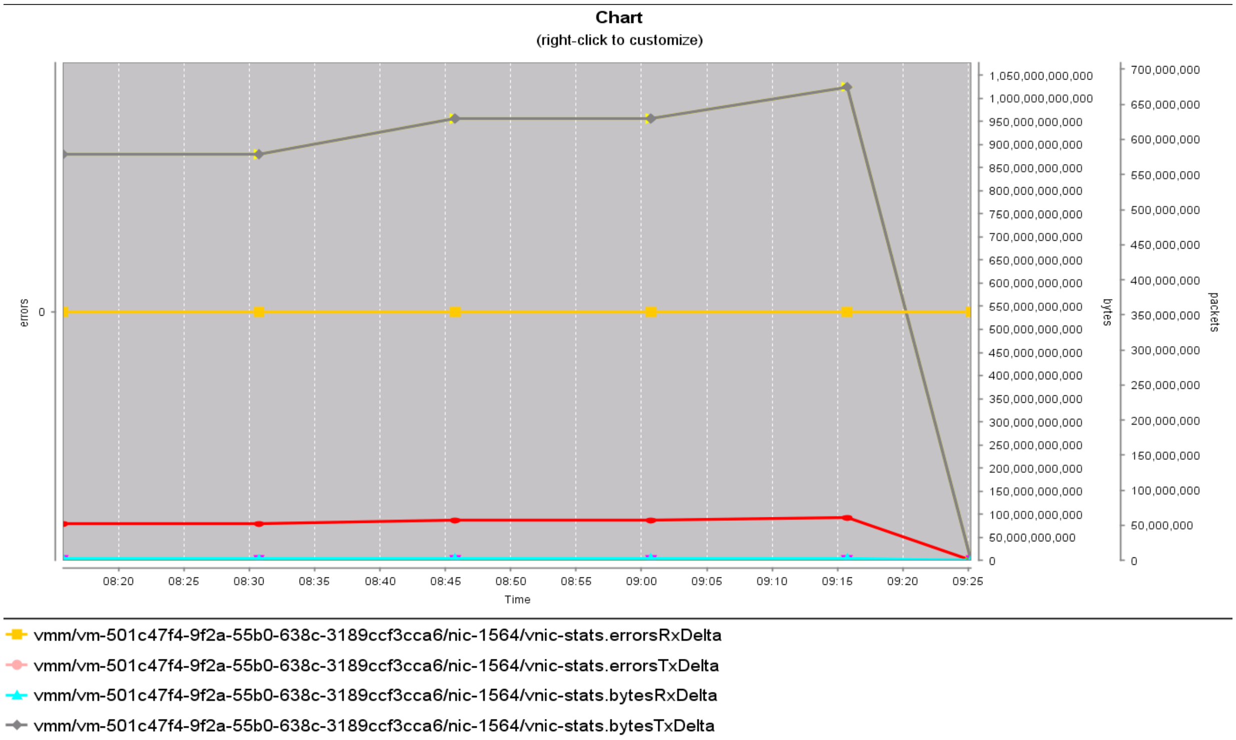


Figure 9: VM-FEX statistics network data plot for virtual desktops and VMkernel interfaces.

WHAT WE TESTED

Cisco UCS 5108 Blade Server Chassis

We used a Cisco UCS 5108 Blade Server Chassis, which holds a maximum of eight Cisco UCS B230 M2 Blade Servers.

To learn more about the Cisco UCS 5100 Series Blade Server Chassis, visit http://www.cisco.com/en/US/products/ps10279/index.html.

Cisco UCS 6120XP Fabric Interconnects

We connected a Cisco UCS 5108 Blade Server Chassis to a redundant pair of Cisco UCS 6120XP Fabric Interconnects. The connection supports redundant 4x10Gb links via eight 10Gb SFP connections—four to Interconnect A and four to Interconnect B. The Cisco UCS 6120XP Fabric Interconnects act as convergence points for all network and fabric uplinks into the connected Cisco UCS 5108 Blade Server Chassis. We created our UCS Service Profiles and deployed them to our Cisco UCS B230 M2 blades inside the Cisco UCS 5108 Blade Server Chassis.

To learn more about the Cisco UCS 6120XP Fabric Interconnect, visit http://www.cisco.com/en/US/products/ps10301/index.html.

Cisco UCS B230 M2 Blade Server

We used a VDI-optimized, dual-socket Cisco UCS B230 M2 Blade Server with Intel Xeon processor E7-4870s, two 32GB Intel X-25E SATA SSDs, and 512 GB of system memory. We installed a Cisco M81KR Virtual Interface Card (VIC) into the server, which is a dual-port 10Gb Converged Network Adapter (CNA) optimized for virtualization. The M81KR supports up to 128 PCIe-compliant virtual interfaces and Cisco VN-Link technology. The VIC ensures reliable 10Gb, low-latency connectivity to SAN and LAN, while allowing for greater flexibility and ease of management. Additionally, the Cisco UCS B230 M2 blade server provides support for two hot-swappable SSD drives that are accessible from the front of the server, and for an LSI SAS2108 RAID controller.

To learn more, see Appendix A for more detailed hardware specifications, or visit http://www.cisco.com/en/US/products/ps11583/index.html.

Cisco UCS Manager

The Cisco UCS Manager enables unified, embedded management that integrates the management of both software and hardware on the Cisco UCS solution. The UCS Manager centralizes server management, making it easier in several key ways. First, role-based management makes it easy to assign unique management roles to different administrators (i.e., server, network, or storage admins) so that each can be assigned his or her own unique policies and permissions, while still being part of an integrated management environment. Policy-based provisioning provides managers with the ability to create service profile templates that they apply to one or 100 servers, making it easy to apply consistent policies. The Cisco USC Manager makes server management less about managing isolated, single hardware components and more about managing many hardware components (up to 40 chassis and 320 blades) as a single management domain. The use of service profiles allows managers to allocate and reallocate server resources, which the UCS Manager views as “raw computing capacity.” This way, server capacity allocation becomes more dynamic and efficient, with managers able to deploy and reallocate server resources in a matter of minutes.

To learn more about the Cisco UCS Manager, visit http://www.cisco.com/en/US/products/ps10281/index.html.

About VMware View 5

VMware designed its View 5 desktop virtualization software to simplify IT management of virtual desktops from within the cloud. A centralized interface allows administrators to manage upwards of tens of thousands of end-users. An administrator can easily manage settings such as policy enforcement, performance monitoring, connection brokering, and provisioning, to name a few. The result includes improved security, less costly management, and faster provisioning and maintenance of desktop images and applications. The end-user enjoys easier access to his or her View desktop from a variety of locations, less downtime, a customizable desktop, and robust multimedia capabilities. In our tests, we implemented a new feature of View 5, that of PCoIP Optimization Controls. This feature helps IT administrators better configure bandwidth settings (by user, use case, or network requirements), which can reduce bandwidth by up to 75 percent and improve protocol efficiency.

To learn more about VMware View 5, visit http://www.vmware.com/products/view/overview.html.

About VMware vSphere 5

vSphere 5 is the latest virtualization operating system from VMware. vSphere 5 allows companies to virtualize their server, storage, and networking resources, achieving a consolidation ratio greater than 15:1. Features such as automated management and dynamic resource allocation improve efficiency. The services that vSphere 5 provides fall into two categories: Infrastructure services or application services. The former handle the virtualization of resources and their allocation to application when most needed, while the latter provide service-level controls to applications running on vSphere 5.

To learn more about VMware vSphere 5, visit http://www.vmware.com/products/vsphere/overview.html.

VM Fabric Extender (VM-FEX) technology

VM-FEX technology allows administrators to manage VM network traffic and bare metal (i.e., physical) network traffic all from a single unified infrastructure. The advantages of this are that UCS Manager bypasses the vSwitch and manages the card, therefore achieving higher performance throughput with VMware Direct I/O, and that a per-port QoS policy allows you to prioritize traffic for each PCI device. Essentially VM-FEX lets you eliminate the intermediary and obtain faster performance.

To learn more about VM-FEX, visit http://www.cisco.com/en/US/netsol/ns1124/index.html#~overview.

SUMMARY

The combination of the Cisco UCS and VMware allows for an easily managed, feature-rich View 5 environment. Companies who need their VDI environment to be up and running as quickly and smoothly as possible, or who are adding to their existing infrastructure, would be wise to consider the Cisco-VMware combination as their solution.

APPENDIX A – SERVER AND STORAGE CONFIGURATION INFORMATION

Figure 10 provides detailed configuration information about the test servers. Note that we used the Cisco UCS B230 M2 Blade Server for the systems under test and used the Cisco UCS B200 M2 Blade Server for our testbed infrastructure. Figure 11 details the storage we used in our tests.

System	Cisco UCS B230 M2 Blade Server	Cisco UCS B200 M2 Blade Server
Enclosure		
Blade enclosure	Cisco UCS 5108	Cisco UCS 5108
Power supplies		
Total number	4	4
Wattage of each (W)	2,500	2,500
Cooling fans		
Total number	8	8
Dimensions (h x w) of each	3-5/8" x 5-1/2"	3-5/8" x 5-1/2"
General		
Number of processor packages	2	2
Number of cores per processor	10	6
Number of hardware threads per core	2	2
CPU		
Vendor	Intel	Intel
Name	Xeon	Xeon
Model number	E7-4870 (functionally the same as the E7-2870 in a two-socket configuration)	X5670
Stepping	A2 (SLC3T)	CO
Socket type	LGA 1567	LGA 1366
Core frequency (GHz)	2.40	2.93
Bus frequency (GT/s)	6.4	6.4
L1 cache	32 KB+ 32 KB (per core)	32 KB+ 32 KB (per core)
L2 cache	256 KB (per core)	256 KB (per core)
L3 cache (MB)	30	12
Platform		
Vendor and model number	Cisco UCS B230 M2 Blade Server	Cisco UCS B200 M2 Blade Server
Motherboard model number	B230-Base-M2	N20-B6625-1
Motherboard chipset	Intel 7500	Intel 5520
BIOS name and version	B230.2.0.1c.100520111716	Cisco S5500.2.0.1d.093030111102
BIOS settings	Default	Default
Memory module(s)		
Total RAM in system (GB)	512	96
Vendor and model number	Samsung M393B2K70CMB-YF8	Samsung M393B5170FH0-YH9
Type	DDR3 PC3-8500	DDR3 PC3-10600
Speed (MHz)	1,067	1,333
Speed running in the system (MHz)	1,067	1,333

System	Cisco UCS B230 M2 Blade Server	Cisco UCS B200 M2 Blade Server
Size (GB)	16	8
Number of RAM module(s)	32	12
Chip organization	Double-sided	Double-sided
Hard disk		
Vendor and model number	Intel X-25E SATA SSD	Seagate ST9146803SS
Number of disks in system	2	2
Size (GB)	32	146
RPM	N/A	10,000
Type	SATA	SAS
Controller	LSI™ MegaRAID® 9240	LSI Logic® SAS 1064E
Operating system		
Name	VMware vSphere 5 (504890)	VMware vSphere 5 (504890)
File system	VMFS	VMFS
Kernel	5.0.0	5.0.0
Language	English	English
Network adapter (mezzanine card)		
Vendor and model number	Cisco UCS M81KR Virtual Interface Card	Cisco UCS M71KR-Q QLogic® Converged Network Adapter

Figure 10: Detailed configuration information for the servers.

Storage array	iSCSI storage array
Array	1
Number of active storage controllers	1
Number of active storage ports	2
Firmware revision	5.0.7
Switch number/type/model	Cisco Nexus™ 5010
Disk vendor and model number	Seagate ST330065SS
Disk size (GB)	300
Disk buffer size (MB)	16
Disk RPM	15,000
Disk type	SAS

Figure 11: Detailed configuration information for the storage array.

APPENDIX B – TESTBED SETUP

Figure 12 shows our testbed configuration.

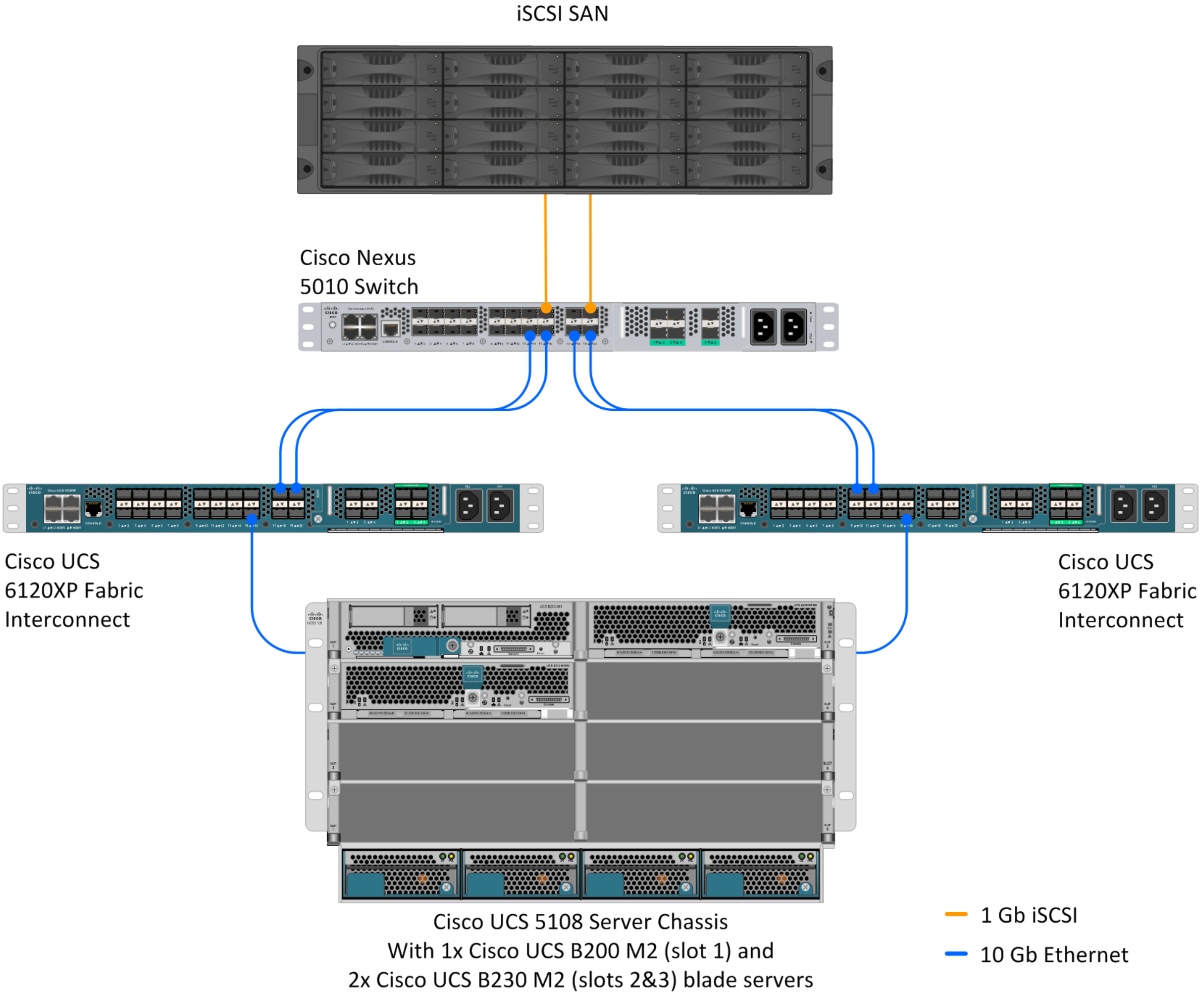

iSCSI SAN
Cisco Nexus 5010 Switch
Cisco UCS 6120XP Fabric Interconnect
Cisco UCS 6120XP Fabric Interconnect
Cisco UCS 5108 Server Chassis
With 1x Cisco UCS B200 M2 (slot 1) and
2x Cisco UCS B230 M2 (slots 2&3) blade servers
1 Gb iSCSI
10 Gb Ethernet

Figure 12: Our testbed setup.

APPENDIX C – TEST METHODOLOGY

Running the Auto Deploy test

We set up VMware View to use our view-cluster, and set up all Cisco UCS, VMware Auto Deploy, and VMware Host Profiles features. To add virtual desktop capacity to our VMware View cluster, we physically installed a blade and configured the answer file for the host Profile.

1. Boot the B230-M2 in slot 3 (please note the install process is not instantaneous).
2. Open vSphere client, and log into vCenter.
3. Browse to Home→Management→Host Profiles→vCenter, and open the Host and Clusters tab.
4. Select the host 172.0.0.91, right-click, and select Apply profile…

Configuring a new answer file for 172.0.0.91

1. For Software iSCSI initiator Selection, click Next.
2. For the initiator IQN section, click Next.
3. For the iSCSI alias, click Next.
4. For the MAC address, leave it blank, and click Next.
5. For the iSCSI address, enter a valid iSCSI address and subnet mask.
6. Leave the vMotion VMkernel MAC address blank, and click Next.
7. Enter a valid vMotion address, and click Update.
8. After the answer file is verified, click OK to finish applying the profile.
9. Exit maintenance mode.

DRS will move virtual desktops to the new cluster node.

Running the QoS test

We placed one of the virtual desktops in the platinum DVS port, another virtual desktop in the bronze DVS port, and another in the best_effort DVS port. We put the vMotion VMkernel interfaces into the vMotion DVS port. We then ran jperf from the three VMs to an external server while executing a vMotion of 30 virtual desktops. We then removed the QoS settings from the Cisco UCS Manager and reran the test. Using esxtop, we recorded bandwidth and compared the results.

Setting up the storage

Setting up the iSCSI storage

We hosted all VMware View virtual machines on a Cisco UCS B200 M2 blade. We installed VMware vSphere 5 on the Cisco UCS B200 M2 local storage. We hosted all virtual machine storage on an iSCSI Storage array and enabled jumbo frames on the UCS service profiles, the switches, and on each NIC on the iSCSI storage. We installed and configured VMware Auto Deploy to automatically deploy stateless ESXi to our Cisco UCS B230.

The iSCSI array contained 16 drives. We configured a single storage group with the array as the only member. We configured the storage group to have a single storage pool in RAID 50 mode. On the storage pool, we created one 1,024 GB LUN.

Setting up the external storage

1. Using the command-line console, via serial cable, reset the first iSCSI array by using the reset command.
2. Supply a group name, group IP address, and IP address for eth0.

3. After group creation, using a computer connected to the same subnet as the storage, use the iSCSI array's Web interface to do the following:
    a. Assign IP addresses on the remaining NIC (eth1). Enable both NICs.
    b. Set a MTU size of 9,000 on each NIC on the array.
    c. Create a storage pool by right-clicking Storage pools, and choosing Create storage pool.
    d. Choose Yes when prompted to configure the member.
    e. Choose RAID 50 for the RAID Policy.
    f. Create a 1024GB volume to host all View infrastructure and virtual desktops.
    g. For the volumes created in the previous step, limit access to IP address, and enter the class C address range for storage network (example:192.168.10.*).

Setting up the Cisco Unified Computing System

We used Cisco Unified Computing System guides to physically install and properly power the UCS chassis and fabric interconnects. For more information on the guide, see http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/ucs5108_install.html.

We configured a UCS cluster with two fabrics and defined a cluster IP address to enable the use of the Cisco UCS Manager. In the UCS Manager, we setup network VLANs, QoS policies, and service profiles for our three blades.

Defining all VLANs on the Cisco UCS

1. In the UCS Manager, go to the LAN tab.
2. Open LAN→LAN Cloud→VLANs, right-click, and select create VLAN.
    - Name=`MGMT-NET`
    - VLAN ID=`10`
3. Open LAN→LAN Cloud→VLANs, right-click, and select create VLAN.
    - Name=`VDI-NET`
    - VLAN ID=`100`
4. Open LAN→LAN Cloud→VLANs, right-click, and select create VLAN.
    - Name=`Storage`
    - VLAN ID=`222`
5. Open LAN → LAN Cloud→VLANS, right-click, and select create VLAN.
    - Name=`vMotion`
    - VLAN ID=`200`

Defining all QoS classes

1. In the UCS Manager, go to the LAN tab.
2. Open LAN→LAN cloud→QoS system class.
3. Enable Platinum.
    - COS=`5`
    - Weight=`10`
    - MTU=`9000`
4. Enable Bronze.
    - COS=`1`
    - Weight=`4`
    - MTU=`9000`
5. Edit Best Effort.
    - COS=`2`

    - Weight=4
    - MTU=9000
6. Open LAN→Policies→root→QoS Policies, right-click and create QoS Policies.
    - Name=Best_Effort, priority=Best Effort, Rate=line-rate, Host control=Full
    - Name=vMotion, priority=Platinum, Rate=1000000, Host Control=Full
    - Name=Platinum, priority=Platinum, Rate=line-rate, Host control=Full
    - Name=Bronze, priority=Bronze, Rate=line-rate, Host control=Full

Defining Dynamic vNIC policy

1. In the UCS Manager, go to the LAN tab.
2. Open LAN→Policies→root→Dynamic vNIC Policies, right-click Create Dynamic vNIC Connection Policy.
3. For name, type VM-FEX
4. For Number of Dynamic vNICs, select 9.
5. For adapter Policy, select VMware PassThru.
6. For Protection, select Protected Perf B, click OK to create the Create Dynamic vNIC Connection Policy.

Configuring Cisco Unified Computing profiles policies

Configuring KVM for blades

1. In the UCS System Manager, click the Admin tab→filter: Communication Management→Management IP address.
2. Click the General tab.
3. Click Create Block of IP addresses.
4. Create a block of 10 addresses on the management network.

Creating a MAC pool

1. In the UCS Manager, go to the LAN tab.
2. Open Pools→root→MAC pools, and right-click and select Create MAC Pool.
    - Name=VDI
    - From: 00:25:B5:AB:CD:01   To: 00:25:B5:AB:CD:20

Creating a vNIC template

1. Open LAN→Policies→root→vNIC Templates, and right-click and select Create vNIC Template.
    - Name=FAB-A
    - Adaptor=Fabric A
    - Target=Adaptor (*deselect VM*)
    - Template type=Updating template
    - MTU=9000
    - MAC pool=MAC-pool
    - QoS Policy=none
    - VLANS=10,100,200,222 (10=native)
2. Open LAN→Policies→root→vNIC Templates, right-click, and select Create vNIC Template.
    - Name=FAB-B
    - Adaptor=Fabric B
    - Target=Adaptor (*deselect VM*)
    - Template type=Updating template
    - MTU=9000

- MAC pool=`MAC-pool`
- QoS Policy=`none`
- VLANS=`10,100,222,200` (10=native)

Creating a PXE boot policy

1. In the UCS Manager, go to the Servers tab.
2. Open Servers→Policies→root→Boot Policies, right-click and select Create Boot Policy, and click OK.
3. For the name, type `PXE`
4. Click Add LAN Boot.
5. In the Add LAN Boot window, leave the LAN name blank and select OK.
6. Click OK to finish the PXE Boot policy.

Creating BIOS policies

1. In the UCS Manager, go to the Servers tab.
2. Open Servers→Policies→root→BIOS Policies.
3. Right-click BIOS Policies, and select Create BIOS policy.
4. Type `B200-M2` for the policy name, and assign all platform defaults.
5. Right-click BIOS Policies, and select Create BIOS policy.
6. Type `VM-FEX` for the policy name, and enable the following:
    - Processor - Enable Virtual Technology (VT) and Direct Cache Access.
    - Intel Directed IO - VT for Directed IO, Interrupt Remap, Coherency Support, ATS Support, and Pass Through DMA Support.

Creating host firmware policies

1. In the UCS Manager, go to the Servers tab.
2. Open Servers→Policies→root→Host firmware.
3. Right-click and select create host firmware package.
4. For Name, type `b200-m2`
    a. Click the Adaptor tab, enable the checkbox for Cisco M71KR-Q, and select version: 2.0(1s)
    b. Click the BIOS tab, enable the checkbox for Cisco B200-M2, and select version: S5500.2.0.1d.0.093020111102, and click OK to create the host firmware package.
5. Right-click and select Create Host Firmware Package.
6. For Name, type `b230-m2`
    a. Click the Adaptor tab, enable the checkbox for Cisco M81KR, and select version: 2.0(1s)
    b. Click the BIOS tab, enable the checkbox for B230-M2, and select version: B230.2.0.1c.0.100520111716
    c. Click the Board Controller tab, select the checkbox for Cisco UCS B230 M2, and select version: B320100C, and click OK to create the host firmware package.

Creating Management Firmware Package

1. In the UCS Manager, go to the Servers tab.
2. Open Servers→Policies→root→Management Firmware Packages.
3. Right-click and select Create Management Firmware Package.
4. For Name, type `CIMC`
5. Enable the check box for Model: Cisco UCS B230 M2, and Cisco UCS B200 M2, select version: 2.0(1s), and click OK to create the management firmware package.

Creating service profile templates for all blades

Creating a profile template for the Cisco UCS B200 M2 Blade Server

1. In the UCS Manager, go to the Servers Tab.
2. Open Servers→ Service Profile Templates→Root, right-click root, and select Create Service Profile Template.
3. In the Create Service Profile Template page 1, enter the following:
   - Name: `B200-template`
   - Type: `updating template`
4. Select Next.
5. In the Create Service Profile Template page 2 (storage), select default for local storage, WWNN and both vHBA fabrics, and click Next.
6. In the Create Service Profile Template page 3 (Networking), do not select a dynamic vNIC policy, and click the button next to Expert to view more options.
7. Click the Add button to add a vNIC.
8. In the Create a vNIC workspace, select use a LAN connectivity template.
9. Name the vNIC `vNIC0`, for vNIC Template, select FAB-A, and for Adaptor policy, select VMware. Click OK.
10. Click the Add button to add a second vNIC.
11. In the Create a vNIC workspace, select use a LAN connectivity template.
12. Name the vNIC `vNIC1`, for vNIC Template, select FAB-B, and for Adaptor policy, select VMware. Click OK.
13. Click Next to finish networking.
14. In the Create Service Profile Template page 4 (vNIC/vHBA Placement), click Next.
15. In the Create Service Profile Template page 5 (Server Boot Order), select localdisk, and click Finish.
16. Click the B200-template, and select the Policies tab.
17. In the BIOS Policy, select B200-M2.
18. In the Firmware Polices, select B200-M2 for Host firmware, and CIMC for Management firmware, and click Save changes.

Creating profile templates for the Cisco UCS B230 M2 Blade Servers

1. In the UCS Manager, go to the Servers Tab.
2. Open Servers→Service Profile Templates→Root. Right-click Root, and select Create Service Profile Template.
3. In the Create Service Profile Template page 1, enter the following:
   - Name: `B230-template`
   - Type: `updating template`
4. Select Next.
5. In the Create Service Profile Template page 2 (storage), select default for local storage, WWNN and both vHBA fabrics, and click Next.
6. In the Create Service Profile Template page 3 (Networking), select VM-FEX as the dynamic vNIC policy, and click the button Next to Expert.
7. Click the Add button to add a vNIC.
8. In the Create a vNIC workspace, select use a LAN connectivity template.
9. Name the vNIC `vNIC0`, for vNIC Template, select FAB-A, and for Adaptor policy select VMWare. Click OK.
10. Click the Add button to add a vNIC.
11. In the Create a vNIC workspace, select use a LAN connectivity template.
12. Name the vNIC `vNIC1`, for vNIC Template, select FAB-B, and for Adaptor policy select VMWare. Click OK.
13. Click Next to finish networking.
14. In the Create Service Profile Template page 4 (vNIC/vHBA Placement), click Next.

15. In the Create Service Profile Template page 5 (Server Boot Order), select PXE, and click Finish.
16. Click the B230-template, and select the Policies tab.
17. In the BIOS Policy, select VM-FEX.
18. In the Firmware Polices, select B230-M2 for Host firmware, and CIMC for Management firmware. Click Save changes.

Creating service profiles from template for the first B200 M2 blade

1. In the UCS Manager, go to the Equipment Tab.
2. Open Equipment→Chassis→Chasis1→Servers→Server 1.
3. In the left window, right-click Server 1, and select Create Service Profile for Server.
4. Select the Template based Service profile option.
5. In the Service Profile box titled name, type `infra`
6. Select b200-template in the Service Profile Template menu.
7. Click OK to complete the profile.

Creating two service profiles for future B230 M2 blade deployment

1. In the UCS Manager, go to the Servers Tab.
2. Open Servers→Service Profile Templates→root→Service Template B230-template, right-click and select Create Service Profiles From Template.
3. For the Service Profiles Naming Prefix type `View-` and for number, type `2`
4. Click OK to create the two UCS profiles.
5. Open Servers→Service Profiles→root→view-1, right-click and select Change Service Profile Association.
6. In the Associate Service Profile box, select pre-provision a slot, and select Chassis ID:1, Slot ID:2, and click OK.
7. Open Servers→Service Profiles→root→view-2, right-click and select Change Service Profile Association.
8. In the Associate Service Profile box, select pre-provision a slot, and select Chassis ID:1, Slot ID:3, and click OK.

Setting up the infrastructure server (infra)

The Cisco UCS service profile installs and configures BIOS and firmware on all components on the Cisco B200-M2. It assigns two vNICs to the server, and configures local storage. When the service profile was deployed to the server, we installed vSphere 5 on the Cisco B200-M2's local storage.

Installing VMware vSphere 5 (ESXi) on the Cisco UCS B200 M2 (infra)

1. Insert the ESXi 5.0 disk, and select boot from disk.
2. On the Welcome screen, press Enter.
3. On the End User License Agreement (EULA) screen, press F11.
4. On the Select a Disk to install or Upgrade screen, select the relevant volume to install ESXi on, and press Enter.
5. On the Please Select a Keyboard Layout screen, press Enter.
6. On the Enter a Root Password screen, assign a root password, and confirm it by entering it again. Press Enter to continue.
7. On the Confirm Install screen, press F11 to install.
8. On the Installation Complete screen, press Enter to reboot.

Configuring ESXi after installation (network)

1. On the ESXi 5.0 screen, press F2, enter the root password, and press Enter.
2. On the System Customization screen, select Troubleshooting Options, and press Enter.
3. On the Troubleshooting Mode Options screen, select Enable ESXi Shell, and press Enter.
4. Select Enable SSH, press Enter, and press Esc.
5. On the System Customization screen, select Configure Management Network.

6. On the Configure Management Network screen, select IP Configuration.
7. On the IP Configuration screen, select Set static IP; enter an IP address, subnet mask, and default gateway; and press Enter.
8. On the Configure Management Network screen, press Esc. When asked if you want to apply the changes, press Y.
9. Log into infra as `root` with the vSphere client.
10. Select the Configuration tab, and click Networking.
11. Configure vSwitch0 by clicking Add Networking…
12. Click the Network Adaptors tab.
13. Click Add…
14. Select vmnic1, and click Next.
15. Position vmnic0 as active and vmnic1 as a standby, and click OK.
16. Click the Ports tab, and edit the vSwitch.
17. Change the MTU of vSwitch0 to 9,000, and click OK.
18. In the vSwitch0 properties, click Add…
19. Create a virtual machine network called `VDI-NET` with a VLAN ID of `100` Click Next, and click Finish.
20. In the vSwitch0 properties, click Add…
21. Create a VMkernel network called `iSCSI` with VLAN a ID of `222` Select the checkbox Next to Use this port group for management traffic. Click Next twice.
22. Enter the address the VMkernel, click Next, and click Finish.
23. In the vSwitch0 properties, select iSCSI, and click Edit.
24. Change the MTU from 1,500 to 9,000, and click OK.

Configuring ESXi after installation (storage)

1. Click the Configuration tab, and click Storage Adapters.
2. Click Add.
3. Click Add software iSCSI adapter.
4. Click OK.
5. Select the iSCSI adaptor, right-click and select Properties.
6. In the iSCSI initiator workspace, select the dynamic tab.
7. Add the IP address for the PS4000 storage array.
8. Click Close, and click Rescan all.
9. Click Add storage…
10. Click Disk/LUN, and click Next.
11. Select the 1024 GB EQLOGIC iSCSI Disk, and click Next.
12. Select VMFS-5, and click Next.
13. For name, type `data1` and click Next.
14. Select available space, and click Next.
15. Click Finish to create the VMFS datastore.

Configuring ESXi after installation (DNS, and NTP)

1. Select the Configuration tab, and click Time configuration.
2. Select Properties, and click Options.
3. In the General settings, select Start automatically if any ports are open, and Stop when all ports are closed.
4. In the NTP settings, add a reliable NTP server.
5. Close NTP settings.
6. Select the Configuration tab, and click DNS and routing.
7. Type `infra` for name, and `view5.com` for domain.
8. Enter the IP address for DC1 for preferred DNS.

9. Close DNS.

Setting up a VM to host Microsoft Windows Active Directory® server (DC1)

1. Connect to the infra server via the VMware vSphere client.
2. Log in as `root` to the infra server.
3. In the vSphere client, connect to the vCenter Server, and browse to the ESXi host.
4. Click the Virtual Machines tab.
5. Right-click, and choose New Virtual Machine.
6. Choose Custom, and click Next.
7. Assign the name `DC1` to the virtual machine, and click Next.
8. Select infra for the host, and click Next.
9. Select data1 for the storage, and click Next.
10. Choose Virtual Machine Version 8, and click Next.
11. Choose Windows, choose Microsoft Windows Server 2008 R2 (64-bit), and click Next.
12. For CPUs, select one virtual processor socket and two cores per virtual socket, and click Next.
13. Choose 4GB RAM, and click Next.
14. Click 1 for the number of NICs, select VMXNET3, connect to the VDI-NET network, and click Next.
15. Leave the default virtual storage controller, and click Next.
16. Choose to create a new virtual disk, and click Next.
17. Make the OS virtual disk size 20 GB, choose thick-provisioned lazy zeroed, specify the OS datastore on the external storage, and click Next.
18. Keep the default virtual device node (0:0), and click Next.
19. Click Finish.
20. Right-click the VM, and choose Edit Settings.
21. On the Hardware tab, click Add…
22. Click Hard Disk, and click Next.
23. Click Create a new virtual disk, and click Next.
24. Specify 20GB for the virtual disk size, choose thick-provisioned lazy zeroed, and specify datastore1.
25. Choose SCSI (1:2) for the device node, and click Next.
26. On the Hardware tab, click Add…
27. Click Finish, and click OK.
28. Click the Resources tab, and click Memory.
29. Select reserve all guest memory, and click OK.
30. Connect the VM virtual CD-ROM to the Microsoft Windows Server 2008 R2 installation disk.
31. Start the VM.

Installing the Microsoft Windows Server 2008 R2 operating system on the VM

1. Choose the language, time and currency, and keyboard input. Click Next.
2. Click Install Now.
3. Choose Windows Server 2008 R2 Enterprise (Full Installation), and click Next.
4. Accept the license terms, and click Next.
5. Click Custom.
6. Click the Disk, and click Drive options (advanced).
7. Click New→Apply→Format, and click Next.
8. After the installation completes, click OK to set the Administrator password.
9. Enter the administrator password twice, and click OK.
10. Connect the machine to the Internet, and install all available Windows updates. Restart as necessary.
11. Enable remote desktop access.

12. Change the hostname to `DC1` and reboot when prompted.
13. Run diskmgmt.msc.
14. Select the 20 GB secondary volume, format it NTFS, and assign it drive letter `E`
15. Set up networking for the data network:
    a. Click Start→Control Panel, right-click Network Connections, and choose Open.
    b. Right-click the VM traffic NIC, and choose Properties.
    c. Uncheck TCP/IP (v6).
    d. Select TCP/IP (v4), and choose Properties.
    e. Set the IP address as `172.0.0.10/255.255.252.0`
16. Install VMware Tools. For more information, see

    http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=340

17. Reboot.

Installing Active Directory and DNS services on DC1

1. Click Start→Run, type `dcpromo` and click OK.
2. At the Active Directory Domain Services Installation Wizard welcome screen, check the Use advanced mode installation option, and click Next.
3. In the Choose a Deployment Configuration dialog box, select Create a new domain in a new forest, and click Next.
4. At the FQDN page, type `View5.com` and click Next.
5. At the NetBIOS name prompt, leave the name View5, and click Next.
6. At the Forest Functionality level, select Windows Server 2008 R2, and click Next.
7. At the additional Domain Controller Options, leave DNS server selected, and click Next.
8. At the System Folder Location screen, change to `E:\` leave the default options, and click Next.
9. Assign a Directory Services Restore Mode Administrator account password, and click Next.
10. At the Summary screen, review your selections, and click Next.
11. Once Active Directory Domain Services finishes installing, click Finish, and restart the system.
12. Run dnsmgmt.msc.
13. Create a reverse lookup zone for DC1.
14. Create static entries for infra.
15. Open Windows Explorer, and create a file called `e:\profiles`
16. Assign permissions of read/write to the view5\everyone group.

Configuring the Windows time service on DC1

To ensure reliable time, we pointed our Active Directory server to a physical NTP server.

1. Open a command prompt.
2. Type the following:

```
32tm /config /syncfromflags:manual /manualpeerlist:"<ip address of a NTP
server>"
W32tm /config /reliable:yes
W32tm /config /update
W32tm /resync
Net stop w32time
Net start w32time
```

Setting up DHCP services on DC1

1. Click Start→Administrative Tools→Server Manager→Add Roles.
2. Select DHCP Server, and click Next.

3. At the Introduction to DHCP Server screen, click Next.
4. At the Specify IPv4 DNS Settings screen, type `view5.com` for the parent domain.
5. Type the preferred DNS server IPv4 address, and click Next.
6. At the Specify IPv4 WINS Server Settings screen, select WINS is not required for applications on the network, and click Next.
7. At the Add or Edit DHCP Scopes screen, click Add.
8. At the Add Scope screen, enter the Name DHCP Scope name.
9. In the next box, set the following values, and click OK.
   - Start IP address=`172.0.0.101`
   - End IP address=`172.0.3.200`
   - Subnet mask=`255.255.252.0`
10. Check the Activate This Scope box.
11. At the Add or Edit DHCP Scopes screen, click Next.
12. Click the Enable DHCP v6 Stateless Mode radio button, and click Next.
13. Leave the default IPv6 DNS Settings, and click Next.
14. At the Authorize DHCP server dialog box, select Use current credentials.
15. At the Confirm Installation Selections screen, click Next. If the installation is set up correctly, a screen displays saying that DHCP server install succeeded.
16. Click Close.
17. Click Start→Run and type `DHCPmgmt.msc`
18. DHCP→dc1.view5.com→IPv4→Server Options.
19. Right-click Server Options, and select Configure options.
20. Activate option 66 Boot Server Host Name.
   - String value= `<ip of the vCenter>`
21. Activate option 67 Boot file Name.
   - String value= `undionly.kpxe.vmw-hardwired`
22. Click OK.

Setting up DHCP reservations for the B230 M2 servers

1. In the UCS Manager, go to the Servers tab.
2. Open Servers→Service Profiles →vdi1→vNIC0
3. In the workspace on the right, select the General tab, and locate the MAC address of vNIC0.
4. Open Servers→Service Profiles→vdi2→vNIC0.
5. In the workspace on the right, select the general tab, and locate the MAC address of vNIC0.
6. Open the DHCP manager.
7. Open DHCP→dc1.view5.com→Scope, right-click Reservations, and select New reservations.
8. Create a reservation:
   - Name= `View-1`
   - IP reservation= `172.0.0.90`
   - MAC address <from step 3>
9. Create a reservation:
   - Name= `View-2`
   - IP reservation= `172.0.0.91`
   - MAC address <from step 6>
10. Close DHCP.

Setting up a VM to host the vCenter server

1. Connect to the infra server via the vSphere client.
2. Log into infra with the VMware vSphere client.
3. In the vSphere client, connect to the vCenter Server, and browse to the ESXi host.
4. Click the Virtual Machines tab.
5. Right-click, and choose New Virtual Machine.
6. Choose Custom, and click Next.
7. Assign the name `vCenter` to the virtual machine, and click Next.
8. Select infra for the host, and click Next.
9. Select data1 for the storage, and click Next.
10. Choose Virtual Machine Version 8, and click Next.
11. Choose Windows, choose Microsoft Windows Server 2008 R2 (64-bit), and click Next.
12. For CPUs, select one virtual processor socket and two cores per virtual socket, and click Next.
13. Choose 4GB RAM, and click Next.
14. Click 1 for the number of NICs, select VMXNET3, connect to the VDI-NET portgoup, and click Next.
15. Leave the default virtual storage controller, and click Next.
16. Choose to create a new virtual disk, and click Next.
17. Make the OS virtual disk size 40 GB, choose Thick-provisioned lazy zeroed, specify the OS datastore on the data1, and click Next.
18. Keep the default virtual device node (0:0), and click Next.
19. Connect the VM virtual CD-ROM to the Microsoft Windows 2008 R2 installation disk.
20. Click Finish.
21. Start the VM.

Installing the Microsoft Windows Server 2008 R2 operating system on the VM

1. Choose the language, time and currency, and keyboard input. Click Next.
2. Click Install Now.
3. Choose Windows Server 2008 R2 Enterprise (Full Installation), and click Next.
4. Accept the license terms, and click Next.
5. Click Custom.
6. Click the Disk, and click Drive options (advanced).
7. Click New→Apply→Format, and click Next.
8. After the installation completes, click OK to set the Administrator password.
9. Enter the administrator password twice, and click OK.
10. Connect the machine to the Internet, and install all available Windows updates. Restart as necessary.
11. Enable remote desktop access.
12. Change the hostname to `vCenter` and reboot when prompted.
13. Set up networking for the data network:
    a. Click Start→Control Panel, right-click Network Connections, and choose Open.
    b. Right-click the VM traffic NIC, and choose Properties.
    c. Uncheck TCP/IP (v6).
    d. Select TCP/IP (v4), and choose Properties.
    e. Set the IP address, subnet, gateway, and DNS server.
14. Join the View5 domain.
15. Install VMware Tools. For more information, see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=340
16. Reboot the system.

Installing vCenter

1. Log onto the vCenter as `View5\administrator`
2. From the VMware vCenter 5 install media, click Autorun.
3. Click VMware vCenter, and click Install.
4. Select the install wizard language as English, and click OK.
5. At the Install wizard welcome screen, click Next.
6. Agree to the license agreement, and click Next.
7. Enter user information and a license key, and click Next.
8. Select Install the SQL express instance, and click Next.
9. Select the system account for the vCenter Server service account, and click Next.
10. Keep the installation directory as C:\Program Files\VMware\Infrastructure\, and click Next.
11. Select Create a standalone VMware vCenter Server instance, and click Next.
12. Keep the vCenter default ports, and click Next.
13. Select 1024 MB for the JVM memory, and click Next.
14. Click Install to finish the vCenter server installation.
15. When the installation completes, restart the server.

Configuring the vCenter cluster

1. Using the vSphere client, log into vCenter as `view5\administrator`
2. Right-click the root of vCenter, and click New Datacenter.
3. Name the New Datacenter `Datacenter`
4. Add `infra.view5.com` to the Datacenter.
5. Right-click Datacenter, and select create new cluster.
6. Name the cluster `view-cluster` and click Next enable HA and DRS.
7. Leave the DRS settings at defaults, and click Next.
8. Leave power management off, and click Next.
9. Select Disable for admission control, and click Next.
10. Leave the restart options as default, and click Next.
11. Leave VM monitoring disabled, and click Next.
12. Enable EVC for Intel hosts, select Westmere Gen. for EVC mode, and click Next.
13. Leave the swap file policy as default, and click Next.
14. Click Finish to create the cluster.

Installing VMware Composer on the vCenter cluster

1. Open the ODBC administrator.
2. Add a system DSN named composer, use the VCENTER\VIM_SQLEXP server.
3. Run the VMware composer.exe.
4. Accept the file agreement, and click Next.
5. Accept the destination folder path, and click Next.
6. Enter `composer` for the name of the ODBC name with the View5\administrator User id and password, and click Next.
7. Accept the default SOAP port, and click Next.
8. Click Install.

Installing VMware Update Manager on the vCenter cluster

1. Log onto the vCenter as `View5\administrator`
2. From the VMware vCenter 5 install media, click Autorun.
3. Click VMware vSphere Update Manager, and click Install.
4. Select English, and click OK.

5. At the welcome screen, click Next.
6. At the End-User Patent agreement, click Next.
7. Accept the end user license agreement, and click Next.
8. Select Download updates from default sources immediately after installation, and click Next.
9. Enter vCenter for name and the domain admin user ID and password.
10. Configure an ODBC connection for database connectivity, and click Next.
11. Use the IP address to identify the VUM server, and click Next.
12. Click Install.
13. Click Finish when completed.

Installing VMware Update Manager client on the vCenter

1. Open a vSphere client, and connect to vCenter.
2. Right-click the Plug-ins menu, and select Manage plug-ins…
3. Click Download and install to enable the update manager plugin for vSphere client.
4. Click Run to begin the install of the update manager client.
5. At the Welcome screen, click Next.
6. Accept the end user license agreement, and click Next.
7. Click install, and finish.

Configuring Update Manager and adding the Cisco UCS VEM module to the VUM repository

1. Open vSphere client, and connect to vCenter.
2. Open Home→Solutions and applications→Update manager→vCenter.
3. Open the Configurations tab, and select ESX Host/Cluster settings.
4. Check the box next to Allow installation of additional software on PXE booted ESXi 5.x hosts, and click Apply.
5. Open a Web browser, and open the UCS Manager Web page.
6. Click the link to obtain Cisco UCS Virtual Machine Fabric Extender (VM-FEX) Software.
7. Download the VEM500-20110825132140-BG-release.zip file.
8. In the vSphere client, browse Home→Solutions and applications→Update Manager→vCenter.
9. Click the Patch Repository tab, and click Import Patches.
10. Browse to the .zip from step 7.
11. Click Next, and click finish.

Configuring VM-FEX

1. Open UCS Manager.
2. Select the VM tab, and click VMware in the right pane.
3. Click Configure VMware integration.
4. In the Configure VMware integration box, click Export to export the vCenter extension plugin.
5. Choose a save location, and click OK.
6. Open vSphere client, select the Plug-ins drop down menu, and select Manage plug-ins…
7. Right-click the Plugin manager, and select New plugin…
8. Browse to the location specified in step 5, and click Register plugin.
9. Ignore the certificate error.

Configuring a DVS for VM-FEX

1. Open UCS Manager.
2. Select the VM tab, and click VMware in the right pane.
3. Select VMware, right-click and select configure vCenter.
4. Type `vCenter` for name, and type the IP of the vCenter.
5. Do not add a folder, and click Next.
6. Do not add a Datacenter, and click Next.

7. Right-click vCenter, and select Create datacenter.
8. Name the Data Center, and click Next.
9. Click Add to add a folder.
10. Name the folder, and click Next.
11. Click add DVS.
12. Name the DVS, and click enable and OK.
13. Click Finish.

Creating port profiles on the Distributed vSwitch

1. In the UCS Manager, right-click Port Profiles.
2. Create a port profile:
    - Name: `platinum`
    - QoS policy = platinum
    - Select VLAN 100 and select native vlan
    - For Host Network I/O performance, select High performance.
3. Create a port profile:
    - Name: `bronze`
    - QoS policy = bronze
    - Select VLAN 100 and select native vlan
    - For Host Network I/O performance, select High performance.
4. Create a port profile:
    - Name: `best_effort`
    - QoS policy of = best_effort
    - Select VLAN 100 and select native vlan
    - For Host Network I/O performance, select High performance.
5. Create a port profile:
    - Name: `vMotion`
    - QoS policy = platinum
    - Select VLAN 222 and select native vlan
    - For Host Network I/O performance, select High performance.

Creating Profile clients on the Distributed vSwitch

1. In the UCS Manager, expand the Port profiles icon.
2. Right-click Port profile named platinum, and select Create profile client.
3. Name the Port profile client `platinum` select the appropriate folder and DVS, and click OK.
4. Right-click Port profile named bronze, select Create profile client.
5. Name the Port profile client `bronze` select the appropriate folder and DVS, and click OK.
6. Right-click Port profile named best_effort, select create profile client.
7. Name the Port profile client `best_effort` select the appropriate folder and DVS, and click OK.
8. Right-click Port profile named vMotion, and select create profile client.
9. Name the Port profile client `vMotion` select the appropriate folder and DVS, and click OK.

Installing VMware Auto Deploy

VMware Auto Deploy requires a TFTP server. For our Auto Deploy procedure, we used http://www.solarwinds.com. Our TFTP service was installed on the vCenter. Auto Deploy also requires the installation of vSphere PowerCLI. For more information on PowerCLI, visit http://www.vmware.com/support/developer/PowerCLI/.

We installed VMware Auto Deploy on the vCenter and configured it to apply an offline ESXI bundle to any PXE boot server that is in the range of 172.0.0.90-100. After that, we powered on our first B230-M2.

1. Log onto the vCenter as `View5\administrator`
2. From the VMware vCenter 5 install media, click Autorun.
3. Click VMware Auto Deploy.
4. Select English, and click Next.
5. At the install wizard welcome screen, click Next.
6. Agree to the license agreement, and click Next.
7. Select 2 GB for the repository size, and click Next.
8. Enter the vCenter IP address, for user name type `administrato`r, and enter the password for the administrator account.
9. Use the default server port 6501, click Next.
10. Select the option to Use the IP address of the server to identify auto deploy on the network, and click Next.
11. Click Install.
12. Click Finish.
13. In the vSphere client, click Plug-ins, and click Manage plug-ins…
14. Right-click Auto Deploy, and click Enable.
15. Ignore the security warning, and click the box next to the text that reads Install this certificate and do not display any security warnings about this host.
16. Close the Plug-in manager.
17. In the vSphere client browse to home→Administration→Auto Deploy→vCenter.
18. Click the Download the TFTP boot zip link.
19. Extract the TFTP boot files to the TFTP server (vCenter).

Configuring Auto Deploy ESXI software depot and deployment rule.

VMware Auto Deploy uses PowerCLI, and ESXi offline bundles to create ESXi deployment repositories, and deployment rules based on user preferences. We instructed Auto Deploy to create a rule called IP-deploy. The IP-deploy rule was associated with an ESXi image, and when activated the IP-deploy rule would automatically deploy a stateless ESXi image with any server set to PXE boot that falls within the IP address 172.0.0.90 to 172.0.0.100. We instructed Auto Deploy to add the new ESXi server to our View 5 cluster.

1. Download the ESXi 5.0 Offline Bundle from www.vmware.com.
2. Open PowerCLI.
3. Type `Set-ExecutionPolicy Unrestricted`
4. Type `Connect-VIServer vCenter`
5. Type `Add-EsxSoftwareDepot` <location of the file in step 1>
6. Type `Get-EsxImageProfile` and make note of the name for standard (example: ESXi-5.0.0-20111104001-standard).
7. Type `new-deployrule -name "IP-deployrule" -item "<name from step 6>","view-cluster" -Pattern "ipv4=172.0.0.90-172.0.0.100`
8. Type `Add-DeployRule -DeployRule "IP-deployrule"`

Boot a Cisco B230 M2 and create a VMware Host Profile

We pre-provisioned Cisco UCS Service Profiles for the two Cisco UCS B230- M2 blades and setup VMware Auto Deploy to install a stateless ESXi OS on the server. When powered on, the blade automatically begins setup and is added to the virtual desktop cluster. We configured the new blade and created a VMware Host Profile.

1. Open the Cisco UCS Manager, and open a KVM session to slot 2.

2. From the KVM session, power on the B230-M2 in slot 2.
3. On the ESXi 5.0 screen, press F2, enter the root password, and press Enter.
4. On the System Customization screen, select Troubleshooting Options, and press Enter.
5. On the Troubleshooting Mode Options screen, select Enable ESXi Shell, and press Enter.
6. Select Enable SSH, press Enter, and press Esc.
7. Close the KVM.
8. Log into vSphere client.
9. Select the cluster view-cluster →172.0.0.90, select the Configuration tab, and click Networking.
10. Configure vSwitch0 by clicking Add Networking…
11. Click the Network Adaptors tab.
12. Click Add…
13. Click the Ports tab, and edit the vSwitch.
14. Change the MTU of vSwitch0 to 9,000, and click OK.
15. In the vSwitch0 properties, click Add…
16. Create a virtual machine network called `VDI-NET` with a VLAN ID of `100`
17. Click Next, and click Finish.
18. In the vSwitch0 properties, click Add…
19. Create a VMkernel network called `iSCSI` with VLAN ID of `222`
20. Select the checkbox next to Use this port group for management traffic. Click Next twice.
21. Enter the address the VMkernel, click Next, and click Finish.
22. In the vSwitch0 properties, select iSCSI, and click Edit.
23. Change the MTU from 1,500 to 9,000, and click OK.

Configuring ESXi after installation (storage)

1. Click the Configuration tab, and click Storage Adapters.
2. Click Add.
3. Click Add software iSCSI adapter.
4. Click OK.
5. Select the iSCSI adaptor, right-click, and select Properties.
6. In the iSCSI initiator workspace, select the Dynamic tab.
7. Add the IP address for the PS4000 storage array.
8. Click close, and click Rescan all.
9. Ensure the 172.0.0.90 host can see the 1024GB datastore named data1.

Configuring ESXi after installation (DNS, and NTP)

1. Select the Configuration tab, and click Time configuration.
2. Select Properties, and click Options.
3. In the General settings, select Start automatically if any ports are open, and Stop when all ports are closed.
4. In the NTP settings, add DC1.view5.com.
5. Close NTP settings.
6. Select the Configuration tab, and click DNS and routing.
7. Type `view5.com` for domain.
8. Enter `DC1.view5.com` for preferred DNS.
9. Close DNS.

Adding nic1 to the DVS

1. Open vCenter.
2. Open Home→Inventory→Networking.
3. Right-click the DVS in the view5 cluster, and select Add host…

4. Select the check box for vNIC1 on the server 172.0.0.90, and click Next.
5. Do not migrate any of the VMkernel interfaces, and click Next.
6. Do not migrate virtual machine networking.
7. Click Finish to add the ESXI host to the DVS.

Adding a vMotion interface on the DVS

1. In the vSphere client, open 172.0.0.90, select the Configuration tab, and click Networking.
2. Click vSphere Distributed Switch.
3. Click Manage virtual adaptors.
4. Click Add.
5. Click New virtual adaptor, and click Next.
6. For adaptor type, ensure VMkernel is selected, and click Next.
7. Select the vMotion port group, check the box next to Use this virtual adaptor for vMotion, and click Next.
8. Enter an address and subnet for vMotion, and click Next.
9. Click Finish.

Creating a host profile called 230_DVS

1. Open vSphere client and navigate to Home→Management→Host Profiles.
2. Select Create Profile.
3. In the Create Profile Wizard, select Create Profile from existing host, and click Next.
4. To specify the reference host, browse to vCenter→Infra→ view-cluster →172.0.0.90, and click Next.
5. Name the profile `230_dvs`
6. Select the profile named 230_DVS, and click Edit profile.
7. Edit 230_DVS→Firewall configuration→Rulesset configuration→Fault tolerance→Rulesset.
8. Change Fault tolerance→ Rulesset to User must explicitly choose the policy option, and click OK.
9. Right-click the 230_DVS profile, and select enable/disable profile configuration…
10. Expand Storage Configuration.
11. Expand the Pluggable Storage Architecture (PSA) configuration.
12. Deselect the check box next to PSA Device Configuration.
13. Expand Native Mulitpathing (NMP).
14. Expand PSP and SATP Configuration for NMP Devices.
15. Deselect the check box next to PSP configuration for, and click OK.
16. Select attach Host/cluster.
17. Add the view-cluster cluster to the attached entries, and select OK.
18. In the 230_DVS hosts and clusters tab, right-click 172.0.0.90, and select Check profile compliance.

Applying the host profile to the DRS cluster

1. Right-click the 172.0.0.90 host, and select Maintenance mode.
2. Right-click 172.0.0.90, and select Apply profile.
3. In the Apply host profile wizard, select all defaults.
4. Right-click the 172.0.0.90 host, and select Maintenance mode.

Setting up a VM to host the VMware View 5 connection server

1. Log into vCenter with the VMware vSphere client.
2. In the vSphere client, browse to the ESXi host named infra.
3. Click the Virtual Machines tab.
4. Right-click, and choose New Virtual Machine.
5. Choose Custom, and click Next.
6. Assign the name `View5` to the virtual machine, and click Next.

7. Select infra for the host, and click Next.
8. Select data1 for the storage, and click Next.
9. Choose Virtual Machine Version 8, and click Next.
10. Choose Windows, choose Microsoft Windows Server 2008 R2 (64-bit), and click Next.
11. For CPUs, select one virtual processor socket and two cores per virtual socket, and click Next.
12. Choose 4GB RAM, and click Next.
13. Click 1 for the number of NICs, select VMXNET 3, connect to the VDI-NET portgourp, and click Next.
13. Leave the default virtual storage controller, and click Next.
14. Choose to create a new virtual disk, and click Next.
15. Make the OS virtual disk size 40 GB, choose thick-provisioned lazy zeroed, specify the OS datastore on the external storage, and click Next.
16. Keep the default virtual device node (0:0), and click Next.
17. Connect the VM virtual CD-ROM to the Microsoft Windows Server 2008 R2 installation disk.
18. Click Finish.
19. Start the VM.

Installing the Microsoft Windows Server2008 R2 operating system on the VM

1. Choose the language, time and currency, and keyboard input. Click Next.
2. Click Install Now.
3. Choose Windows Server 2008 R2 Enterprise (Full Installation), and click Next.
4. Accept the license terms, and click Next.
5. Click Custom.
6. Click the Disk, and click Drive options (advanced).
7. Click New→Apply→Format, and click Next.
8. After the installation completes, click OK to set the Administrator password.
9. Enter the administrator password twice, and click OK.
10. Connect the machine to the Internet, and install all available Windows updates. Restart as necessary.
11. Enable remote desktop access.
12. Change the hostname to `view5` and reboot when prompted.
13. Set up networking for the data network:
    a. Click Start→Control Panel, right-click Network Connections, and choose Open.
    b. Right-click the VM traffic NIC, and choose Properties.
    c. Uncheck TCP/IP (v6).
    d. Select TCP/IP (v4), and choose Properties.
    e. Set the IP address, subnet, gateway, and DNS server.
14. Join the View5 domain.
15. Install VMware Tools. For more information, see

    http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=340

16. Reboot.

Installing the VMware View 5 connection server

1. Log into the server named view5.
2. Click Install Media for View Connection Server.
3. To begin the install wizard, click Next.
4. Agree to the license agreement, and click Next.
5. Keep the destination directory as C:\Program Files\VMware View\Server\, and click Next.
6. Select View Standard Server, and click Next.

7. Allow View Server to configure the firewall, and click Next.
8. Click Next.
9. Click Finish.
10. Open a command window, and type `gpupdate /force`
11. Reboot the View 5 server.
12. Log out of View 5.

Configuring the VMware View 5 connection server

1. Open a Web browser to <the view server ipaddress>/admin.
2. Log in as `administrator`
3. Open View Configuration→Servers.
4. In the vCenter Servers workspace, click Add…
5. In the add vCenter Server settings, add the vCenter, and enable View composer. Click OK.
6. Open View Configuration→Product Licensing and Usage.
7. Click Edit license…
8. Enter a valid license serial number, and click OK.
9. Close the View 5 administrator.

Setting up a Windows 7 Enterprise x64 image for VMware View 5 linked clone gold image

Using the vSphere client, we created a Windows 7 Enterprise x64 VM. We then optimized the Windows 7 Enterprise x64 VM for View 5 linked clone deployment on the cluster named view-cluster.

Installing the Windows 7 Enterprise (x64) VMware View 5 gold image

1. Log into vCenter.
2. In the vSphere client, connect to the vCenter Server, and browse to the ESXi host named view-1.
3. Click the Virtual Machines tab.
4. Right-click, and choose New Virtual Machine.
5. Choose Custom, and click Next.
6. Assign the name `gold_image` to the virtual machine, and click Next.
7. Select infra for the host, and click Next.
8. Select data1 for the storage, and click Next.
9. Choose Virtual Machine Version 8, and click Next.
10. Choose Windows, choose Microsoft Windows 7 (64-bit), and click Next.
11. Choose one virtual processor socket, and two cores per virtual socket, and click Next.
12. Choose 2 GB RAM, and click Next.
13. Click 1 for the number of NICs, select VMXNET3, add it to the VDI-NET portgroup, and click Next.
14. Leave the default virtual storage controller, and click Next.
15. Choose to create a new virtual disk, and click Next.
16. Make the OS virtual disk size 20 GB, choose thin-provisioned, and click Next.
17. Keep the default virtual device node (0:0), and click Next.
18. Click Finish, and click OK.
19. Edit the gold_image VM.
20. Remove the virtual floppy, and click OK.
21. In the Options tab→General, deselect Enable logging, and click OK.
22. Click the Resources tab, click Memory, click the box next to Reserve all guest memory, and click OK.
23. Connect the VM virtual CD-ROM to the Microsoft Windows 7 x64 installation disk.
24. Start the VM.

Installing the Microsoft Windows 7 Enterprise x64 operating system on the VM

1. When the installation prompts you, press any key to begin setup.
2. Enter your language preferences, and click Next.
3. Click Install.
4. Accept the license terms, and click Next.
5. Select Custom, and select the drive that will contain the OS.
6. Click Install, and the setup begins.
7. Type `user` for the username and change the computer name, and click Next.
8. Enter no password, and click Next.
9. For system protection, select Use recommended settings, and click Next.
10. Enter your time zone, and click Next.
11. Select the Work Network setting, and click Next.
12. Use Windows Update to patch the Windows 7 installation.
13. Install VMware Tools. For more information, see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=340
14. Reboot.
15. Join the View5.com domain, and reboot.
16. Open a command prompt as administrator.
17. Type `net user administrator /active:yes`
18. Type `net user administrator *`
19. Enter the password for administrator twice.

Installing Windows 7 Enterprise, (x64) optimizing Windows 7

Adjusting page file

1. Log in as `administrator`
2. Right-click Computer→Properties→Change settings→Advanced→Performance→Settings.
3. In Performance settings, select the Advanced tab, and select Change for Virtual Memory.
4. Deselect Automatically manage page file.
5. Select Custom size, type `2048` for both values, and select Set.

Disabling Windows Firewall

The domain GPO automatically disables the Windows Firewall.

Installing the VMware View agent on gold_image

1. Log into the gold_image.
2. Browse to the VMware View agent media.
3. At the Welcome screen and License agreement, accept the terms, and click Next.
4. Accept install defaults, and click Next.
5. Select Do not enable the remote desktop capability on this computer, and click Next.
6. Keep default install directory, and click Install.
7. Start the Windows Registry Editor, and navigate to this registry: key:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vmware-viewcomposer-ga.
8. Navigate to the SkipLicenseActivation registry value. The default value is 0.
9. Set the value to 1.
10. Reboot the VM gold_image.

Installing jperf on the virtual desktop image

1. Download and extract http://sourceforge.net/projects/iperf/files/ to the c:\ dir of Gold_image.

Cleaning up the VM on Windows 7 virtual desktop

1. Click Start→Run→services.msc.
2. In the Services menu, select Windows Search, and change it from Disabled to Automatic (delayed start).
3. Close the Services menu.
4. Click Start→Control Panel→View Devices and Printers.
5. In the Services and Printers window, delete the XPS printers and document writers.

Optimizing the Windows 7 virtual desktop, and final preparation of the gold image

For our testing, we optimized the Windows 7 gold image for performance using the commands.bat: http://www.vmware.com/files/pdf/VMware-View-OptimizationGuideWindows7-EN.pdf.

1. Run commands.bat.
2. Shut down the VM.
3. Log into vCenter with the vSphere client.
4. Take a snapshot of the gold_image VM called view5_ready.

Configuring the View 5 server - creating a pool of 33 virtual desktops.

1. Open the View Administrator.
2. Log in as `View5\administrator`
3. Click Pools, and in the right window, click Add…
4. Select Automatic pool, and click Next.
5. Select Floating, and click Next.
6. Select View Composer Linked clones, and click Next.
7. Use the vCenter(administrator) as the source, and click Next.
8. Type `pool` for the pool ID and display name, and click Next.
9. Leave the pool settings as defaults, and click Next.
10. Keep the disposable disk size as 4,096, and click Next.
11. Type a naming pattern of `View-` and type `33` for both max number of desktops, and number of spares.
12. Enter the virtual machine settings as follows:
    - Default image as: `view5_ready`
    - VM folder: `/Datacenter/vm/pool`
    - Host or cluster: `/datacenter/host/view-cluster`
    - Resource pool: `/datacenter/host/view-cluster/Resources`
    - Datastore: `data1`
13. Choose the AD container OU=Computers,OU=Login_VSI, and use quickprep.
14. Click Finish to create the pool.
15. Highlight the pool named Pool, and click Entitlements.
16. Click Add, select login_VSI/view5.com, and click OK.
17. Ensure all 33 desktops have a status of ready.

APPENDIX D– JPERF CONFIGURATION

```
#
#Mon Jan 30 13:37:11 EST 2012
print-mss-enabled=false
transmit-unit=seconds
tcp-mss-enabled=false
tos=NONE
mode=client
client-limit-enabled=false
compatibility-mode-enabled=false
tcp-no-delay-enabled=true
test-mode-port=5001
test-mode-trade-enabled=false
udp-bandwidth-unit=MEGABYTES_PERSEC
output-format=GBITS
udp-bandwidth=1.0
tcp-buffer-length-unit=MBYTES
listen-port=5001
server-port=5001
clientside-parallel-streams=0
udp-buffer-size-unit=KBYTES
tcp-window-size-enabled=true
server-address=172.0.0.124
ttl=1
udp-buffer-size-enabled=false
transmit-value=60
ipv6-enabled=false
udp-buffer-size=41.0
transport-protocol=tcp
test-mode-dual-enabled=false
tcp-buffer-length-enabled=true
tcp-buffer-length=8.0
tcp-mss-unit=KBYTES
report-interval=1
udp-packet-size-enabled=false
udp-packet-size=1500.0
tcp-mss=1.0
serverside-parallel-streams=6
client-limit=
tcp-window-size-unit=BITS
tcp-window-size=8972.0
udp-packet-size-unit=BYTES
bind-to-host=
```

ABOUT PRINCIPLED TECHNOLOGIES

Principled Technologies, Inc.
1007 Slater Road, Suite 300
Durham, NC, 27703
www.principledtechnologies.com

We provide industry-leading technology assessment and fact-based marketing services. We bring to every assignment extensive experience with and expertise in all aspects of technology testing and analysis, from researching new technologies, to developing new methodologies, to testing with existing and new tools.

When the assessment is complete, we know how to present the results to a broad range of target audiences. We provide our clients with the materials they need, from market-focused data to use in their own collateral to custom sales aids, such as test reports, performance assessments, and white papers. Every document reflects the results of our trusted independent analysis.

We provide customized services that focus on our clients' individual requirements. Whether the technology involves hardware, software, Web sites, or services, we offer the experience, expertise, and tools to help our clients assess how it will fare against its competition, its performance, its market readiness, and its quality and reliability.

Our founders, Mark L. Van Name and Bill Catchings, have worked together in technology assessment for over 20 years. As journalists, they published over a thousand articles on a wide array of technology subjects. They created and led the Ziff-Davis Benchmark Operation, which developed such industry-standard benchmarks as Ziff Davis Media's Winstone and WebBench. They founded and led eTesting Labs, and after the acquisition of that company by Lionbridge Technologies were the head and CTO of VeriTest.

Disclaimer of Warranties; Limitation of Liability:
PRINCIPLED TECHNOLOGIES, INC. HAS MADE REASONABLE EFFORTS TO ENSURE THE ACCURACY AND VALIDITY OF ITS TESTING, HOWEVER, PRINCIPLED TECHNOLOGIES, INC. SPECIFICALLY DISCLAIMS ANY WARRANTY, EXPRESSED OR IMPLIED, RELATING TO THE TEST RESULTS AND ANALYSIS, THEIR ACCURACY, COMPLETENESS OR QUALITY, INCLUDING ANY IMPLIED WARRANTY OF FITNESS FOR ANY PARTICULAR PURPOSE. ALL PERSONS OR ENTITIES RELYING ON THE RESULTS OF ANY TESTING DO SO AT THEIR OWN RISK, AND AGREE THAT PRINCIPLED TECHNOLOGIES, INC., ITS EMPLOYEES AND ITS SUBCONTRACTORS SHALL HAVE NO LIABILITY WHATSOEVER FROM ANY CLAIM OF LOSS OR DAMAGE ON ACCOUNT OF ANY ALLEGED ERROR OR DEFECT IN ANY TESTING PROCEDURE OR RESULT.

IN NO EVENT SHALL PRINCIPLED TECHNOLOGIES, INC. BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH ITS TESTING, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL PRINCIPLED TECHNOLOGIES, INC.'S LIABILITY, INCLUDING FOR DIRECT DAMAGES, EXCEED THE AMOUNTS PAID IN CONNECTION WITH PRINCIPLED TECHNOLOGIES, INC.'S TESTING. CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES ARE AS SET FORTH HEREIN.