Delivering Epic Hyperspace Through VMware View Using Kiosk Mode and Zero Clients

Reference Implementation for a VMware Point-of-Care Solution

WHITE PAPER

vmware®

About VMware Reference Implementations

VMware® Reference Implementation documents describe how real VMware customers have architected virtual desktop environments and deployed VMware View™ in them. In contrast to *reference architectures*, reference implementations focus on actual customer environments and include deployment information about the client access devices, access infrastructure, virtual infrastructure, virtual desktops, session management and other key elements of the customer implementation.

Customer Background

Healthcare providers need complete technology solutions that address their specific needs and requirements. The VMware customer referenced in this document is a major healthcare provider in the Midwestern United States. It operates multiple clinics and hospitals throughout a major metropolitan area and a large expanse of rural territory.

By using Epic electronic medical record (EMR) software to access patient records and input patient data in all its exam rooms, the customer has taken a huge step forward in serving rural communities. However, delivering the Epic software to traditional Windows PCs created its own challenges. Desktop support technicians were frequently called to remote sites for support issues, taking them away from other duties for long periods of time. And every time a new Windows or Epic update was released, the updates consumed a great deal of bandwidth and were never 100 percent successful, further increasing the need for onsite support. Epic is a client-server electronic medical record application. The client portion is called Epic Hyperspace and is typically installed on a PC or delivered through a Terminal Services model. The Hyperspace client connects back to a Cache database running on servers in the datacenter.

Security was another major concern, in part because many endpoints were at remote facilities in rural areas. The customer maintained a highly controlled electronic health record (EHR) environment: Users were given access to patient records only on specific endpoints in examination rooms, and no other applications were installed on those devices. However, users shared a single password to access each endpoint—much like a kiosk computer—and data was stored on locally attached hard drives. Loss or theft of a Windows PC could result in a security breach.

Key Requirements

Because cost reduction was a primary goal for the implementation project, senior IT leadership at the organization needed assurance that the solution would be financially practical. The implementation team knew it could reduce costs, improve clinician efficiency and improve security by replacing PCs with zero-client devices—but it didn’t want to sacrifice user functionality or access to the local printers in each exam room. Saving time was also a key objective, and the customer needed a solution that would improve productivity for IT staff and clinicians alike. Consequently, the solution had to pass both a rigorous cost-benefit analysis to demonstrate its financial value and a proof of concept so that IT teams could demonstrate its technical feasibility.

Solution: A Virtual Desktop Infrastructure

After a thorough evaluation, the customer decided to implement a virtual desktop infrastructure (VDI) solution based on VMware View. This solution enabled the customer to centralize and automate its Epic environment by running the EMR software on virtual machines housed in the centralized datacenter, which clinicians access from local or remote locations using zero-client terminals. The new solution provided clinicians fast access to the Epic software, with near-native performance and seamless access to local printers and other peripheral devices.

Solution Components at a Glance

- Epic 2009
- VMware View 4.6
- Cisco UCS
- IBM XIV
- Wyse P20 zero clients
- LAN and WAN access
- VMware View security server for remote access

Design Approach

A good VMware View architecture leverages basic design principles and best practices. A building-block approach provides the flexibility to create a comprehensive VDI that meets or exceeds desired goals and functionality while maintaining a logical, straightforward architecture.

The VMware View architecture begins with the client access devices layer and continues through to the *session management layer* (see Figure 1). This approach enables each functional area's services to be clearly defined independently of the others'—while still providing a cohesive structure for addressing the interdependency of all solution components.

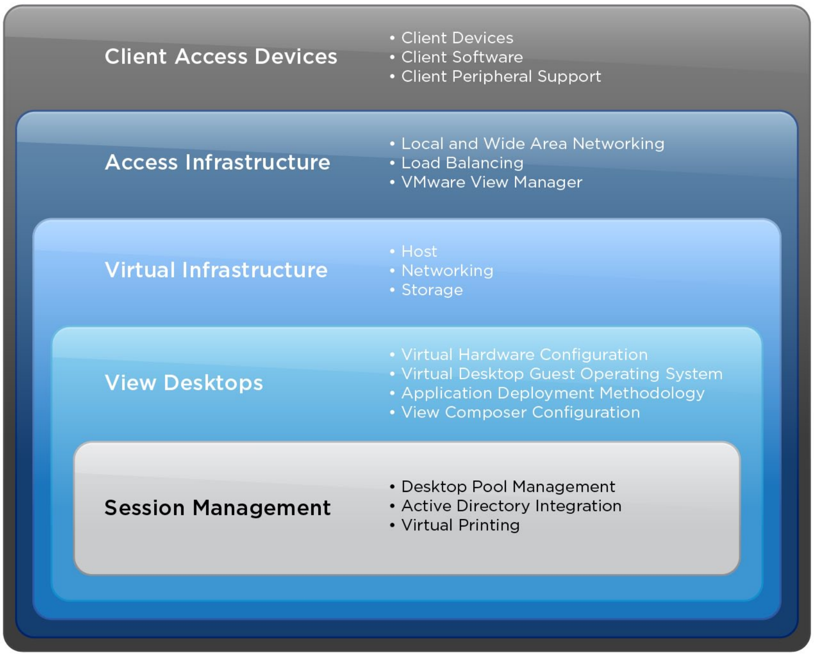
Client Access Devices
• Client Devices
• Client Software
• Client Peripheral Support
Access Infrastructure
• Local and Wide Area Networking
• Load Balancing
• VMware View Manager
Virtual Infrastructure
• Host
• Networking
• Storage
View Desktops
• Virtual Hardware Configuration
• Virtual Desktop Guest Operating System
• Application Deployment Methodology
• View Composer Configuration
Session Management
• Desktop Pool Management
• Active Directory Integration
• Virtual Printing

Figure 1. VMware View Reference Architectural Layers and Their Components

Client Access Devices

The client access devices layer consists of the hardware and software components needed to deliver a rich user experience. Components of this layer include

- Client hardware device
- Client software
- Peripheral support

The customer chose to implement approximately 1,500 Wyse P20 zero-client terminals in all patient examination rooms. Users were granted access only to the Epic client application—Epic Hyperspace—and local peripheral devices. PC-over-IP (PCoIP) zero clients are a popular choice for healthcare because they essentially eliminate the need for desktop management and have no CPU, operating system, device drivers, fan or hard drive. The benefits include low operational cost, increased security capabilities, a rich user experience and future-proof desktop scalability. The customer chose to implement the end point devices using VMware View Kiosk mode.

Kiosk mode is when the Zero Client device only runs the VMware View Client software. End users do not need to log in to access the Zero client device but rather log in at the application level – some healthcare organizations use this type of solution to lessen the number of clicks necessary for caregivers to reach their patient care application.

Access Infrastructure

The access infrastructure layer consists of the networking and connectivity elements used to facilitate client access. Components of this layer include

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

Users can access virtual desktops from both LAN and WAN connections, although access is limited to specific endpoint devices in patient examination rooms. LAN access is provided by a 100-Mbps link to the client devices; there are no wireless LAN users. The customer provides WAN access to remote locations from security servers outside the firewall. WAN connections range from 10 to 20Mbps.

Virtual Infrastructure

The virtual infrastructure layer defines the elements used to host the virtual desktop operating systems and supporting VMware View infrastructure. Components in this layer include

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

Host Infrastructure

To host the virtualized desktops in the datacenter, the customer deployed VMware vSphere on 19 Cisco USC B200 M2 Blade Servers, each with dual 6-core Intel Xeon 5680 processors and 96GB of RAM.

For data storage, the customer implemented a mix of HP StorageWorks EVA and IBM XIV equipment into three clusters, as outlined in Table 1.

Table 1. VDI Storage Configuration

CLUSTER 1	EVA	XIV	TOTAL # OF LUNS	TOTAL SPACES (GB)
100-GB LUNs	1		1	100
300-GB LUNs	5	5	10	3000
CLUSTER 2	**EVA**	**XIV**	**TOTAL # OF LUNS**	**TOTAL SPACE (GB)**
300-GB LUNs	2	3	5	1500
400-GB LUNs	3	2	5	2000
CLUSTER 3	**EVA**	**XIV**	**TOTAL # OF LUNS**	**TOTAL SPACE (GB)**
400-GB LUNs	5	5	10	4000
TOTALS (AT 1180 ONLY)			**31**	**10600**

For the SAN, the customer used Brocade switches and DCX directors, with approximately 432 ports per fabric. To manage and automate data backup and restore functions, the customer used IBM Tivoli Storage Manager software.

Virtual Desktops

The customer's implementation was designed to support approximately 1,500 virtual desktops. Each virtual desktop was configured to run the Epic Hyperspace client application on Microsoft Windows 7 with a 2-GHz virtual processor, 1GB of RAM and support for 1024x768 monitors.

Session Management

The session management layer defines the deployment and management of virtual desktops and user sessions. The components in this layer include

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

Session Management

The customer chose to implement a "generic" login for client access and did not make use of single sign-on. Instead, users share access to a single virtual machine and use unique credentials to authenticate themselves within the Epic software before being given access to patient records. In addition, users are provided with "location-aware" network printing through Active Directory group membership.

Desktop Provisioning and Pooling

Because users share access to each virtual desktop, the customer chose not to use persistent desktop pools. Instead, the customer arranged its virtual desktops into floating stateless pools. When stateless pools are used, virtual desktops are not assigned to specific users, and they do not persist beyond a single user session. Instead, end users always get a clean and functional desktop when they log in. This approach significantly reduced the customer's storage and network footprint. In addition, the customer utilized linked clones in its desktop pools, which further reduced its storage needs and enabled IT staff to manage all Epic Hyperspace and Windows updates through a single master image.

Linked Clones Defined

A linked clone is a copy of a virtual machine that shares virtual disk space with its parent virtual machine while maintaining a unique identity. This capability of VMware View helps customers significantly reduce storage requirements—depending on the size and architecture of the IT environment—and enables IT to manage large numbers of virtual desktops from a single image.

Location-Aware Virtual Printing

Although the benefits of using zero clients are substantial, these devices also introduce a unique challenge because they have no traditional local operating system to map a default printer.

In the legacy environment, printing mapped for the most part to the default Windows printer. However, some UNIX-based printers are also provided to the user session based on the name of the computer from which the user is running the software. Mapping of the UNIX-based printer to the computer name is set up within the Epic software, and the computer name is queried when the Epic software is initially launched. This mapping has the potential to present a specific patient's record based on where the clinician is accessing the application from—for example, a specific patient room. It was necessary to change this variable to one that reflects the physical endpoint device.

The customer worked around this issue by using descriptive device names for each zero client, with a login script that parses this information and maps a default printer. The device-name components are delimited by dashes and consist of a Z as the first letter to signify it is a zero client, a location ID to specify where it resides, the asset-tag ID of the physical device, the computer name and finally the default printer name it should be mapped to. The computer-name component is the same name as the device the zero client is replacing—regardless of device type—to maintain the Epic mapping already in place. For net-new devices, the customer creates the mapping in the Epic software for the computer name.

The login script parses the device-name components and performs some key actions. It uses the computer-name component to create a system environment variable—separate from %COMPUTERNAME%—to signify the physical end-device computer name that the Epic software needs to use for mapping purposes. It uses the default-printer-name component to map the default printer in the VMware View Agent. These two actions must take place on the View Agent before the Epic software launches. Finally, it uses the entire device name to create the desktop wallpaper that displays this information in case the user needs to supply it to help-desk personnel.

Architectural Design Summary

Figure 2 provides a high-level overview of the solution architecture.

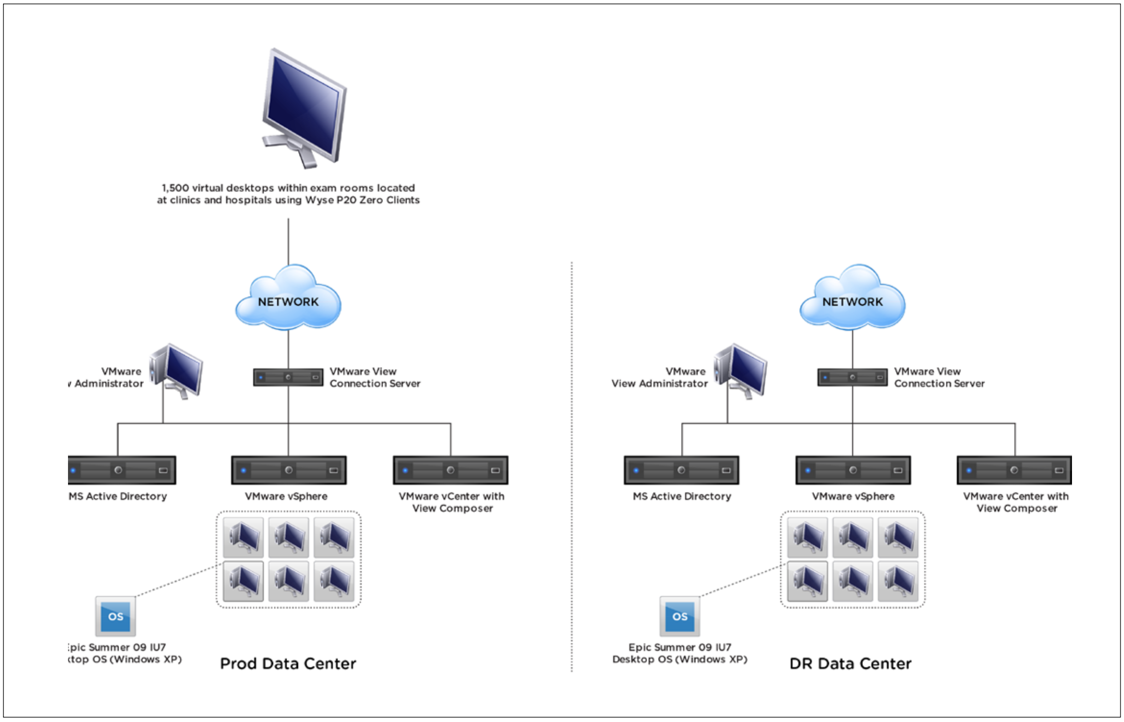

Figure 2. Architectural Design Summary

Conclusion

The customer has already implemented nearly 1,000 virtual desktops as it progresses through a phased plan to replace PCs with zero clients in each clinic. The organization credits part of its success to prior experience with VMware server-virtualization solutions in the datacenter. The customer plans to expand its VDI so that it can support highly mobile disease- and case-management workers. VMware Professional Services worked directly with the customer to ensure the success of this implementation. It can also work with you to ensure successful implementation of a custom solution that fits your organization's unique needs and helps you achieve maximum cost savings. Learn more at http://www.vmware.com/services/by-product/desktop.html.

About VMware

VMware, the global leader in virtualization and cloud infrastructure, delivers customer-proven solutions that accelerate IT by reducing complexity and enabling more flexible, agile service delivery. VMware enables enterprises to adopt a cloud model that addresses their unique business challenges. The VMware approach accelerates the transition to cloud computing while preserving existing investments and improving security and control. With more than 250,000 customers and 25,000 partners, VMware solutions help organizations of all sizes lower costs, increase business agility and ensure freedom of choice.

VMware View: Deliver Desktops as a Managed Service

VMware View is a complete virtual desktop solution that enables healthcare organizations to significantly improve point-of-care workflows for caregivers and the quality of care for patients. Built to deliver desktops and applications as a secure managed service, this solution simplifies desktop administration and management while increasing security of data by establishing a modern end-user–computing architecture.

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