Technical Report

NetApp Clinical Desktop Reference Architecture for VMware AlwaysOn Point of Care

Monty Zarrouk, NetApp

February 2013 | TR-4132

Abstract

This paper details a new reference architecture for delivering clinical desktops and patient care applications as nonstop services. The validated designs and reference architecture were created through architectural design development and lab testing.

TABLE OF CONTENTS

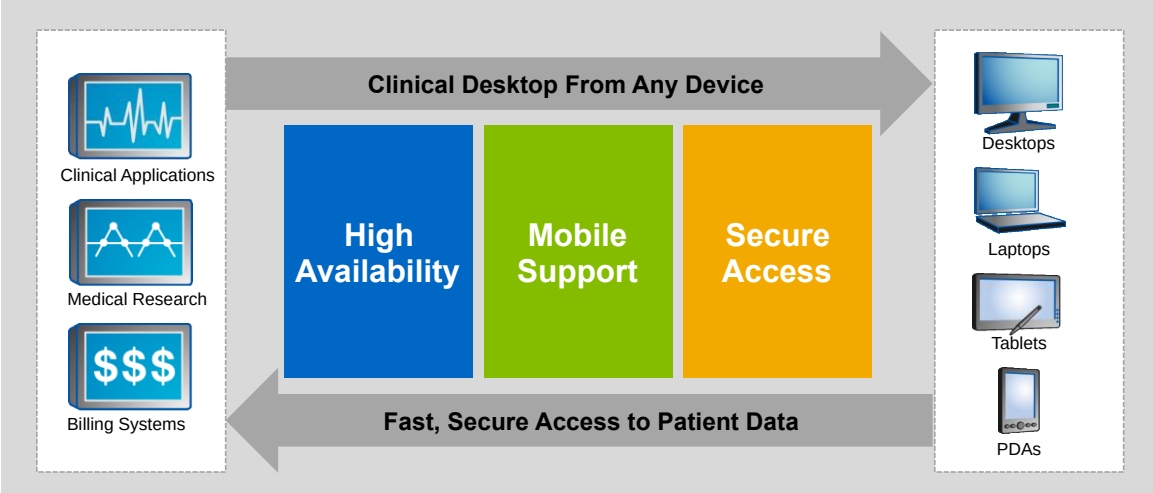
LIST OF TABLES

LIST OF FIGURES

1 Introduction

Today's healthcare IT environment is experiencing a dramatic change with the advent of new technologies, cost pressures, and increasing regulations. With computers and mobile devices quickly replacing traditional patient charts, the number of electronic medical records (EMRs) and electronic health records (EHRs) has skyrocketed. Healthcare organizations now face a compelling need for solutions that simplify access to patient records from both traditional and mobile devices; protect the confidentiality of patient information with secure, authorized access to information systems; and enable applications to be always available.

Figure 1) Empower caregivers with always-on, anywhere access.



Virtual desktop infrastructures can significantly reduce cost, however, many functions within healthcare organizations also need high availability to prevent downtime due to unplanned or even planned activities. With the decreasing costs of hardware and technology, coupled with the increasing costs of downtime, healthcare organizations realize that mobile solutions that deliver the required availability for secure, continuous access are now within reach.

Industry Trend

As organizations move toward virtual desktops, providing high availability becomes even more critical. That is because any downtime due to planned or unplanned activities directly impacts workers' productivity and, in this case, patient care.

1.1 Federal Mandates

Conformance requirements for federal mandates mean healthcare organizations need to keep an ever-growing amount of patient data. At some point this will break the budget. Eventually it will be necessary to think differently and to evaluate ways to keep more data while spending less.

Cost of Compliance

With the growing reliance on information technology in the healthcare industry, the privacy of medical records is not just a civil right, but also a government regulation. The advances in EMR/EHR systems, collaboration in diagnosis and research, and integrated billing systems all require that the healthcare

industry demonstrate compliance with both the Health Insurance Portability and Accountability Act (HIPAA)[1] and the Joint Commission on Accreditation of Healthcare Organizations (JCAHO).[2] IT infrastructure, from the endpoints of mobile users to the storage systems, must show proof that they meet these requirements to safeguard against data loss and access by unauthorized individuals.

As hospitals gear up to meet the Health Information Technology for Economic and Clinical Health (HITECH)[3] Act (the mandate for all patients to have electronic patient records by 2014), information systems officers must also contend with participation in regional and national health information exchanges and networks as well as the implications regarding data growth, availability, and portability of patient data in a secure environment. Although many of the large integrated delivery networks already have a secure electronic communication platform in place, no one single standard or set of standards has been agreed upon to handle the management.

Affordable Care Act

The Affordable Care Act was passed into law in 2010 with the goal of improving our current healthcare system by increasing access to health coverage for uninsured Americans and introducing new protections for people who have health insurance. In addition, a number of policies have been defined to help physicians, hospitals, and other caregivers improve the safety and quality of patient care and make healthcare more affordable.

As 2014 approaches, payers and providers will experience a significant increase in patient data as more insured Americans enter the system. This increased volume of patients in the healthcare system will require clinical systems that provide high availability and ready access to patient data to help doctors and nurses make better decisions and collaborate with their peers on treatment plans. By focusing on the needs of patients and linking payments to outcomes, these delivery system reforms will help improve the health of individuals and communities and slow cost growth.

1.2 Available Data Helps Clinicians Make Informed Decisions

The benefits of EMRs/EHRs are widely known: standardized delivery of medical records, reduced errors, improved patient care, quicker reimbursements, and decreased costs. Adoption of EMRs/EHRs is essential to transforming and modernizing the healthcare industry. At the same time, recent passage of the ARRA HITECH Act provides additional incentives to implement an EMR/EMR strategy sooner rather than later.

However, several challenges must be addressed before EMRs/EHRs can be widely implemented across healthcare facilities. Foremost among these is the data storage and management challenge. The increased complexity and sheer volume of data that must be stored and managed make it more difficult to enhance data availability and to protect private patient data.

The desktop as we know it, however, is changing. For example, nurses at many hospitals use a variety of endpoints, logging in from different locations, multiple times during a single shift. Over the course of a single shift, this approach takes a significant amount of time away from patient care.

With today's advances in technology, caregivers can now perform their job from virtually anywhere using mobile devices such as smartphones and tablets with access to applications, information, and services in cloud infrastructures. Desktop virtualization technology is one technology that furthers this goal. The

---

[1] The Health Insurance Portability and Accountability Act of 1996 establishes national standards for secure electronic transactions between and among healthcare participants, including care providers, health insurers, pharmacies, and employers.

[2] The Joint Commission on Accreditation of Healthcare Organizations performs accreditation and related services to support quality care in a hospital setting.

[3] The Health Information Technology for Economic and Clinical Health Act 2009 addresses the privacy and security concerns associated with the electronic transmission of health information.

software allows you to deploy and manage desktop environments and applications centrally. This includes all of the devices and applications that physicians, nurses, and administrators use to access patient data and other information throughout hospitals, clinics, and remote locations.

Figure 2) Caregivers are working differently and have high expectations.

Many healthcare organizations have adopted desktop virtualization to improve IT efficiencies and streamline the way people work. A physician's time is expensive and valuable to a hospital. When a physician is unproductive because of technology issues, patient care and billing are both affected.

In addition, virtual desktop technology helps IT organizations reign in operational costs by centralizing desktop administration from the data center.

- Cut operational costs for patching and maintaining desktops.
- Reduce administration expense while increasing the number of virtual desktops deployed.
- Eliminate downtime so users have access to information when needed**.**

1.3 Securing Protected Health Information

Security and compliance have always been major concerns for the healthcare industry, but the proliferation of electronic health information has led to increased attention to data security breaches involving protected health information.

In response to this the federal government mandated significant penalties for security lapses as part of the HITECH Act. For example, public notification of breaches of more than 500 records is now mandatory, including a requirement to post details on the Department of Health and Human Services' Web site, and HITECH permits fines of up to $1.5 million for violations. Meeting the stricter guidelines is especially difficult in environments in which clinicians demand remote access to patient data and support for laptops, smartphones, tablet computers, and other mobiles devices, most of which are hard to secure and vulnerable to theft and loss.

1.4 Providing Continuous Availability for Nonstop Care

The failure of a mission-critical system can become a disaster for any organization, but in a clinical setting where caregivers completely depend on electronic solutions, system availability can literally be a matter of life and death. As computing devices replace paper charts and physician prescription pads, these endpoints become critical IT systems that must deliver the highest possible levels of security, reliability, and availability to enable patient safety. In short, EMR/EHR systems must be accessible as a nonstop service that is available to clinicians wherever and whenever they need patient information.

2 Requirements for High-Availability Desktops

When taken together, the challenges of achieving meaningful use, protecting patient information, and enabling continuous secure access to point-of-care solutions have created a dilemma that can't be solved with traditional approaches to desktop and application management. To overcome these and other challenges, healthcare providers need a new approach to point-of-care delivery, one that will enable them to modernize their IT infrastructures so they can improve patient outcomes and get the most from the millions of dollars they are investing in EMR/EHR technology.

2.1 Business Challenge

As clinicians strive to deliver excellence in patient care, it is critical to provide ready access to the information needed to make informed decisions regarding treatment plans while protecting the confidentiality of patient information. Healthcare IT is being pressured to deliver a new approach to point-of-care delivery that meets the growing mobility demands of caregivers. By modernizing IT infrastructures with continuous, secure access to point-of-care solutions, clinicians can improve patient outcomes and healthcare organizations can maximize the business benefits from their EMR/EHR technology investments.

2.2 Business Drivers

Organizations have different user types, each with its own unique requirements for availability. Although any planned or unplanned downtime of the desktops affects all the user profiles in the organization, the degree of disruption to productivity depends on the nature of the work performed by the users. For example, while a back-office desk clerk might tolerate a few minutes of downtime to his desktop without significant loss of productivity, an emergency room desk clerk needs nonstop access to her desktop and applications.

For this reason, it is critical to understand and segment the user types within an organization before designing the solution. For always-on desktops (AODs), it is necessary to identify the recovery time objective (RTO) and the recovery point objective (RPO) for different user types. This is a key component of the active-active design, and the size of the environment will be determined by the recovery time SLAs defined by the organization.

Table 1) Business drivers for high-availability desktops.

Requirements	Description
Business Requirements	• Tier 1 critical desktop require fast recovery and application continuity during disasters • Session mobility, a required feature tied to the productivity of mobile employees; a "follow me" desktop is the only way to meet this requirement
End-User Experience Requirements	• Desktops that are always on and enable fast logon • Desktop that follow the user in the event of failover • User name persistence to the same desktop across desktop sessions • Secure access from any endpoint device, from any location • Familiar interface to sustain the same application workflow
High-Availability / Disaster Recovery Requirements	• Uptime: DR solutions should offer quick restores with minimal or no manual steps after the recovery (RTOs) • Reliability: Addressing database transactional consistency, avoiding corrupted file systems, and enabling system boot when restored are key to addressing this concern (RPOs) • Cost: The cost of many different software solutions or replicating storage arrays can be cost prohibitive • Complexity: Minimize the number of systems involved in the solution

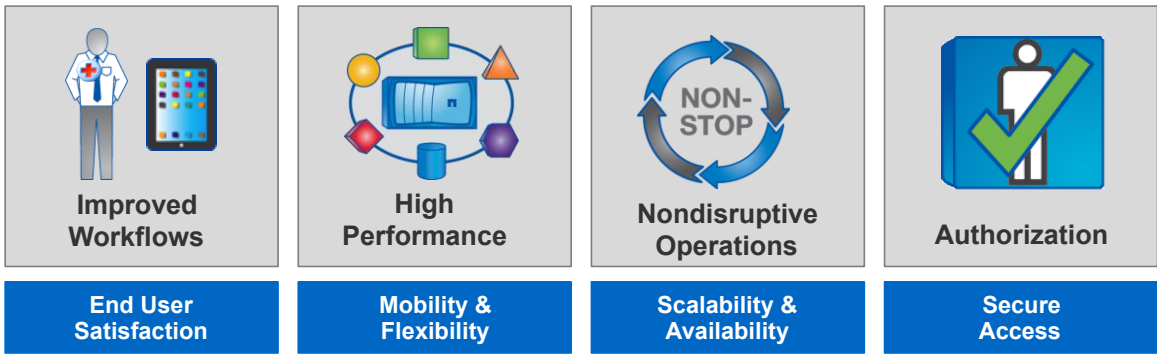
3 VMware AlwaysOn Point of Care Solution

The VMware® AlwaysOn Point of Care solution provides a virtual desktop environment that is secure, cost effective, and easy to deploy, providing users with:

- Nonstop access to desktops with fast logon times
- Desktops that follow the user in the event of a site failure
- Connectivity to desktops from any endpoint device from anywhere
- Familiar interface to sustain the same application workflow
- Consistent access across desktop sessions through user name persistence

Clinicians can now access clinical applications from a virtual environment, allowing continued access to the application as the clinician moves from patient to patient, floor to floor, or building to building. This mobile desktop solution provides high availability to the clinical applications within the provider environment with response times meeting or exceeding those required by the clinical application vendor. It also provides appropriate security for a healthcare environment.

Figure 3) VMware AlwaysOn Point of Care benefits.



3.1 Solution Purpose

The VMware AlwaysOn Point of Care solution:

- Delivers a simplified desktop environment with a validated infrastructure, making it easy to update the operating system, patch applications, enable compliance, and provide support from central locations. The solution delivers a consistent user experience for professionals whether they are within a hospital or at a remote location.
- Leverages site-aware distribution mechanisms and the deployment of several desktop infrastructures, so end users always have access to their desktops.
- Provides nonstop access to clinical desktops even in the case of a site failure or disaster.

3.2 Technology Solution

Based on VMware View™, organizations can build a virtual desktop infrastructure to provide nonstop access to desktops hosted in the data center while streamlining application updates, enhancing data security, and delivering the highest-fidelity user experience.

The solution enables an organization to address these three key requirements.

Availability

The AlwaysOn Point of Care solution is designed to provide nonstop access to desktops hosted in the data center. An active-active configuration is used for the VMware View infrastructure so that the data center resources are utilized optimally and end users are provided with the best user experience. With a

stateless desktop model and constant replication of master images and user data between the two pods (at the same location or two different locations), end users are provided with their desktops even if any one site becomes unavailable, and they have true high availability. Through intelligent local and global traffic management and health monitoringF5 BIG-IP application delivery controllers improve the performance and reliability of VMware View while enabling greater scalability.

Mobility

The solution is built on VMware vSphere and VMware View to deliver the highest-quality desktops to end users accessing from any endpoint device. Since the desktops are hosted in the data center, end users have the option of using any endpoint device (zero clients, tablets, laptops, and so on) to access their desktops. By using F5 BIG-IP application delivery controllers, the solution also provides session persistence across devices, which lets users access their desktops from different devices. And with the use of the PCoIP protocol, VMware View delivers the best desktop user experience from any device. As users move between terminals, laptops, and other devices in a multipod VMware View environment, they can lose the workspace from their original pod. F5 provides user name persistence that enables users to reconnect with the same workspace they were running and enjoy a more productive virtual desktop experience.

Security

Security is a key consideration for any organization; VMware, in the AlwaysOn Point of Care solution, provides the highest level of security for end-user desktops and data. From the integration of two-factor authentication solutions to hypervisor-based antivirus products, the solution enables the highest level of security in the organization without disrupting the end-user experience. The solution also incorporates products that enable regulatory compliance with any industry standard. F5 BIG-IP application delivery controllers provides secure remote and local access and integration with authentication, authorization, and accounting (AAA) services. Imprivata OneSign single sign-on (SSO) streamlines the user experience to improve both security and productivity.

4 AlwaysOn Point of Care Solution Overview

VMware AlwaysOn Point of Care offerings are purpose-built for healthcare organizations to address the high-availability and disaster recovery needs of mission-critical clinical desktops. This solution combines VMware View AlwaysOn Point of Care, NetApp® storage, Cisco® Unified Computing System™, F5 BIG-IP application delivery controller, and Imprivata OneSign single sign-on solution.

4.1 Design Approach

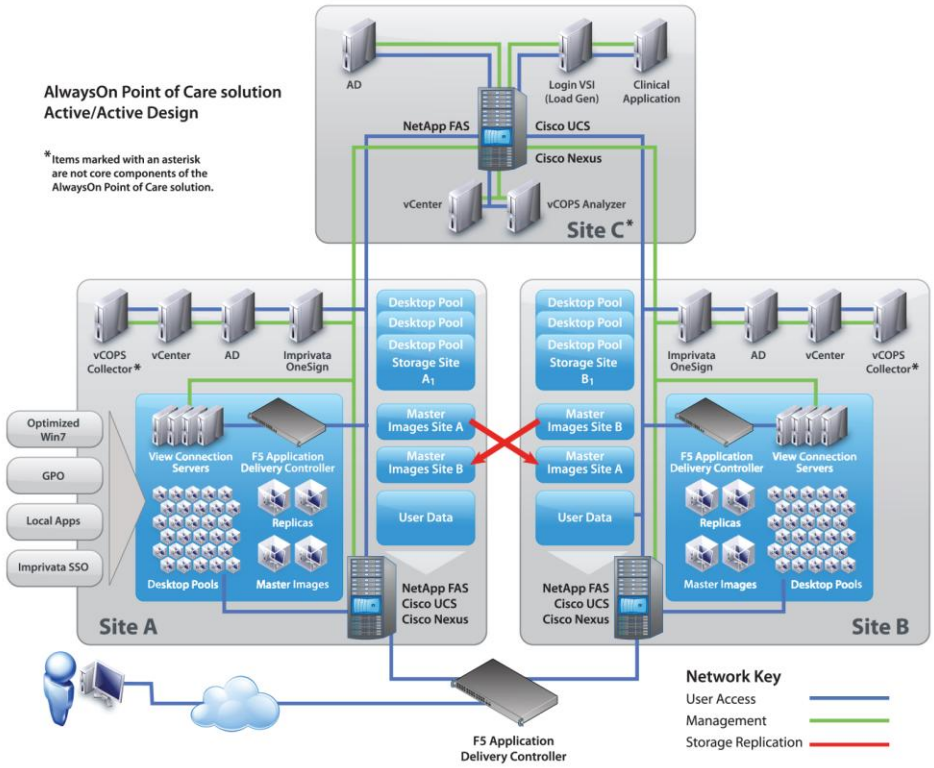
Individual laptops, desktops, tablets, and other mobile devices are typically managed as standalone entities residing outside the data center and are not always subject to an organization's information security, backup and recovery, and application usage policies. As enterprises and IT organizations require more secure, highly available, and efficient means for managing corporate resources, the need to bring all of these resources under the control of a centralized data center managed by IT becomes paramount.

This solution has been designed as a low-impact, cost-effective approach to bring all of these resources under the control of the data center while providing a rich, single view of an end user's applications and data.

4.2 Solution Description

Figure 4 shows the logical overview of the AlwaysOn Point of Care solution.

Figure 4) AlwaysOn Point of Care logical design.



The solution consists of two identical VMware View pods in an active-active configuration. Each View pod consists of two virtual machine clusters: the Management cluster and the Virtual Desktop cluster for scalability purposes. Each pod is self-sufficient, that is, all management components, including Active Directory®, View Connection Manager, and Security Server, are built in each site. This allows complete redundancy between the two pods and enables the environment to deliver desktops even if one site goes down completely.

The underlying hardware is segregated efficiently to optimally utilize the resources for the two clusters. The NetApp storage is segmented to provide datastores for various types of workloads, including virtual desktops, user data files, and management VMs.

A separate site is used in the architecture to host shared applications between the two sites. This represents the legacy application cluster in any organization, which will be accessed by desktops from both sites.

The infrastructure is front-ended by F5 BIG-IP application delivery controllers to efficiently route the traffic between two sites. Depending on the organization's needs, the traffic can be routed by user IDs, source IP, geo locations, or latency while maintaining end-user persistence.

To provide a consistent user experience, the master images in both the View pods are synchronized using replication software. This enables the desktops created in both the sites to be identical. In addition to that, user data between the two sites is synchronized so that a desktop delivered to a user from either site is personalized to that user.

The View pods are built based on the scalable reference architecture published by VMware and is scalable.

4.3 Core Components

Virtualization Operating System

The solution is built on top of VMware vSphere, the industry-leading virtualization platform. With new memory management and expanded resource pooling capabilities, VMware vSphere accelerates the evolution of data centers and service providers into cloud computing environments.

VMware View

The central component of the solution architecture is VMware View, which is the industry-leading mobile desktop product. A detailed description is provided in the following section.

Storage Solution

Storage is a critical part of any desktop virtualization solution; however, healthcare storage costs have traditionally been one of the inhibitors of virtual desktop adoption. When evaluating any desktop virtualization solution, the ability to reduce total storage requirements should be a top priority. NetApp delivers the cost-effective storage solutions designed with the scalability and continuous operations demanded by mobile desktops.

Security and Compliance

VMware vShield™ provides best-in-class security to the virtual desktop environment. VMware vShield EndPoint with hypervisor-based antivirus protection (from leading AV vendors) provides tremendous benefits in terms of management and ease of use for the environment. In addition, vShield Manager's Compliance module enables organizations to meet any compliance requirement.

Replication Software

Replication between the two View pods is critical to providing high-availability functionality in the architecture. There are many replication software alternatives, from file- to block-level replication, that can be used to achieve replication. NetApp SnapMirror® data replication technology leverages NetApp unified storage to provide fast, efficient data replication and disaster recovery (DR). SnapMirror technology can be easily tuned to meet recovery point objectives ranging from zero seconds to hours.

Single Sign-on

Imprivata OneSign single sign-on (SSO) software and tap-and-go cards provide access control for numerous related but independent software systems. Using SSO products in the architecture enhances the user experience, since users have to log in to the environment only once to access all the applications provisioned for them. SSO software can be used in conjunction with a tap-and-go card, which enhances the user experience even further.

Application Delivery Controller

Application Delivery Controllers are a critical component in the AlwaysOn Point of Care design. In addition to providing standard load balancing, the F5 BIG-IP application delivery controllers provide intelligent routing based on user name, source IPs, geolocation, or latency. This enables users to be always routed to their preferred site; only in the case of a site failure is the connection routed to the next available site.

4.4 Additional Components

Management

With the environment spread across two sites, streamlined management and a single-pane dashboard become a necessity for IT to effectively manage the environment. VMware vCenter™ Operations Manager for View is an option for the management and dashboard functionality required at each site for efficient and seamless management for the IT team.

Compute and Network Solution and Components

The Cisco Unified Computing System (UCS™) is the backbone of the virtual infrastructure, providing a data center architecture for an administrator that is easy to use and manage. The platform, optimized for virtual environments, is designed with open industry-standard technologies and aims to reduce TCO and increase business agility. The system integrates a low-latency, lossless 10-Gigabit Ethernet unified network fabric with enterprise-class x86-architecture servers. The system is an integrated, scalable, multichassis platform in which all resources participate in a unified management domain.

5 VMware View

The central component of the solution architecture is VMware View, which is the industry-leading mobile desktop product. Using VMware View's virtual desktop infrastructure technologies, which include VMware View Manager's administrative interface, desktops can be quickly and easily provisioned using templates. The technology permits rapid creation of virtual desktop images from one master image, enabling administrative policies to be set and patches and updates applied to virtual desktops in minutes, without affecting user settings, data, or preferences.

The VMware View key components are:

- **View Connection Server:** Acts as a broker for View client connections. It authenticates the users through the Active Directory and then directs that request to the virtual desktop.
- **View Client:** Client software for accessing the virtual desktop from a Windows® PC, a Mac® PC, a thin client, a zero client, or a tablet. The administrator can configure the client to allow users to select a display protocol such as PCoIP or RDP.
- **View Agent:** Enables discovery of the virtual machine used as the template for virtual desktop creation. Additionally, the agent communicates with the View client to provide features such as access to local USB devices, printing, and monitoring connections.
- **VMware View Manager:** An enterprise-class desktop management solution that streamlines the management, provisioning, and deployment of virtual desktops. The View Manager is installed at the same time as the connection server, and it allows the user to administer the View Connection Server. For this RA, four View Connection Servers were deployed in each site to illustrate the internal load balancing.
- **Centralized Virtual Desktops:** A method of managing virtual desktops that enables remote sites to access virtual desktops residing on server hardware in the data center.
- **VMware View Composer:** An optional tool that uses VMware Linked Clone technology, employing a master image to rapidly create desktop images that share virtual disks. This conserves disk space and streamlines management.

VMware View also has the capability to meet the demanding needs of the different types of user profiles, whether on the local area network (LAN) or wide area network (WAN). Combining VMware, F5 Application Delivery Controller, and Imprivata OneSign SSO with NetApp storage enables excellent user experiences and desktop availability, which in turn mean acceptance of the virtual desktop deployment within organizations.

6 NetApp Storage Solution

6.1 NetApp Agile Data Infrastructure

The NetApp agile data infrastructure changes the way that healthcare IT can architect its data infrastructure to drive efficiencies across a shared environment. Much like a network, storage is a lasting infrastructure that can grow and change while maintaining stability and predictability of services. This enables much higher levels of agility at a much lower cost than ever before, allowing healthcare organizations to optimize staff productivity, enhance physician satisfaction, and improve the overall quality of care.

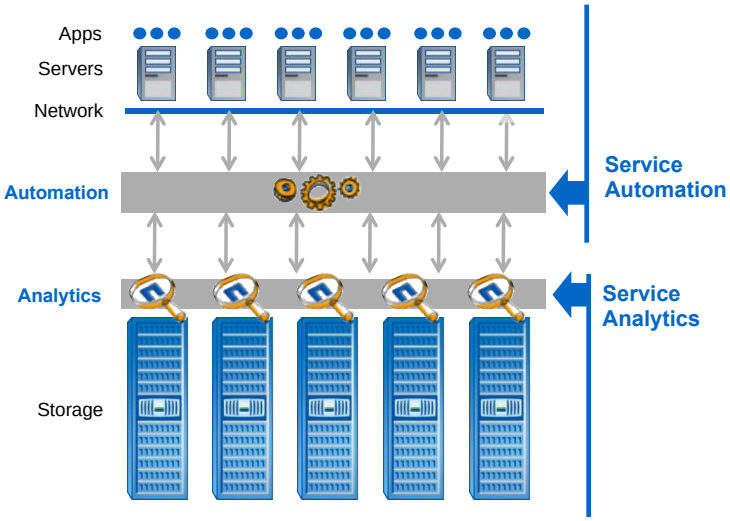
6.2 Intelligent Data Management

The cornerstone of an agile data infrastructure is intelligent data management. By automating the ability to deploy, adjust, and control data storage attributes, healthcare IT can now respond with the agility needed to accommodate growing volumes of patient data and provide the time-sensitive access to patient records demanded by doctors and nurses.

Service Automation and Analytics

NetApp simplifies the complexity of managing patient data with policy-based management. Routine operations such as creating a LUN, establishing a replication pair, and monitoring performance bottlenecks become increasingly easier when multiplied by hundreds or thousands of instances, and they eliminate the need for manual intervention unless an out-of-policy condition exists. Healthcare IT can now easily support terabytes to petabytes of patient files while reducing the time it takes to perform routine administrative tasks. And with improved policies and processes, IT is positioned to manage more terabytes per full-time employee with the push of a button.

Figure 5) Self-managed storage scales capacity, not people.



Storage Efficiency

NetApp storage efficiency technologies and techniques are designed to reduce unchecked storage growth while lowering costs, enabling healthcare IT to maximize investments in storage technology. In use by thousands of customers in a broad range of environments, NetApp storage can help lower the cost structure by reducing overall data storage costs by 50% or more while offering an infrastructure that enables clinicians to provide quality of care. We employ a variety of data reduction techniques, including

primary-level deduplication, compression, and more. The variety of data reduction techniques reduces the amount of data on the disk and traveling over the network.

Flexible Online Tiering Options for Primary and Archived Storage

NetApp storage solutions are designed to handle the growing volume of data generated by medical imaging, streamlining the footprint for long-term archiving. NetApp provides flexible solutions that enable healthcare organizations to consolidate tiers and that result in a cost-effective and efficient storage solution with fewer controllers. Consolidating multiple terabytes of EMR patient files, PACS data and additional hospital records on NetApp storage can considerably reduce the number of servers and storage devices that your IT team must manage, maximizing your return on IT investment. This helps simplify data management, increase storage utilization and availability, and enhance backup, recovery, and archiving processes.

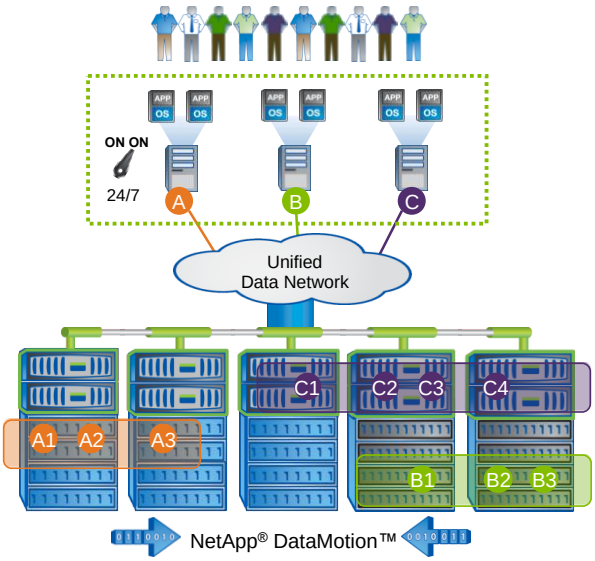
6.3 Immortal Data Operations

Not much patient data is deleted these days. There are some valid reasons for this, such as the healthcare mandates that require long-term data retention. And, over time, it's been proven that it's more cost effective to keep all data rather than spend the time to analyze what should be deleted. This means that the majority of your data will eventually outlive your equipment several times over.

Nondisruptive Operations and Continuous Access

Nondisruptive operations allow nurses to readily access medical records so that the correct patient gets the right treatment at the right time. This higher quality of care requires that healthcare IT personnel deploy storage solutions that can both store and manage large amounts of data while retaining the ability to quickly retrieve content when patient files or historical content is required to aid a diagnosis or treatment plan.

Figure 6) Zero downtime for routine upgrades and replacements.



To help avoid unplanned downtime, NetApp combines the proven reliability of its base hardware with innovative solutions to continue operations in the face of hardware failures or disasters that affect a site or region. NetApp storage systems in active-active controller configurations deliver uptime greater than 99.999% on average. This translates to less than five minutes of downtime per year, making scheduled downtime a relic of the past, which is increasingly important in delivering continuity of patient care.

Embedded Data Security

Patient satisfaction increases when an accurate diagnosis is received. And with today's ability to confer online with specialists at remote facilities, physicians can accelerate the time to get treatments underway. However, sensitive patient information must be shared securely as mandated by HIPAA, and that information spans both data in motion and data at rest. A range of NetApp embedded data security technologies helps healthcare organizations comply with the regulatory requirement to protect stored patient data while enabling physicians to effectively treat their patients.

NetApp Storage Encryption provides full disk encryption using self-encrypting drives from leading vendors. This allows healthcare organizations to secure confidential patient data, comply with government regulations, and preserve the reputation of healthcare organizations by avoiding a publicized data security breach—all without compromising storage efficiency.

NetApp Storage Encryption supports the entire suite of storage efficiency technologies from NetApp, including deduplication and compression, providing you with the efficiency savings you see with unencrypted volumes. Array-based antivirus (AV) scanning is also supported.

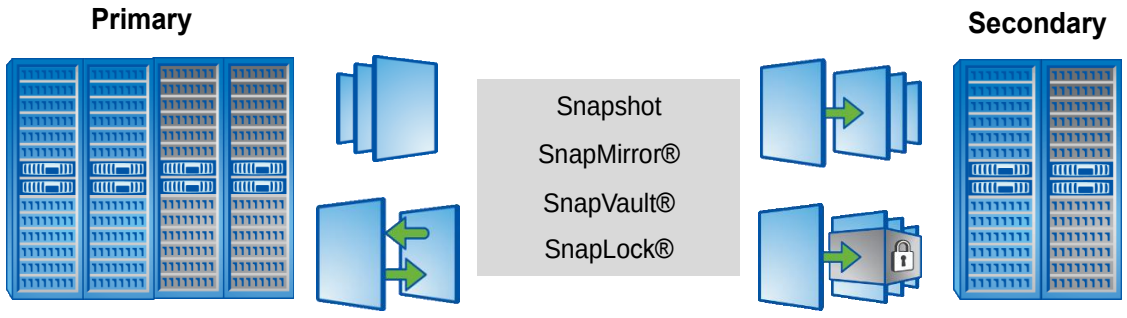
- Implements full disk encryption at the hardware level
- Prevents access to data until the drive is unlocked by an authorized administrator
- Supports storage efficiency: FAS deduplication and storage compression
- Supports Integrated Data Protection: backup/recovery and SnapMirror, SnapProtect™, and SnapVault® technologies
- Is file system and network independent

Integrated Data Protection

Joint Commission on Accreditation of Healthcare Organizations (JCAHO) accreditation requires hospitals to create effective failover procedures on site to protect stored patient images and other medical records. In addition to maintaining a data recovery backup system in the event of an unexpected equipment failure for online and near-line storage, HIPAA mandates now require that medical information management executives establish remote long-term data archive as part of a comprehensive disaster recovery plan.

Data protection needs to become as "set it and forget it" as possible. This principle holds whether the process is integrating applications to provide local availability, providing network-efficient and storage-efficient disk for backup and disaster recovery, or using exactly the same formats for long-term retention.

Figure 7) "Set it and forget it" data protection removes human error.



NetApp delivers automation of routine operational tasks, providing efficiencies that eliminate time-consuming, error-prone activities so patient data is not compromised. The ability to automate at this level is becoming more and more critical in order to deal with storage environments that need to constantly expand and change to support growing patient files.

- Enable continuous availability. Built-in high-availability features in the Data ONTAP® 8 operating system protect against hardware and disk failures as well as operational downtime due to system upgrades or routine management tasks.
- Provide Integrated Data Protection. Data ONTAP 8 provides Integrated Data Protection—including Snapshot™ copies, SnapMirror replication, and integration with data protection software partners—so that data is protected, even across numerous data centers.

6.4 Infinite Data Scaling

NetApp has always offered the ability to efficiently scale up in modular increments, as compared to competitive solutions that typically require a forklift upgrade whenever a workload outgrows the architecture of its specialized (and nonunified) storage systems.

Scale-Out Architecture Accommodates Growing Content Repositories

With the introduction of Data ONTAP 8, NetApp offers the healthcare industry the ultimate in seamless scaling: the ability to scale out performance and capacity for both NAS and SAN environments to accommodate a range of medical applications. Petabytes of patient data and billions of files can now be stored across numerous sites in a single, location-independent namespace, with retention policies defining where and how long data should reside.

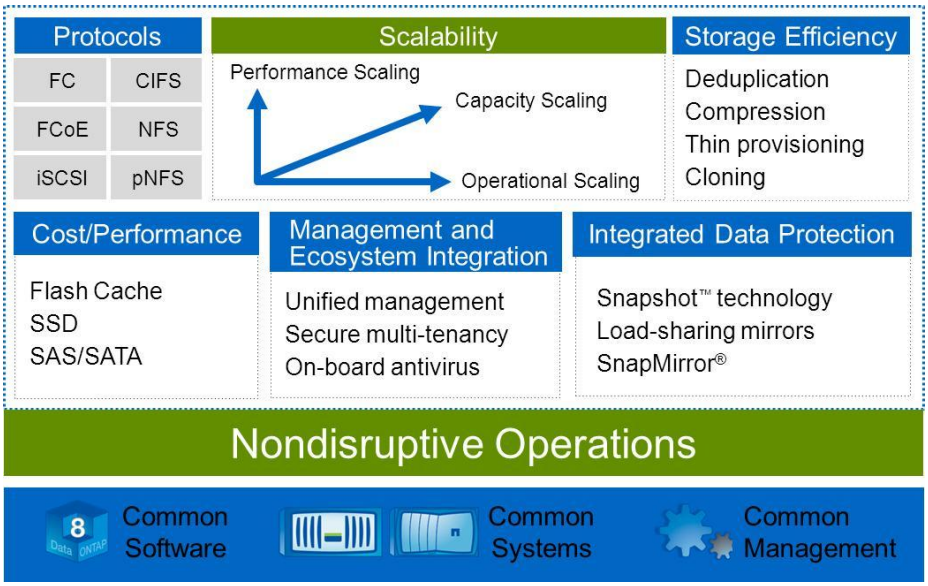
With Data ONTAP 8, healthcare organizations can consolidate file services workloads and business applications onto a dynamic storage cluster by adding nodes, disk technology, and caching as needed for a flexible, scalable file services infrastructure. The ability to numerous multiple workloads and deploy several technology options across a single architecture gives you the flexibility to deal with change, because whatever storage requirements you have today, they will change again in the next 12 to 18 months.

Unified Architecture

The NetApp Unified Storage Architecture and the NetApp clustered Data ONTAP operating environment provide the foundation for an agile data infrastructure that delivers the flexibility to support a diverse set of medical and business applications, numerous protocols, diverse workloads, and the changing requirements that confront healthcare organizations today.

- **Unified Architecture.** Get NAS and SAN under the same roof. It provides single system management and is a fully integrated solution.
- **Nondisruptive Operations.** Because the environment is architected as an “always-on” infrastructure, clinicians have continuous access to medical data access, and it eliminates the need for planned downtime for maintenance or upgrades.
- **On-Demand Flexibility.** Get ahead of the market with an agile data infrastructure that seamlessly adjusts to evolving business requirements with dynamic, transparent, and on-demand reconfiguration capabilities.
- **Operational Efficiency.** This fully integrated solution from NetApp reduces risk with a unified architecture that scales massively to meet changing business requirements.
- **Storage Efficiency.** The storage efficiency features such as deduplication, compression, thin provisioning, and cloning that are built into clustered Data ONTAP provide substantial space savings, allowing more data to be stored at a lower cost. Data protection provides replication services, enabling valuable patient data to be backed up and recoverable.

Figure 8) One architecture for many diverse workloads.



NetApp Data ONTAP delivers superior capabilities for file services across file shares and virtual infrastructures supporting PACS, EMR, and EHR. The real benefits of unified storage are at the architecture level, not at the box level. A unified architecture means that you don't need to take a rip-and-replace approach when you need more I/O or a mix of I/O and cost profiles for different applications and storage needs. You can increase storage utilization by using a single architecture rather than a multiarray approach that requires you to break it up into smaller pieces.

The ability to handle numerous workloads and deploy several technology options across a single architecture gives you the flexibility to deal with change, because whatever storage requirements you have today, they will change again in the next 12 to 18 months.

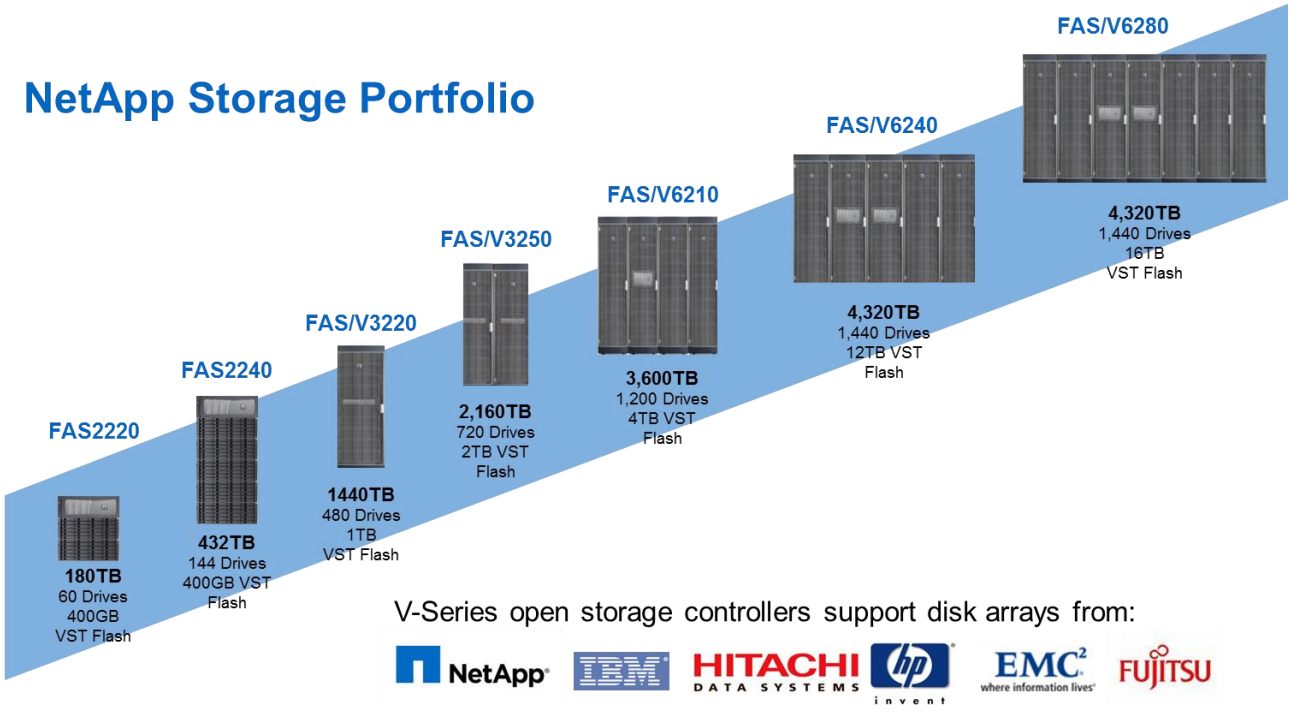
The combination of compelling functionality with massive scale is unprecedented in the industry and enables NetApp to offer optimal solutions for the widest range of workloads with a common set of tools, processes, and compatible hardware.

Consistent Building Blocks

The NetApp fabric-attached storage (FAS) family of enterprise-class storage platforms and NearStore® networked storage systems work in concert with leading healthcare systems to provide affordable image management and archiving that are easy to deploy and manage. Consolidating numerous terabytes of medical imaging files, patient data, and additional hospital records on NetApp storage can considerably reduce the number of servers and storage devices that your IT team must manage. You can accommodate your growing demands for records retention without adding headcount, maximizing your return on IT investment.

As an innovation leader, NetApp also partners with leading vendor-neutral archive (VNA) companies such as Acuo, DeJarnette, and TeraMedica to help you establish a single repository for patients' medical images. By interfacing with numerous PACS providers, the VNA gives central access to medical images for second opinions, EHR integration, provision to health information exchanges (HIEs), and more.

Figure 9) NetApp storage solution building blocks.



Secure Multi-Tenancy

With NetApp software, you can share storage with maximum privacy and data security. In addition, NetApp with Cisco and VMware helps provide secure, end-to-end multi-tenancy across applications and data so you can reap all the benefits and business advantages of a shared IT infrastructure with virtualized computing.

7 Imprivata OneSign

Fast, secure access to patient information takes more than a simple **single sign-on** (SSO) solution. Healthcare environments are unique and complex, and they require solutions that work with care providers, whatever the workflow, application, or desktop. Imprivata saves care providers from unnecessary interruptions, optimizing clinical workflows, increasing EMR/EHR utilization, and enhancing care delivery.

OneSign records all application access events in a centralized database and can track activity down to the application screen level. At the push of a button, administrators can run any number of reports that can identify users sharing passwords to mapping which applications users have access to and the credentials they use.

VMware View supports direct single sign-on from a local endpoint to a virtual desktop and bypasses the two log-on prompts for a typical Windows sign-on experience. VMware View works with leading SSO products.

Table 2) Capabilities of Imprivata OneSign.

Capability	Description
Fault tolerance/disaster recovery/site failover	For fault tolerance within a site that has numerous appliances, OneSign can accommodate a failure of one appliance with no interruption or degradation of service. Additional appliances at the site can provide higher levels of availability. Appliances in numerous sites can provide fault tolerance by serving as backups to one another over a WAN. User enrollments, policies, and SSO data are constantly synchronizing among sites. If all appliances in a site are inaccessible, OneSign agents can communicate with appliances in other sites and the switchover occurs automatically. If an entire site is down, an appliance at another site can serve agents.
Primary and secondary failover sites	For each site in the OneSign enterprise, a primary and a secondary failover site can be designated. Go to the Sites tab under Properties and drill down to a specific site to set an assignment. It is not necessary to specify failover rules at an appliance level. OneSign agents automatically fail over to appliances within the same site first and only then fail over to an appliance within the failover sites specified. Users are always challenged when failing over to an appliance in another site (because a new OneSign session must be established).
Agent failover	Once all servers in the home site become unavailable, agents switch to using a failover site (if specified). After a failover is completed, the OneSign session will preserve the connection to the appliance in the failover site for the duration of the session lifetime. Once appliances in the home site become available again, new sessions authenticated on computers that belong to this site start connecting back to the home site. However, active sessions do not automatically switch back. To force agents to fail back to the active session, users must lock and unlock their OneSign session or log out and log back in.
Agent determination of a home site	Each agent determines its home site based on the workstation's IP configuration. According to the OneSign enterprise topology, each active site has a list of IP address ranges for subnets belonging to this site. The initial attempt to determine the agent's home site involves matching the workstation IP address against any range in any site. If a range is found, then the site owning this range is considered the home site for the agent. In case this direct IP matching fails, the agent analyzes the routing table on the workstation. The route lookup involves trying to find a route that covers any IP range for any site. Route lookup helps to determine location for a VPN client outside the corporate network when direct IP address matching does not work. IP ranges are not meant for restricting access. Instead, they help determine the preferred site to use. With this in mind, in most corporate environments there exists a nondefault route to the corporate network. Therefore, for several sites with restrictive IP ranges within the corporate network subnet, the first one is chosen through the route rules.

8 F5 BIG-IP Application Delivery Controllers (ADCs)

F5 BIG-IP® is a family of application delivery solutions that optimize network traffic between users and applications. VMware AlwaysOn Point of Care offerings recommend an application delivery solution to increase the availability and scalability of VMware View and provide a seamless user experience for healthcare workers as they move between different devices or even different healthcare facilities.

The F5 BIG-IP solution provides the capability to integrate with Active Directory for user name to View pod mapping. This capability allows the use of a single name space for all View client connections. This unique capability also allows user name persistence, whereas other load-balancing solutions are limited

to device-centric session persistence. User name persistence allows the user to disconnect from one physical device, reconnect via a different physical device, and be reconnected to the same View pod and thus to the same View desktop. This greatly enhances the AlwaysOn Point of Care solution such that a healthcare professional can automatically be reconnected to his or her View desktop session independent of the endpoint device from which he or she establishes the connection.

Table 3) BIG-IP capabilities.

Capability	Description
High scalability and availability for VMware View	F5 BIG-IP Local Traffic Manager™ (LTM) provides intelligent traffic management and health monitoring for the VMware View Connection Servers. BIG-IP LTM deploys at each healthcare site and employs a full-proxy architecture to optimize traffic between View desktops and View Connection Servers. This enables greater scalability for VMware View, since additional View Connection Servers can be quickly deployed to support higher concurrent desktop connections without any user impact. In addition, BIG-IP LTM reduces downtime and improves availability for the View environment by monitoring the health of individual View Connection Servers and automatically redirecting user traffic to other servers if and when needed.
Single namespace for global access	With VMware AlwaysOn Point of Care, the F5 BIG-IP Global Traffic Manager (GTM) provides global traffic management for VMware View environments in distributed healthcare organizations. BIG-IP GTM continuously monitors both transient network conditions as well as the health of View Connection Servers across numerous sites. Mobile healthcare workers can connect to their View desktops from any location, and BIG-IP GTM will automatically redirect them to the nearest or highest-performing site in order to provide the best user experience.
Seamless user experience with user name persistence	BIG-IP Access Policy Manager® (APM) provides a seamless user experience for healthcare workers who work from several locations across the organization on a daily basis. BIG-IP APM saves the VMware View desktop session state and automatically reconnects users to their existing sessions as they move between several devices or locations, providing consistent access to their View desktops and higher productivity.

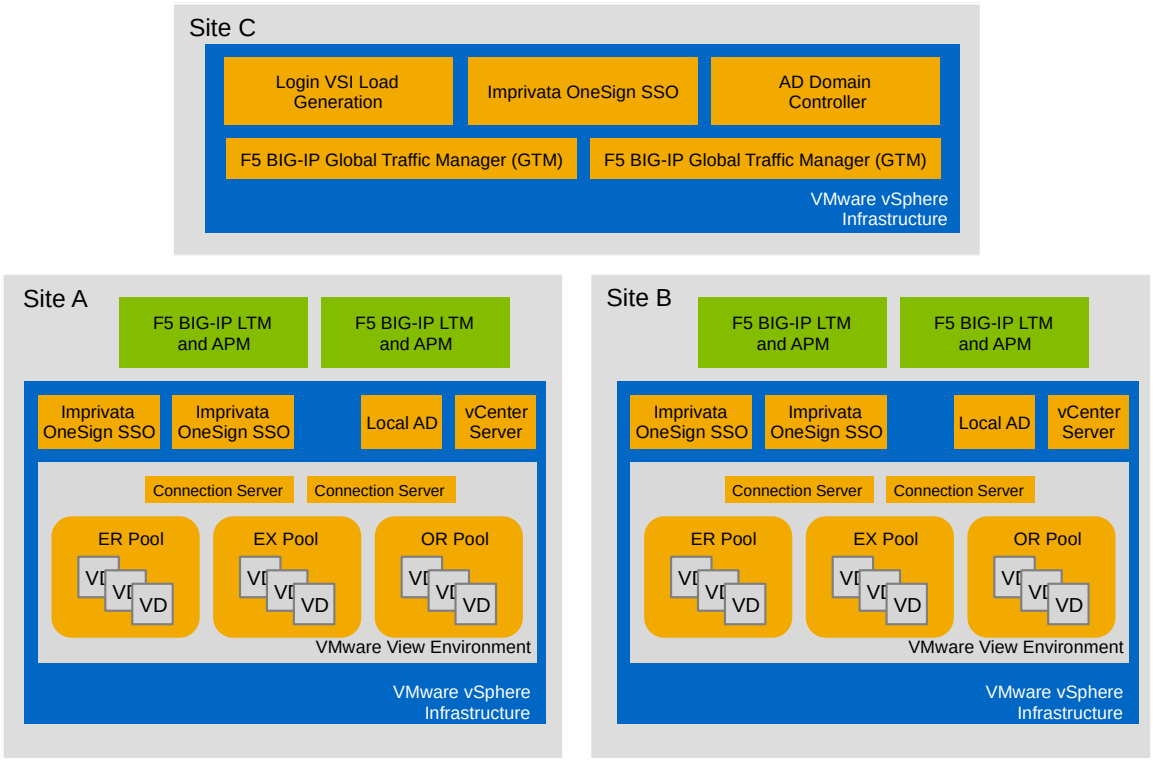
9 NetApp Lab Validation of AlwaysOn Point of Care Solution

A lab environment was deployed and configured to validate the VMware AlwaysOn Point of Care solution with NetApp storage systems, Cisco UCS servers, F5 BIG-IP application delivery controllers, and Imprivata OneSign.

The lab implementation for the validation was designed to accommodate 350 virtual desktop users generating a medium knowledge worker workload and did not include the user data component of the VMware AlwaysOn Point of Care solution. The environment consisted of three logical sites. Two sites, Site A and Site B, host the virtual desktop services delivered by the VMware AlwaysOn Point of Care solution. A third site, Site C, represents existing customer infrastructure and hosts the components required to administer, manage, and test the virtual desktops.

So that no performance impact is experienced by end users in the event of a site failure, sufficient resources must be available at both Site A and Site B to accommodate all 350 users simultaneously. To facilitate the validation, Site A was designed to support the full 350 concurrent virtual desktop users targeted for the validation while Site B was designed to support only 175 virtual desktop users. This configuration enables the testing of the failure of Site B without any anticipated performance degradation for end users when all users are directed to desktop sessions hosted from Site A. Figure 10 shows the logical overview of the three sites in the lab environment.

Figure 10) Logical overview of the lab environment.



9.1 Hardware

This section describes the hardware that was used in the lab environment for the validation. A summary of the hardware deployed at each site is provided in Table 4.

Table 4) Summary of the hardware used in the lab environment.

Site	Hardware deployed
Site A	• 1 NetApp FAS3240C with 2 DS2246 Disk Shelves and Flash Cache • 2 F5 BIG-IP 3600 Appliances • 6 UCS B200M3 Blades • 1 UCS 5108 Blade Chassis • 2 UCS 2204 Fabric Extenders • 2 UCS 6104 Fabric Interconnects • 2 Nexus 5548UPs
Site B	• 1 NetApp FAS3270C with 2 DS2246 Disk Shelves and Flash Cache • 2 F5 BIG-IP 3600 Appliances • 2 UCS B200M2 Blades • 1 UCS B250M2 Blade • 1 UCS 5108 Blade Chassis • 2 UCS 2204 Fabric Extenders • 2 UCS 6104 Fabric Interconnects • 2 Nexus 5548UPs
Site C	• 1 NetApp FAS3270C with 2 DS2246 Disk Shelves and Flash Cache • 2 Fujitsu RX200-S6s

Storage

A NetApp FAS3240C was deployed at Site A, while Site B and Site C each hosted a local FAS3270C. To provide the required storage capacity and performance, two DS2246 disk shelves with 24 450GB 10K RPM SAS drives were connected to the storage controller pair at each site using a full multipath high-availability cabling configuration. Each controller in the environment was assigned all of the 24 disks in one of the DS2246 shelves. Nineteen disks in each shelf were dedicated to supporting the VDI workload, three were allocated to the root aggregate of the storage system, and two were designated as spares.

All controllers in the lab environment contained 256GB of Flash Cache, one two-port 10GbE expansion network card, and a four-port expansion SAS card.

Servers

Cisco UCS B-Series blades provided the compute and memory resources for the virtual desktops at Site A and Site B in the lab environment. Site A hosted six B200M3 blades in a UCS 5108 Blade Chassis. Site B hosted two B200M2 blades and one B250M2 in a UCS 5108 Blade Chassis. Site C was composed of two Fujitsu RX200-S6 servers.

Load Balancing

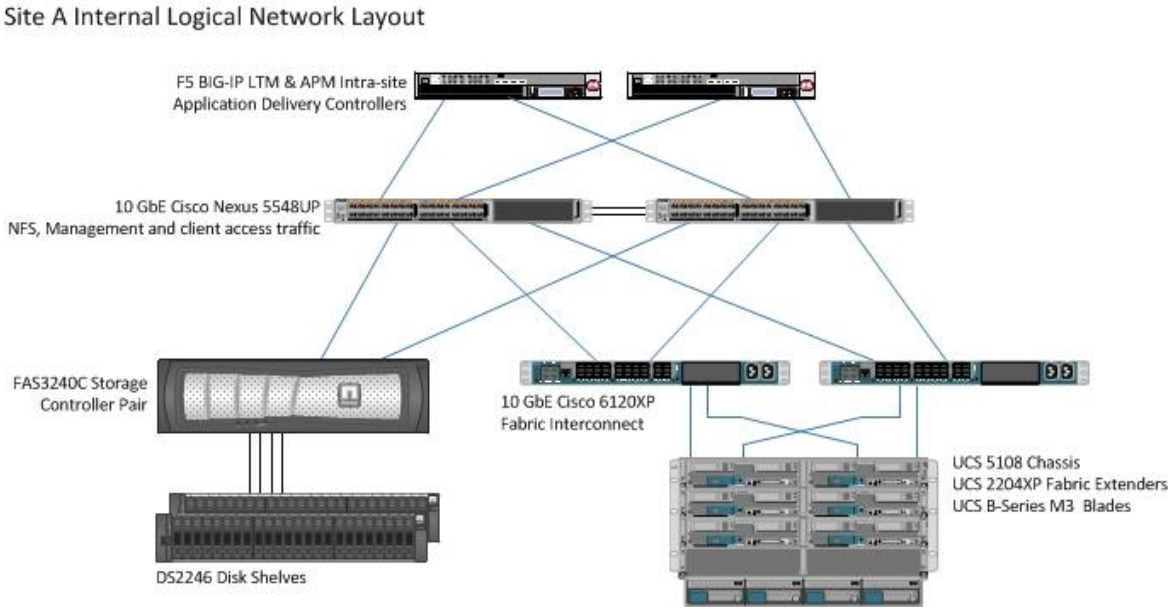
F5 BIG-IP application delivery controllers provided traffic management in the lab environment. At both Sites A and B, two F5 BIG-IP LTM-3600s were deployed in a redundant configuration to provide access policy management and traffic management for the VMware View services within each site. Site C hosted two F5 BIG-IP GTM Virtual Edition virtual machines. The GTM provides site-level traffic management, distributing requests from users across Sites A and B.

Network

Networking within both Sites A and B was provided by Cisco Nexus 5548UP. The Nexus switches provide converged Ethernet and Fibre Channel networks connecting the UCS blades and the NetApp storage. The Ethernet network was used to present NFS volumes to the blades and the FC network to present LUNs for the installation of the ESXi™ hypervisor.

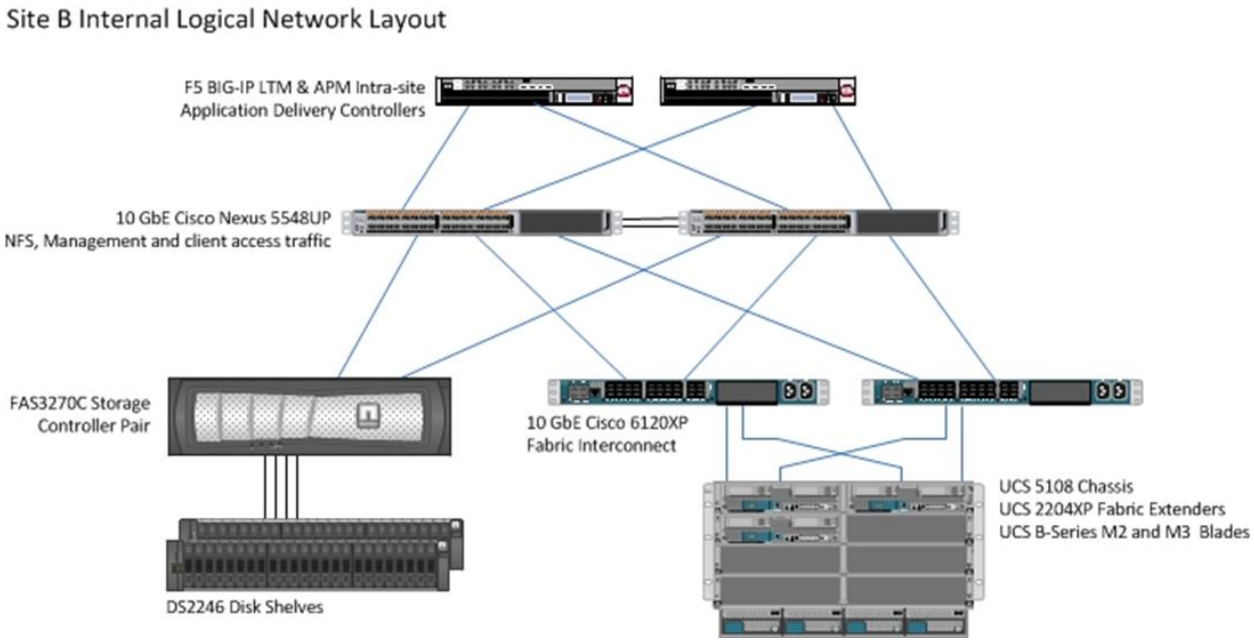
Within each site, three VLANs were created. One network was dedicated to management traffic, one to application traffic, and one to storage traffic. All VLANs were routable to all other VLANs within the environment. The network layout within Site A is shown in Figure 11.

Figure 11) Site A lab environment logical networking.



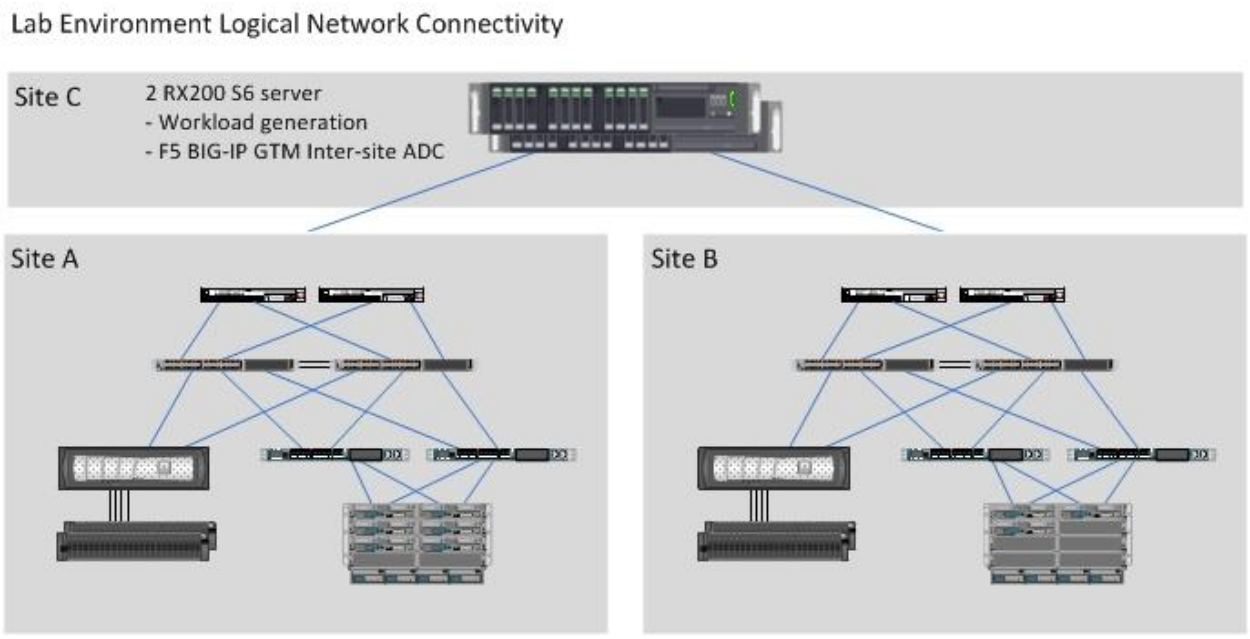
The network layout within Site B is shown in Figure 12.

Figure 12) Site B lab environment logical networking.



The lab environment network layout between Sites A, B, and C is shown in Figure 13.

Figure 13) Lab environment logical network connections.



9.2 Software Components

This section discusses the software used in the lab environment. A summary of all the components and versions used for the validation is listed in Table 5.

Table 5) Software components used in the lab environment.

Product	Version
Data ONTAP	• Data ONTAP 8.1.1 7-Mode
VMware vSphere	• vSphere 5.0
VMware ESXi Hypervisor	• ESXi version 5.0.0 build 821926
VMware vCenter	• vCenter version 5.0.0 build 804277
VMware View Connection Server	• VMware View Manager 5.1.1 build-799444
VMware View Composer (Linked Clones)	• VMware View Composer 3.0.0.5518 build 691993
F5 Application Delivery Controller	• F5 BIG-IP -11.2.1.797.0
Master Image Replication Software	• NetApp SnapMirror
Single Sign-On (SSO)	• Imprivata OneSign version 4.6-101
Windows Server®	• Windows 2008 R2 Enterprise
Windows Desktop	• Windows 7

Data ONTAP

Data ONTAP was configured according to best practices outlined in TR-3749 NetApp Storage Best Practices for VMware vSphere.

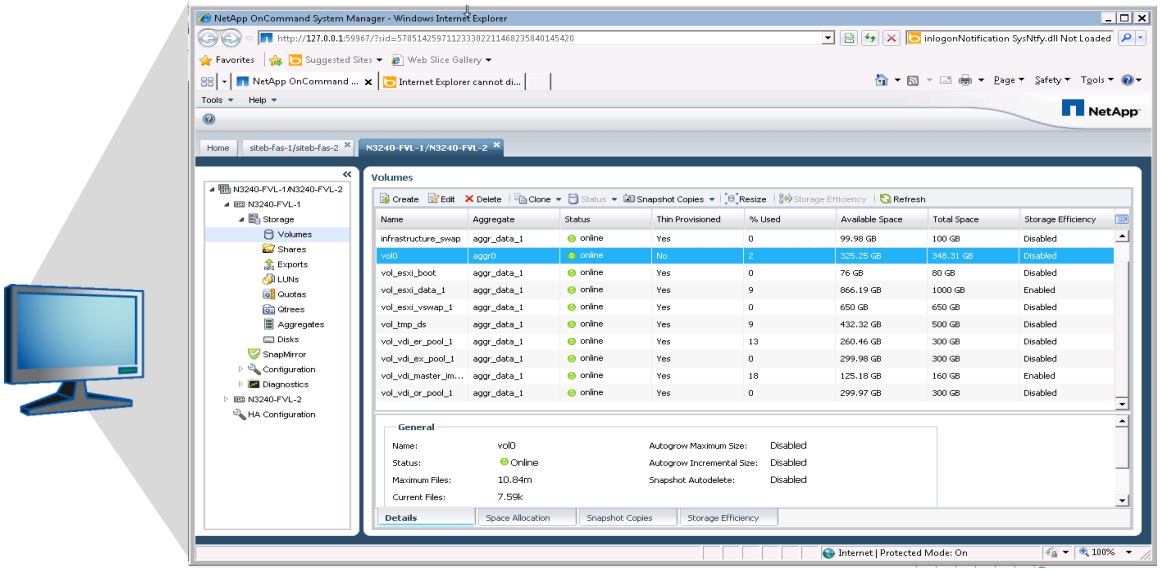
FlexVol Volumes

At Sites A and B, six FlexVol® volumes were created on each controller.

- Infrastructure VM volume, used to store the VMDKs for the infrastructure components
- Master Images volume, used to store the master images for the local desktop pools
- Master Images Mirror volume, used as the destination volume for the replication of master images from the remote site
- ER Desktop Pool volume, used to store the linked clones for the Emergency Room pool
- EX Desktop Pool volume, used to store the linked clones for the Exam Room pool
- OR Desktop Pool volume, used to store the linked clones for the Operating Room pool

The volumes were presented to the local ESXi hosts over NFS. Storage DRS was then used to create four datastore clusters, one for infrastructure VMs and one for each of the three VMware View pools. This configuration distributes the storage workload across both controllers and is shown in Figure 14.

Figure 14) NetApp FAS volume layout.



SnapMirror

In order to support disaster recovery and to simplify the task of creating similar master images at Sites A and B, synchronous SnapMirror relationships were established between the NetApp storage controllers hosting the master image volumes at Site A and Site B. The volume hosting the master images for Site A was synchronously mirrored to Site B, and the volume hosting the master images for Site B was synchronously mirrored to Site A.

When a new master image is deployed, it can be created at either Site A or Site B. As the image is created, it is synchronously mirrored to the other site. A new master image created at Site A will be replicated to the mirrored volume at Site B immediately. However, the mirrored volume is restricted and read-only, so in order to deploy the replicated image at Site B a local clone must be created. The new clone can then have any customizations specific to Site B applied. Once it has been customized a new

VMware snapshot is taken of the clone and is used to compose a new pool, or to recompose an existing pool.

Deduplication

Deduplication was enabled on the master image volumes and the infrastructure VM volumes at all sites. Deduplication reduces the storage capacity required for the master images and infrastructure VMs, since the master images share a common operating system and the infrastructure VMs share a common operating system. This results in a large number of shared blocks within the volume that can be deduplicated.

Flash Cache

A 256GB Flash Cache module was deployed in all of the storage controllers in the lab environment. All Flash Cache modules were configured to cache metadata and normal, frequently read blocks. Flash Cache is deduplication aware; blocks common to master images or infrastructure VMs are only cached once.

NetApp System Manager

All of the storage controllers in the environment were managed using NetApp System Manager (NSM). NSM enables the management of several storage systems through a single Web-based interface.

NetApp Virtual Storage Console

The NetApp Virtual Storage Console (VSC) for VMware was used to automatically apply best practice tuning to ESXi hosts and create rapid clones of the master images.

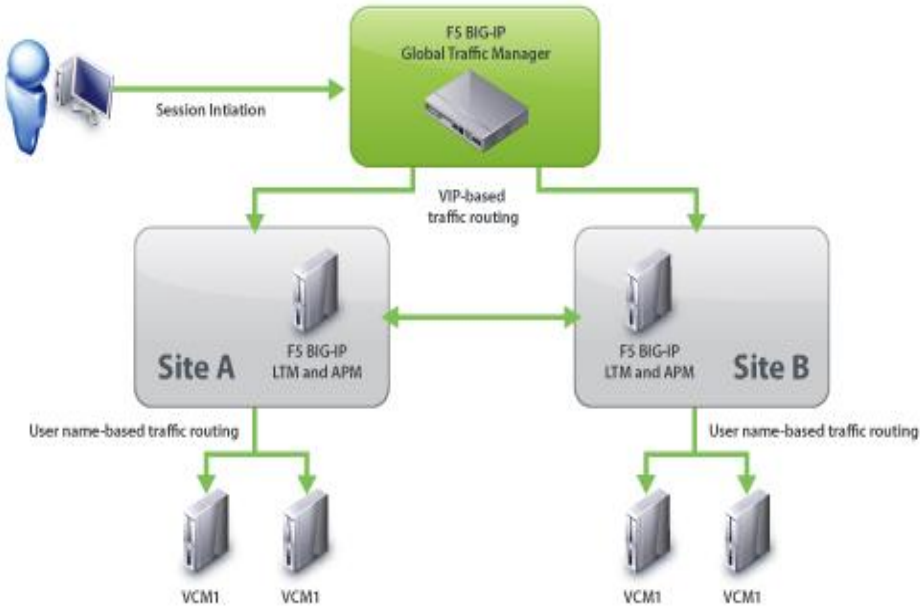
Network Configuration

Network design plays a key part in routing traffic optimally and intelligently between Sites A and B. Key design considerations include:

- Creating sufficient VLANs to efficiently and optimally segregate traffic at the sites
- Deploying the Application Delivery Controllers / Load Balancers to intelligently route incoming connections to the appropriate sites

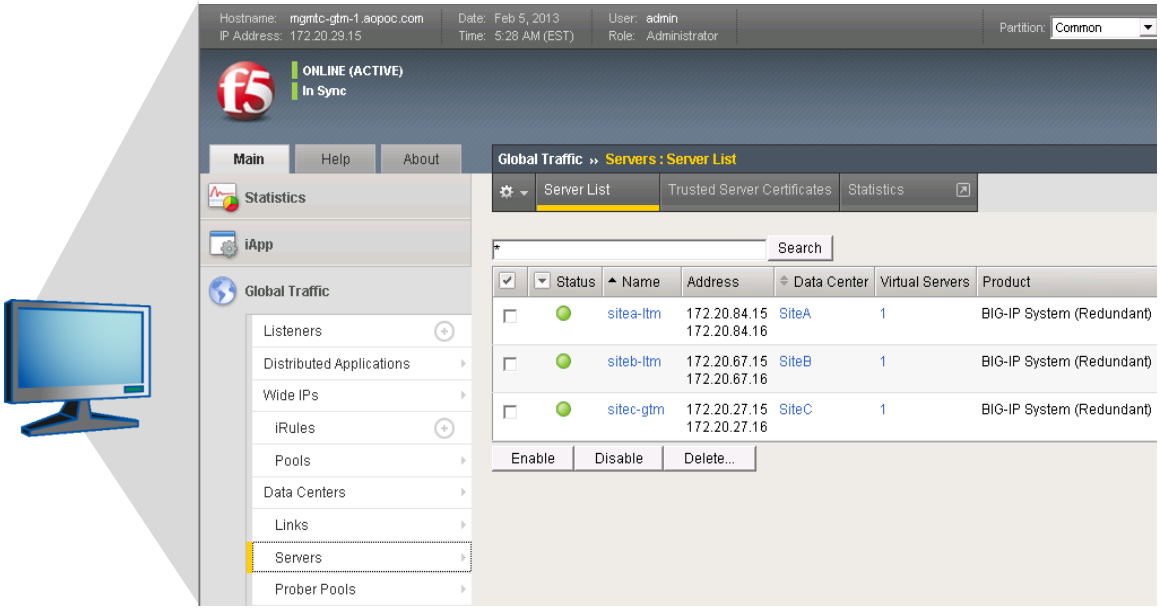
For the lab validation, redundant F5 BIG-IP LTM and APM modules were deployed at Sites A and B, and redundant F5 BIG-IP GTM Virtual Edition virtual machines were deployed at Site C. The GTM is aware of the status of the LTM modules at Sites A and B, and routes traffic in a round-robin fashion between sites depending on LTM service availability. An overview of the traffic flow from the client device through the GTMs to the LTMs is shown below. The server configuration for the GTM is shown in Figure 15.

Figure 15) Logical flow of incoming requests.



The GTM module provides a single point of access common to clients at both sites. This significantly enhances the user experience, since users working at or travelling between several locations access their desktops using the same URL.

Figure 16) F5 Global Traffic Manager network server summary.

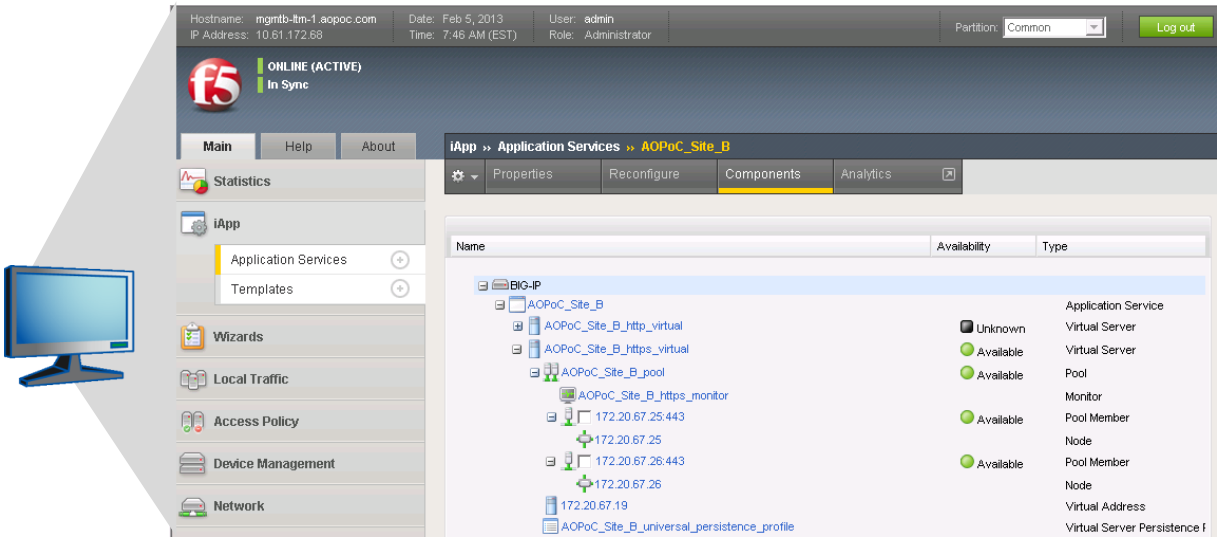


The LTM and APM modules provided the functionality required to provide user name–based session persistence. This enables a user to roam across devices or sites and still connect to an existing desktop session. An access policy is used to define an affinity for each user to either Site A or Site B based on

Active Directory group membership. The LTM module then uses iRules to determine if any existing connection servers are hosting an active session for the user, and, if so, directs any new connection attempts to the connection server hosting the existing session.

In the event that the user does not have an existing session, the LTM balances the load evenly across the connection servers based on the number of active VMware View client connections to the connection servers. The access policies and iRules are assigned to an Application Service configuration for VMware View in the environment at each site. The Site B Application Service configuration is shown in Figure 17.

Figure 17) F5 Local Traffic Manager Application service configuration for Site B.



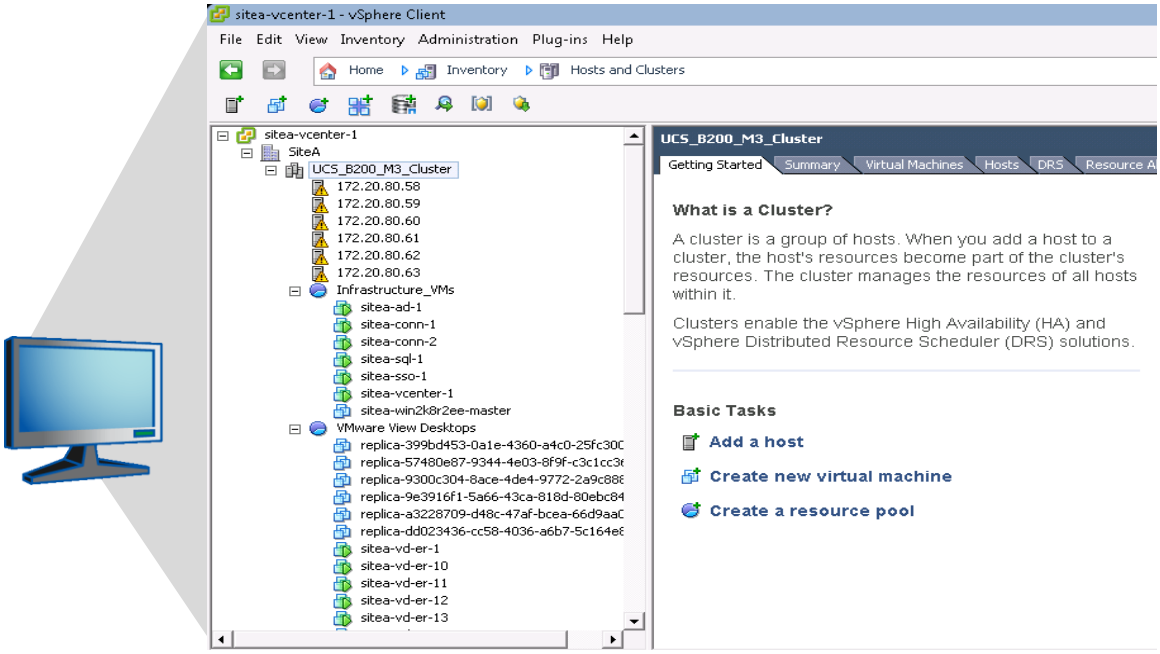
VMware vSphere Configuration

VMware vSphere provides the virtualization infrastructure for the environment. The ESXi hypervisor was deployed on the UCS blades at Sites A and B, as well as the Fujitsu RX200-S6 servers at Site C. VMware vCenter was deployed at each site to manage the virtualization infrastructure.

Within Site A and Site B, all available Cisco UCS B-Series blades were configured as a DRS cluster. This configuration allows the management and distribution of resources across the available ESXi hosts to occur automatically. It also enables the use of vSphere high availability, which automatically restarts VMs in the event the ESXi host on which they are running fails.

Within each DRS cluster, two resource pools were created. The first resource pool hosts the infrastructure VMs that support the virtual desktops at the site, including a local Active Directory server instance, redundant Imprivata OneSign virtual appliances, vCenter, and the VMware View connection servers. The second resource pool contains the virtual desktops managed by VMware View. The infrastructure resource pool was configured with a higher resource allocation priority than that of the resource pool containing the virtual desktops. The DRS and resource pool configuration of Site A is shown in Figure 18.

Figure 18) Server configuration for Site A.



The two RX200-S6 servers at Site C were also configured as a DRS cluster. Two resource pools were created, one containing the infrastructure VMs and the second containing the LoginVSI load generation VMs.

VMware View Configuration

The lab environment was designed to address a scenario in which three different master virtual desktops were required. The three types used for the validation were emergency room (ER) desktops, exam room (EX) desktops, and operating room (OR) desktops. All pools were configured to use floating nonpersistent desktops that were based on a common master image and refreshed after user logoff. A different master image was created for each of the three pools.

A single base image was created at Site A. Microsoft Windows 7 was installed in the base image and configured according to the VMware View Architecture Planning Guide for View 5.1. Following the installation of Windows, the Microsoft Office suite of applications, the LoginVSI target package, and the Imprivata OneSign SSO agent were installed. Once all the utilities required to perform workload testing on the virtual desktops were deployed, LoginVSI was used to connect to the master image to create the user profiles within the base image required for the 350 simulated users who were needed to test the architecture.

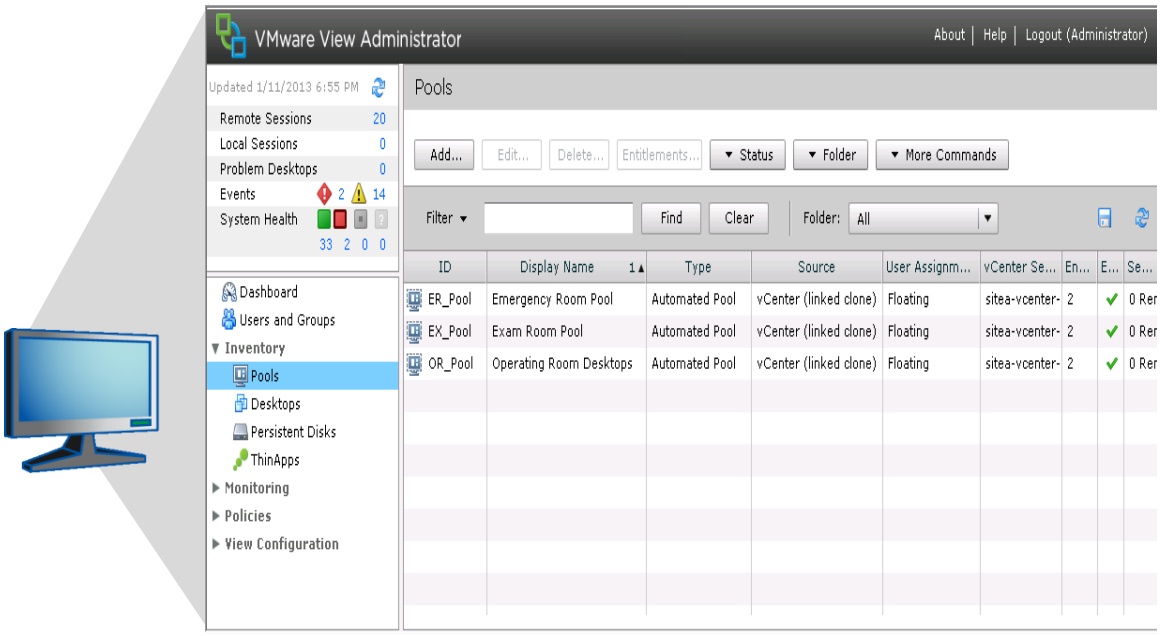
Three new master images were created from the base image using the NetApp Rapid Cloning Utility, one for each pool. A new VMware snapshot of the master images at Site A was taken. The master images had automatically been synchronously mirrored to Site B and were used to create new master images at Site B, as described in the “Data ONTAP SnapMirror” section.

Once the master images were available, three new VMware View Pools were created at Site A and Site B. At Site A, the ER and EX pools were each sized to contain 150 virtual desktops and the OR pool to contain 50 virtual desktops. At Site B, the ER and EX pools each contained 75 virtual desktops and the OR pool 25 virtual desktops. All pools were configured to automatically refresh desktops on user logout.

Once the pools were created, groups containing the Login VSI users and the domain administrators group were entitled to use the pool.

Note: Following VMware View best practices, the users are grouped and the group is entitled in the VMware View Connection Manager. Pool configurations in Site A are shown in Figure 19.

Figure 19) VMware View configuration.

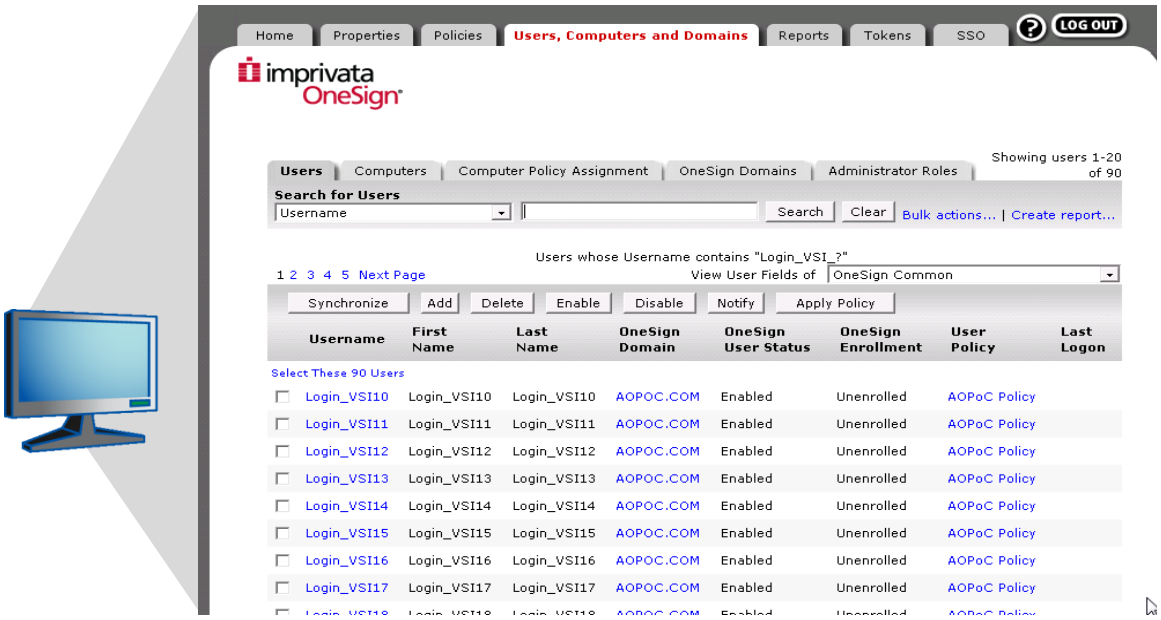


Single Sign-On Configuration

Imprivata OneSign was used to provide single sign-on capabilities in the lab environment. Two instances of the Imprivata OneSign virtual appliance were deployed at each site and the Imprivata OneSign agent was installed in a shared workstation configuration in the master images for each pool. A OneSign enterprise deployment was configured that was composed of all of the Imprivata appliances in the lab environment.

The OneSign enterprise was set up to authenticate against the Active Directory domain for the lab environment. A new user policy was created for the environment, allowing users to authenticate either via password or proximity card. Users were imported from the Active Directory Domain and were assigned the user policy, as shown in Figure 20. A new computer policy was also created and applied to the virtual desktops.

Figure 20) Imprivata OneSign users.



9.3 Test Results

The following test cases were validated in the lab.

Table 6) Test results from lab validation.

Test Name Description	Methodology	Execution Status
Verify authentication using SSO functionality	1. Connect as Site A user by authenticating using the SSO Tap-in functionality.	Pass
Verify SSO Tap-in functions during storage failover	1. Connect as one Site A user by authenticating using SSO Tap-in. 2. Initiate a graceful storage controller takeover at Site A. 3. Connect to a new virtual desktop using the SSO Tap-in functionality.	Pass
Verify SSO Tap-in functions during server failover	1. Connect as one Site A user by authenticating using SSO Tap-in. 2. Shut down an ESXi host at Site A. 3. Connect to a new virtual desktop using the SSO Tap-in functionality.	Pass
Single namespace access via F5 GTMs and LTMs	1. For each connection server at Site A, initiate a new client session as a Site A user. 2. For each connection server at Site B, initiate a new client session as a Site B user. 3. Verify that Site A user sessions are directed to Site A connection servers, and that Site B user sessions are directed to Site B connection servers. 4. Verify that each connection server is handling exactly one user session.	Pass
Mobility—reconnect to the same VDI session	1. Connect as one Site A user by authenticating using the SSO Tap-in functionality.	Pass

from several devices	2. Lock the session. 3. From another device, reconnect to the existing virtual desktop using the SSO Tap-in functionality.	
View Composer functionality while SnapMirror is running	1. Create virtual desktop pools based on the master image at both Site A and Site B. 2. Using Login VSI, generate a “medium workload” to both Sites A and B with the 10 user sessions. 3. Connect as a user into both Site A and Site B. 4. From the logged-in user sessions, confirm that “test.txt” is empty. 5. Log off from both sessions. 6. Start master image at Site A and add text to the “test.txt” text file. 7. Stop master image at Site A. 8. At Site B, create a new clone of the Site A master image. 9. Create a new VMware Snapshot copy of the master image virtual machine and clone. 10. Recompose the virtual desktop pool at both Site A and Site B using the newly created Snapshot copy of the master image in the previous step. 11. Connect as a user into both Site A and Site B. 12. Confirm the text file “test.txt” contains the text added in step 6.	Pass
Application Delivery Controller user name persistence	1. Connect as one Site A user by authenticating using the SSO Tap-in functionality. 2. Lock the session. 3. From another site, reconnect to the existing virtual desktop using the SSO Tap-in functionality.	Pass
Application Delivery Controller traffic routing in the event of a site failure	1. Connect as one Site A user and one Site B user. 2. Disconnect Site B from the Global Traffic Managers. 3. Reconnect the Site B user session using SSO Tap-in functionality. 4. Verify that a new desktop session is created for the user from a Site A connection server.	Pass

10 Summary

Healthcare organizations are turning to virtual desktop technologies to address the operational and strategic issues related to traditional desktop environments, disaster recovery, and business continuity. Working together, NetApp, F5, and VMware enable healthcare IT to deliver a highly available desktop environment that provides clinicians with the secure access to their desktop and clinical applications needed to provide a high level of quality of care.

The NetApp reference architecture helps healthcare organizations meet regulatory compliance and provide ease of use, ease of management, and decreased resource demand in a complex environment. In addition, F5’s products and solutions bring an improved level of reliability, scalability, and security to VMware View deployments. For large VMware View deployments requiring numerous pods or several data centers, F5’s products provide the intelligent load balancing and traffic management needed to satisfy the requirements of customers around the world.

- Fast access to desktops
- Desktop follows user with existing session
- Access from any endpoint device anywhere
- Familiar interface since all desktops are spawned from the same master image
- Highest level of security

- Increased management and visibility into environment operations
- Enhanced user experience with SSO

NetApp helps healthcare organizations successfully design and deploy desktop virtualization. With NetApp, you can get the flexibility, high availability, and cost effectiveness required to grow your virtual desktop environment. Selecting the right storage platform for virtualizing your desktop systems is a critical component of virtualized desktops. It allows you to enable the scalability demanded by your operations, reduce IT costs, and improve users' performance—without any trade-offs.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

Go further, faster®

NetApp

www.netapp.com