Business Process Desktop

VALIDATED DESIGN GUIDE

vmware®

Table of Contents

About the Validated Design Guide

VMware's Validated Design Guides provide an overview of the solution architecture and implementation. The validated designs and solutions have been created through architectural design development and lab testing.

The guide is intended to provide guidance for the introduction of proof of concepts, emerging new technology and architectures, as well as enhancement of customer use cases.

The Validated Design Guides:

- Incorporate generally available products into the design
- Employ repeatable processes for the deployment, operation, and management of components within the solution.

Validated Designs are tested for a specific use case or architectural practice on a limited scale and duration. These guides ensure the viability of theoretical designs or concepts in real world practices.

The Validated Design Guides provide an overview of the solution design and implementation guidance that includes:

- Use cases that are catered to the design
- Products that were validated as part of design testing
- Software that was used for each component of the design
- Configurations used to support the design test cases
- A list of design limitations and issues discovered during the testing

Introduction

This Validated Design Guide provides you an overview of the Business Process Desktop solution. The architecture uses products from VMware and its ecosystem of partners to build a comprehensive desktop solution for centrally managing offshore and outsourced workers.

Leveraging VMware and 3rd party technology, the VMware Business Process Desktop is designed to meet specific requirements for managing and enabling offshore or outsourced workers, including data backup , restore, data encryption , security, endpoint device management, and WAN optimization .

This document will provide an overview of the various requirements, the logical solution architecture and the results of the validation. The solution is not exclusive to the products tested within the architecture and is intended as a blueprint design which customers and partners can use as a 'toolkit' to pick and choose components with their preferred vendors.

Audience

This document is intended to assist solution architects, sales engineers, field consultants, advanced services specialists and customers who will configure and deploy a Business Process Desktop solution.

For more information on contact center and unified communication solutions, please refer to On-Demand Call Center with VMware View.

Business Case

The VMware Business Process Desktop enables organizations looking to offshore or outsource processes to remote or third party locations to:

- Increase security and compliance by centralizing business-critical information
- Simplify and centrally manageme desktops to drive down operational expenses
- Improve SLAs by ensuring fast, easy and uninterrupted access to data and applications for end users across the WAN
- Ensure desktops are backed up, data is easily retrievable and desktops can be delivered on demand as a service to support changing business dynamics and requirements.

What is a Business Process Desktop?

Increasingly, organizations across the globe are turning to outsourcing to improve SLAs, increase operational efficiencies and drive down costs. Whether it is outsourcing non-core activities or combining internal teams with outsourced teams for collaborative design, development, engineering, or manufacturing - outsourcing provides an attractive vehicle for getting work done in today's economy

Popular functions that are being outsourced today include enterprise services such as HR, legal and finance, customer management through third party contact centers and testing and development work.

A snapshot of the various outsourced segments of a typical enterprise is below:

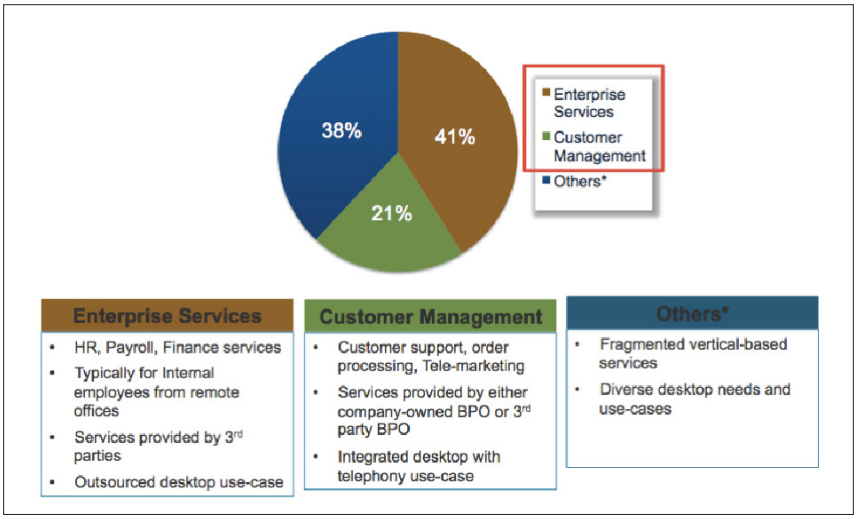

Figure 1: Outsourced Enterprise Segments

This design guide addresses outsourced or offshored enterprise services. It does not provide guidance around design considerations for customer management implementations.

Enterprise services, for the purpose of this document have been broken into two categories:

1. Enterprise Offshore Desktops (owned by corporate enterprise to service application developers and offshore IT testing). These end users require:
   - Corporate quality, hi-fidelity desktop to be used by power users.
   - Access to many complex applications
   - Requirement for high resolution graphics
   - Higher storage and network requirement
2. Enterprise Offshore Desktops (outsourced to 3rd party backoffices that can be offshore or local). These end users require:
   - Conventional desktops used primarily by process workers with low to medium desktop complexity
   - Desktops with access to limited set of 5-8 applications to deliver the services.
   - Desktops with low to medium hardware resource utilization in terms of CPU, memory, network and storage.
   - Desktops with no dependency on communication resources like softphone or VOIP

Design Overview

The design enables you to address the following requirements for the outsourced/offshored desktops:

- Security and Compliance
- Centralized Management
- ManagementData back up and recovery
- Scale on Demand

Security and Compliance

- Single namespace and global load balancing
- Centralized management
- Management data backup and recovery
- The ability to scale on demand

In the business process desktop design, there are multiple VMware View virtual desktop instances, and as a result there is a requirement for a simplified user access strategy to route users to their appropriate sites and ensure security and auditing at the network edge.

To achieve this, a global single namespace and load balancing solution is deployed to handle global incoming traffic for desktop connection.

The access infrastructure allows us to direct all users to a central point for connection, there we can evaluate the security requirements based on credentials, then redirect the connection to the appropriate site and initiate the connection with the correct desktop.

This also allows us to redirect in the event of maintenance or outage, and scale out to new sites transparently to the user population. To further enhance security RADIUS was implemented in the VMware View brokering layer to provide 2-factor challenge authentication to the users and groups requiring robust security features.

VMware virtual infrastructure can be easily augmented with the vShield suite of security products, vShield App, vShield Edge and vShield Endpoint.

In this design we leverage vShield App to provide a hypervisor based application aware firewall to protect and monitor intra-VM communications. This allows us to provide policy based access for the different “zones” in the infrastructure, limit or block intra-VM communication and provide reporting for compliance. For secure 3rd party accesss, vShield Edge enabled VPN will be open on demand.

Security from malware for the virtual desktop and infrastructure services in the design are of paramount importance. To provide a scalable and high performing solution we leverage vShield endpoint, which allows us to offload security tasks such as scanning and on-access protection to a security virtual machine on each ESX host. This optimizes the process by taking the processing overhead out of the virtual machines and placing it on the hypervisor, allowing us to accommodate the performance requirements in the sizing process. By having ’out of band’ security process and management we can realize much greater efficiency and control with respect to our virtual machines.

For monitoring and compliance we implemented vCenter Operations Manager (vCOps) for View, which

includes vCenter configuration manager to ensure compliance in the environment.

Management

- User and persona management
- Desktops and applications
- PCoIP optimization for WAN remote access
- Distributed vCenter (linked mode) and vCOps for View (V4V)

As a requirement of the stateless desktop architecture we implemented Persona Management, a VMware View feature, to roam user desktop and application specific data and settings. In concert with standards based practice around folder redirection, we have enabled a user to roam to any desktop in any site and have their corporate and personal data delivered to the desktop. Applications are virtualized using VMware ThinApp and assigned to users leveraging existing Microsoft Active Directory best practice with Group Policy preference extensions.

In some circumstances users in the business process desktop solution may have to traverse a WAN in order to connect to their View desktop. In order to optimize the user experience PCoIP tuning policies were implemented in the Active Directory to ensure the best possible experience with constrained bandwidth.

In this distributed configuration, the last thing you want to deal with is the multiple granular management consoles or dashboards. With vCOps for View, it helps provide the single pane of view into your complete corporate operations from security, compliance and the health of desktop infrastructure.

Scale On Demand

- Stateless architecture
- Modular sizing for linear scaling
- Performance

In the business process desktop design, we deployed VMware View infrastructure to support users at both the HQ Datacenter and Corp colocation datacenter sites.

In both sites the virtual desktop infrastructure is based on the VMware View reference architecture for stateless virtual desktops.

By leveraging the stateless design we give the maximum possibly flexibility for partners and customers by providing a pre-sized and pre-validated building block or blueprint which can be followed to accelerate the design phase of a virtual desktop deployment.

The stateless design allows a customer or partner to right size the virtual desktop design first time and scale out incrementally by deploying more “blocks” as needed. This allows for a standardized and repeatable deployment strategy that scales up and down inline with capacity requirements.

By using this blueprint as a basis for your deployment capacity and performance scale proportionately to user capacity.

After reviewing the solution features, the following sections will provide a quick snapshots on the user profiles and how their daily workload routine looks like.

User Profiles

In a typical organization, there are multiple user profiles with unique requirements. This solution architecture caters to the following user profiles within the Business Process Desktop use case. These can all be fulfilled using the stateless desktop design.

USER PROFILE	CHARACTERISTICS
Productivity Task Workers	Workers who participate in a limited number of business processes in a clearly defined fashion. Examples would include most back-office administrative functions, like accounts payable. Outsourced functions often match this profile. These users typically need access to a small number of applications (<10) in a controlled and managed fashion. They are unlikely to be mobile, but might work from more than one fixed location. They will have little autonomy in the way they can access processes (applications) and data.
Content / Media worker / Software developer (offshore)	Workers with a high level of expertise in an area of creativity or science that requires detailed manipulation of content. These are traditional power users. Examples include engineers, graphic designers and some developers. They typically require a narrow, but specialized portfolio of applications. They are unlikely to be mobile and will normally work from a single, fixed location. They will also need some level of control over how they access applications and data, but not full administrative control and may be ring-fenced from other corporate functions. They will require high levels of computation capability and graphical display. They may also require specialized peripheral devices.
Communications Task Workers (covered in the Unified Communications with View solution design; not part of this architecture)	Workers with a front line customer or colleague facing activity that they execute in a clearly defined fashion. Examples include call centers, retail assistants. In technology terms, they will typically use only one or two applications, but require access to rapid communication and collaboration capabilities. These capabilities may be multichannel. They are unlikely to be mobile, but might work from more than one fixed location. They will have little autonomy in the way they can access processes (applications) and data

These three business user profiles can be transposed to 2 distinct user workload profiles as listed below:

USER PROFILE	REQUIREMENTS
Task Worker	Application Profile: MS Office, Adobe, IE, Firefox, Chrome, Outlook, Corporate Apps, Antivirus Network Profile: LAN (remote office LAN); UC traffic over WAN Security Profile: Audit capability, Antivirus and Data Loss Protection
Knowledge Worker	Application Profile: MS Office, Adobe, IE, Firefox, Chrome, Outlook, SaaS Apps, Windows Apps, multimedia players (Flash etc), Antivirus, WebEx Network Profile: LAN (remote office LAN) Security Profile: Audit capability and GPO settings for UX policy; Antivirus and Data Loss Protection Other: Multi-monitor; print to nearest printer

The validated design in this document supports the unique requirements of these user profiles and also helps the IT team manage the environment securely.

Overview of Architecture

In the Business Process Desktop design there are multiple View deployments at various corporate owned, corporate leased and 3rd party sites. It is imperative to have a robust security and back-up infrastructure, which includes role based access and administrative privileges. Each site is built per the View best practices guide, with emphasis on inter-site connectivity and enhancing user experience through Single Namespace and WAN optimization. Within each site, the infrastructure consists of 2 clusters: management and virtual desktop clusters. The management infrastructure is typically separated from the virtual desktops for scalability purposes, as depending on the needs of the business, another virtual desktop pod can be added to the existing infrastructure to scale up. In addition to the above, a 3rd cluster can be created to host all the applications.

The architecture uses the Corporate owned datacenter (enterprise headquarters) as the main site to host all management components. vCOps provides very efficient management of the entire infrastructure from one site. The unified communications infrastructure will also be in the enterprise headquarters and will be shared across all the sites. We will go through the design based on the requirements.

Logical Design

The following diagram shows the logical topology for the Business Process Desktop solution:

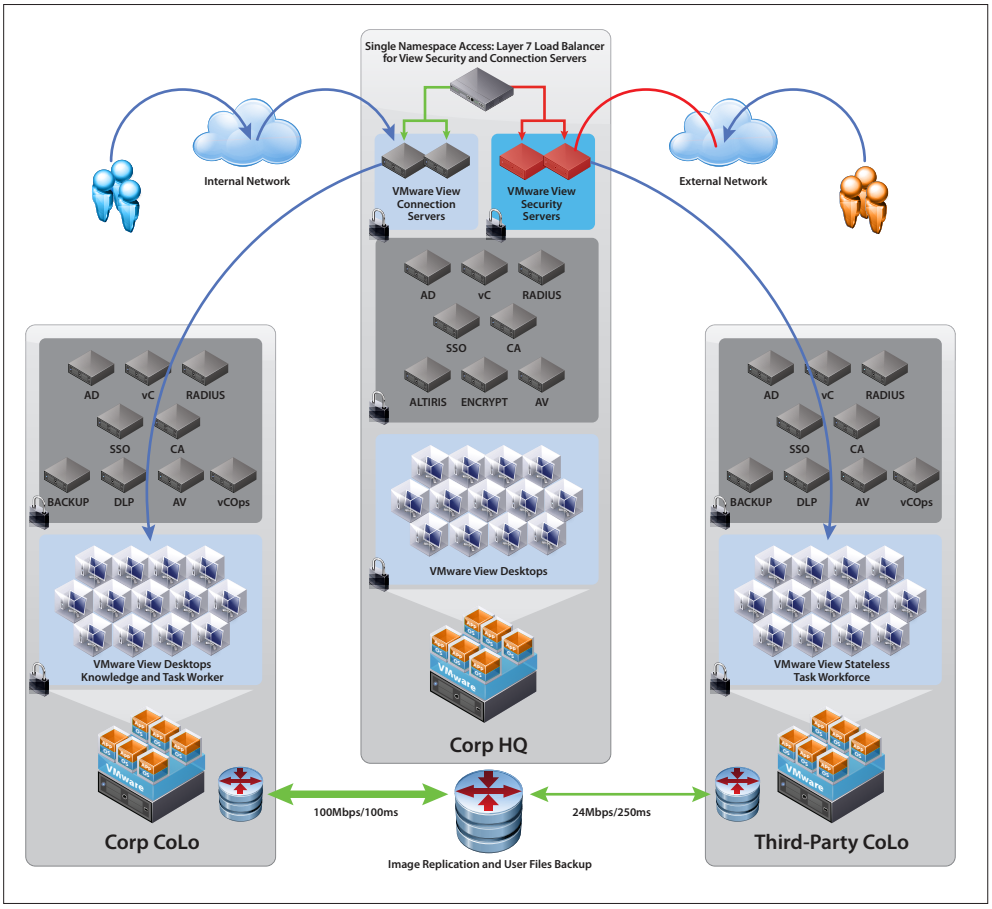

Figure 2: Business Process Desktop Reference Architecture

The design assumes 3 sites, to simulate a corporate headquarters (enterprise owned facility), corporate colocation center (enterprise leased) and 3rd party remote colocation center (3rd party owned or leased). The enterprise HQ hosts all the management components like vCOps etc (Call Manager for Unified Communications will be hosted in the enterprise headquarters although this is not covered in this paper). The 2 remote sites – Corporate Colocation center and 3rd party Colocation center hosts the full View infrastructure to be self-sufficient and cater to the local user requirements. All critical data, including Persona and profile data in the remote sites is backed up to the datacenter in the enterprise headquarters.

Each site consists of two discrete virtualized environments, for management and virtual desktop services respectively.

The management cluster includes all vSphere and View related management infrastructure and the Virtual Desktop Cluster hosts all the virtual desktops.

The VDI infrastructure is based on VMware's reference architecture for stateless virtual desktops. One of the design drivers behind keeping the VDI infrastructure separate is to allow the virtual desktop platform to be scaled up as necessary, independently of the management infrastructure.

All the components in this validated design guide were installed and configured following VMware and vendor best practices.

Key Components of the Architecture

Though the architecture is vendor agnostic, below is a list of components that are part of the architecture:

Core Components

vSphere including vCenter: The solution is built on top of vSphere, the industry leading virtualization platform. There are many benefits to using the vSphere platform and more information on the platform can be found at www.vmware.com/products/vsphere.

VMware View

VMware View simplifies desktops and applications by moving them into the cloud and delivering them as a managed service. With VMware® View™ and ThinApp™ IT can grant or restrict access to desktops, data, and applications based on endpoint device configuration, network location, and user identity. More information on VMware View can be found at www.vmware.com/products/view

VMware vShield Edge, App and Endpoint

VMware vShield provides best in class security to the virtual desktop environment. vShield EndPoint with the Hypervisor based AntiVirus protection (from our leading AV vendors), provides tremendous benefits in terms of management and ease of use for the environment. In addition, vShield App and vShield Edge products add security to the environment. More information on the vShield line of products can be found at www.vmware.com/products/vShield

Restore and Backup

Backup and Restore feature is added as a core component in this design to protect the data at remote sites and to provide fail-over capabilities if a site goes down. This design incorporates two types of backup: Image-level protection and Guest-level protection. Image-level protection enables backup clients to make a copy of all the virtual disks and configuration files associated with the particular virtual desktop in the event of hardware failure, corruption or accidental deletion of a virtual desktop.

Guest-Level protection runs like traditional backup solutions. Guest-level backup can be used on any virtual machine running an operating system with the backup agent installed. It enables fine-grained control over the content and inclusion and exclusion patterns. This can be leveraged to prevent data loss due to user errors, such as accidental file deletion. This allows for the end-user to recover their data themselves.

User Experience: User experience, though qualitative, is included as one of the core requirements of the solution. User experience in this design is enhanced by providing single namespace access to all the sites, and by providing a similar or better experience than traditional PCs using PCoIP.

vSphere and vCenter: The solution is built on top of vSphere, the industry-leading virtualization platform. There are many benefits to using the vSphere platform and more information on the platform can be found at www.vmware.com/products/vsphere.

Additional Components:

Management
With the environment spread across multiple sites, streamlined management and single pane dashboard become a necessity for IT to effectively manage the BPD environment. VMware vCOps for View, in the enterprise headquarters, provides the management infrastructure required for the entire environment, including the remote sites. More information on VMware vCOps can be found at http://www.vmware.com/products/desktop_virtualization/vcenter-operations-manager-view/overview.html

Compliance
One of the key requirements of many vertical industries is the ability to manage compliance to various industry regulations. The DLP is included in the vShield Manager and comes with the compliance template. You can also have the option to use vCenter Compliance Manager(vCM) in vCOps for further governance guidance.

The next section of the document details the architecture as it was built for testing within the lab environment at VMware.

Validation Configuration

The solution implemented in the lab was sized to scale to thousands of desktops per the sizing guidelines provided in the reference architectures published. The architecture was built in 'pods' or 'building blocks' to be scaled easily. For the functional testing aspects, the solution was implemented with 250 desktops and was deployed on the following hardware in the validation.

Lab Equipment List

PRODUCT	FUNCTION / DESCRIPTION / VERSION
Servers	2U server with 2 Intel Xeon E5 2620 2 GHz processors, 128GB RAM 1U server with 2 Intel Xeon E7 5645 2.4 GHz processors, 96GB RAM (Colocation1)
	1U server with 2 Intel Xeon E7 5645 2.4 GHz processors, 96GB RAM (Colocation 2)
Storage	nimblestorage 260 24Tb (HQ) nimblestorage 210 4Tb (Colocations)
	iSCSI storage array, Raw Disk Capacity: 8TB, Raw Flash Cache 160GB, 24GB RAM, 4 – 1GbE network ports
Networking	Unmanaged layer 3 – 10/100/1000 48 port switch

Solution Components

PRODUCT	FUNCTION / DESCRIPTION / VERSION
vSphere	5.0.1
vSphere with vCenter	5.0
VMware View with Persona Management	5.1
VMware View Composer	3.0
vShield Edge, App, and Endpoint	5.1
SSO with RADIUS	Safenet Authentication Manager v6.1.7
Desktop Antivirus	McAfee MOVE anti-virus
Backup and Restore	EMC Avamar 6.1
Storage Replication	Microsoft Distributed Files System (DFS) Replication

Optional Components

PRODUCT	FUNCTION / DESCRIPTION / VERSION
vCOps for View	1.0
Load Balancer	F5 BigIP GTM LTM APM
Liquidware Lab	FlexApp
Data security	vShield Manager DLP with Compliance configuration

Overview of Workload Profiles

For solution validation in the lab, VMware View Planner was used for the testing with standard workloads, and the mapping of the workloads with the various user profiles is given below:

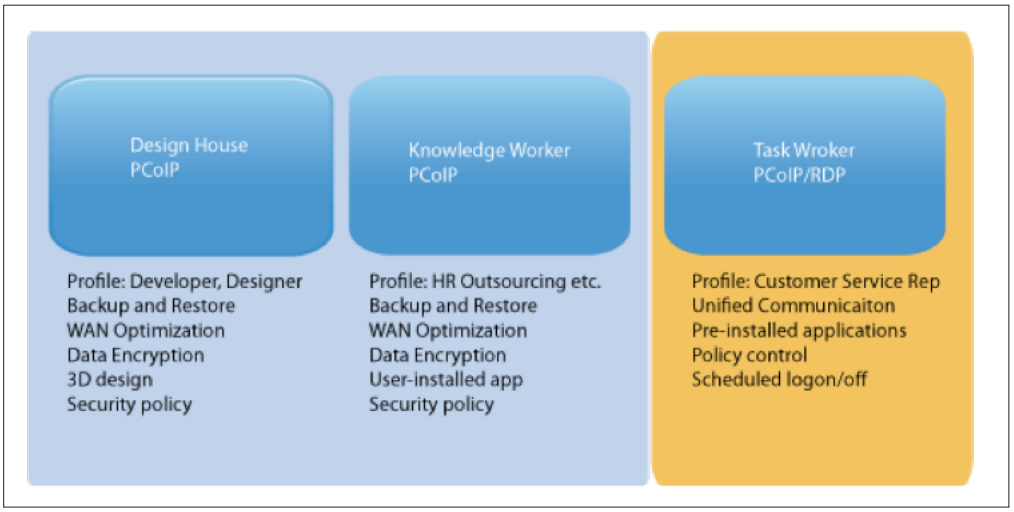

Figure 3: Workload Profiles

Single Namespace and Load Balancing

To provide single namespace access to the users, a load balancer solution is deployed in all the sites. An overview of the single namespace workflow is provided below:

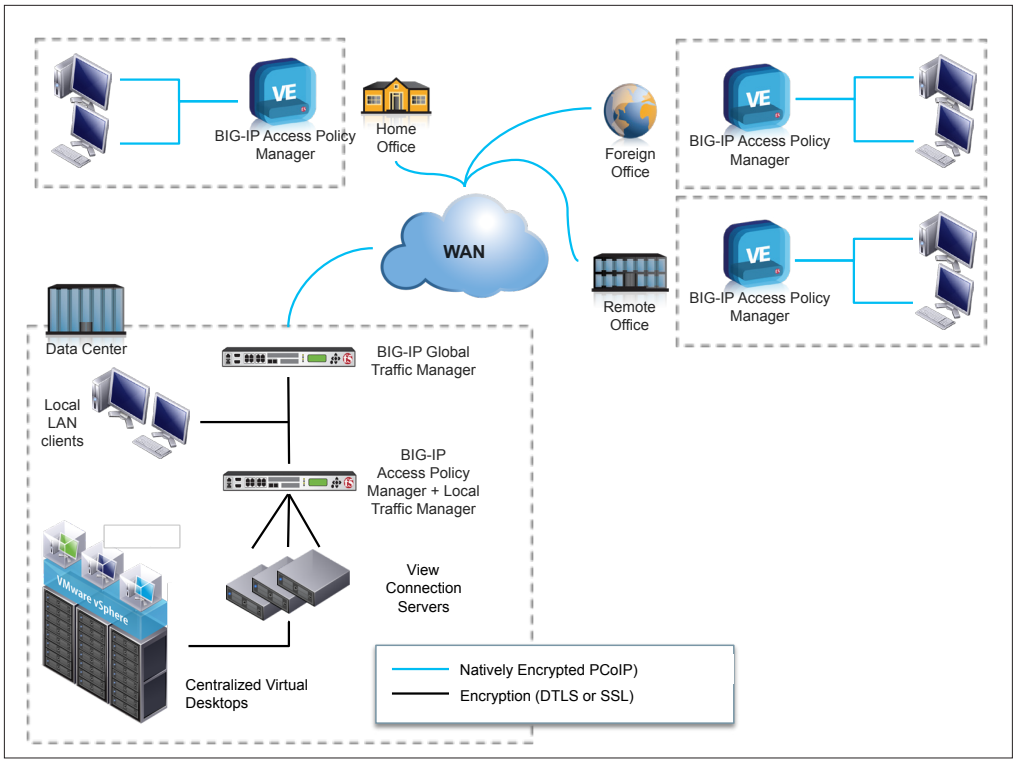

Figure 4: Single namespace using F5 global traffic management

With the single namespace design using a mixture of load balancers, users globally can use a single URL to get to their virtual desktops. This provides a seamless user experience since the user always connects to the same URL, but is provided with a desktop that is geographically local to the user.

All the clients are configured to access the same URL. The URL terminates to the load balancer, and depending on the IP and other parameters, the connection is forwarded to the preferred datacenter by the load balancer.

RADIUS Integration for user authentication

RADIUS Two Factor Authentication

VMware View supports variety of two-factor authentication devices including RSA SecurID, RADIUS compliant One-Time Password token, contacted / contactless card, and smart cards. This architecture employed the RADIUS authentication feature in View 5.1 using SafeNet RADIUS server to authenticate all users.

Once the RADIUS client is added to the server, it was paired with the View Connection Server using the View Admin dashboard, by editing the Connection Server settings in the Admin page, and adding the RADIUS authentication in the "2-factor Authentication" drop down menu in the "Authentication" tab. :

The RADIUS server information was populated using the "Create New Authenticator" button. This provides enhanced authentication using One-Time Security Protocol (OTSP.)

The RADIUS configuration difference at Business Process Desktop over VMware Mobile Secure Deskotp is the multiple sites and server instances configuration.

On your Windows Server machine with RADIUS enabled and your preferred RADIUS enabled 2FA vendor software installed, you will need to add a RADIUS Client to connect to the View Connection Server. Load the Windows Server Manager folder, and navigate to the Roles section -> NPS (Local) -> RADIUS Clients and Servers -> RADIUS Clients. Click on "Configure RADIUS Clients"

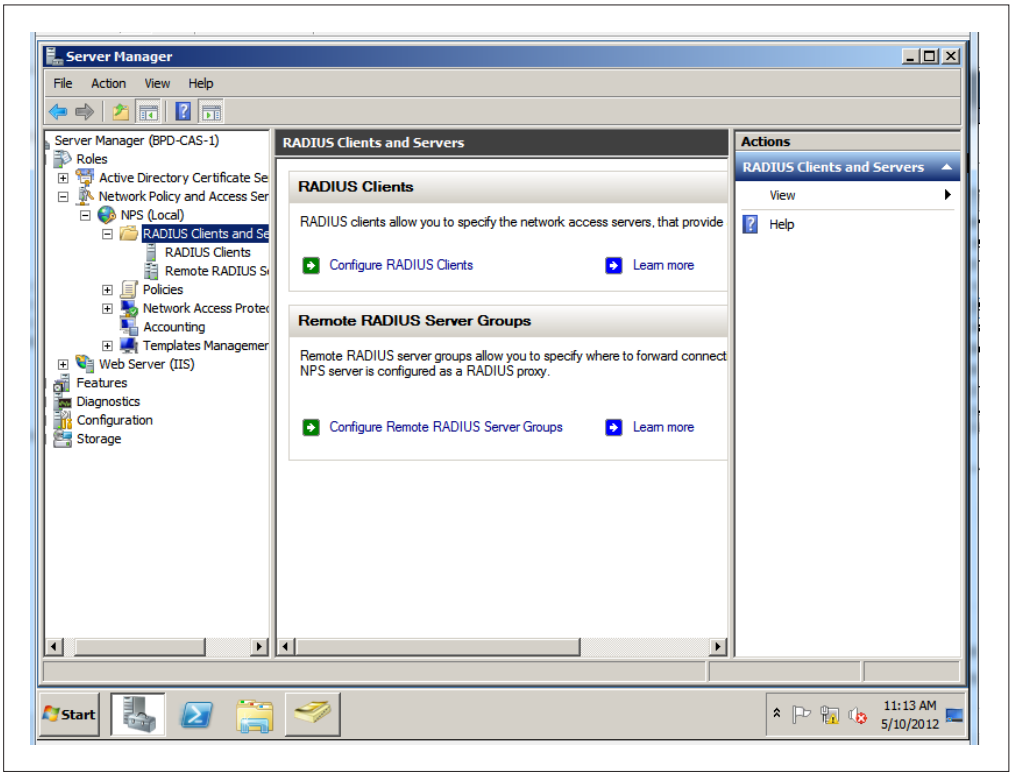

Figure 5: RADIUS Client Configuration

You will see the prompt to add a new RADIUS Client. Fill in the details below.

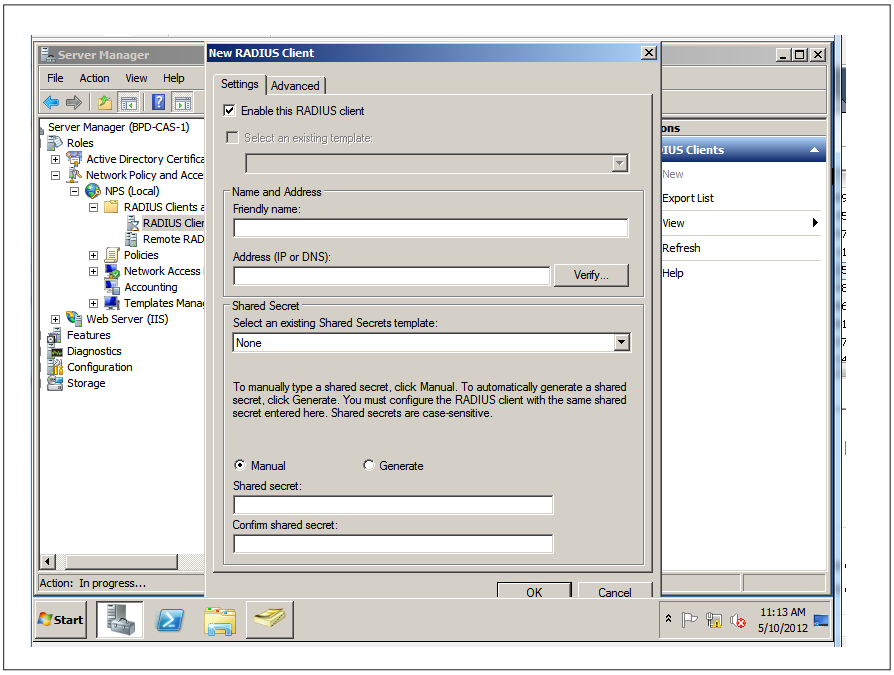

Figure 6: Add Client

Leave the defaults, and fill in the appropriate details below for your environment and press “OK”.

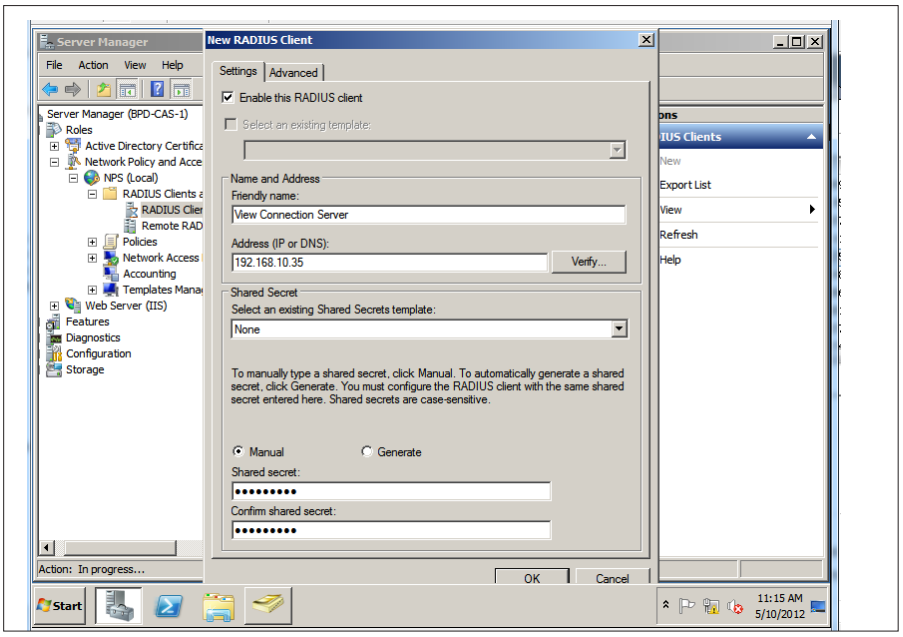

Figure 7: Client Settings

Now you will see the new RADIUS Client added to your list of clients. Next you will need to go into the VMware View Admin dashboard in order to pair your RADIUS server to your View Connection Server.

From the VMware View Administration page, you will want to go to Servers -> Connection Servers and then

click on the Connection Server you wish to pair with your RADIUS Client. Then click on the “Edit...” button.

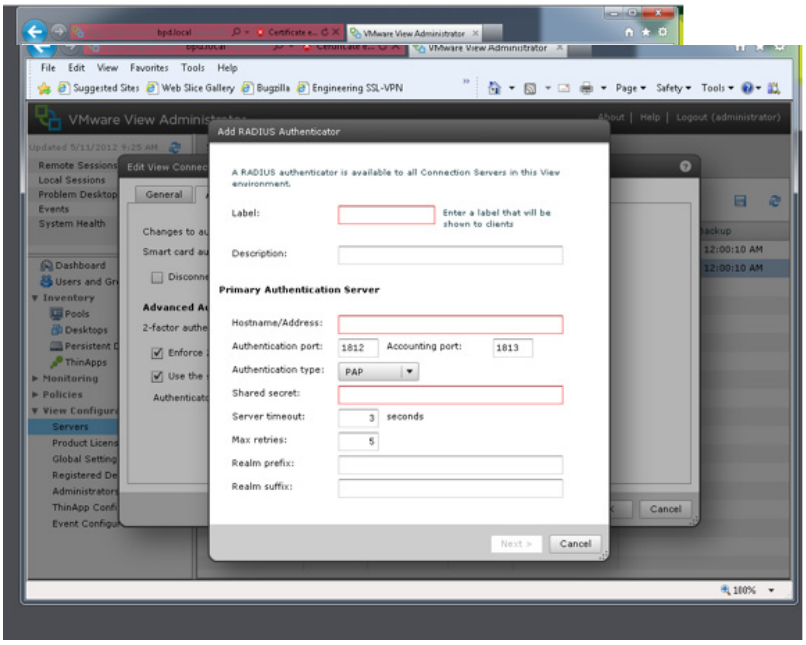

Figure 8: Authenticator Settings

Next choose RADIUS from the “2-factor authentication” drop down menu.

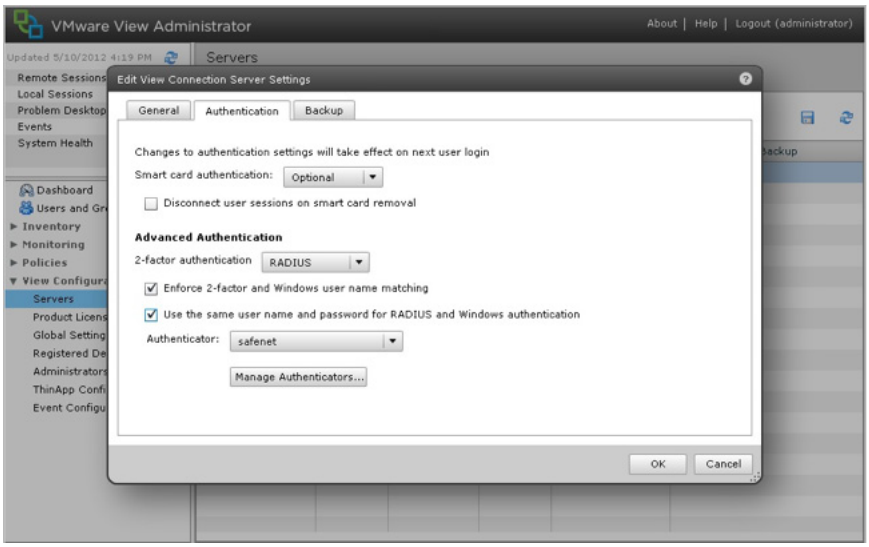

Figure 9: Configure RADIUS in View managment console

Click and check the two boxes “Enforce 2-factor and Windows user name matching” and “Use the same user name and password for RADIUS and Windows authentication”. Under Authenticator, choose “Create New Authenticator” which will launch a new dialog box. Follow through the application dialog and fill in the appropriate fields for your environment and RADIUS server.

Then click on ‘Next >’ and enter a secondary authentication server if desired.

Now your authenticator should show up in the Authentication Window.

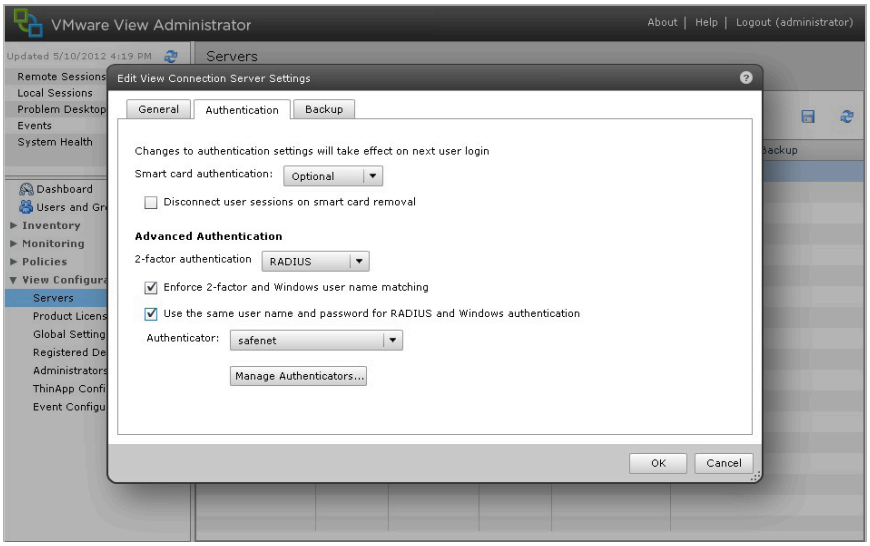

Figure 10: Advanced Authentication

Click OK and now open the View Client to test out your RADIUS Server.

As you can see after connecting to our View Connection Server, it is prompting us for our RADIUSPrefVendor Authenticator passcode. Enter your credentials and enjoy the completion of pairing RADIUS 2FA to VMware View Connection Server.

vShield Edge, App, and Endpoint Deployment

This diagram shows how the vShield App was set up for communication between the Management Components and the Desktop Pools. This configuration is repeated at each site.

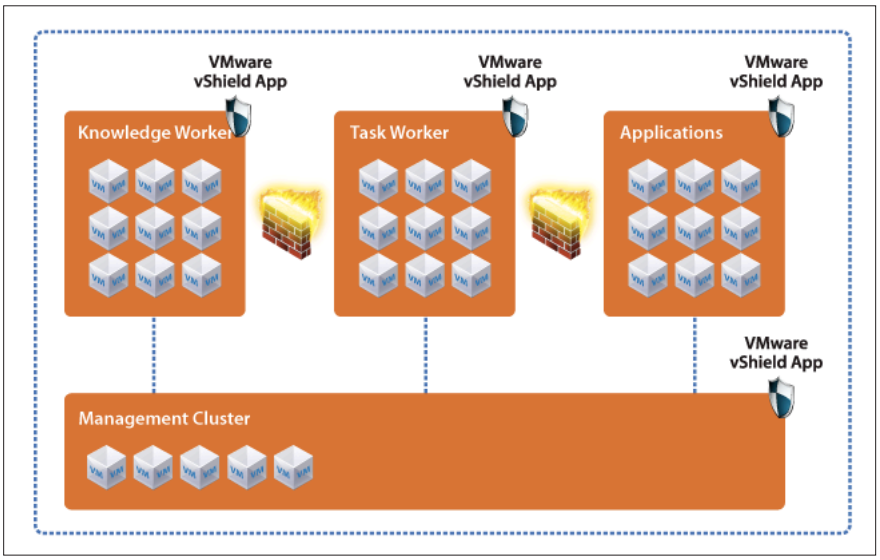

Figure 11: Use vShield App to provide access policy among different functional groups

For zoning concept, the corporate owned colocation datacenter is regarded as the same zone as the corporate datacenter. You can use Active Directory policy or standard Layer2 network security practices for this security zone. For the 3rd party colocation datacetner, use the vShiled Edge to establish VPN for image replication and user file backup from site to site.

vShield Edge allows us to control at a granular level the application traffic flows between discrete components. vShield Edge was used to segregate the management cluster from the desktop cluster at each site. It can also used to segregate pools of desktops which has stringent security requirements (e.g. 3rd party contract worker pool).

vShield App was used as a load balancer for the internal View Connection Managers, used exclusively by users with each site's local network.

VMware vShield Endpoint offloads virtual desktop antivirus and anti-malware scanning operations to a dedicated secure virtual appliance delivered by VMware partners. Offloading scanning operations improves desktop consolidation ratios and performance by eliminating anti-virus storms, while also streamlining antivirus and antimalware deployment and monitoring and satisfying compliance and audit requirements through detailed logging of antivirus and anti-malware activities.

Using vShield Edge for VPN between Sites
In an outsoucing configuration, a VPN is open to allow desktop image replication and continuous backup all data and files in the colocation sites.

Role of vShield Endpoint http://www.vmware.com/products/vshield-endpoint/overview.html

VMware vShield™ Endpoint provides industry standard APIs to optimize antivirus and anti-malware security for virtual environments via integration with VMware partners. VMware vShield Endpoint allows security technology partners to offer more efficient antivirus and anti-malware protection for virtual hosts, including VMware View desktops. You can offload antivirus and anti-malware functions from individual virtual machines to a centralized secure virtual appliance.

Using vShield App with Data Security

Deploying vShield App with Data Security provides the functionality to be able to scan for sensitive data across our entire virtual infrastructure. It includes predefined templates for country and industry specific regulations and will provide reporting of found violations.

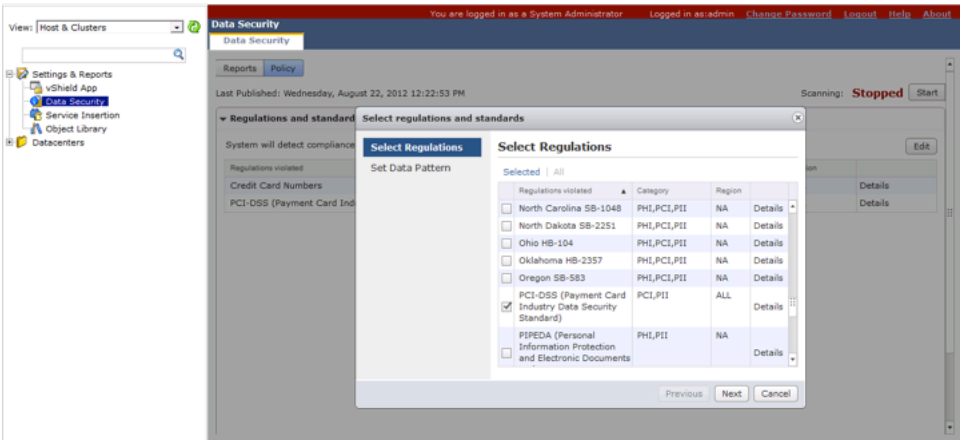

Figure 12: Selecting compliance profiles such as PCI-DSS

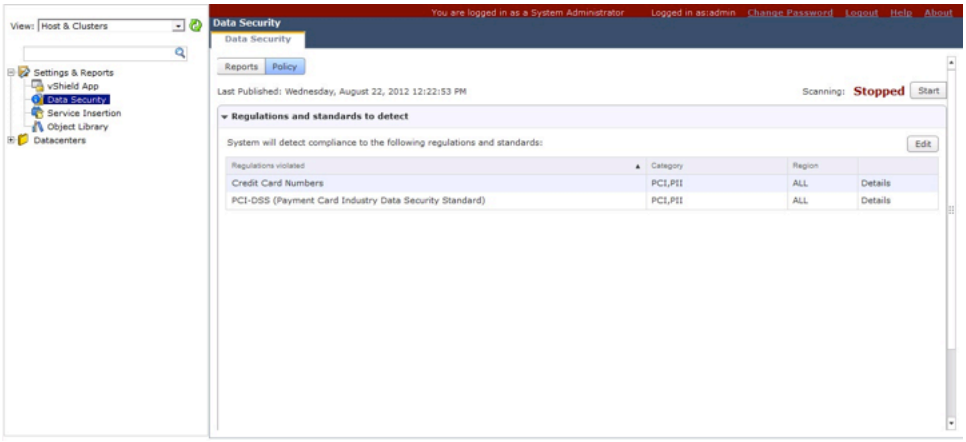

Figure 13: Dashboard displays the compliance profiles enabled.

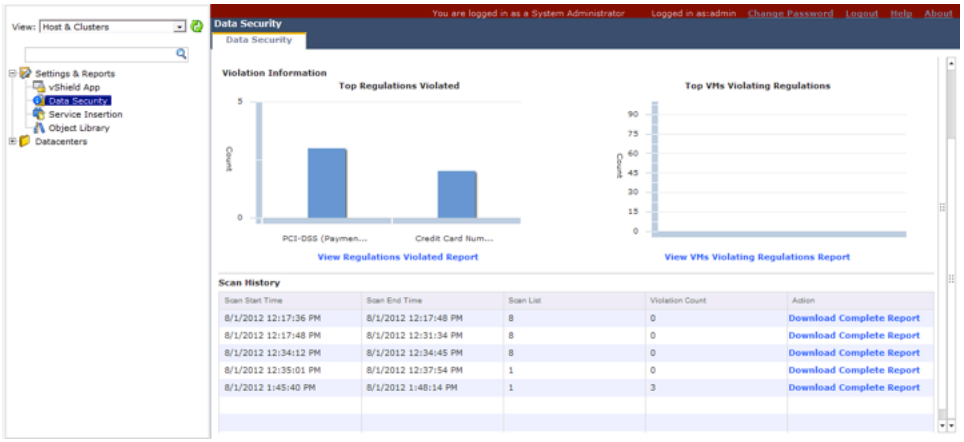

Figure 14: Dashboard showing violations as a result of compliance scanning.

After walking through the modular designs, the following section will review the general storage, network and compute design.

Network Configuration

In the Business Process Desktop design, networking in each site has similar configuration in each datacenter. The lab configuration is shown below.

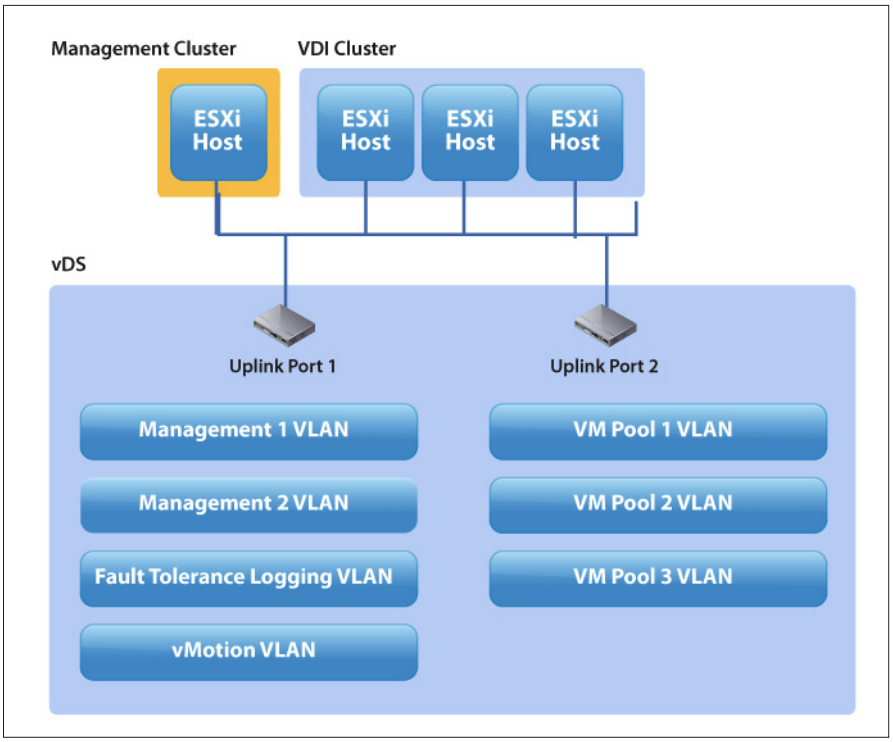

Figure 15: Network design in a single site

Storage Configuration

In the Business Process Desktop design, storage is one of the key elements to ensure user experience and provide back-up and restore capabilities for remote sites. In the lab validation, traditional View pod design is followed with the Management VMs (including AD, View Security Server, vShield, vCOps etc) located in the iSCSI datastore and the virtual desktops in the SSD datastores. The virtual desktops can also be in the FC datastores with the replicas in the SSD (high read capacity) datastores. The user data and persona files are located in the NFS datastores.

High Availability with Backup and Restore

Between the colocation datacenter, user files and data are replicated back to headquarter storage. Folder redirection is accomplished using Microsoft AD GPOs. The GPO maps the end-user's "My Documents" folder to a DFS global name space. Micrsoft DFS replication is used here.

Since continuous access to desktops is a critical need for the business process function, this design incorporates high availability features along with backup and restore for all the critical VMs and master images.

Along with the single namespace configuration, each site is also configured to support users in other site in case of a fail over. The load balancer is configured to route the incoming connections to the closest site, but if the site fails, it routes all the connections to the head quarters.

For quick fail-back, the management VMs at the remote sites are backed-up at regular intervals to a local backup appliance and also to the headquarters. This will help restore the site quickly in case of a failover.

To ensure image consistency, the master image is maintained at the corporate head quarters and replicated to the remote sites. Changes to the master image are usually kept to a minimum.

The configuration is segregated by the type of VMs to facilitate remote back-up and local backup. The management VMs are typically backed-up for immediate restore, using a local backup appliance. In the validation, EMC's Avamar appliance was used to backup all the management VMs.

In this lab validation, EMC Avamar's Virtual Edition is deployed and managed from Corporate HQ. Avamar provides the ability to do both Guest and Image Level backups. In our implementation we take advantage of doing a guest level backup across HQ and Corporate colocation sites.

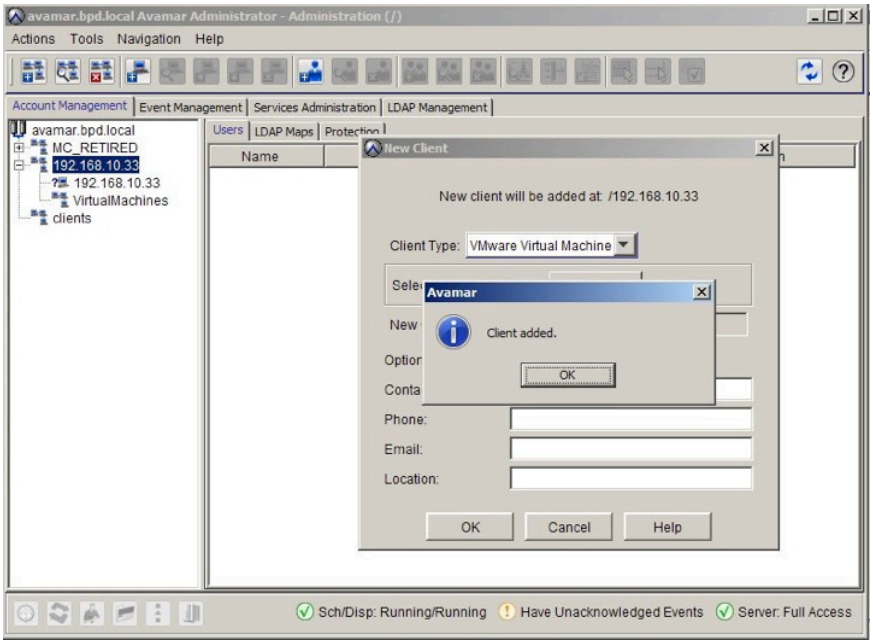

Figure 16: Avamar New Client

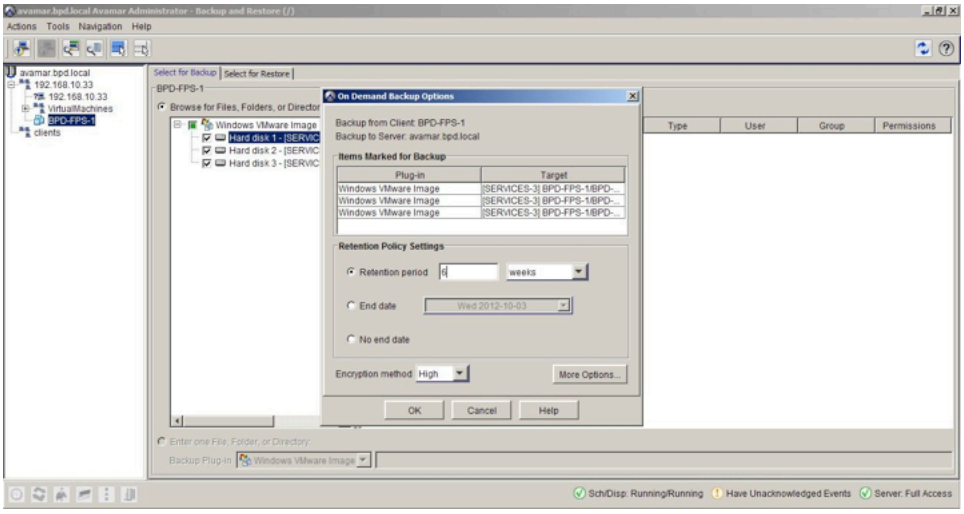

Figure 17: Configure VM level backup including scheduling

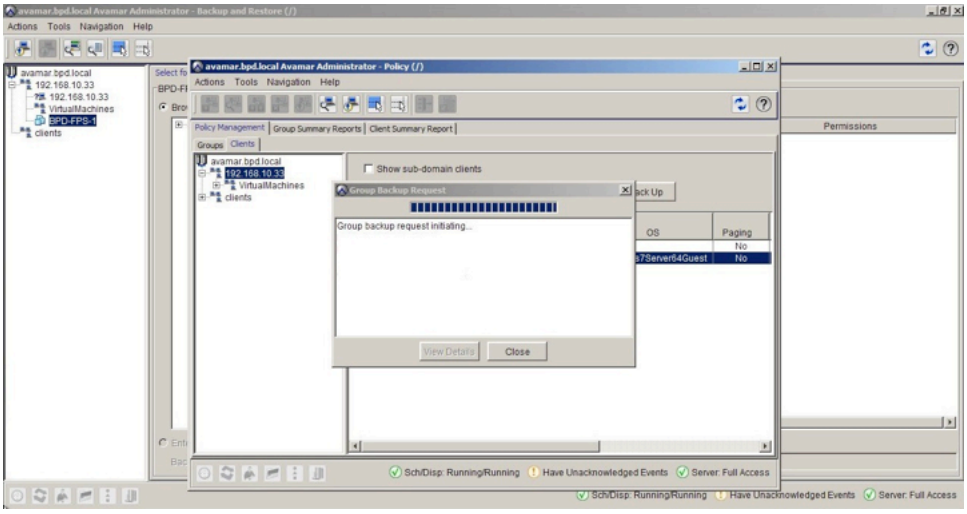

Figure 18: Backup initialized

Installation, configuration, and best practices for EMC Avamar can be referenced from the following guides:

- EMC Avamar Virtual Edition 6.1 Installation Guide
- EMC Avamar Virtual Edition 6.1 Administration Guide
- White paper: Backup and Recovery for VMware Environments with Avamar - A Detailed Review

The user data, located in the NFS datastores, is replicated from the remote sites to the corporate headquarters. This is done to ensure high availability in case of any site failure. The master image is usually replicated from the corporate headquarters to the remote sites to ensure image consistency.

The user data, located in the NFS datastores, is replicated from the remote sites to the corporate headquarters. This is done to ensure high availability in case of any site failure. The master image is usually replicated from the corporate headquarters to the remote sites to ensure image consistency.

DFS Replication Between Sites

Distributed File System (DFS) is a set of client and server services that allows an organization using Microsoft Windows servers to organize many distributed SMB file shares into a distributed file system. DFS provides location transparency and redundancy to improve data availability in the face of failure or heavy load by allowing shares in multiple different locations to be logically grouped under one folder or DFS root.

DFS has two major logical components. First, DFS namespaces provide an abstraction layer for SMB network file shares, allowing one logical network path to be served by multiple physical file servers. Second, DFS supports the replication of data between the servers using DFS Replication (DFSR). For this solution design, a domain- based DFS namespace was used to store user data and DFSR was used to cross-site replicate the files to ensure user access during a site outage.

A domain-based DFS namespace stores the DFS configuration within Active Directory. The DFS namespace root is accessible at \\domainname\<dfsroot> or \\fq.domain.name\<dfsroot>. The namespace roots do not have to reside on domain controllers, they can reside on member servers. If domain controllers are not used

as the namespace root servers, then multiple member servers should be used to provide full fault tolerance. DFS Replication from Microsoft is an efficient, multiple-master replication tool that you can use to keep folders synchronized between servers across limited bandwidth network connections. It replaces the File Replication Service (FRS) as the replication engine for DFS Namespaces, as well as for replicating the Active Directory Domain Services (AD DS) SYSVOL folder in domains. The configuration below shows the mapping for View Persona share in DFS.

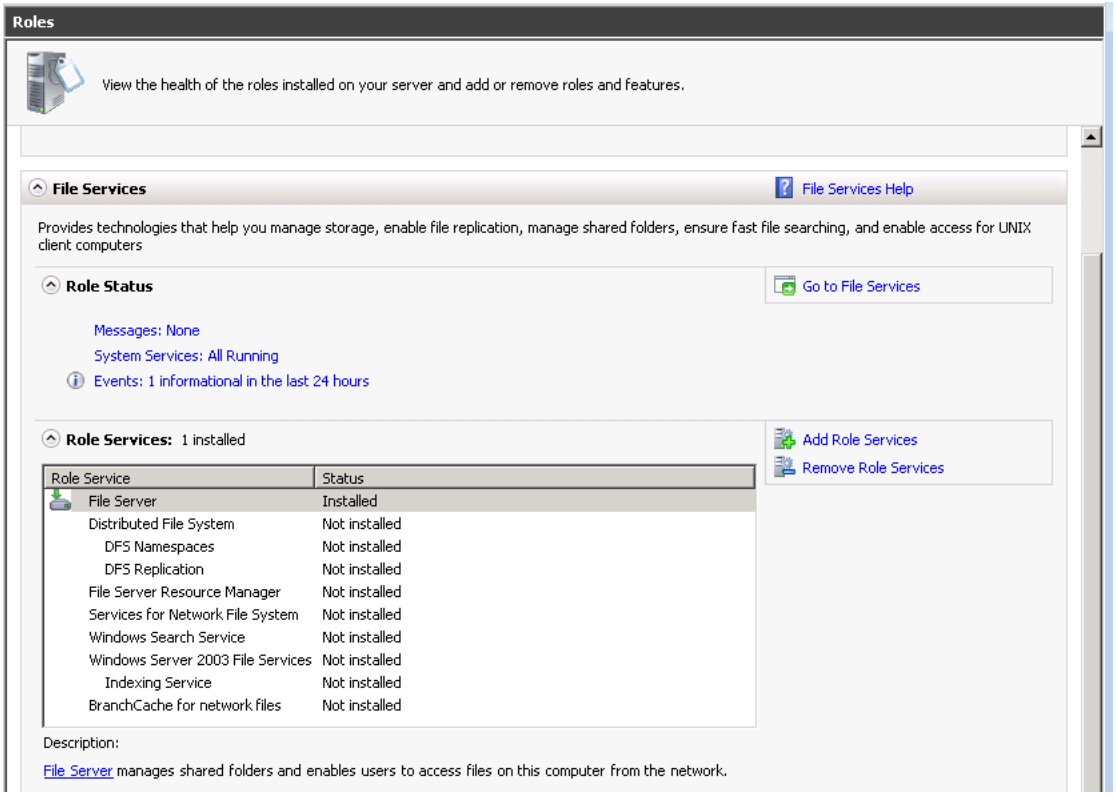

Figure 19: Setting up DFS in Windows 2008 Server

After selecting the role services for DFS replication and DFS namespace, in the Business Process Desktop scenario, you can map the DFS namespace to something like \\bpd.local\bpdcorpdata to replicate user files. from the colocation datacenters.

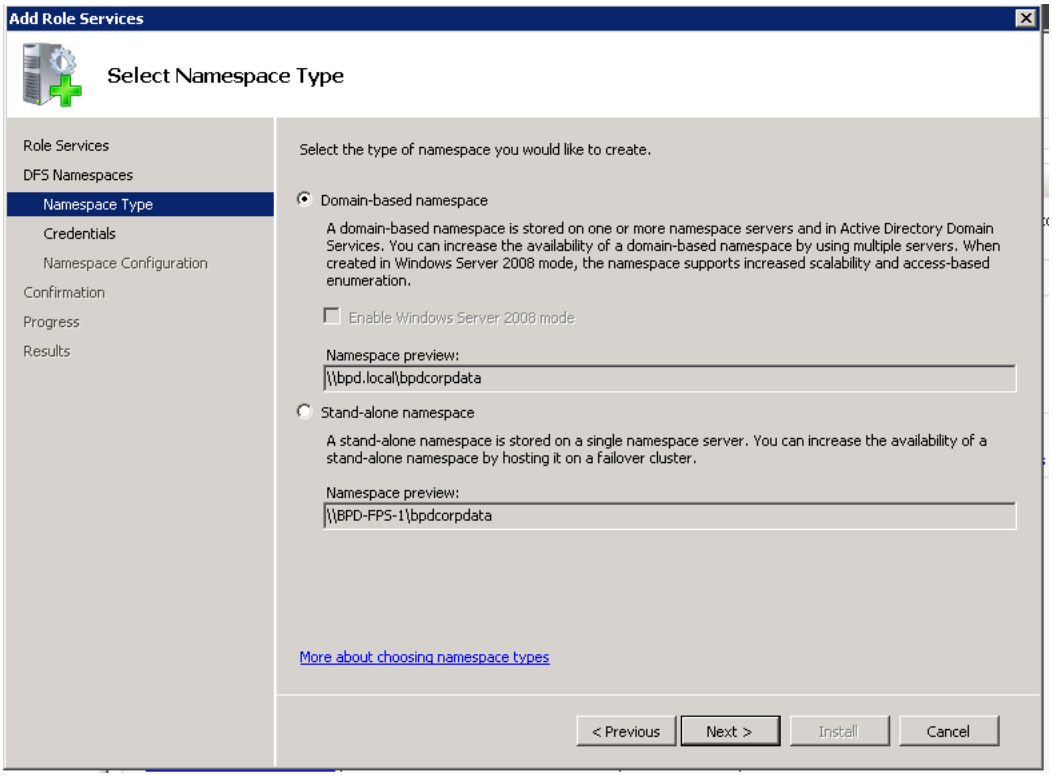

Figure 20: File Share Mapping in DFS Configuration

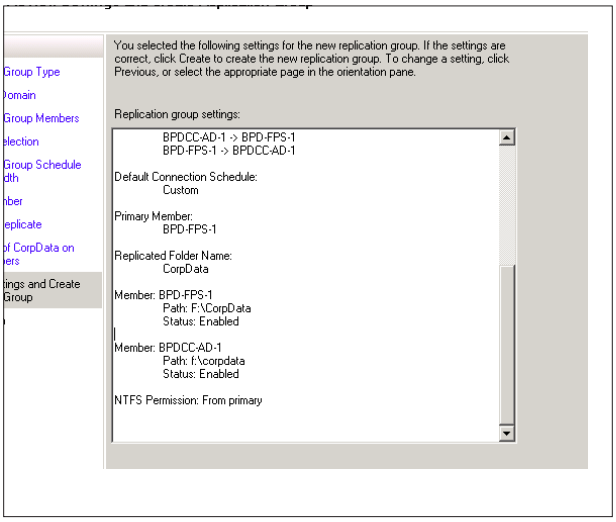

Figure 21: Figure X: Lab DFS Configuration

For more information on the Microsoft DFS, please reference to http://technet.microsoft.com/en-us/library/cc771058.aspx

Networking

vSphere Distributed Switch (vDS) was used in the solution validation to simplify the configuration of various sites. vLANs were used to segregate management, virtual desktop and UC traffic. All uplink ports were configured as VTP trunk ports into the vSphere hosts and the networking was then broken out at the virtual distributed switch level.

User Access

In the business outsourcing scenario, the significant risk posed by the need to share proprietary and confidential information across widely geographically dispersed third parties. it is even more critical than ever to route the users to their designated workspace. In this design, the user experience is enhanced by collocating the View infrastructure geographically local to the users, and by providing high availability, single namespace access and WAN acceleration (optionally) to enhance TCP traffic between sites.

This Business Process Desktop logical diagram shows how each software component was deployed on each host within a site. All sites contain a full View infrastructure to cater to the users local to that site. The infrastructure is replicated across all the sites. Depending on the size and the needs of an organization, existing AD the significant risk posed by the need to share proprietary and confidential information across widely geographically dispersed third parties nfrastructure is used or a new (child) AD is created.

For the corporate owned colocation center and the 3rd party center, in addition to the standard host configuration, the site also includes a back-up VM and optionally, a WAN accelerator for the TCP traffic

In all the sites, the infrastructure components are configured in the Management cluster and the virtual desktops are in the Virtual Desktop cluster.

For the validation, a separate AD and DNS infrastructure was created for all the sites. The management cluster in all the sites includes two AD VMs for redundancy, a virtual center server with SQL VM and a RADIUS server for authentication.

The cluster also includes standard View components like View Connection Manager, View Security Server and a stand alone View Composer.

Monitoring

VMware vCenter Operations Manager (vCOps) for View extends the trusted analytical capabilities of the vCenter Operations Manager product family to the View desktop environment. vCOps for View focuses on the virtual desktop end-users' experience, providing monitoring and management of performance metrics critical to superior View user performance. vCOps for View monitors the View desktop, as well as all of the supporting elements of the virtual infrastructure, from a "View-specific" customized console.

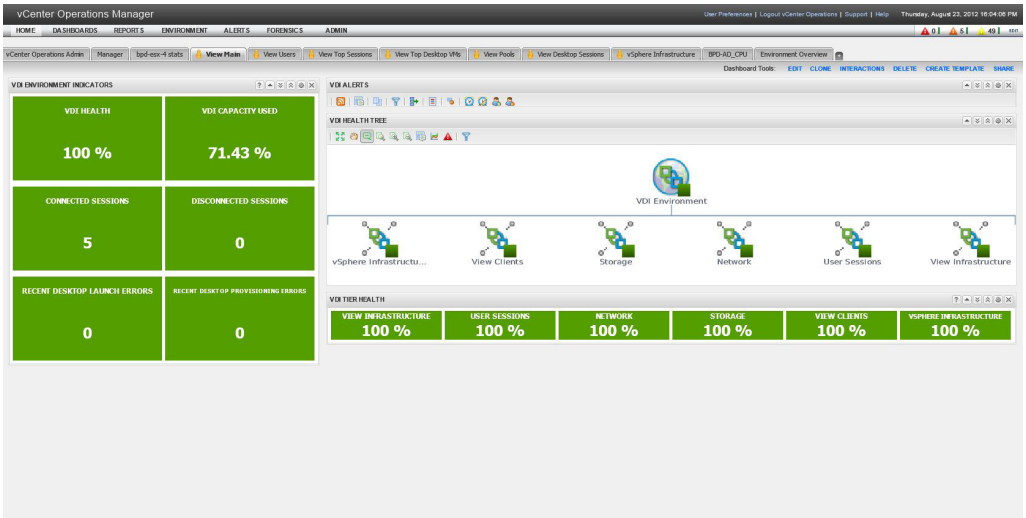

Figure 22: vCOps for View Dashboard – VDI Health

vCOps for View is deployed in the Corporate headquarters and is used to monitor all the remote sites. This provides a single dashboard for monitoring the entire infrastructure for the organization. You can use vCOps to monitor multiple VMware View infrastructure and datacenter located in the distributed location by configuring the analyzer at the HQ and the collectors at any site where you can gather analytics.

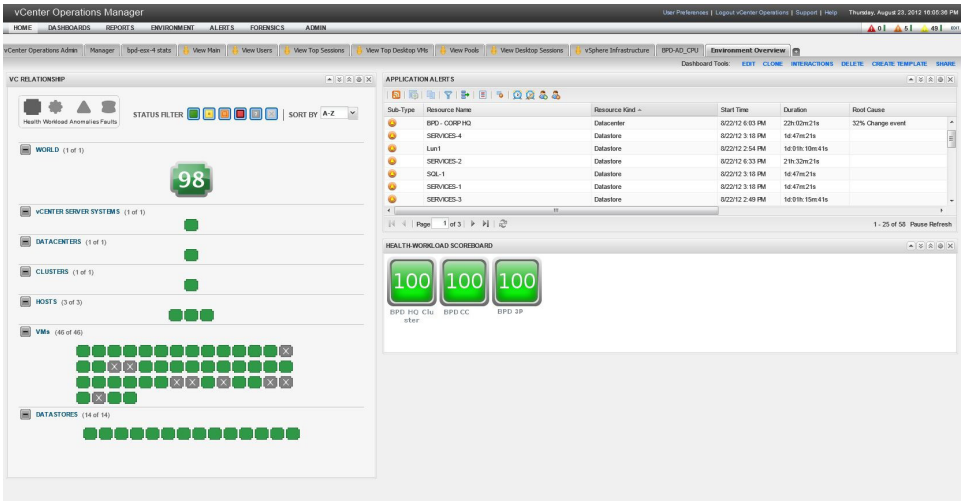

Figure 23: vCOps Dashboard Environment Overall Health

Summary

In a recent KPMG International Firms' Shared Services and Outsourcing Advisor, top drivers for global business service improvement efforts were cited as: reducing operating costs, supporting business growth/expansion agendas, and improving global delivery and operating models.

The VMware Business Process Desktop solution architecture provides businesses across the globe with a cost-effective blueprint to support offshore and outsourced employees that improves user access, centralizes desktop management, enhances data security, and maximizes employee uptime.

The cornerstone of the View Business Process Desktop solution, VMware View modernizes desktops and applications by moving them to the cloud and delivering them as a managed service. With View, IT has the ability to grant or deny access to desktops, data, and applications according to endpoint device configuration, network location, and user identity. View with Persona Management further makes it possible for end users to work from virtually any location using any qualified device to access their personal desktops.

By leveraging stateful desktops with Persona Management, IT can ensure end users can carry their persona with them across sessions and devices for a more personalized desktop. End user access via RADIUS two-factor authentication is secured via the VMware View security server or SSL. vShield products, together with VMware View and leading security vendor solutions, allow IT to offload AV and provide high levels of isolation between resource pools and networks. This allows IT to apply policies across virtual machines and pools of users. And IT organizations can streamline and automate desktop management with VMware vCenter Operations Manager. This architecture further ensures that organizations can quickly recover and restore data across sites to ensure 24/7/365 uptime and desktop availability.

Appendix A: Performance Validation Methodology

In order to emulate a WAN environment, we deployed an appliance to bridge our View client and View desktop networks. VMware selected an industry standard appliance in order to simulate the T1 (1.544Mbps/100ms) and T3 (44.736Mbps/60ms) connections to the corporate colocation site for our geographically remote users.

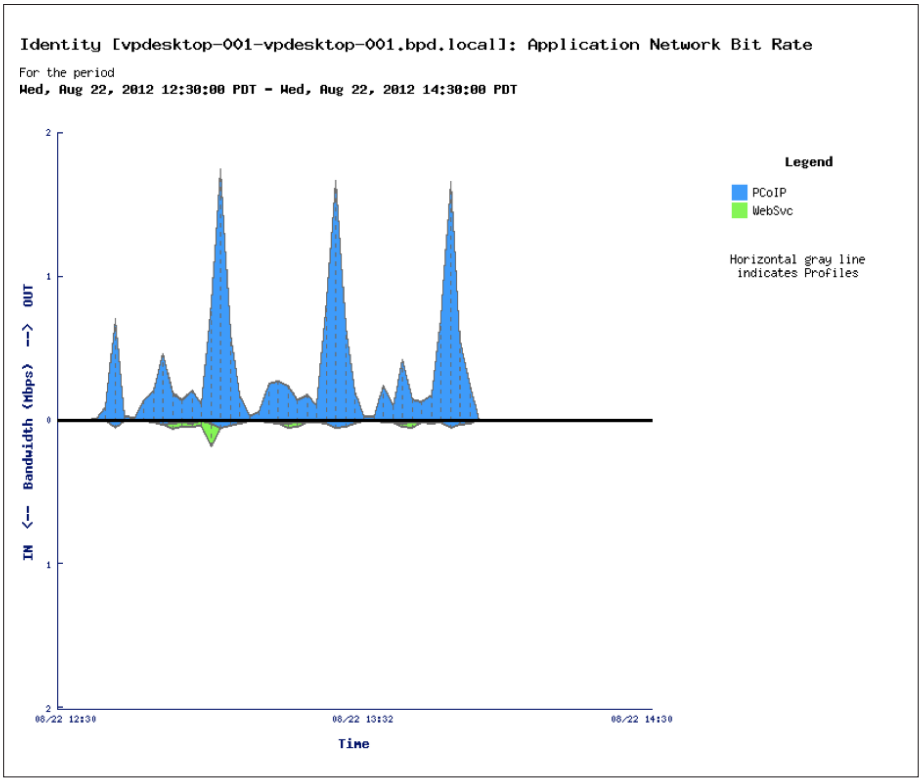

Figure 24: PCoIP Untuned Profile in LAN (Source: Xangati)

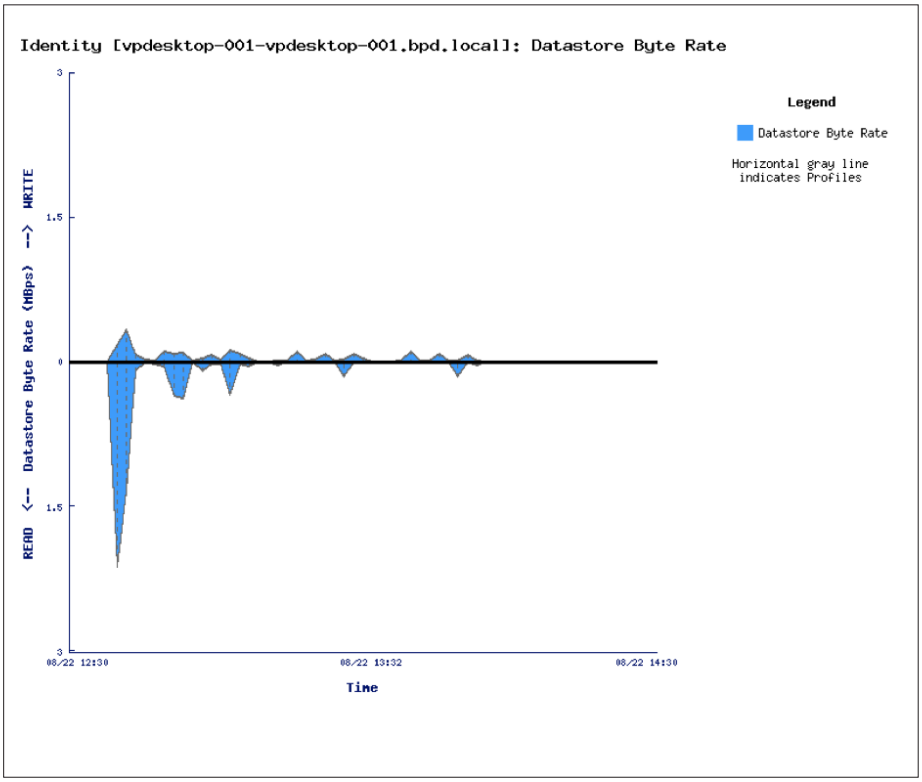

Figure 25: Datastore Byte Rate (Source: Xangati)

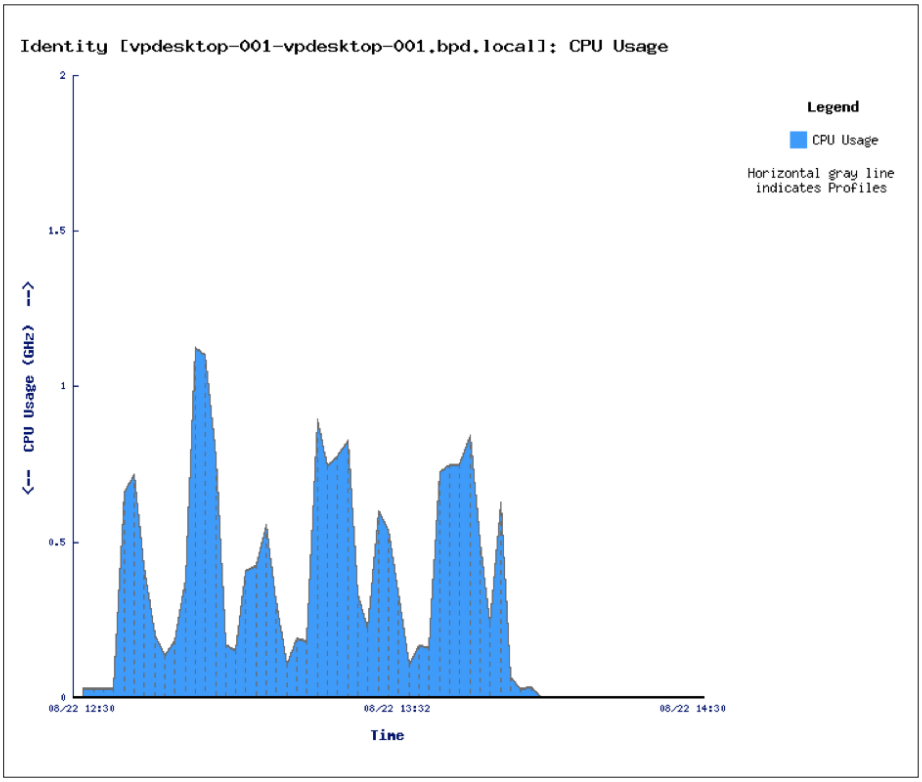

Figure 26: CPU Usage (Source: Xangati)

Using VMware's View Planner tool, we generated a standard three-iteration workload which generates a 1:1 connection from the clients to the desktop virtual machines, with VMware PCoIP as the display protocol.

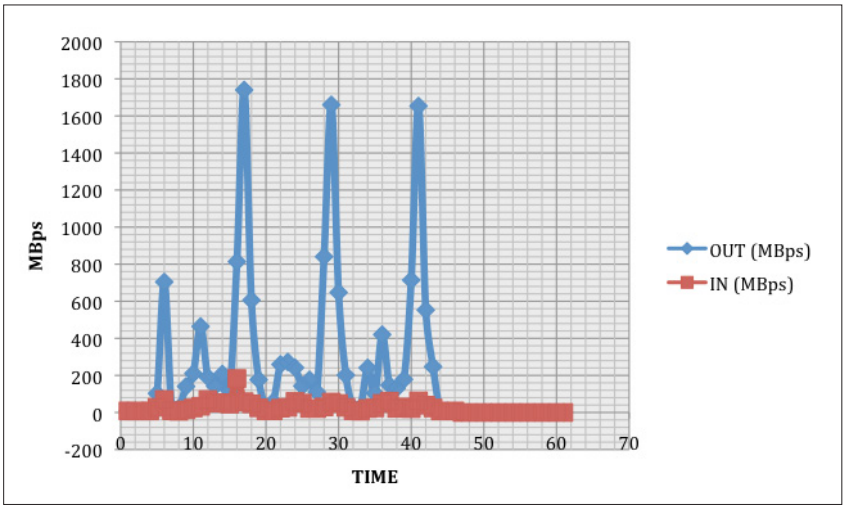

Figure 27: Bandwidth Utilization in LAN

To collect performance data, we ran three discrete tests with an identical workload.

- LAN based scenario using an untuned PCoIP image
- T3 scenario using a lightly tuned PCoIP policy
- T1 scenario using a bandwidth limited policy.

Performance data was then collected to show network bandwidth utilization over the emulated links for each test case to demonstrate the dynamic behavior of VMware PCoIP on the WAN.

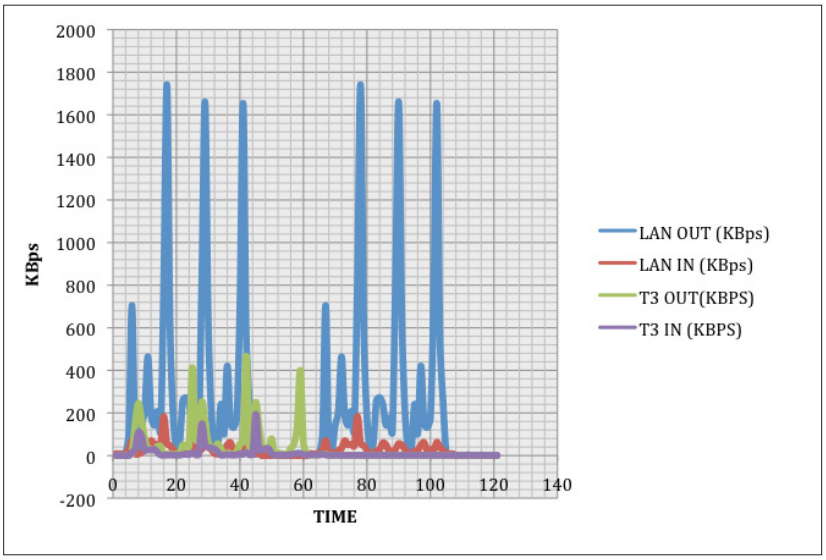

Figure 28: The Composite LAN vs. T3 PCoIP Bandwidth Diagram, XLS, and Xangati Traces from the T3 Run

You can see with only BTL switched off and limit frame rate set to 30fps, bandwidth utilization is ~60% less running the same workload.

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