

# GovConnection<sup>®</sup>

## US Army Thin Client/Client Computing Whitepaper



## Terms and Notices

The assessments, findings, recommendations, and other materials presented herein are provided for the exclusive benefit of the customer. The information was gathered via various 3<sup>rd</sup> party software and hardware tools developed by manufacturers and not created by PC Connection, Inc. or any of its subsidiaries. Such tools are not guaranteed to be free from error, nor are they guaranteed to provide 100% complete information about the customer's environment. The information in this document may also have been gathered via manual data collection processes, interviews, workshops, questionnaires, and other interactions between PC Connection, Inc. and the customer, customer staff, and customer equipment. Such interactions are not guaranteed to produce 100% reliable or accurate information. PC Connection, Inc. has provided the information herein as it was collected (including any possible inaccuracies that were not evident during the data collection process), has analyzed the information, and has provided suggestions for remedy of any problems or issues discovered based on the information available. These suggestions or "recommendations" for action represent the opinions in good faith and on the best research and analysis available to PC Connection, Inc. at the time of writing, and are not to be interpreted as representing the opinions or advice of any 3<sup>rd</sup> party hardware or software manufacturer that may be referenced herein. The assessments, findings, and recommendations do not constitute a Warranty of any kind; warranty coverage, if any, will be stated in a limited warranty set forth in the agreement under which this Assessment was created.

## Document Credits

This document is presented to Army Contracting Command on June 24, 2016 as a solution design document and a deliverable product of a professional services engagement: SOW # 327215.

Army Contracting Command  
David Gannon  
Contracting  
Rock Island Arsenal  
Rock Island, IL 61299  
David.A.Gannon.civ@mail.mil  
(309) 782-0868

By: GovConnection

Author: Kathy Orben-Hall  
Converged Datacenter System Engineer  
korben@pccpro.com

Author: Steve Stiefel  
Converged Datacenter System Engineer  
sstiefel@pccpro.com

Author: Gary Hicks  
Converged Datacenter Practice Manager  
ghicks@pccpro.com

Contributor: Tony D'Ancona  
PC Connection VP Services  
tdancona@pccpro.com

Contributor: Kurt Hildebrand  
Converged Datacenter Practice Director  
khildebrand@pccpro.com

Sales: Jeff Trent  
GovConnection Sr. Director of Federal Sales  
jtrent@govconnection.com

Thank you.

Thank you for choosing GovConnection, Inc. ("GovConnection"), a PC Connection Company, as your consulting services partner. We utilize best practice methods and data-driven analysis combined with a commitment to understanding our customers' needs to set our professional services apart from the competition.

PC Connection, Inc. is a Fortune 1000 Company with more than 30 years of experience providing innovative technology solutions backed by exceptional customer service. Our team of Account Managers and technical experts can help your organization realize greater performance, efficiency, and savings with end-to-end IT solutions across the following information technology areas:

- Server Consolidation and Management
- Data Storage and Protection
- Network Integration and Management
- Server and Network Virtualization
- Software Installs/ Migrations/ Upgrades
- Lifecycle Management Services
- Multi-Site Rollout Services
- Asset Disposition Services

Our mission is to serve as a one-stop source for all of your technology needs. Whether your project involves imaging and asset tagging, implementing a new virtual environment, or anything in between, we have the resources and the expertise to meet your needs and exceed your expectations.

Once again, thank you for choosing GovConnection, Inc. We looking forward to helping you achieve your IT goals. Please feel free to contact your support team if you have any questions, comments, or feedback about any of the information in this document.

Sincerely,  
The GovConnection Team

Contents

Terms and Notices..... 2

Document Credits..... 2

Thank you..... 3

Section 1: Executive Summary..... 7

1.1. Project Overview..... 7

1.2. Project Goals ..... 7

1.3. Solution Summary..... 8

Section 2: Virtual Desktop Design Methodology..... 9

Section 3: Design Concepts..... 11

3.1. Thin Clients ..... 11

3.1.1. Thin Client Definition..... 11

3.1.2. Thin Client Advantages and Disadvantages ..... 11

3.1.3. Types of Thin Clients ..... 11

3.1.4. Choosing the Right Thin Client for your Needs..... 12

3.1.4.1. Important Considerations and Options..... 12

3.1.4.2. Major Manufacturers ..... 12

3.1.4.3. Form Factors ..... 12

3.1.5. Thin Client Types..... 13

3.1.5.1. Microsoft Windows Embedded ..... 13

3.1.5.2. Linux Thin Clients ..... 14

3.1.5.3. Flexible Thin Clients..... 15

3.1.5.4. Zero Clients..... 16

3.1.6. Thin Client Management ..... 17

3.1.6.1. Major Vendors..... 17

3.1.6.2. Typical Management Functions..... 17

3.2. VMware Horizon 7 ..... 18

3.2.1. VMware Horizon 7 Benefits and Features ..... 18

---

3.2.2.	VMware View Connection Server/Security Server/Access Point.....	20
3.2.3.	The VMware Horizon Client.....	21
3.2.4.	VMware View Administrator.....	21
3.2.5.	VMware vCenter Server.....	22
3.2.6.	VMware App Volumes.....	22
3.2.6.1.	VMware App Volumes Components.....	23
3.2.6.2.	How VMware AppStack and Writeable Volumes Work.....	24
3.2.6.3.	Other App Volume Features.....	25
3.2.7.	User Environment Manager.....	26
3.2.8.	Identity Manager.....	27
3.2.9.	Transport Protocol.....	28
3.2.9.1.	Remote Desktop Protocol (RDP).....	28
3.2.9.2.	PCoIP.....	29
3.2.9.3.	VMware Blast Extreme.....	30
3.2.10.	VMware vRealize Operations for Horizon 7.....	30
3.2.10.1.	Key Benefits.....	31
3.2.10.2.	Key Troubleshooting Benefits.....	31
3.2.11.	VMware Virtual SAN.....	32
3.2.12.	Security Design Considerations.....	33
3.3.	HP Device Manager.....	34
3.3.1.	VMware Horizon View Topology.....	36
Section 4: Thin Client Solution for 500 Seats and Below.....		37
4.1.	Solution Design Recommendation.....	37
4.2.	Bill of Materials (500 seats and below).....	38
4.3.	Major Component Details.....	39
4.4.	Proposed Solution Architecture.....	40
4.4.1.	Management and Desktop Clusters (POD).....	40
4.5.	Description of Costs and Project Timeline.....	41
Section 5: Thin Client Solution for 500 Seats and Above.....		42

---

---

5.1.	Solution Design Recommendation.....	42
5.2.	Bill of Materials (500 seats and above) .....	43
5.3.	Major Component Details.....	45
5.4.	Proposed Solution Architecture – AlwaysOn.....	46
5.4.1.	AlwaysOn Architecture .....	46
5.4.2.	Virtual Desktop.....	47
5.4.3.	RDSH Published Applications .....	48
5.5.	Description of Costs and Project Timeline.....	48
Section 6:	Attachments and References .....	50
6.1.	Acceptance Criteria/Virtual Desktop Profile.....	50
6.2.	VDI Assessment Data Gathering Example Questionnaire.....	50
	Document Control.....	53

## Section 1: Executive Summary

### 1.1. Project Overview

This whitepaper document is intended to provide a strong survey of current design considerations for US Army and other US Government clients considering a transition from traditional desktop computing to virtual desktop computing including thin client technologies. In addition, this whitepaper makes specific sample recommendations for Government clients with fewer than 500 seats as well as those with greater than 500 seats.

GovConnection's approach is always to customize virtual desktop solutions based on each client's specific needs to produce the infrastructure most suited to those needs. Thus, the intent of this document is to serve as a general example of each environment that will hopefully prove to be foundational to specific client requests.

Section 2 reviews the methodology that GovConnection employs to design and deliver a successful virtual desktop solution.

Section 3 details the key design concepts of a virtual desktop solution and surveys the design considerations for choosing appropriate thin clients. It also provides operational details for the recommended desktop virtualization platform: VMware Horizon View 7 and explains many of the key virtualization concepts integral to Horizon View 7.

Section 4 defines the recommended sample solution for clients with fewer than 500 seats.

Section 5 defines the recommended sample solution for clients with greater than 500 seats.

Section 6 documents the acceptance criteria and virtual desktop profile choices associated with the recommended sample solutions.

### 1.2. Project Goals

The goals of this project are to educate the reader on the many design choices and concepts associated with virtualized desktop environments including thin client technologies; to explain the process and methodology for moving to a virtualized desktop environment; and to illustrate typical virtualized desktop environments by way of examples.

### 1.3. Solution Summary

**Under 500 seats:**

The 500 seats or fewer solution consists of the following major components:

- (3) HP DL360 Gen9 Management Servers
- (6) HP DL360 Gen9 VMware Horizon View Servers
- (500) HP t620 Flexible Series Thin Clients
- VMware Horizon 7 Enterprise

**Over 500 seats:**

The 500 seats or greater solution consists of the following major components:

- (6) HP DL360 Gen9 Management Servers
- (20) HP DL360 Gen9 VMware Horizon View Servers
- (1000) HP t620 Plus Flexible Series Thin Clients
- VMware Horizon 7 Enterprise

Both solutions are largely built on the same server building block: HP's DL 360 Gen9 servers for both management servers and VMware Horizon View servers. The over 500 seat configuration incorporates VMware's AlwaysOn architecture which sets up two parallel highly-available instances that can each service end users. End user/thin clients may connect to either infrastructure at any particular time. From the user's point of view, the experience with either infrastructure is completely transparent.

As a result, the management and VMware Horizon View server counts are larger than in the under 500 seat scenario not just because the seat count is higher but also because of the need to build out parallel infrastructures.

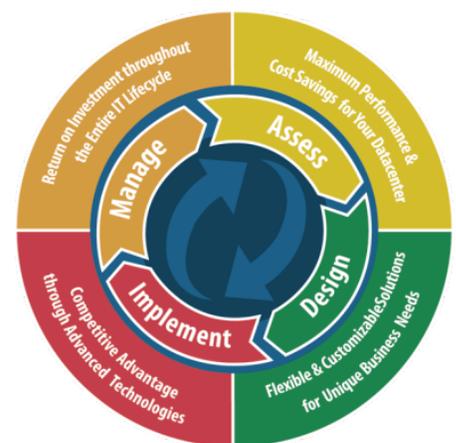
The other difference between the two scenarios is that the under 500 seat configuration is comprised of HP t620 thin clients while the over 500 seat configuration employs HP t620 Plus thin clients. The primary difference between thin client models is that the Plus thin clients can support Quad Graphics.

## Section 2: Virtual Desktop Design Methodology

When GovConnection began actively working on Virtual Desktop Infrastructure (VDI) initiatives with our customers, it became clear that VDI can be designed and implemented in any number of ways and that some of those ways led to successful adoption and others did not. We combined our experience with manufacturer best practices to develop the following VDI methodology. We based our methodology on the industry best-practice ADIM (Assess, Design, Implement, and Manage) model used prevalently throughout our services organization.

Each phase of the ADIM model leads logically into the next and adherence to the model results in well-managed, efficient and productive IT solutions.

Our Service Practice teams also focus on delivering best-practice results and identifying emerging solution offerings. This allows our customers to consistently benefit as new technologies mature into mainstream adoption.



### Assessment

The key to knowing where you are going is first knowing where you are. In the Assessment phase, we will assess the physical infrastructure to collect metric data on how the current environment is performing. This lets us understand your starting point. Next, we work with you to understand where you want to go. These requirements become the Critical Success Criteria that we use to design a successful proof of concept (POC). With those requirements defined, we can then track towards measurable outcomes at the end of the POC. This helps you understand whether all the functionality you require will be available in a Virtual Desktop Infrastructure and whether it makes sense to continue your VDI journey.

### Design

Once you have defined your current state and planned your future state, it's time to develop a well-formed design to accomplish that transition. We'll take the data gathered in the assessment and POC and use it to scope a pilot environment. We'll virtualize a test group of users and measure their experience in the pilot VDI environment. This will essentially confirm the requirements needed for your production environment and further validate how this technology will function in your unique environment.

**Implementation**

In the Implementation phase, we will build out your production environment, customize additional product functionality, and roll out the environment to user groups. This is also where you will develop strategies on how to manage the environment moving forward with regards to: backup, persona management, application management, client management, anti-virus, and graphic acceleration. Regular use of monitoring tools will greatly affect your success since you will be able to identify performance issues as you grow and remediate.

**Maintain**

Maintaining involves more than just moves, adds, and changes. In this phase, you need to acquire and maintain training, implement advanced functionality, and update the software as new minor and major releases occur. Regularly performed health checks are a key ingredient to ensure that your environment is configured consistently to best practices as you grow and expand it. You will also be actively engaged in managing the backup strategy developed during the implementation phase.

## Section 3: Design Concepts

### 3.1. Thin Clients

#### 3.1.1. Thin Client Definition

A thin client is a lightweight stateless computer with no hard drives or fans. It is purposely built to display a remote desktop session running on a remote server. All data processing which typically takes place locally on a desktop PC, including applications, memory, storage ,etc., are located safely back in the data center. If a thin client is damaged or stolen no data is at risk.

#### 3.1.2. Thin Client Advantages and Disadvantages

##### **Advantages of Thin Clients**

- Centralized management
- Enhanced security
- Cost Saving over a desktop
- Power savings over a desktop
- Enhanced reliability, no moving parts

##### **Disadvantages of Thin Clients**

- Needs to connect to a remote server to access data
- Requires management
- No local storage for most thin clients

#### 3.1.3. Types of Thin Clients

##### **Types of Clients**

- Windows Embedded
- Linux based
- Flexible Thin Clients
- Zero Clients

### 3.1.4. Choosing the Right Thin Client for your Needs

#### 3.1.4.1. Important Considerations and Options

Below is a guide to help design the ideal thin client model for your environment. Knowing exactly what you require will help you avoid purchasing a thin client that is not suited for its intended job.

- RAM memory to run programs
- Flash storage to hold OS and data
- Networking-(Ethernet/Wi-Fi)
- Number of displays required
- Expandability (the ability to add additional display adapters, network cards, etc.)
- OS Type (Windows, Linux, Zero)
- Manageability
- Security (CAC)
- Flexibility
- VDI Brokers supported

#### 3.1.4.2. Major Manufacturers

- Dell\Wyse
- HP
- Samsung

#### 3.1.4.3. Form Factors

- Desktop (requires connection a monitor)
- All in One (one piece includes thin client and monitor)

### 3.1.5. Thin Client Types

#### 3.1.5.1. Microsoft Windows Embedded

Windows Embedded thin clients run a light version of Windows and are considered the fattest of the thin clients because of the size of the embedded Windows operating system.

**Use Case:** Windows embedded thin clients are a good choice when the most user flexibility is desired. Windows embedded thin clients have the ability to log into multiple remote sessions such as VMware View, Citrix, or RDSH (Terminal Server). They can also run Windows applications and web-based applications from the thin client itself.

#### **Pros**

- Most flexible of the thin clients
- Can run certain Windows applications and multiple broker clients simultaneously
- Browser support allows access to the internet and web-based applications
- Wireless enabled
- Manageability through vendor tools

#### **Cons**

- Large software footprint
- May need occasional patching and updating
- Not as secure as zero clients
- More expensive than a zero client
- Software based PCoIP

### 3.1.5.2. Linux Thin Clients

Linux thin clients are based on a hardened modified Linux kernel which is smaller in size and presents a smaller attack surface compared to Windows embedded OS.

**Use Case:** Use this operating system when a more secure user environment is required. It can run multiple connection brokers and web based applications as well.

#### **Pros**

- Smaller software footprint than Windows embedded thin clients
- Can run multiple broker clients simultaneously
- A built-in browser allows access to internet and web-based applications on the thin client
- More secure than Windows embedded thin clients and with a smaller attack profile
- Wireless enabled
- Manageability through vendor tools

#### **Cons**

- Not as flexible as Windows embedded thin client
- Usually contains a proprietary Linux kernel making modifications difficult
- Still requires updating and still has an attack profile
- Software based PCoIP
- Device drivers not as available

### 3.1.5.3. Flexible Thin Clients

Flexible thin clients are the chameleons of the thin client landscape as they can change their identity and job role simply by changing their software. A flexible thin client can be a Windows embedded, Linux, or even software based zero client. The advantage to flexible thin clients is that they can adapt and change as your environment and your needs evolve. There is no need to purchase new hardware.

**Use case:** As implied, they are flexible and easily adapt to new requirements. Flexible thin clients are a good choice if you want to have different brokers and requirements for different sets of users but yet still maintain a single hardware platform.

#### **Pros**

- Flexible configuration (Windows, Linux, Smart Zero)
- Wireless enabled (excludes zero clients)
- Not dedicated to a single configuration
- Manageability through vendor tools
- Can change settings/profile to enhance performance based on transport protocol

#### **Cons**

- PCoIP is software based rather than hardware
- Not a secure hardware-based zero client

### 3.1.5.4. Zero Clients

Zero clients have the smallest operating system of all the thin clients.

**Use Case:** Zero clients are purpose driven, thus they only work with a specific type of connection broker. They are very easy to replace and upgrade as there is no user data held on the client.

#### **Pros**

- Software is ROM-based and not easily compromised
- Require minimal or no configuration
- Do not require software patching and updating like Windows thin clients
- Hardware based PCoIP
- Smallest physical footprint

#### **Cons**

- Single broker - you must purchase the correct model for your environment
- Zero clients cannot be repurposed for different VDI brokers
- No hardware expandability
- Not wireless enabled
- Limited Manageability through vendor tools (usually limited to just firmware and configuration)

### 3.1.6. Thin Client Management

#### 3.1.6.1. Major Vendors

##### **Major Vendors**

- HP Device Manager
- Dell/Wyse Device Manager
- Teradici console

Each manufacturer has a management platform for their thin clients. As most features are hardware or agent based they cannot manage another vendor's thin clients. The Teradici Console can manage all hardware-based Teradici PCoIP chipset clients regardless of the vendor.

#### 3.1.6.2. Typical Management Functions

##### **Typical management functions include (but vary depending on the thin client OS):**

- Asset and inventory management
- Thin client settings and connection cloning
- Software updates
- Patch and client updates
- Remote control
- Remote power management
- Inventory, firmware updating, and configuration changes

## 3.2. VMware Horizon 7

VMware Horizon 7 is an application and desktop delivery solution that provides end users with access to all of their virtual desktops, applications, and online services through a single digital workspace.

### 3.2.1. VMware Horizon 7 Benefits and Features

- When you manage enterprise desktops with Horizon 7, the benefits include increased reliability, security, hardware independence, and convenience
- Desktops and applications can be centralized by integrating with VMware vSphere® and virtualizing server, storage, and networking resources. Placing desktop operating systems and applications on a server in the datacenter provides the following advantages:
  - Access to data can easily be restricted. Sensitive data can be prevented from being copied onto a remote employee's home computer
  - Integration with Workspace means that end users have on-demand access to remote desktops through the same Web-based application catalog they use to access SaaS, Web, and Windows applications. Inside a remote desktop, users can also use Workspace Catalog to access applications
  - Remote desktops and applications that are hosted in a datacenter experience little or no downtime
  - Virtual machines can reside on high-availability clusters of VMware servers
- Provisioning desktops and applications for end users is a quick process. It does not require installation of applications one by one on each end user's physical PC. End users connect to a remote application or a remote desktop complete with applications. End users can access their same remote desktop or application from various devices at various locations
- Using VMware vSphere to host virtual desktops and RDS host servers provides the following benefits:
  - Administration tasks and management chores are reduced. Administrators can patch and upgrade applications and operating systems without touching a user's physical PC
  - Integration with Workspace means that IT managers can use the Web-based Workspace administration interface to monitor user and group entitlements to remote desktops

- 
- With View Persona Management, physical and virtual desktops can be centrally managed, including user profiles, application entitlement, policies, performance, and other settings. Deploy View Persona Management to physical desktop users prior to converting to virtual desktops
  - Features included in Horizon support usability, security, centralized control, and scalability
  - The following features provide a familiar experience for the end user:
    - Use multiple monitors. With PCoIP multiple-monitor support, you can adjust the display resolution and rotation separately for each monitor
    - Access USB devices and other peripherals that are connected to the local device that displays your virtual desktop
    - You can specify which types of USB devices end users are allowed to connect to. For composite devices that contain multiple types of devices, such as a video input device and a storage device, you can split the device so that one device (for example, the video input device) is allowed but the other device (for example, the storage device) is not
    - Use View Persona Management to retain user settings and data between sessions even after the desktop has been refreshed or recomposed. View Persona Management has the ability to replicate user profiles to a remote profile store (CIFS share) at configurable intervals
    - You can also use a standalone version of View Persona Management on physical computers and virtual machines that are not managed by View
  - Horizon offers the following security features, among others:
    - Use of two-factor authentication, such as RSA SecurID or RADIUS (Remote Authentication Dial-In User Service), or smart cards to log in
    - Use pre-created Active Directory accounts when provisioning remote desktops and applications in environments that have read-only access policies for Active Directory
    - Use SSL tunneling to ensure that all connections are completely encrypted
    - Use VMware High Availability to ensure automatic failover
    - Smart Policies with Streamlined Access
      - Improve end user satisfaction by simplifying authentication across all desktop and application services while improving security with smarter, contextual, role-based policies that tie to the user, device or location.
  - Scalability features depend on the VMware virtualization platform to manage both desktops and servers:
-

- 
- Use View Composer to quickly create desktop images that share virtual disks with a master image. Using linked clones in this way conserves disk space and simplifies the management of patches and updates to the operating system
  - The following features provide centralized administration and management:
    - Use Microsoft Active Directory to manage access to remote desktops and applications and to manage policies
    - Use View Persona Management to simplify and streamline migration from physical to virtual desktops
    - Use the Web-based administrative console to manage remote desktops and applications from any location
    - Use App Volume to inject the right app stack for each user group or use case
    - Use View Administrator to distribute and manage applications packaged with VMware ThinApp for Create conflict free applications and allow legacy applications to run on newer operating systems
    - Integrate with Workspace™ so that end users can access remote desktops through the Workspace user portal on the Web, as well as use the Workspace user portal on the Web from inside a remote desktop
    - Integrate with Mirage™ to manage locally installed virtual machine desktops and to deploy and update applications on dedicated full-clone remote desktops without overwriting user-installed applications

### 3.2.2. VMware View Connection Server/Security Server/Access Point

This software service acts as a broker for client connections. View Connection Server authenticates users through Windows Active Directory and directs the request to the appropriate virtual machine, physical PC, or Microsoft RDS host.

- View Connection Server provides the following management capabilities:
  - Authenticating users
  - Entitling users to specific desktops and pools
  - Assigning applications packaged with VMware ThinApp to specific desktops and pools
  - Managing remote desktop and application sessions
  - Establishing secure connections between users and remote desktops and applications
  - Enabling single sign-on

- Setting and applying policies
- Inside the corporate firewall, you install and configure a group of two or more View Connection Server instances. Their configuration data is stored in an embedded LDAP directory and is replicated among members of the group
- Outside the corporate firewall, in the DMZ, you can install and configure View Connection Server as a security server. Security servers in the DMZ communicate with View Connection Servers inside the corporate firewall. Security servers ensure that the only remote desktop and application traffic that can enter the corporate data center is traffic on behalf of a strongly authenticated user. Users can access only the resources that they are authorized to access
- Security servers offer a subset of functionality and are not required to be in an Active Directory domain. You install View Connection Server in a Windows Server 2008, Windows Server 2012, or Windows Server 2012 R2 server, preferably on a VMware virtual machine

### 3.2.3. The VMware Horizon Client

- The client software for accessing remote desktops and applications can run on a tablet, a phone, a Windows, Linux, or Mac PC or laptop, a thin client, and more.
- Features differ according to which Horizon Client you use. This guide focuses on Horizon Client for Windows. The following types of clients are not described in detail in this guide:
  - Details about Horizon Client for tablets, Linux clients, and Mac clients. For more information, see the Horizon Client documentation at [https://www.vmware.com/support/viewclients/doc/viewclients\\_pubs.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html)

### 3.2.4. VMware View Administrator

This web-based application allows administrators to configure View Connection Server, deploy and manage remote desktops and applications, control user authentication, and troubleshoot end user issues.

When you install a View Connection Server instance, the View Administrator application is also installed. This application allows administrators to manage View Connection Server instances from anywhere without having to install an application on their local computer.

---

### 3.2.5. VMware vCenter Server

This service acts as a central administrator for VMware ESXi servers that are connected on a network. vCenter server provides the central point for configuring, provisioning, and managing virtual machines in the datacenter.

- In addition to using these virtual machines as sources for virtual machine desktop pools, you can use virtual machines to host the server components of View including View Connection Server instances, Active Directory servers, Microsoft RDS hosts, and vCenter Server instances
- You can install View Composer on the same server as vCenter Server or on a different server. vCenter Server then manages the assignment of the virtual machines to physical servers and storage and manages the assignment of CPU and memory resources to virtual machines
- You can install vCenter server either as a VMware virtual appliance or install vCenter Server in a Windows Server 2008 R2 server, a Windows Server 2012 server, or a Windows Server 2012 R2 server, preferably on a VMware virtual machine

### 3.2.6. VMware App Volumes

VMware App Volumes is a real-time application management tool for delivering and maintaining applications in virtual desktop environments. App Volumes makes it possible to provision and upgrade applications through virtual disks, without having to package, modify or stream the applications. Optimized to run within VMware vSphere, App Volumes applications can target specific users, groups or devices. Once IT installs an application, an administrator can deliver or upgrade its workload in seconds. IT controls the entire application lifecycle, from installing to updating to replacing the application. From the end user's perspective, the application performs just like one that is natively installed.

- App Volumes applications are stored on read-only virtual disks, with a writeable volume available to each user so that any customized settings and data persist upon virtual desktop logon and logoff. IT admins can set up the disks on any supported vSphere data store, such as VMware Virtual SAN, allowing IT to implement the most appropriate storage for their organization, rather than having to stream the applications across the network

- App Volumes is a good way to deliver applications from a non-persistent state while still persisting user data
- App Volumes then uses virtual machine disks to deliver applications to VMware Horizon virtual desktops, without needing to modify the desktops or the applications. That helps reduce storage requirements, lowering the overall cost of managing virtual desktops. App Volumes provides users with persistent applications on top of non-persistent virtual desktop pools, delivering the applications from one virtual disk to multiple desktops. Administrators can deliver and upgrade the applications in real time and make them immediately available to users, while they're already logged in or at boot up

### 3.2.6.1. VMware App Volumes Components

- There are several components that go into an App Volumes installation. App Volumes, vSphere and Horizon work together to deliver the applications to virtual desktops (Figure 1)

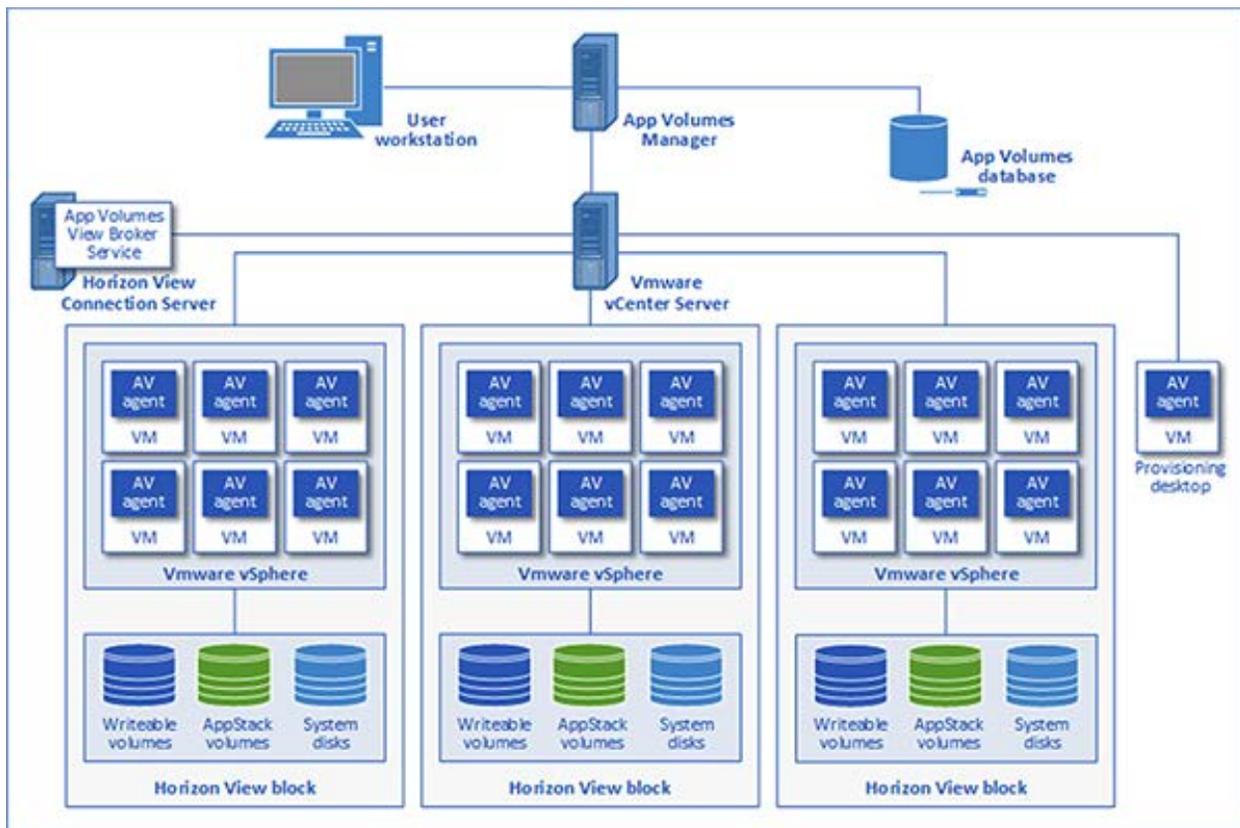


Figure 1. How App Volumes fits into VMware VDI

- The App Volumes Manager server provides a Web-based interface for administering and configuring App Volumes, as well as assigning the read-only virtual disks -- called AppStack volumes -- and the writeable virtual disks -- writeable volumes. App Volumes Manager also serves as a broker for the App Volumes agent that runs within each virtual machine (VM)
- App Volumes uses a SQL Server database to store configuration information for the AppStack and writeable volumes, as well as information about users, physical and virtual machines, data transactions and application access rules
- Another important player in the App Volumes ecosystem is vCenter Server. In addition to managing the vSphere infrastructure, vCenter Server provides App Volumes with operational connectivity to VM, storage and vSphere host resources as well as makes application inventory information available. App Volumes facilitates faster user logins by running the App Volumes View Broker Service on the Horizon View Connection Server
- Finally, App Volumes requires that IT installs its agent on each vSphere VM. The agent runs as a service, handling application calls and file system redirects to the AppStack and writeable volumes. The agent must also run on the target virtual desktop

### 3.2.6.2. How VMware AppStack and Writeable Volumes Work

At the heart of the App Volumes operation are the AppStack volumes, read-only disks containing one or more Windows applications. Each AppStack volume can support multiple systems or users. Administrators can assign volumes to Active Directory user accounts, groups or organizational units, as well as to computer accounts.

- There is a default 20 GB template for AppStack volumes, but administrators can also create customized templates. A customized template can target a specific application deployment scenario and be smaller than 20 GB, allowing it to deploy faster than the default one
- If there is a dependency between applications, they should run on the same AppStack volume. Also, if an application such as antivirus or security software needs to run when users are logged out, it should not run on an AppStack volume, but instead be installed on the base image

- Unlike the AppStack volumes, the writeable volumes provide a way to persist user data. Each one is specific to a user and is used to store customized data such as local profile information, application settings or user-installed applications. IT can only associate a writeable volume with one user at a time, making it possible for the volume to move with the user from one VM to the next. The volume deploys when the user authenticates their login on the virtual desktop
- App Volumes is a good way to deliver applications from a non-persistent state while still persisting user data. According to VMware, App Volumes will also support non-VMware virtual desktop environments, such as Citrix XenDesktop and Microsoft Remote Desktop Session Host. IT shops will have to determine whether the benefits of using App Volumes are enough to offset the licensing fees or whether they even need to introduce this type of application layering

### 3.2.6.3. Other App Volume Features

- **AppToggle** – A new patent pending capability that enables per user entitlement and installation of applications within a single AppStack for maximum flexibility. This helps IT reduce the number of AppStacks that need to be managed, lowers storage capacity and management costs even further, improves performance, and allows applications to share or have different dependencies in a single AppStack. The AppToggle architectural approach of only installing entitled applications also offers greater security as opposed to simply hiding installed applications, which can easily be exploited.
- **AppCapture with AppIsolation** – A new capability that easily captures and updates applications to simplify application packaging, delivery and isolation with a command line interface that enables IT to distribute AppStack creation to different teams and merge AppStacks for simplified delivery and management. With support for AppIsolation, AppCapture also integrates with VMware ThinApp to enable IT to deliver native applications and VMware ThinApp applications in one consistent format through AppStacks.
- **AppScaling with Multizones** – Allows integrated application availability across datacenters so customers no longer need additional software to replicate AppStacks across sites. IT admins can add multiple file shares to host AppStacks and pair them to VMware vCenter™ instances. An import service will then scan the file shares and populate the AppStacks into the data stores of the vCenter instances. This removes the requirement of having a shared data store between vCenter instances to replicate AppStacks.

- **Integrated Application, User Management and Monitoring Architecture** – A new modern architecture for the VMware App Volumes manager component offers the industry's only solution that combines application and user environment management with monitoring. With an architecture streamlined for faster provisioning and context-aware user policy, this offers a flexible and reliable application and lifecycle management solution for the digital workspace.
- **Unified Administration Console** – A single pane of glass across application management, user environment management and monitoring. This next-generation admin view recognizes patterns to create simple, yet powerful workflows for application delivery, user environment management (beta for this release), and desktop and published application environment monitoring. This removes the complexity of managing multiple consoles but still enables customers to use legacy consoles if desired. Out of the box functionality also enables IT admins to address end-user needs quickly and efficiently.

### 3.2.7. User Environment Manager

User Environment Manager simplifies end-user profile management with a single, scalable solution that leverages existing infrastructure.

- Centralized and simplified user environment management
- Simple profile and policy management makes adoption, management and day-to-day operations easy, while enabling compliance
- Easy-to-apply policy follows users across devices and locations and helps accelerate management, migrations and onboarding, including configuration settings for applications, shortcuts, mappings and group policy settings
- Integration with Horizon Cloud Manager eases deployment and reduces management complexity
- Enterprise-grade user management with low up-front investment.
- Scale out services with a single solution that supports virtual, physical and cloud-hosted environments
- Drive down user management costs and leverage existing infrastructure.
- Respond to changing business dynamics with the ability to quickly add and remove profile and personalization services
- Personalized end-user experience. User Environment Manager (UEM) gives end-users a consistent and personalized experience across devices and locations

- Consistent and personalized experience across devices and locations
- Maintain personalized settings across multiple devices, even non-persistent VDI sessions
- Experience auto-mapping printers and networks as you roam between locations
- Enjoy speedy logon times and faster time-to- application, with minimal downtime



Figure 2. User Environment Manager Logical Diagram

### 3.2.8. Identity Manager

VMware Identity Manager™ is identity management for the mobile/cloud era that delivers on consumer grade expectations like one-touch access to apps, optimized with AirWatch Conditional Access and backed by a self-service app catalog with enterprise-class management and security expected from the leader of hybrid cloud infrastructure.

#### Overview of True SSO

True SSO provides a way to authenticate to Microsoft Windows, retaining all of the users' normal domain privileges, without requiring them to provide AD credentials! True SSO is a VMware Horizon technology that integrates VMware Identity Manager 2.6 with Horizon 7. VMware Identity Manager Standard is included in VMware Horizon 7 Advanced and Enterprise Editions.

With True SSO, a user can log into Identity Manager using any non-AD method (for example, RSA SecurID credentials) and once authenticated, the user is able to launch any entitled desktop or app (hosted from any domain) without ever being prompted for a password again!

True SSO uses SAML (Security Assertion Markup Language) to send the User Principal Name (for example, [jdoe@example.com](mailto:jdoe@example.com)) to the identity provider's authentication system to access AD

credentials. Horizon 7 then generates a unique, short-lived certificate for the Windows login process.

### **Benefits of True SSO**

- Separates authentication (validating a user's identity) from access (such as to a specific Windows desktop or application).
- Provides enhanced security. User credentials are secured by a digital certificate. No passwords are vaulted or transferred within the data center.
- Supports a wide range of authentication methods. Selecting or changing authentication protocols has a limited impact on the infrastructure of the enterprise.

### 3.2.9. Transport Protocol

Customers can choose between three transport protocols based on their use cases and client device choices. The transport protocols are:

- Remote Desktop Protocol (RDP)
- PCoIP
- Blast Extreme

#### 3.2.9.1. Remote Desktop Protocol (RDP)

Remote Desktop Protocol is the same multichannel protocol many people already use to access their work computer from their home computer. Microsoft Remote Desktop Connection (RDC) uses RDP to transmit data.

Microsoft RDP is a supported display protocol for remote desktops that use virtual machines, physical machines, or shared session desktops on an RDS host. (Only the PCoIP display protocol is supported for remote applications.) Microsoft RDP provides the following features:

- With RDP 7, you can use multiple monitors in span mode. RDP 7 has true multiple monitor support, for up to 16 monitors

- You can copy and paste text and system objects such as folders and files between the local system and the View desktop
- RDP supports 32-bit color
- RDP Supports 128-bit encryption
- You can use this protocol for making secure, encrypted connections to a Security Server in the corporate DMZ

### 3.2.9.2. PCoIP

PCoIP is a high-performance remote display protocol provided by VMware.

This protocol is available for Horizon desktops that are sourced from virtual machines, Teradici clients, and physical machines that have Teradici-enabled host cards.

PCoIP can compensate for an increase in latency or a reduction in bandwidth, to ensure that end users can remain productive regardless of network conditions. PCoIP is optimized for delivery of images, audio, and video content for a wide range of users on the LAN or across the WAN.

PCoIP provides the following features:

- You can use 3D applications such as Windows Aero themes or Google Earth, with screen resolution up to 1920 x 1200. With this no hardware accelerated graphics feature, you can run DirectX 9 and OpenGL 2.1 applications without a physical graphics processing unit (GPU)
- You can use up to 4 monitors and adjust the resolution for each monitor separately, up to 2560 x 1600 resolution per display. When 3D feature is enabled, up to 2 monitors are supported with a resolution of up to 1920x1200
- You can copy and paste text and images between the local system and the desktop, up to 1MB. Supported file formats include text, images, and RTF (Rich Text Format). You cannot copy and paste system objects such as folders and files between systems
- PCoIP supports 32-bit color
- PCoIP supports Advanced Encryption Standard (AES) 128-bit encryption, which is turned on by default
- Client hardware must support the following requirements:
  - x86-based processor with SSE2 extensions, with a 800MHz or higher processor speed

- ARM processor with NEON (preferred) or WMMX2 extensions, with a 1GHz or higher processor speed

### 3.2.9.3. VMware Blast Extreme

Adding to PCoIP, VMware now offers customers additional choice and flexibility with brand new Blast Extreme display technology, purpose built and optimized for the mobile cloud.

Built on industry-standard H.264 protocol, Blast Extreme supports the broadest range of client devices, billions of client devices are already H.264 capable.

Blast Extreme offers a lot of inherent advantages in addition to client device support. These include:

- Significantly less network bandwidth consumed
- The ability to leverage both TCP or UDP network transport
- Agility in adapting to challenging, lossy network conditions
- Lower CPU consumption for longer battery life on mobile devices
- Additionally, when combined with GPU-based hardware acceleration in the host, such as NVIDIA GRID, VMware has a complete solution that dramatically improves graphics performance end to end for the most visually intensive applications, in any use case.

### 3.2.10. VMware vRealize Operations for Horizon 7

VMware vRealize® Operations for Horizon® provides end-to-end visibility into the health, performance and efficiency of VMware virtual desktop and application environments from the data center and the network, all the way through to devices. It enables desktop administrators to proactively optimize end-user experience, avert incidents and eliminate bottlenecks. Designed for VMware Horizon and XenDesktop environments, vRealize Operations for Horizon reduces costs and expedites Time to Resolution (TTR) with in-depth monitoring.

### 3.2.10.1. Key Benefits

- Comprehensive visibility into the performance and health of Horizon and deployments on VMware vSphere® expedites troubleshooting and improves user experience to enhance workplace productivity
- Intelligent automation of root-cause analysis and auto-correlation of monitoring data across the entire stack reduces troubleshooting times and improves team productivity by up to 50 percent
- Self-learning analytics that notify desktop administrators of impending issues before they impact end users enable proactive management and process improvements
- Out-of-the box reporting templates and remediation recommendations help ensure compliance and enhance SLAs

### 3.2.10.2. Key Troubleshooting Benefits

- Troubleshooting desktop issues has never been easier with intuitive dashboards and heat map that use patented advanced analytics and root cause analysis to identify the problem before the users are impacted
- vRealize for Horizon View provides key troubleshooting data for these metrics and more:
  - PCoIP statistics
  - Network latency
  - CPU usage
  - Memory usage
  - Storage latency
  - Under or oversized VMs
  - vSphere infrastructure health
  - User Sessions
  - Licensing reports
- See figure on next page for an example of the comprehensive dashboard into the VDI environment

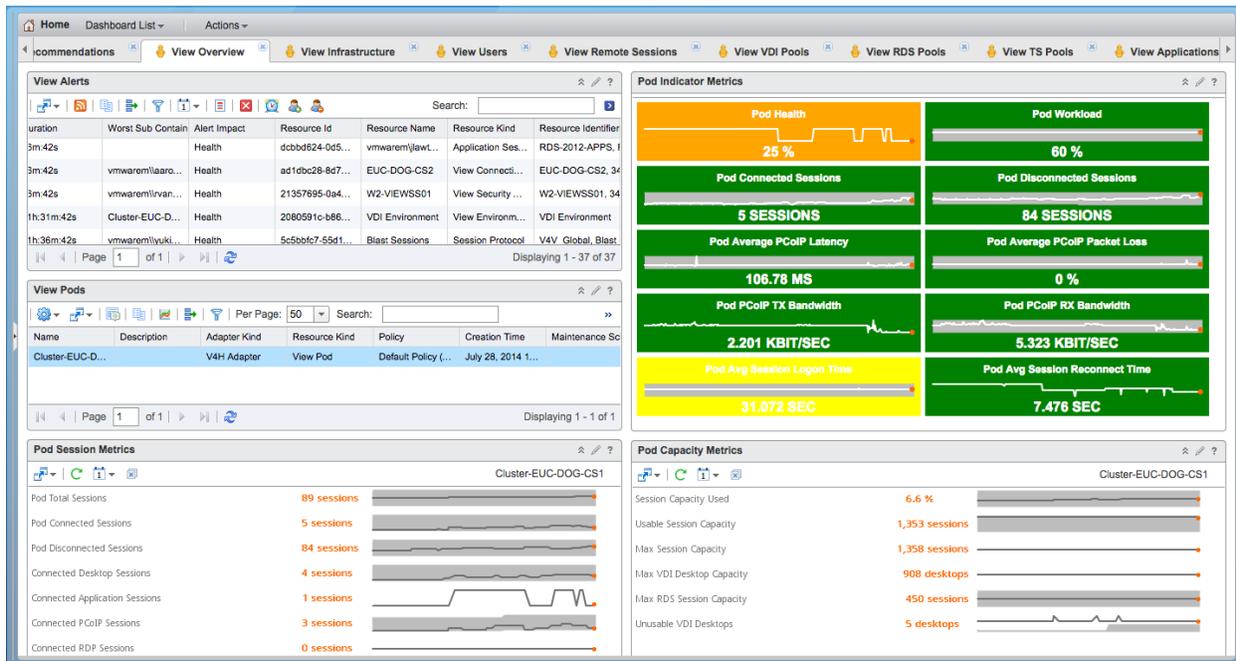


Figure 3. VMware VDI Dashboard Example

### 3.2.11. VMware Virtual SAN

Virtual SAN is a hypervisor-converged, software-defined storage platform that is fully integrated with vSphere. Virtual SAN aggregates locally attached disks of hosts that are members of a vSphere cluster to create a distributed shared storage solution. Because Virtual SAN sits directly in the I/O data path, it can deliver the highest levels of performance, scalability, and resilience without taxing the CPU with additional overhead. Virtual SAN enables the rapid provisioning of storage within VMware vCenter™ during virtual machine creation and deployment operations.

Virtual SAN uses a hybrid disk architecture that leverages flash-based devices for performance and magnetic disks for capacity and persistent data storage. Its distributed datastore is an object-store file system that leverages the vSphere Storage Policy-Based Management feature to deliver centrally managed, application-centric storage services and capabilities.

Administrators can specify storage attributes, such as capacity, performance, and availability, as a policy on a per virtual machine basis. The policies dynamically self-tune and load-balance the system so that each virtual machine has the right level of resources.

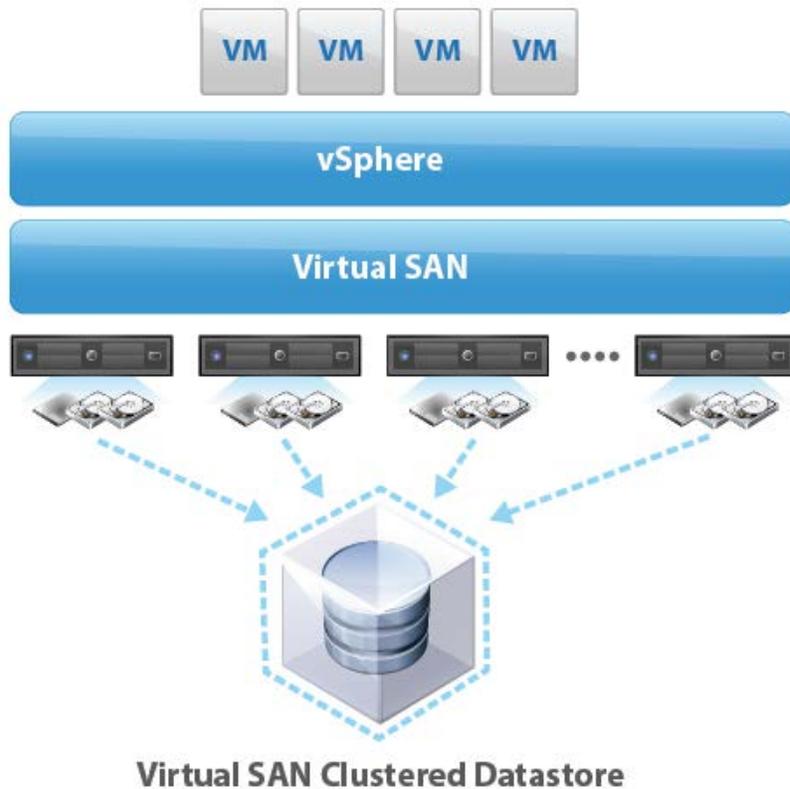


Figure 4. Virtual SAN Architecture

### 3.2.12. Security Design Considerations

Security design is an important part of any desktop virtualization project. This is especially true for the Department of Defense. GovConnection has provided secure infrastructure to the Department of Defense for many years.

GovConnection is very familiar with Department of Defense security design considerations such as aligning the correct authentication appliance with UC/APL and assuring that chosen products have received a Certificate of Networkiness (CoN) in accordance with Department of Defense regulations.

GovConnection understands the Department of Defense's specific security requirements and designs solutions that incorporate those requirements into all facets of a desktop virtualization project.

### 3.3. HP Device Manager

HP Device Manager is enterprise-class thin client management software that allows customers to view their thin client assets remotely and manipulate those thin clients to meet the required business need.

From one interface, HP Device Manager enables management of thin clients for the following:

- Configuration
- Automatic device discovery
- Device grouping for easy recognition
- Security certificate assignments
- FTP loading of images

#### **Asset tracking and inventory management**

HP Device Manager generates detailed reports to track health and performance of hardware and software assets:

- Multiple formats - CSV, Excel, PDF, RTF, HTML
- Auto registration of devices and gateways via DHCP or DNS
- Device Import via CSV file

#### **Thin client settings and connection cloning**

- Back-Up and Restore utility
- Connection management
- System settings
- Task data
- Device data

#### **Imaging and client updates tools**

- OS Imaging
- Operating System upgrades
- Image cloning
- File based imaging for WES

### Remote control

HP Device Manager provides users with cost-effective, one-to-one IT support without physically having to visit endpoint devices for the following: Citrix, RDP, TeamTalk, VDM Web

### Remote power management

Quickly restart, shut down or Wake-on-LAN (WoL) thin clients.

### Help desk and troubleshooting

- Shadowing ( OS dependent)
- PING
- Trace-Route
- Online/Offline status

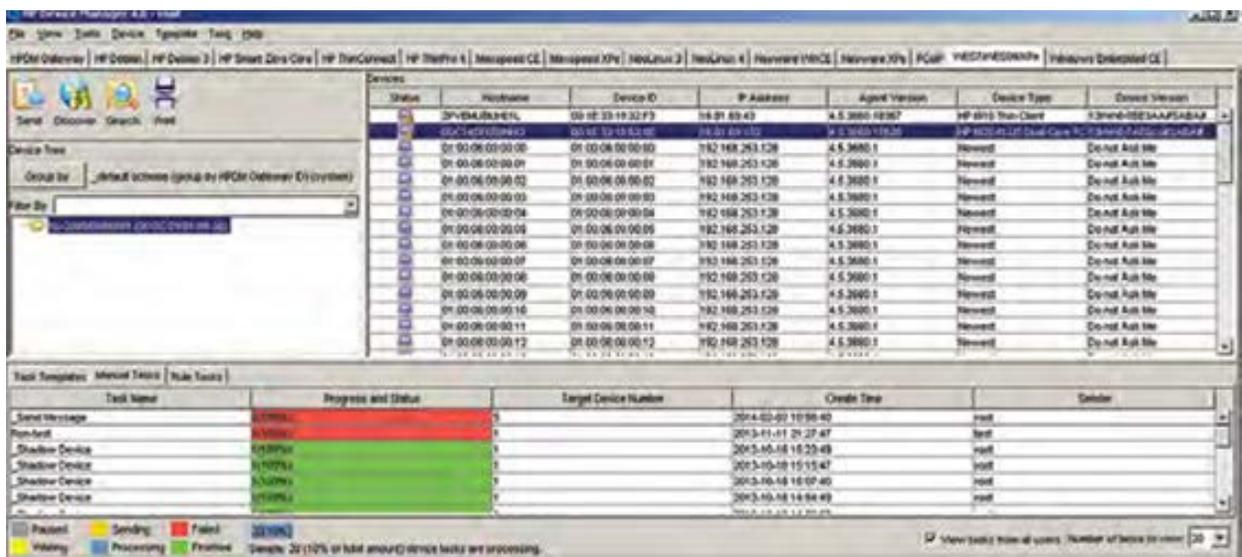


Figure 5. HP Device Manager Management Interface.

### 3.3.1. VMware Horizon View Topology

#### Overall view of VMware Horizon View Environment

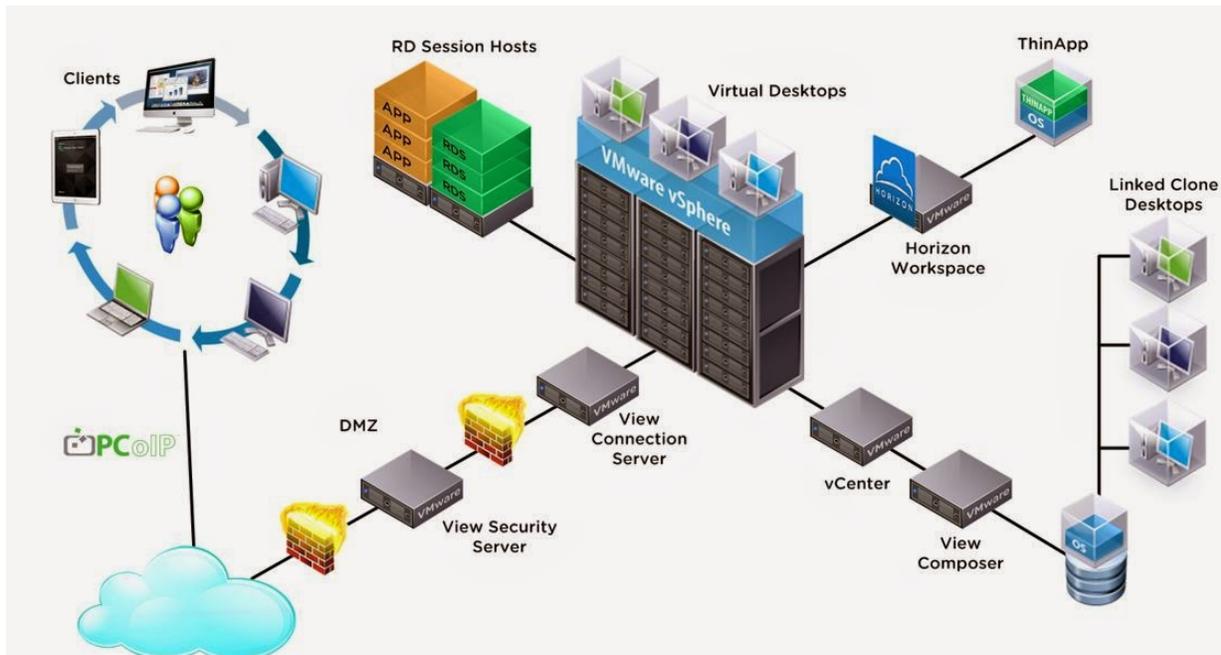


Figure 6. VMware Horizon Architecture Overview

---

## Section 4: Thin Client Solution for 500 Seats and Below

### 4.1. Solution Design Recommendation

GovConnection's solution design for 500 seats and below consists of these major components:

- (3) HP DL360 Gen9 Management Servers
- (6) HP DL360 Gen9 VMware Horizon View Servers
- (500) HP t620 Flexible Series Thin Clients
- VMware Horizon 7 Enterprise

The following assumptions were used in defining this design:

#### **Hardware Assumptions**

- Management server cluster
  - External access is required
  - 100% concurrent access is required
- VMware Horizon View server/desktop cluster
  - Virtual Desktop profile
    - Windows 7
    - 2 vCPU
    - One 40GB hard drive
    - 2.5 GB of RAM
    - Department applications
    - Microsoft Office, internet access
    - Local printing
    - Smart Card authentication
  - Assumptions for Cluster
    - 90% memory utilization
    - 90% CPU utilization
    - 120 users per host (5 users per core)
  - Assumptions for Virtual SAN
    - 1 host failure for fault tolerance
    - RAID 1
    - 60% read
    - 25 IOPS per VM

- Thin client hardware
  - Flexible Thin Clients – HP t620
  - Monitors (as needed, dual video display support standard; HP t620 plus can, with appropriate video card, support quad video displays)

**Software Assumptions**

- VMware Horizon View Enterprise (Licensed per named user)

4.2. Bill of Materials (500 seats and below)

Note: This is a representative bill of materials (BOM). Only major components are listed; items such as switches, cables, monitors, etc. are not included.

QTY	Description
	<b>HORIZON VIEW HOST CONFIGURATION</b>
6	HP DL360 Gen9 E5-2670v3 OneView Svr
72	HP 16GB 2Rx4 PC4-2133P-R Kit
6	HP 400GB 12G SAS ME 2.5in EM SC H2 SSD
24	HP 1.2TB 12G SAS 10K 2.5in SC ENT HDD
6	HP Ethernet 1Gb 4-port 366T Adapter
6	HPE 3Y FC NBD DL360 Gen9 w/OV SVC
6	HP iLO Adv incl 3yr TS U 1-Svr Lic
6	HP OV w/o iLO 3yr 24x7 Phys 1 Svr LTU
	<b>MANAGEMENT CLUSTER</b>
3	HP DL360 Gen9 E5-2670v3 OneView Svr
3	HP 400GB 12G SAS ME 2.5in EM SC H2 SSD
12	HP 1.2TB 12G SAS 10K 2.5in SC ENT HDD
3	HP Ethernet 1Gb 4-port 366T Adapter
3	HPE 3Y FC NBD DL360 Gen9 w/OV SVC
3	HP iLO Adv incl 3yr TS U 1-Svr Lic
3	HP OV w/o iLO 3yr 24x7 Phys 1 Svr LTU
	<b>HORIZON VIEW SOFTWARE and SUPPORT</b>
5	Horizon View software pricing (100 seats per)
5	Horizon View 3 year support (100 seats per)
	<b>THIN CLIENT HARDWARE</b>
500	HP t620 ThinPro AMD Fusion Quad Core 8GF/4GB

4.3. Major Component Details

Management Server Hardware Requirements	
Server Information	Description
<b>HP DL360 Gen9 Server</b>	Quantity: 3 HP DL360 Gen9 servers using Virtual SAN
<b>Recommended Sizing</b>	Three servers for redundancy/failover. These servers will house the following: VMware vCenter, View Composer server, Connection servers, Security servers/Access Points, SQL Server database, AppVolumes servers, profile data, UEM, vRealize Operations for Horizon and HP Device Manager server

VMware Horizon View Server/Desktop Hardware Requirements	
Server Information	Description
<b>HP DL360 Gen9 Server</b>	Quantity 6 DL360 Gen9 rackmount servers, dual 2.50Ghz E5-2680 v3 processors, 12 core, 384GB of RAM, single 400GB SSD drive, four 1TB SAS, 2 x 10GbE Ethernet connections and 4 x 1.2GB Ethernet connections
<b>Recommended Sizing</b>	One server for approximately 120 users, includes failover/load balancing servers to support the 500 users 5+1 for redundancy
<b>Assumption</b>	Customer has open 10GbE ports on existing switches within the environment

Thin Client Hardware Requirements	
Thin Client Information	Description
<b>HP t620 ThinPro AMD Fusion Quad Core 8GF/4GB</b>	Operating System: HP ThinPro 32, 4 GB 1600 MHz DDR3L SDRAM, 8 GB MLC M.2 SSD, Integrated AMD Radeon HD 8330E. Supports Citrix ICA, Citrix HDX, Microsoft RDP, Microsoft RemoteFX (RFX), VMware Horizon View through RDP and PCoIP; (2) USB 3.0 and (6) USB 2.0 ports
<b>Smart Card Reader (CAC)</b>	Gemalto USB-SW Smart Card Reader
<b>Recommended Sizing</b>	One per user

Software Requirements	
Software	Description
<b>VMware Horizon 7 Enterprise</b>	Horizon 7 provides a streamlined approach to delivering, protecting and managing virtual desktops (VDI) and apps while containing costs and ensuring that end users can work anytime, anywhere, across any device -
<b>VMware Horizon 7 Enterprise License</b>	Sold per concurrent user or named user

#### 4.4. Proposed Solution Architecture

##### 4.4.1. Management and Desktop Clusters (POD)

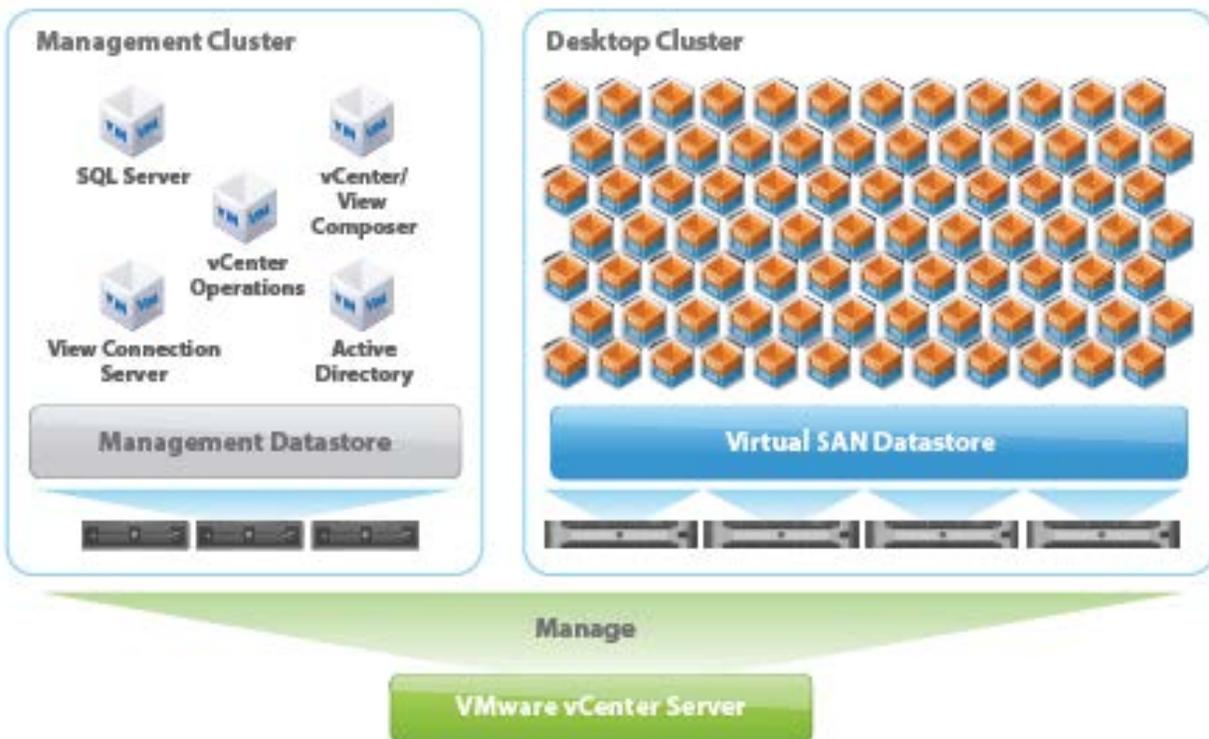


Figure 7. Desktop POD Architecture Overview

The Management Cluster (left) would, for the 500 seat and below configuration, be comprised of three HP DL360 Gen9 servers. The VMware Horizon View servers (lower right) would be comprised of six HP DL360 Gen9 servers. The thin client pool (upper right) would be comprised of up to 500 HP t620 Flexible Thin Clients.

#### 4.5. Description of Costs and Project Timeline

The costs to implement the suggested 500 seat and below configuration would consist of the following:

1. Proof of Concept services
2. Desktop Assessment
3. Hardware, Software and Support costs for the solution
4. Implementation Services
  - a. Hardware Installation
  - b. VMware vCenter Installation
  - c. VMware Horizon 7 Installation
  - d. Documentation and Knowledge Transfer

#### 500 Seats and Below

Description	Duration
Proof of Concept Services	Variable, 4-8 weeks on average
Desktop Assessment	40 days
Hardware, Software and Support for Final Solution	Product Lead Time
Implementation Services for Final Solution: <ul style="list-style-type: none"> <li>• Hardware Installation</li> <li>• VMware vCenter Installation</li> <li>• VMware Horizon 7 Installation</li> <li>• Documentation and Knowledge Transfer</li> </ul>	Variable, 2 weeks on-site 1 week documentation and project close-out

---

## Section 5: Thin Client Solution for 500 Seats and Above

### 5.1. Solution Design Recommendation

GovConnection, Inc.'s solution design for 500 seats and above consists of these major components (there is a doubling of server requirements to support VMware's AlwaysOn functionality (see Section 5.4) in this scenario as well as an increase in the number of Horizon View servers to support the higher seat count):

- (6) HP DL360 Gen9 Management Servers
- (20) HP DL360 Gen9 VMware Horizon View Servers
- (1000) HP t620 Plus Flexible Series Thin Clients
- VMware Horizon 7 Enterprise

The following assumptions were used in defining this design:

#### **Hardware Assumptions**

- Management server cluster
  - External access is required
  - 100% concurrent access is required
- VMware Horizon View server/desktop cluster
  - Virtual Desktop profile
    - Windows 7
    - 2 vCPU
    - One 40GB hard drive
    - 2.5 GB of RAM
    - Department applications
    - Microsoft Office, internet access
    - Local printing
    - Smart Card authentication
  - Assumptions for Cluster
    - 90% memory utilization
    - 90% CPU utilization
    - 120 users per host (5 users per core)
  - Assumptions for Virtual SAN
    - 1 host failure for fault tolerance

- RAID 1
- 60% read
- 25 IOPS per VM
- Thin client hardware
  - Flexible Thin Clients – HP t620
  - Monitors (as needed, dual video display support standard; HP t620 plus can, with appropriate video card, support quad video displays)

**Software Assumptions**

- VMware Horizon View Enterprise (Licensed per named user)

5.2. Bill of Materials (500 seats and above)

Note: This is a representative bill of materials (BOM). Only major components are listed; items such as switches, cables, monitors, etc. are not included.

QTY	Description
<b>HORIZON VIEW HOST CONFIGURATION – SITE 1</b>	
10	HP DL360 Gen9 E5-2670v3 OneView Svr
120	HP 16GB 2Rx4 PC4-2133P-R Kit
10	HP 400GB 12G SAS ME 2.5in EM SC H2 SSD
40	HP 1.2TB 12G SAS 10K 2.5in SC ENT HDD
10	HP Ethernet 1Gb 4-port 366T Adapter
10	HPE 3Y FC NBD DL360 Gen9 w/OV SVC
10	HP iLO Adv incl 3yr TS U 1-Svr Lic
10	HP OV w/o iLO 3yr 24x7 Phys 1 Svr LTU
<b>MANAGEMENT CLUSTER – SITE 1</b>	
3	HP DL360 Gen9 E5-2670v3 OneView Svr
3	HP 400GB 12G SAS ME 2.5in EM SC H2 SSD
12	HP 1.2TB 12G SAS 10K 2.5in SC ENT HDD
3	HP Ethernet 1Gb 4-port 366T Adapter
3	HPE 3Y FC NBD DL360 Gen9 w/OV SVC
3	HP iLO Adv incl 3yr TS U 1-Svr Lic
3	HP OV w/o iLO 3yr 24x7 Phys 1 Svr LTU
<b>HORIZON VIEW HOST CONFIGURATION – SITE 2</b>	
10	HP DL360 Gen9 E5-2670v3 OneView Svr
120	HP 16GB 2Rx4 PC4-2133P-R Kit
10	HP 400GB 12G SAS ME 2.5in EM SC H2 SSD
40	HP 1.2TB 12G SAS 10K 2.5in SC ENT HDD
10	HP Ethernet 1Gb 4-port 366T Adapter
10	HPE 3Y FC NBD DL360 Gen9 w/OV SVC

10	HP iLO Adv incl 3yr TS U 1-Svr Lic
10	HP OV w/o iLO 3yr 24x7 Phys 1 Svr LTU
	<b>MANAGEMENT CLUSTER – SITE 2</b>
3	HP DL360 Gen9 E5-2670v3 OneView Svr
3	HP 400GB 12G SAS ME 2.5in EM SC H2 SSD
12	HP 1.2TB 12G SAS 10K 2.5in SC ENT HDD
3	HP Ethernet 1Gb 4-port 366T Adapter
3	HPE 3Y FC NBD DL360 Gen9 w/OV SVC
3	HP iLO Adv incl 3yr TS U 1-Svr Lic
3	HP OV w/o iLO 3yr 24x7 Phys 1 Svr LTU
	<b>HORIZON VIEW SOFTWARE and SUPPORT</b>
5	Horizon View software pricing (100 seats per)
5	Horizon View 3 year support (100 seats per)
	<b>THIN CLIENT HARDWARE</b>
1000	HP t620 PLUS ThinPro AMD Fusion Quad Core 8GF/4GB Quad Video

5.3. Major Component Details

Management Server Hardware Requirements	
Server Information	Description
<b>HP DL360 Gen9 Server</b>	Quantity: 6 (AlwaysOn) HP DL360 Gen9 servers using Virtual SAN
<b>Recommended Sizing</b>	Three servers for redundancy/failover. These servers will house the following: VMware vCenter, View Composer server, Connection servers, Security servers/Access Points, SQL Server database, AppVolumes servers, profile data, UEM, vRealize Operations for Horizon and HP Device Manager

VMware Horizon View Server/Desktop Hardware Requirements for 1000 users	
Server Information	Description
<b>HP DL360 Gen9 Server</b>	Quantity 20 (AlwaysOn) DL360 Gen9 rackmount servers, dual 2.50Ghz E5-2680 v3 processors, 12 core, 384GB of RAM, single 400GB SSD drive, four 1TB SAS, 2 x 10GbE Ethernet connections and 4 x 1.2GB Ethernet connections
<b>Recommended Sizing</b>	One server for approximately 120 users, includes failover/load balancing servers to support the 1000 users 9+1 for redundancy

Thin Client Hardware Requirements	
Thin Client Information	Description
<b>HP t620 PLUS ThinPro AMD Fusion Quad Core 8GF/4GB Quad Video</b>	Operating System: HP ThinPro 32, 4 GB 1600 MHz DDR3L SDRAM, 8 GB MLC M.2 SSD, Integrated AMD Radeon HD 8400E. Supports Citrix ICA, Citrix HDX, Microsoft RDP, Microsoft RemoteFX (RFX), VMware Horizon View through RDP and PCoIP; (2) USB 3.0 and (6) USB 2.0 ports
<b>Smart Card Reader (CAC)</b>	Gemalto USB-SW Smart Card Reader
<b>Recommended Sizing</b>	One per user

Software Requirements	
Software	Description
<b>VMware Horizon 7 Enterprise</b>	Horizon 7 provides a streamlined approach to delivering, protecting and managing virtual desktops (VDI) and apps while containing costs and ensuring that end users can work anytime, anywhere, across any device -
<b>VMware Horizon 7 Enterprise License</b>	Sold per concurrent user or named user

### 5.4. Proposed Solution Architecture – AlwaysOn

#### 5.4.1. AlwaysOn Architecture

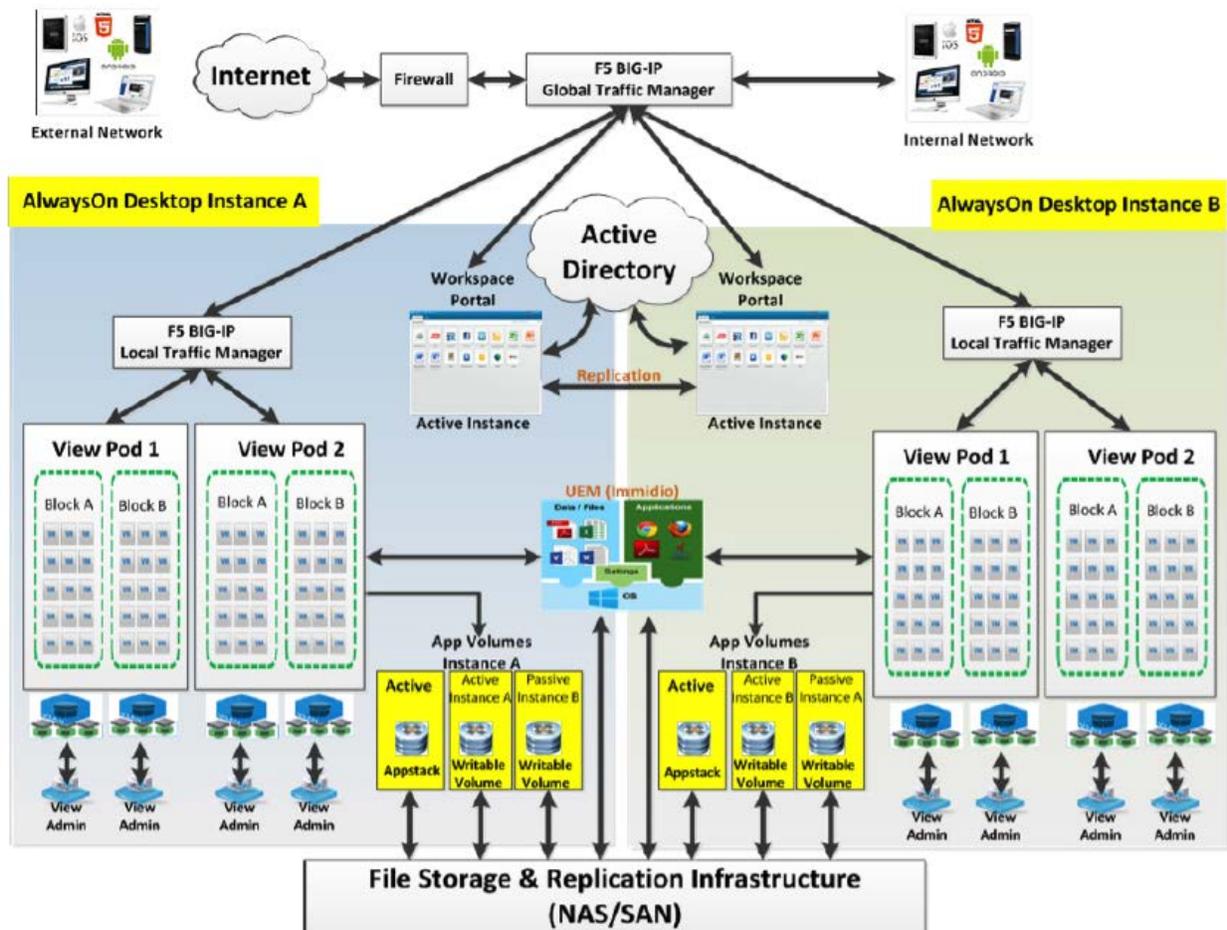


Figure 8. AlwaysOn Architecture Overview Diagram

The diagram above shows the proposed architecture for the initial 1000 desktops. This environment is a pod design which will support up to 2,000 desktops / RDSH sessions. This design is easily scalable by replication. In addition, Horizon 7 supports global pools and namespaces within the cloud pod architecture which would allow scalability of up to 20,000 desktops within a single namespace. These desktop pools and pods can also be separated via WAN to provide disaster recovery or high availability.

#### 5.4.2. Virtual Desktop

The proposed design leverages the Horizon 7 VDI solution with Composer to provide floating pools of either linked clone or instant linked clone desktops. These desktops can be accessed internally or externally via F5 load balanced pairs of connection servers and security servers.

The security servers or access points sit in the DMZ and provide a secure tunnel to the user's VDI or RDSH sessions. This design dedicates a pair of F5 load balanced connection servers for internal use and a pair for external use. Tags can be used to easily specify desktop pools which can only be accessed internal or pools that can only be accessed external to the network.

There is a Virtual Center with the composer service on it installed in the View Management cluster to create and manage the linked clone desktops. By leveraging App Volumes, a generic gold image can be used and groups of applications can be attached dynamically as locally installed applications to the Virtual Desktops based on AD entitlements. App Volumes also allow the installation of user installed applications (if supported) which persist across floating desktop sessions.

VMware User Environment Manager (UEM) will be used to manage Windows settings, Application settings and the user environment (mapped drives, printers, etc.). These settings will persist dynamically between physical systems, virtual desktops and RDSH sessions. When paired with App Volumes the user will have a floating desktop which looks and feels to them exactly like a persistent desktop. Operationally, these floating desktops can easily be patched and the applications designated to them can be modified and updated in real time with App Volumes.

These desktops can be brokered from a native VMware Horizon client leveraging the highly optimized PCoIP protocol or via the HTML5 protocol which can be accessed from any HTML5 browser with no plugins required. The native client is available for iOS and Android, as well as Windows, MAC and Linux. The mobile clients are optimized for mobile devices with the Unity Touch feature set. The workspace portal can also launch virtual desktop sessions via SSO.

Horizon can publish desktops with Windows client or Server OS (both native and desktop compatibility mode) as well as Linux.

### 5.4.3. RDSH Published Applications

Applications can easily be published with Horizon 7. The technology leverages the Windows server RDSH capability and is supported on Windows 2008 R2 as well as Windows 2012 Server. Servers are grouped into farms. Each farm of servers should have the same application set installed. Horizon will load balance sessions across the servers in the farm. Applications can be delivered via the native client or via HTML5 (6.1.2) to any device. Application management in each RDSH farm is simplified by the use of VMware App Volumes which can attach the appropriate applications to each server in the farm in real-time. There is only one instance of the application to manage and update and consistency can be maintained easily.

VMware UEM will be used to manage user settings for the applications which are published. For instance, if a user has particular settings for Microsoft Excel on their physical or virtual desktop, those settings will follow them dynamically to their RDSH published version of Excel on any device. RDSH application publishing is managed from the same administrative console as virtual desktops and it shares the same underlying infrastructure of connection servers for internal access and security servers for external access. RDSH published applications can also be brokered via SSO from the VMware Workspace Portal.

## 5.5. Description of Costs and Project Timeline

The costs to implement the suggested 500 seat and above configuration would consist of the following:

1. Proof of Concept services
2. Desktop Assessment
3. Hardware, Software and Support costs for the solution
4. Implementation Services
  - a. Hardware Installation
  - b. VMware vCenter Installation
  - c. VMware Horizon 7 Installation
  - d. Documentation and Knowledge Transfer

---

**500 Seats and Above**

Description	Duration
Proof of Concept Services	Variable, 4-8 weeks on average
Desktop Assessment	60 days
Hardware, Software and Support for Final Solution	Product Lead Time
Implementation Services for Final Solution: <ul style="list-style-type: none"><li>• Hardware Installation</li><li>• VM vCenter Installation</li><li>• VMware Horizon 7 Installation</li><li>• Documentation and Knowledge Transfer</li></ul>	5 weeks on-site 2 weeks pre-planning, desktop optimization, documentation and project close-out

## Section 6: Attachments and References

### 6.1. Acceptance Criteria/Virtual Desktop Profile

GovConnection uses the following table to help implement a Proof of Concept (POC) within a customer’s environment. The questions help us facilitate a successful POC. For each of the scenarios used within this whitepaper this Acceptance Criteria questionnaire was used to help determine hardware required for the virtual desktop scenarios. The end result for the data we used gave us the following profile for the virtual desktop:

- 2 vCPU
- 2.5GB of RAM
- 40 GB hard drive
  - o May need a second drive to store user installed applications
- Microsoft Office applications
- Department applications
- Smart Card authentication
- Local printing
- Profiles stored in the datacenter

### 6.2. VDI Assessment Data Gathering Example Questionnaire

Criteria	Description	Comments
<b>Desktop Requirements</b>	Please describe your current desktop.	40GB internal Drive. 2GB of RAM, Microsoft applications such as Outlook, Excel, Word, and Internet access
<b>What USB devices need to be tested?</b>	List different USB devices that need for the desktops. i.e. USB microphones, scanners, flash storage	Printer

Criteria	Description	Comments
<b>Printers</b>	<p>End users should be able to print to their local or network-attached printers from within their virtual desktop.</p> <p>Print to a local USB or network-attached printer</p>	yes
<b>Multi monitor capabilities</b>	Do end users need multiple monitors?	Yes
<b>Profile Management</b>	Ability to store profile and user data outside of the system image	Yes
<b>Desktop Antivirus</b>	Offloaded antivirus versus traditional agent	No
<b>Graphics</b>	<p>What graphic intensive apps are they running?</p> <p>Do end users have dedicated graphic cards in their desktops?</p>	None
<b>Remote Users</b>	Do you have users at remote locations?	Yes, we have some users that are allowed access from home
<b>Applications</b>	<p>What are the applications that are needed for the desktops?</p> <p>Are there any user-installed applications that need to be addressed?</p>	<p>MS office applications, a few departmental applications</p> <p>Users are not allowed to install applications</p>

---

Criteria	Description	Comments
	Can users install their own applications?	Some users can install their own applications
<b>Multi-factor Authentication</b>	Do you use multi-factor authentication in your environment, such as smart cards?	Yes, CAC
<b>Voice</b>	Are you using VOIP? Do any soft clients need to be tested?	No

