VMware View™ 4

EVALUATOR'S GUIDE

vmware®

Table of Contents

Welcome

Welcome to the VMware® View™ 4 Evaluator's Guide. The purpose of this document is to support a self-guided, hands-on evaluation of VMware View 4. The content includes a product overview, including the new features of PCoIP, installation instructions, and scenarios to demonstrate how VMware View can help you deliver the desktop as a managed service. The guide is divided into four sections:

1. **Introducing VMware View 4**

2. **What's New in VMware View 4**

3. **VMware View 4 Components Overview**

4. **Installing and Configuring VMware View 4**

This guide is not intended to be a substitute for product documentation. For detailed information regarding installation, configuration, administration, and usage of VMware products, please refer to the online documentation. You may also consult the online Knowledge Base if you have any additional questions.

Introducing VMware View 4

Built on the industry-leading virtualization platform, VMware View 4 is a solution that enables IT organizations to "decouple" a desktop from physical devices or locations and deliver the desktop as a managed service from a centralized location. VMware View makes desktops easily accessible to any end user on multiple devices (thick or thin) over any network connection, complete with all applications and data for an optimized and familiar desktop experience. Purpose-built for delivering desktops as a managed service, VMware View provides the best end user experience and simplifies and automates desktop management.

Unlike other desktop virtualization products, VMware View is a tightly integrated end to end solution allowing customers to extend business continuity and disaster recover features to their desktops and standardize on a common platform from the desktop through the datacenter to the cloud.

Prior to building and planning the VMware View 4 release, the VMware View team reviewed feedback from customers to gauge their challenges and requirements:

• **IT Professionals** indicated that they generally refresh their laptops and desktops every three to four years, but with the tough economy, they are now striving to do more with less. Time, money, and resources are in short supply so they need more efficient ways to deploy and manage their endpoint complexity and boost end-user productivity. They are looking for ways to reduce the complexity of their systems and get more performance from their infrastructure and, are considering desktop virtualization as a solution.

• **Designers and Knowledge Workers** indicated that their work habits are changing. They now need to have the ability to access the work environment from many endpoints, without compromising the rich user experience of their PCs for graphic- or video-intense offline or online content – regardless of the device type or the network to which it is attached.

• **IT Decision Makers** indicated that they are skeptical when it comes to desktop virtualization. Some IT Decision Markers are unsure of the bandwidth necessary for a virtual desktop experience in LAN or WAN settings that could serve virtual desktops with the same quality as locally run OS images.

What's New in VMWare View 4

VMware View 4 is purpose built for desktop delivery and designed for the LAN or WAN configuration. The goal is to continue provide a smooth end-to-end desktop experience via software implementation.
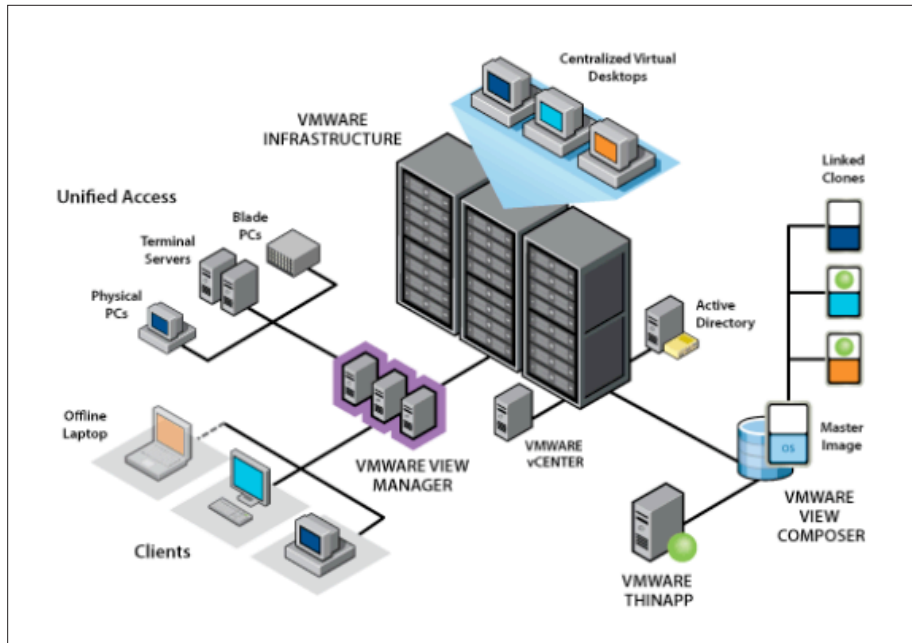

Figure 1.

FEATURE	NEW/ IMPROVED	DESCRIPTION
Quad monitor support	New	Support 32-bit color with 1920 x 1200 display resolution and up to 4 monitors simultaneously. Benefit: True multiple displays allow you to "see more and do more" from a full desktop. This provides the ability to reproduce true color images with support for up to 4.2 billion distinct colors per pixel.
True multi-monitor support on L-shape configuration	New	Support 1 landscape display and 1 portrait display (with pivot monitors), variable resolution support, and auto fit to client. Benefit: Each monitor can be of a different size and be set to a different resolution. Auto Display Scaling/Dynamic Resizing helps desktop publishing, financial application, and high-end graphic design needs.
Guest desktop support Windows Vista and XP OS	New	Support for connecting to virtual desktops from Windows XP and Vista. The VMware View 4 PCoIP is a software-to-software implementation. However, it also supports hardware PCoIP hosts such as the Samsung SyncMaster 930ND 19" monitor and Teradici Tera Portal. http://www.teradici.com/pcoip/pcoip-products/oem-solutions.php Benefit: Provides scalable support to both software and hardware on the local hosts.
Network characteristics and security	New	SSL protection on TCP for session management and AES 128-bit key encryption on UDP for media transfer between host and client system. Benefit: Provides comparable security and encryption found in other protocols.
Protocol intelligence	New	PCoIP protocol provides the intelligence to handle prioritization and quality of services (QOS) for video/mouse/keyboard/sound, etc. Benefit: This greatly helps the user experience by managing bandwidth and content variables.
WAN performance and optimization	New	Operate with up to 250ms of round-trip latency with tolerance on packet loss up to 5%.
VPN tunneling	New	Support Cisco VPN soft client.
RDP virtual channel compatibility for USB redirection	New	Support the comparable list of USB peripherals including biometrics, card readers, webcams, mass storage, flash devices, scanners, etc. The authorization can be done on a per-user/per-group basis to only accept specific devices.
Flash control support for PCoIP	New	PCoIP uses breakthrough graphics compression that is custom built for delivering a user desktop over IP networks. It works in such a way as to support all graphics (full-frame rate 3D for design engineering, video gaming, etc.), and media (HD video, Microsoft video formats, YouTube, Microsoft Silverlight, Google, QuickTime, or Adobe Flash). Benefit: By compressing the display image at the host PC/Server, you avoid application interoperability issues that have plagued thin clients for years and can quickly adapt to physical networks.
Audio redirection	New	New to PCoIP protocol. Redirect audio with dynamic audio quality adjustment on the WAN.
ClearType font	New	Subpixel rendering technology which may help to improve the apperance of text on some computer displays. Newly added to PCoIP protocol.

VMware PCoIP Delivers a Rich Desktop Experience
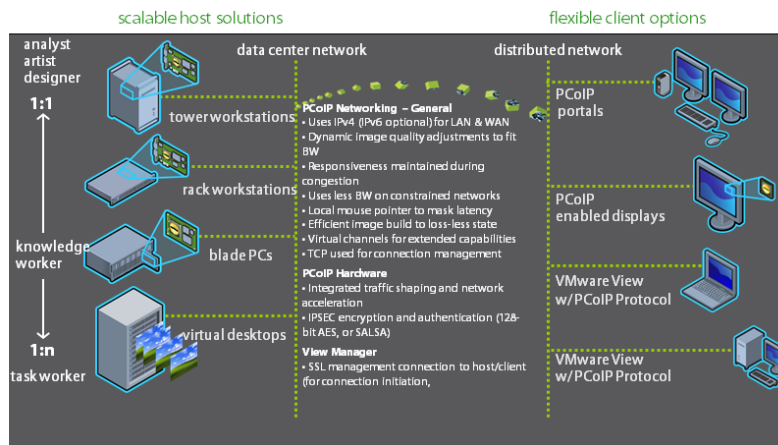

Figure 2.

Operational Efficiency

Enterprises that are struggling with the problem of endpoint security should explore desktop virtualization to lessen the frequency of malware, network breaches, and data loss headaches.

VMware View centralizes the control of desktop PC images, applications, and data. Deploying desktop virtualization with VMware View 4 running VMware vSphere™ can significantly improve security functionality and storage optimization.

For business entities that are subject to stringent regulatory policies such as the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS), VMware View creates a trusted enterprise-computing environment. Security vendors like McAfee and Trend Micro take a proactive role with VMware in raising the bar of security, control, and management available to secure the cloud-based infrastructure.

FEATURE	NEW/ IMPROVED	DESCRIPTION
Full clone pool with thin disk/thin provisioning	New	VMware View 4 provides seamless native support for thin provisioning with the vSphere server. Benefit: Helps reduce storage usage and allows more guest desktops per core while still providing high performance.
Mixed cluster support for backward – forward compatibility	New	This new option in View Administrator allows different versions of clusters to be managed via the same UI.
VWware VMsafe API for better anti-virus optimization and execution	New	VMware vSphere supports VMware VMsafe™ API Security virtual machine deployment, sold separately by security vendors, is consistent with desktop deployment. Protects the virtual machine by inspecting virtual components (CPU, Memory, Network and Storage).

Better Value and Reduced Cost

With VMware View 4, customers will get seamless access to the desktop, and can get access to services and desktop sessions with a single-sign-on (SSO) environment through any supported device.

Enterprises need to make their network and security technology and management structures into one seamless, streamlined operation to ease transition. The security enhancements found in VMware View 4 helps streamline and simplify the prevention of:

• Loss or theft of sensitive data

• Unauthorized access to internal systems

• Uncontrolled consumer application usage at work

• Loss of control of end-user access methods

These all contribute to delivering a better ROI and a lower TCO.

FEATURE	NEW/IMPROVED	DESCRIPTION
Triple single sign — on (3SSO) for sessions/connections keep-alive	Improved	This setting enables "log in as current user" using Active Directory credentials or smart cards over Remote Desktop Protocol. Benefit: Helps eliminate redundant authentication steps or double PIN entry when using smart cards.
Tag-based pool access	New	Administrators can now assign "tags" to connect server and desktop pools. Tag matching rules can be applied to restrict or grant users access to certain desktops.
Smart card removal policy	Improved	This policy setting forces desktops to disconnect when users remove their smart card.
Delete script	Improved	This scripting capability cleanly deletes VMware View desktops and allows extensibility using visual basic scripting.

VMware View 4 Components

VMware View 4 extends the same infrastructure and components as in previous versions. The key software components you need to install VMware View 4 are:

• VMware View Connection Server, installed in a Windows Server 2003 system that is separate from VMware vCenter™

• VMware View Agent, installed in a virtual desktop (XP, Windows 2003, or Vista desktops)

• VMware View Client, installed at the end point device (thin client, local laptop or desktops)

• VMware View Composer, installed in VMware vCenter for Linked Clone provisioning use
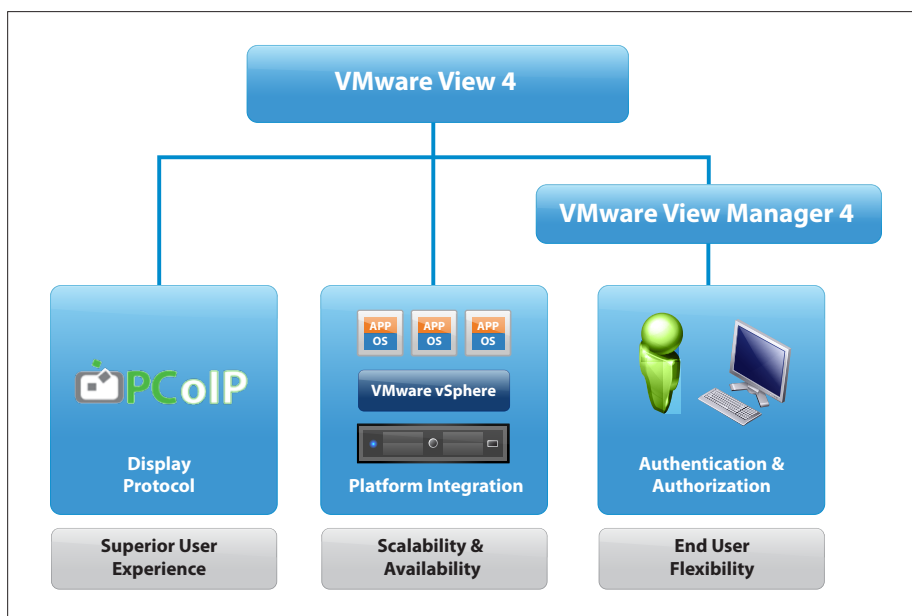
Figure 3.

On the infrastructure side you need to ensure that the following components are provisioned in VMware ESX™ 3.5 or VMware vSphere.

• VMware vCenter and VMware View Composer are installed on the same virtual machine where VMware vCenter is installed.

• SQL Server is required for large virtual desktop deployments. For this evaluation, the SQL Server Express Edition configured during the VMware vCenter installation is used.

• Configure Windows 2003 with Active Directory, DHCP, and DNS service.

• Certificate Authority (if certificate or smart card authentication is required). This is not discussed in this document.

For a detailed, supported version, please reference the VMware View Manager Administration Guide at http://www.vmware.com/support/pubs/view_pubs.html

NFR Licensing for Evaluation Use

To request Not For Resale evaluation licenses, please email desktop-tm@vmware.com.

Deployment Process

In this evaluation, you will experience the VMware View setup and configuration all in a single ESX/ VMware vSphere box. You will also install the needed infrastructure components and virtual machines from scratch. An online connection is required only if you plan to use the Internet.

Before starting the deployment process:

• Set up the networking and IP address in ESX/VMware vSphere with NAT router and VMware vSwitch

• Configure the required infrastructure components, including VMware vCenter, Active Directory, SQL server, and VMware View Connection Server

• Prepare the desktops, snapshots, and templates

The following deployment process is not intended to provide a deep technical explanation of the technologies found in VMware View 4. Nor is it intended to be used as a deployment guide. The tasks include:

• Task 1: Installing the Connection Server

• Task 2: Configuring and Administrating VMware View Manager

• Task 3: Installing the License

• Task 4: Associating and Adding VMware vCenter Server

• Task 5: Configuring Active Directory Users and Computers

• Task 6: Creating and Preparing Virtual Machines

• Task 7: Preparing Virtual Machine Snapshots and Templates

• Task 8: Installing VMware View Composer for Linked Clones

• Task 9: Installing VMware View Client in the Host Desktop or Thin Client (local system)

• Task 10: Adding Desktop Source In VMware View Manager

• Task 11: Desktop Entitlement

• Task 12: Accessing Virtual Desktop via RDP or PCoIP

• Task 13: Additional Virtual Desktop Optimization

• Task 14: WAN Optimization

Preparing for the Installation

Assumptions
To successfully use this guide it is assumed that VMware vSphere ESX Server has been installed and is functioning properly. Please refer to the online documentation http://www.vmware.com/resources/techresources/10020 for further installation assistance.

Before You Begin
Please reference Getting Started with VMware View at http://www.vmware.com/support/pubs/view_pubs.html. For more information on administrating VMware View, you can review the following documentation:

• VMware View Manager Administration Guide

• VMware View Upgrade Guide

• VMware View Architecture and Planning Guide

• Knowledge Base

System Requirements
The following is a description of the hardware and software required (for the major components of VMware View.) You can get more information from the VMware View 4 Architecture Planning Guide.

VMware View Connection Server
VMware View Connection Server is not supported on servers that have the Windows Terminal Server role installed. Remove the Windows Terminal Server role from any server where you will be installing the VMware View Connection Server.

VMware View Connection Server runs on a 32-bit or 64-bit dedicated physical or virtual server with the following specifications:

• Pentium IV 2.0Ghz processor or higher — dual processors are recommended

• 2GB RAM or higher — 3GB RAM is recommended for deployments of 50 or more View Manager desktops. VMware View connection server can handle 2,000 connections in clear mode and 750 in tunneled mode. The following VMware vSphere document lists the limits for the server side: http://www.vmware.com/support/pubs/vs_pages/vsp_pubs_esx40_vc40.html.

• One or more 10/100Mbps network interface controllers (NIC) — 1Gbps NIC is recommended

Supported Operating Systems
The VMware View Connection Server can be installed on the following 32-bit operating systems:

• Windows Server 2003 R2 Standard Edition with SP2

• Windows Server 2003 Standard Edition with SP2

• Windows Server 2003 R2 Enterprise Edition with SP2

• Windows Server 2003 Enterprise Edition with SP2

Prerequisites
VMware View Connection Server has the following prerequisites:

You will need a valid license key for VMware View Manager. The following types of licenses are available:

• VMware View Manager

• VMware View Manager with View Composer

• VMware View Manager with View Composer, and Offline Desktop

For the VMware virtualization environment, you will need one of the following:

• VMware vSphere 4 Update 1 (U1 is required)

• VMware Infrastructure 3.5 (U3 or U4 recommended, U5 not supported)

• VMware Infrastructure 3.0.2 (supported)

• Both ESX and ESXi hosts are supported, VMware vCenter is required

Required Host operating systems for standard or replica VMware View Connection Server instances are joined to an Active Directory domain. The following versions of Active Directory are supported. You will need one of the following:

• Windows 2000 Active Directory

• Windows 2003 Active Directory

• Windows 2008 Active Directory

IP Addressing

For easy configuration, this evaluation scenario specifies a standalone LAN environment with IP addressing based on the following assumptions:

• One VMware vSwitch is configured as the External Network for static, manually assigned IP addressing.

VIEW COMPONENTS	IP ADDRESSING
Virtual Center (vCenter)	Static 192.168.13.247
View Connection Server 1 (View1)	Static 192.168.13.246
View Connection Server 2 (View2)	Static 192.168.13.245
Active Directory (ActiveDirectory)	Static 192.168.13.252

• VMware vCenter installation provides SQL Server Express Edition. You do not need a separate SQL Server instance for this evaluation.

• This evaluation asks you to set up two VMware View Connection Servers. This will be used in the evaluation of the new "tag entitlement" feature later. It's an optional task if you just need to review the basic functionalities.

• If you already have networking setup, you can assign a static IP to infrastructure components needed for this evaluation.

• You can also access the Internet if it's available by separate 2 vLANs, and configure the open source Yvetta NAT appliance. You can find additional instructions at http://www.vyatta.com/downloads/swdl.php.

• You will prepare three virtual machines, including XP and/or Vista, for the scenario. These desktop virtual machines have IP addresses assigned using DHCP.
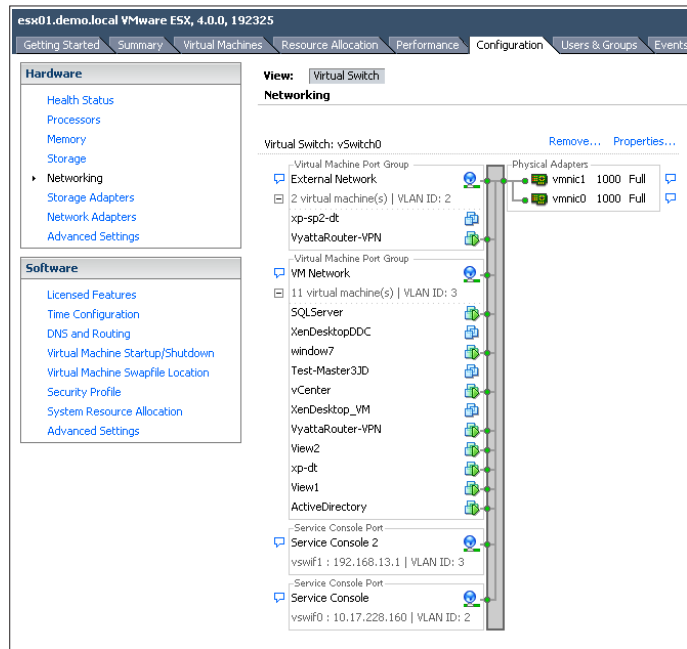
Figure 4.

The network configuration can be customized based on your network availability. Figure 4 is a sample configuration. Make sure the infrastructure components have a static, routable, and pointable IP address and complete a ping test from the servers to the desktops and from the desktops to the servers. The IP configuration is critical to a successful evaluation.

Installing and Configuring VMware View

Before You Begin

VMware View is tightly integrated with VMware vCenter. You can install VMware vCenter as a standalone server or as a hosted server under the same ESX box for the testing purposes. Please assign a static IP for your VMware vCenter IP configuration.
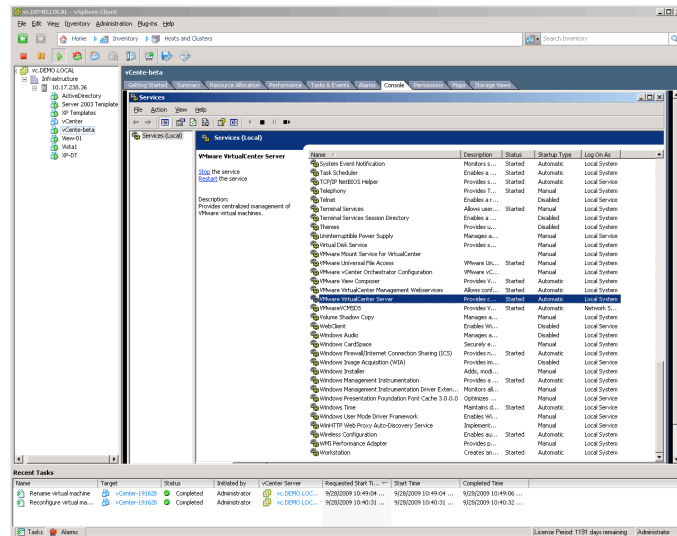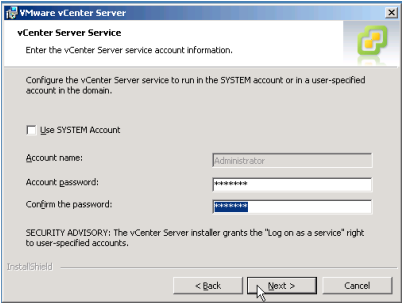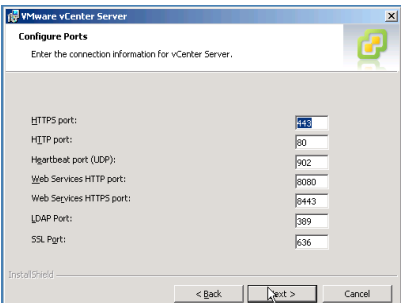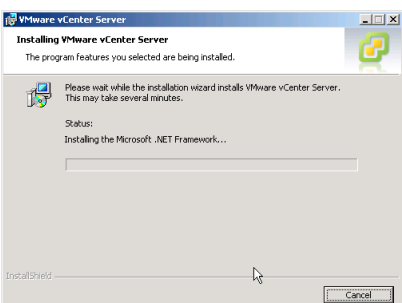
Figure 5.

- In your physical ESX host, create a Windows Server 2003 virtual machine for the VMware vCenter installation.
- Make sure to assign it with a routable static IP. In this setting, VMware vCenter can be pinged through vc.demo.local.
- Select **Create a stand-alone VMware vCenter** and click **Next**.
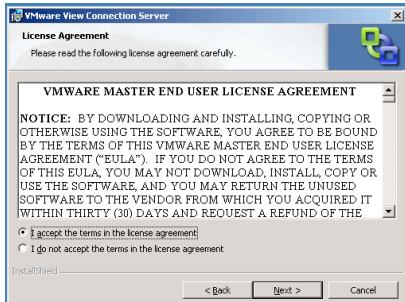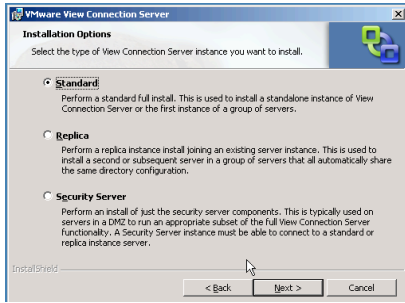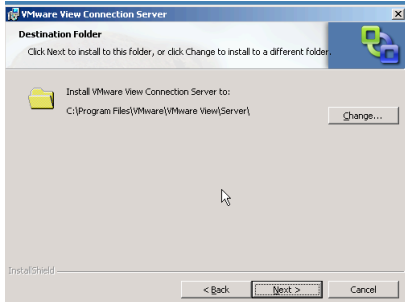
• In this evaluation, the default Microsoft SQL Server Express instance for the storage is used.
• Uncheck the System Account.
• Enter the default Administrator credentials:
  - Username: Administrator
  - Password: b1gd3m0
• Click **Next**.	

• Based on your network setting, you can adjust the ports used by vCenter. If it is an isolated network environment, leave the default port as they are and click **Next**.	
• Click **Next** until the installation is finished. Now you have completed the vCenter configuration process.	

VMware View Manager Administration

VMware View Connection Server acts as a connection broker for client connections by authenticating and then directing incoming remote desktop user requests to the appropriate virtual desktop, physical desktop, or terminal server. You can run VMware View Connection Server on a 32-bit or 64-bit virtual server. For detailed information about the hardware, operating system, and Active Directory requirements for VMware View Connection Server, see the System Requirements section of the VMware View Manager Administration Guide.

A standard server deployment creates a single, standalone VMware View Connection Server. You can have multiple connection server instances in the same domain and point them all to the same VMware vCenter if desired. For a different Connection Server deployment, such as Replica or Security Server (DMZ), please refer to the View Administration Guide.

Task 1: Installing the Connection Server

When the VMware Installation wizard appears, click **Next**.	
Accept the VMware license terms and click **Next**.	
Select the **Standard** deployment option and click **Next**.	
• Click **Install**. • Click **Finish**.	

Task 2: Configuring and Administrating View Manager

- After you install the VMware View Connection Server, validate your View Manager Administration in a Web browser by entering http://<your-connection-server-ip>/admin.
- Enter the Administrator username and password and click **Login**.
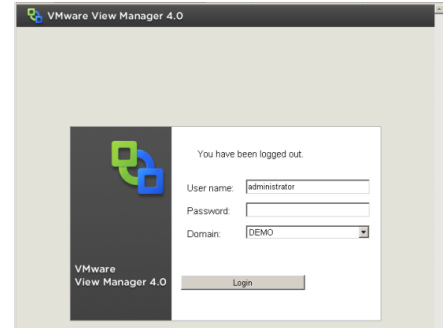
- You will notice a certificate error next to the URL field. VMware View Administrator is accessed using a secure (SSL) connection. The first time you connect, your Web browser might present you with an intermediary page that warns you that the security certificate associated with the address is not issued by a trusted certificate authority. This response is expected because the default root certificate supplied with View Connection Server is self-signed.
- Click **Ignore** to continue using the current SSL certificate.
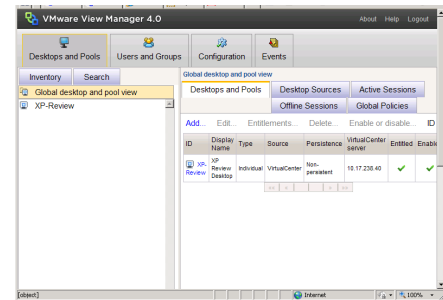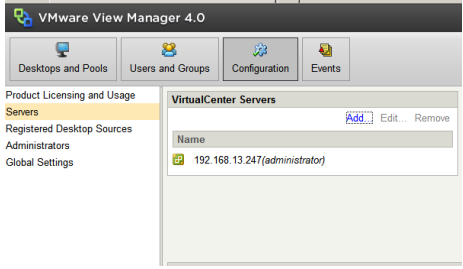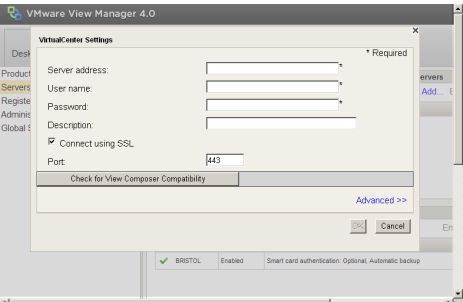
Task 3: Installing the Product License

- From the Configuration tab, click **Product Licensing and Usage**.
- Enter the license key provided with the evaluation.
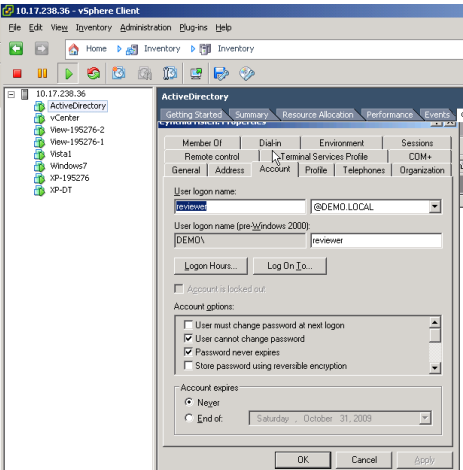
Task 4: Associating and Adding VMware vCenter Server

• From the **Configuration** tab, select **Servers** on the left menu panel. • Select **Add** under the VirtualCenter Servers pane. • Click **Add.**	
• Enter the fully qualified domain name (FQDN) or the IP address of the VMware vCenter Server you want VMware View Manager to communicate with in the **Server address** text box. • Enter Administrator username and password for the vCenter login.	

Note: For evaluation purposes, advanced or optional tasks will not be covered. If you have DNS services installed, you can configure an external URL for the Connection Server. Those tasks are covered in the Getting Started Guide or Administration Guide.
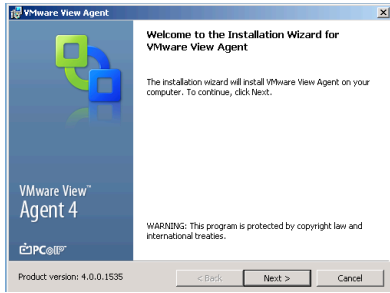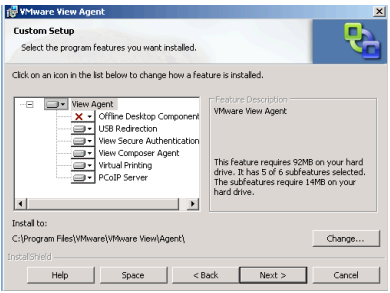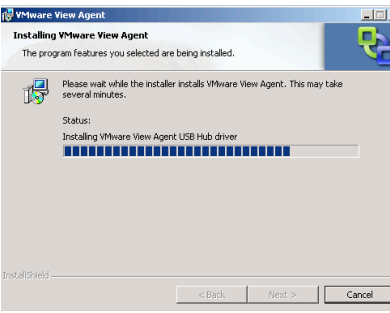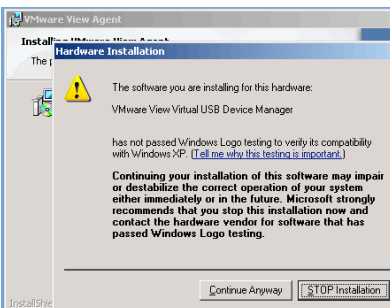
Task 5: Configuring Active Directory Users and Computers
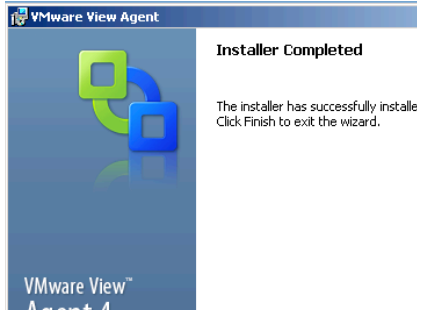
In this evaluation, the virtual machine (ActiveDirectory) is promoted as Domain Controller, hosted in Windows Server 2003 with a single local domain name called demo.local.

• Before you can entitle a user access to the desktop, you need to create three users in the Active Directory named *reviewer_1, reviewer_2, and reviewer_3*.	

Task 6: Creating and Preparing Virtual Machines

The following steps assume that the user has already created a virtual machine and has installed the guest OS (XP/VISTA), joined AD domain, turned on the RDP remote connection, added user groups to the remote users list, and turned off the firewall in the guest OS.
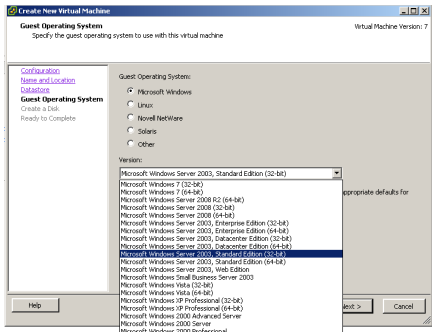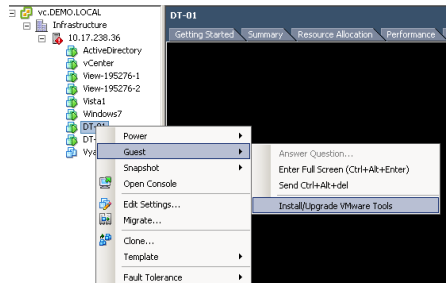
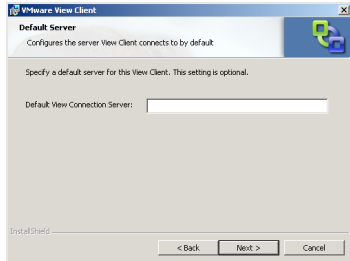|	
• Run the **View Agent** executable on the guest system. • When the VMware Installation wizard appears, click **Next**. • Accept the VMware license terms and click **Next**.	
Select your custom setup options. The offline desktop is optional and does not appear as the default in all agents.	
Click **Install** to begin the installation process.	
Select **Continue Anyway** for the installation alert.	

Click **Finish**.	

At this point, you have the main VMware View components installed and configured. Before you proceed further, you can do a quick ping test from the View Connection Server virtual machine to the Guest Desktop virtual machine and vice versa. The components should be pingable and routable between each.

Task 7: Preparing Virtual Machine Snapshots and Templates

The guest system of the virtual machine, which you create in vCenter, provides the basis for virtual desktop deployment. To prepare a guest system for deployment, perform the following tasks:

• Install the guest operating system. Select **Inventory** from the menu and click **Virtual Machine** to start the creation of a new virtual machine.	
Once you configure the OS and it's up and running: • Install the latest version of VMware Tools (provided with VMware Infrastructure).	

- Configure Active Directory settings: Configure the preferred and alternate DNS servers to use your Active Directory server addresses. For example, on Windows XP, configure the DNS server settings from the properties menu: **Start > Control Panel > Network Connections > LAN > Properties Internet Protocol (TCP/IP) > Properties > Use (VM:ActiveDirectory) IP Address 192.168.13.252**
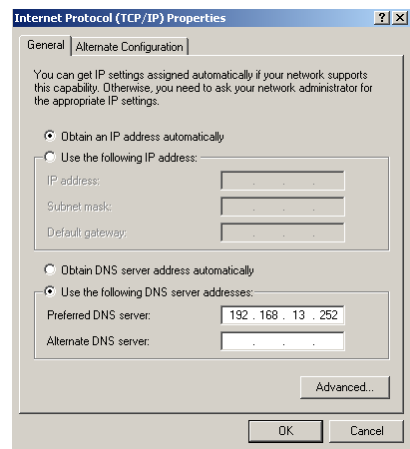
- Make sure that you have administrative rights to the guest system.
- Join the desktop to the AD domain. Add guest system to the domain (demo.local).
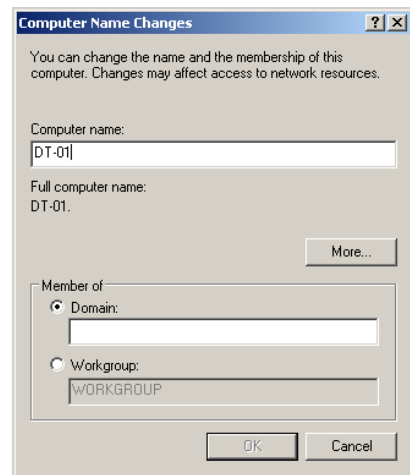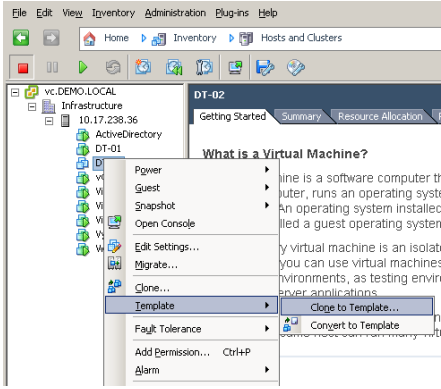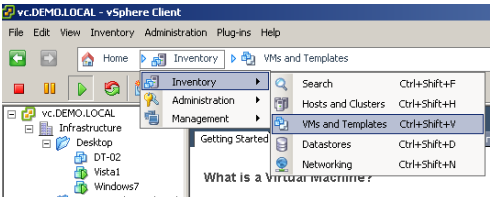
• In Control Panel, turn **Off** Windows Firewall. • In Control Panel, select **System Properties** > **Remote tab**. • Check **Allow User to Connect Remotely**.	
• Take a virtual machine Snapshot — Once the virtual machine template is fully prepared, you can power off the virtual machine and right — click **Guest** and select **Take Snapshot**. • Snapshot is used for Linked Clone creation, discussed in the later sandbox scenario.	
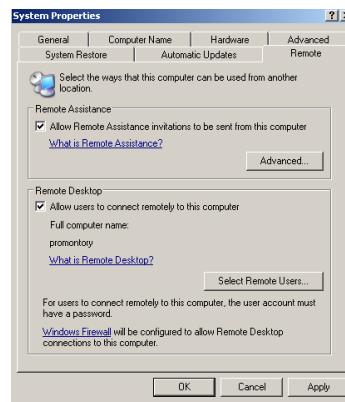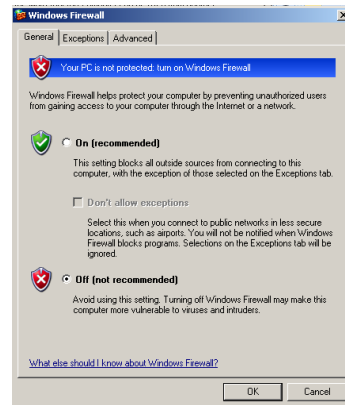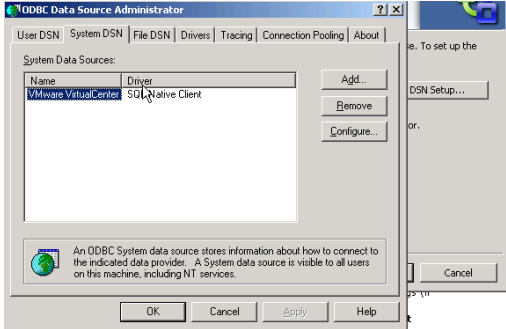
Create a Desktop Template:
 	
• Power off the virtual machine.
 	
• Right-click the previously configured guest system and select one of the following options:
 	
  - **Clone to Template** — select this option if you want to use the selected guest system as the basis for a new template without altering the virtual machine itself. Choose this and walk through the dialogs boxes to create a virtual machine template.
 	
  - **Convert to Template** — select this option if you want to change the guest system into a template. This process happens instantly.	

• To get a quick view of the template created, go to **Inventory** and select **VM and Templates**. The highlighted template will appear in VMware Center.	

You can repeat the same procedures for Windows 7 and Vista desktops with the same configuration if you wish. At the end of the task, you will have three prepared guest systems ready for VMware View Manager to use.

Task 8: Installing VMware View Composer for Linked Clones
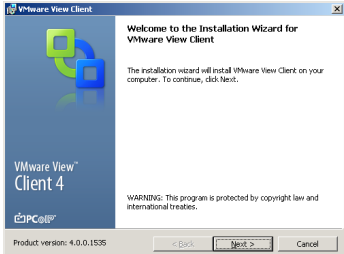
VMware View Composer provides a highly efficient storage alternative to creating and managing many standalone virtual machines. With VMware View Composer Linked Clone technology, you can rapidly clone and deploy multiple desktops from a single centralized base image. Subsequent changes to this image can be automatically proliferated among all desktops in a Linked Clone pool. After the desktops are created, they remain indirectly linked to a snapshot residing on the parent virtual machine. View Composer needs to be installed on the system where VMware vCenter is installed.
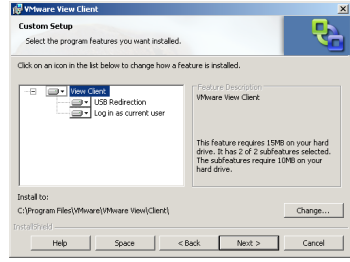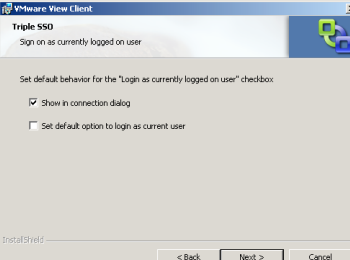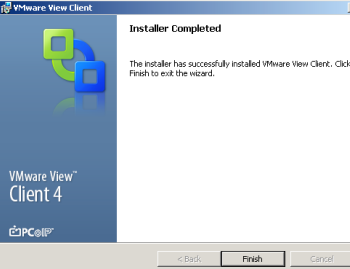
• VMware View Composer installation is optional in the VMware View installation process if you don't plan to have Linked Clone in your production environment. However, with this evaluation you can see the benefits of having VMware View work with VMware vSphere's thin-provisioning feature. Start the VMware View Composer installer you have in your media.	

• During installation of VMware vCenter, the Microsoft SQL Servers 2005 Express instance is provided with VMware vCenter default. Select **System DSN Setup** and type exactly the same SQL Server instance as VMware vCenter.
• Type **VMware VirtualCenter** in the System DSN field.
• Use the system login your created in vCenter where used earlier:
  - Login: Administrator
  - Password: b1gd3m0
• Next, go through the installation and click **Finish** to complete the View Composer installation.	

VMware View Client Installation and Configuration

Task 9: Installing the VMware View Client in the host desktop or thin client (local system)
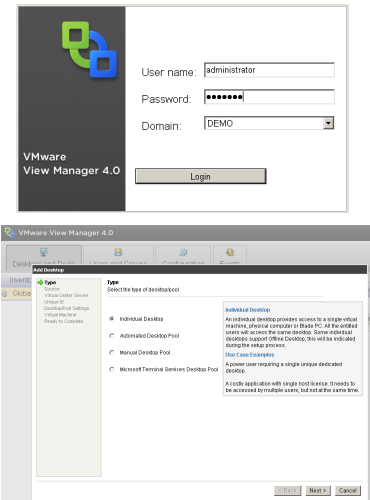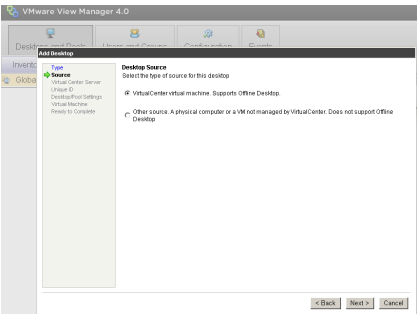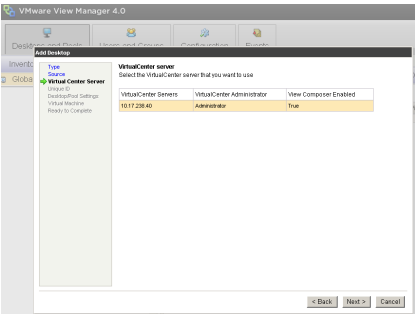
• Run the VMware View Client executable on the system that will host the client, where xxxxxx is the build number of the file: VMware-viewclient-xxxxxx.exe	
• When the VMware Installation wizard appears, click **Next**. • Accept the VMware license terms and click **Next**.	
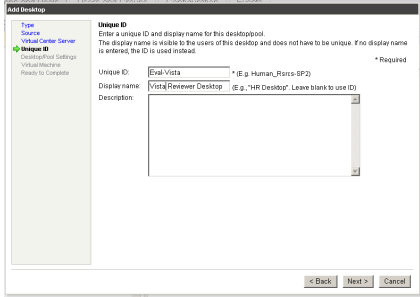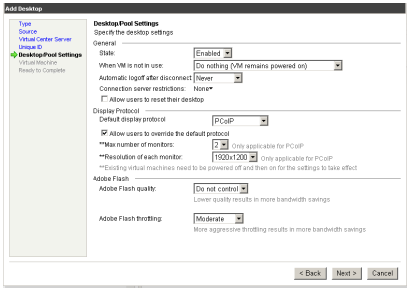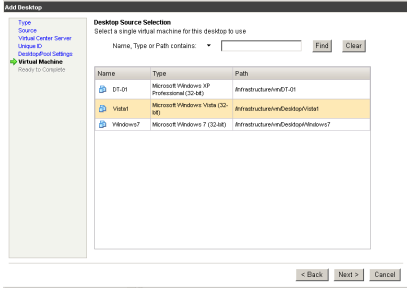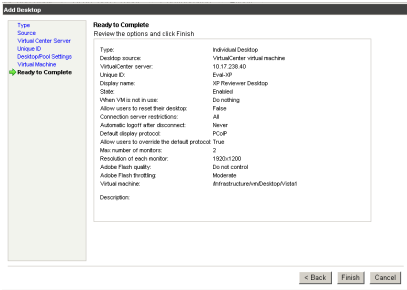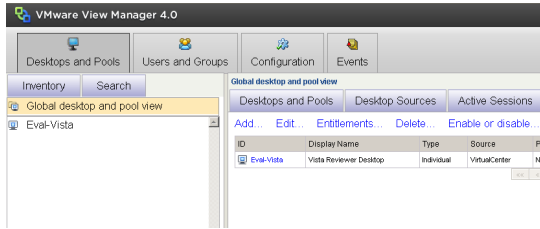
- Choose your custom setup options:
  - Deselect the **USB Redirection** component if you do not want users to access locally connected USB devices through their desktops.
  - Deselect the **Log in as current user** component if you want to require all users to provide identity and credential information to log in to a View Connection Server and again to access a VMware View desktop.
- For this evaluation, simply leave them as the **selected** default. This is a new improved feature, which allows single sign-on to the guest desktop.

- Enter the IP address of the VMware View Connection Server that this client will connect to. For this evaluation, enter 192.168.1.247.

- Leave the login as **current user unchecked**.

- Select **Continue Anyway** for the Virtual USB software installation.

- Select **Finish** and **Exit** installation. If VMware View Client does not start automatically after installation, double-click the desktop shortcut or click
  Start > **Programs** > **VMware** > **VMware View Client**.

Task 10: Adding Desktop Source in VMware View Manager
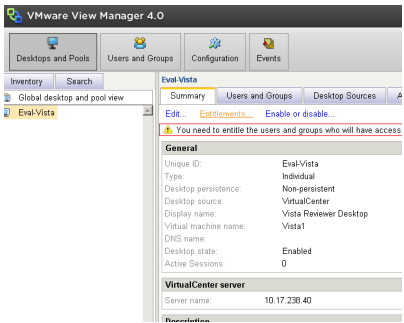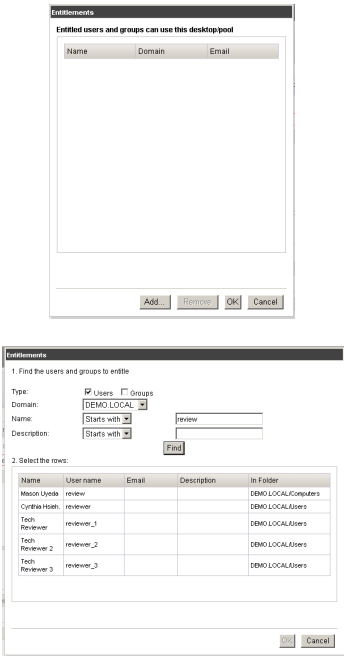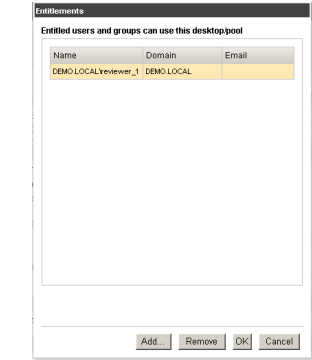
The infrastructure components are now configured in VMware vCenter. Now, go back to VMware View Manager and configure the desktop resource for an individual desktop provisioning use.

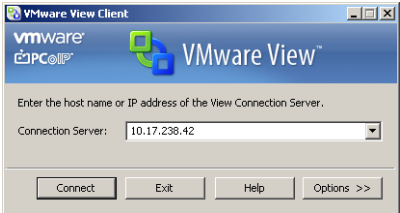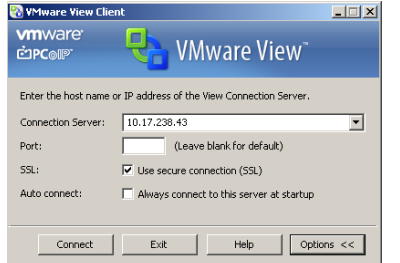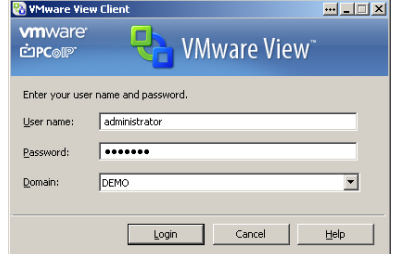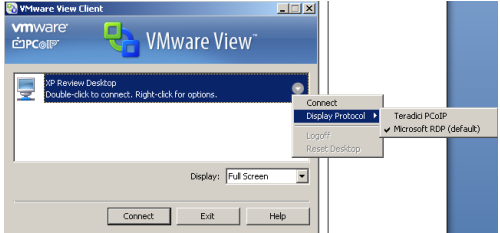|	
• Enter the VMware View Connection Server IP address/admin as the URL in a Web browser. • Login as Administrator. • From within View Administrator, click **Desktops and Pools**, and click the **Inventory** tab. • In the Global desktop and pool view pane, make sure that the **Desktops and Pools** tab is selected and click **Add**. • When the **Add Desktop** wizard appears, select **Individual Desktop** and click **Next**.	
• Select **Desktop Source** from VMware vCenter.	 Need new image
• From the list provided, select the **VMware vCenter Server** to be used by this desktop and click **Next**.	

• Enter the **Unique ID**, **Display name** (optional), and **Description** (optional), and click **Next**.	
• Configure the desktop properties and click **Next**. Since the new PCoIP features are being evaluated, set the default protocol as PCoIP and allow users to change the setting at connection. When set to **Do Not Control for Adobe Flash** quality, bandwidth is not a concern with the LAN deployment.	
• Configure the desktop provisioning properties and click **Next**. • Select the desktop to use as the base image for the deployment and click **Next**.	
• Click **Finish** to complete one guest desktop provisioning.	
• Once the desktop provisioning is complete, you can see a desktop under **Desktops and Pools** tab.	

This shows the basic steps on how to provision one desktop. For more advanced features, you can refer to the VMware View Administration Guide. In a later scenario, a PCoIP pool is created through similar provisioning.

Task 11: Desktop Entitlement

• From within View Administrator, click **Desktops and Pools**, and click the **Inventory** tab. • In the Global desktop and pool view pane, select the desktop or pool you want to entitle and click **Entitlements**.	
• Click **Add**. The user and group entitlement dialog box appears. From here you can view, search on, and filter all Active Directory users within the domain forest. • Select the **Demo.Local** domain created and enter wildcard user match **review**, VMware View Manager should display all users that contain the phrase.	
• Entitle the user **reviewer_1** to use the Vista desktop.	

Figure 6.

Once this is set and done, you will see a green checkmark under **Global Desktop and View** showing Entitled and Enabled for the guest desktop.

Task 12: Accessing Virtual Desktop via RDP or PCoIP

• In the **Connection Server** drop-down menu, enter the host name or IP address of a VMware View Connection Server. • Select **Options**.	 Need New Image
• Select **Log in as current user** to be authorized to log in to the VMware View Connection Server. You will not be prompted to enter login credentials in the guest desktop login. This is an enhancement for single sign-on.	 Need New Image

• Enter the credentials with desktop entitlement:
  - Username: Administrator
  - Password: b1gd3m0	

• In VMware View 4, you have the option to use the preferred protocols of either Teradici PCoIP or Microsoft RDP. Select **Teradici**. • Select the XP desktop you want to access.	

Task 13: Additional Virtual Desktop Optimization

• Adjust **ClearType Settings** in **Control Panel** > **Display** > **Advanced Tab** > **Fonts** and choose **ClearType**.

• Turn off Windows Firewall Settings in **Control Panel** > **Windows Firewall** and select the **Off** radio button.

• Multiple Display Configuration.

• In VMware View Manager Administration, you can centrally configure the desktop monitors that are supported in the local systems.	
• In the guest desktop, check the Display settings that have been changed to multiple displays.	

Note: PCoIP also supports pivot mode for one landscape and one horizontal configuration.

Task 14: WAN Optimization

PCoIP technology uses low-latency image compression algorithms to optimize the user experience for wide area network (WAN) applications. The WAN enhancements dramatically improve the user experience to provide support for multi-media and 3D graphics, audio, and I/O responsiveness over long-distance/high-latency and low-bandwidth networks.

Key PCoIP WAN Capabilities:

• **Reduced Minimum Bandwidth:** To support the lower bandwidth typically available over a WAN, the minimum peak bandwidth required for a PCoIP connection is 1 Mbps. Because PCoIP only transmits changes to the desktop image, the actual bandwidth used may be much lower if the screen is not changing significantly or rapidly.

- **Local Keyboard and Mouse:** To provide instant response over high-latency networks, the mouse pointer can be displayed locally on the desktop (within VMware View Agent) in addition to being sent to the host. Local keyboard capability is also provided to prevent lost keystrokes due to network delay.

- **Packet Reordering:** To accommodate the out-of-order packets often produced by network links on a WAN, the PCoIP portal in VMware View Agent can create multiple packet chains as out-of-order packets received and connect chains to restore the correct sequence. Without this, out-of-order packets can result in data retransmission and delays.

- **Bandwidth-Sensitive Audio Compression:** PCoIP transmits compressed or uncompressed audio–switching dynamically based on the available bandwidth to provide the best possible user experience.

Since PCoIP is integrated seamlessly into the VMware View Agent and fully optimized into VMware View infrastructure, as the administrator, you simply need to configure the desktop protocol and its bandwidth throttling from the administration UI.

Configure Flash contents bandwidth allowance.	

For an optional task to test WAN performance with PCoIP, try to access your corporate desktop from home by connecting through IPSec VPN.

Scenario Overview

This document provides several different test scenarios to review the tasks you performed earlier and experience the combined advantages of using VMware View. To compare a variety of WAN connectivity scenarios, you can consider using either WANEM http://wanem.sourceforge.net/ or Shunra VE SMB Edition Free Trial http://www.shunra.com/ve-smb-trial.php for WAN emulation.

• Scenario 1: Provision and use PCoIP 25 persistent desktops, and one non-persistent PCoIP pool that contains 25 desktops using a Linked Clone. You can adjust the actual number of desktops based on your local storage allowance.

 – Create a snapshot on both Windows XP SP3 and Windows 7

 – Add desktops and pools using automatic pools and Linked Clone

 – Administrate users and entitlements

 – Create fully Linked Clones

 – Configure pools in mixed cluster environment

 – Configure for WAN tag and LAN tag use

 – Delete desktops and pools

• Scenario 2: Configure 50 PCoIP fully Linked Clones in VMware vSphere

 – Create desktops and pools

 – Leverage ThinDisk/Provisioning in VMware vSphere

 – Check storage saving comparison

 – Review VMware VMsafe Security virtual machine functionalities

• Scenario 3: Set-up Triple SSO in VMware View 4 (PCoIP)

 – Use archive directory credentials to login with "Login as current user" checked

 – Access from the Replica View Connection Server and login to see the same session running

Scenario 1:
Provision and Use PCoIP Desktops and Pools

Get Started with PCoIP
PCoIP is a software-to-software display protocol fully integrated with the VMware View infrastructure. The PCoIP portal (server) is installed with the agent. The proprietary SVGA driver is included as part of the PCoIP portal.
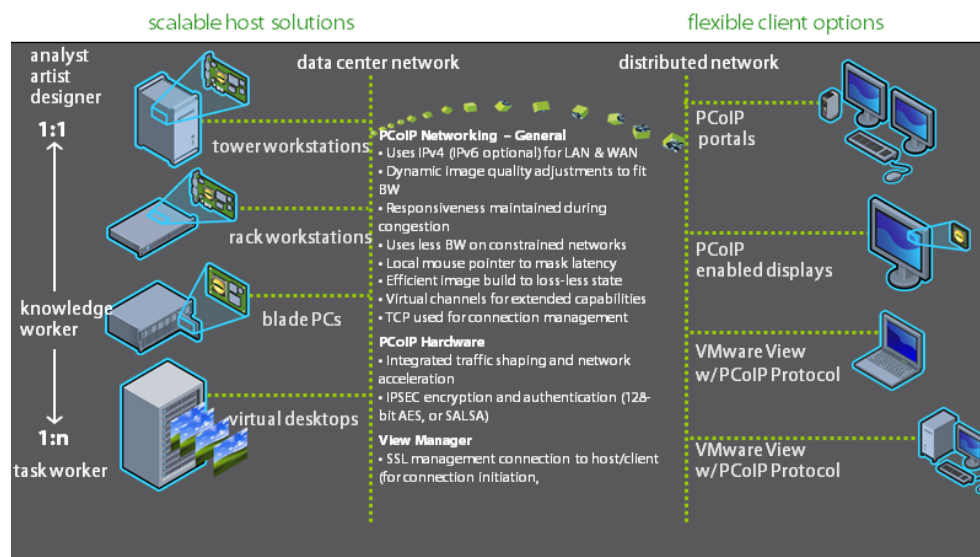

Figure 7.

The PCoIP client is included in the standard VMware View client installation on your end point device, so there are no additional installation procedures required for PCoIP. From the end user perspective, there are no configurations needed for using PCoIP. As an administrator, you can configure the PCoIP protocol through VMware View Administrative Settings/Policies. Default RDP setup is to be tunneled, but the default PCoIP setting is directly connected. Some other configurations on bandwidth throttling for Flash video or on USB redirection policy are consistent as the previous View administration.

Lossy and Lossless Compression
Image compression in PCoIP includes both lossless and lossy compression schemes. Lossy compression allows for higher levels of compression on initial screen change, and subsequent image quality improvement for static screen regions. Lossless motion compensation is also supported. Image compression bandwidth management is supported using packet loss as an indicator of congestion or lower bandwidth limits.

Network Bandwidth and Characteristics
The host to client network connection operates with up to 250ms of round-trip latency. The host to client network connection operates with <0.1 percent packet loss, but will tolerate periods of up to 5 percent packet loss, and will survive short durations of loss of connectivity.

A single TCP connection (SSL) is used between the host and client for session management. A single UDP connection using UDP encapsulated IPSec-ESP [rfc 3948] with AES 128-bit key encryption is used between the host and client for media traffic supporting unreliable and reliable transport. Port numbers, keys, and other connection parameters are exchanged via the SSL connection. You can reference the VMware View Deployment Guide for further end-to-end performance measurements.

Step 1: Creating the Replica Connection Server

The installation package for the Connection Server also contains the installation source for the VMware View Replica Server. Launch the VMware View Connection Server installer and select **Replica server** for the second Connection Server. Select **Agree** to the VMware View product licensing terms.	
A VMware View Replica Server is a Connection Server with its own replica of the ADAM database stored locally. All configuration data and changes are instantaneously replicated to all replica servers, resulting in entirely independent Connection Servers, which can act independently in case of failure of other replica servers. Enter the first VMware View Connection Server instance IP address (View1: 192.168.13.246). Click **Next**.	
Complete the Replica Connection Server instance installation. Select **Finish**.	

Step 2: Creating Linked Clone Pools

DESKTOP TYPE	OS TYPE	PERSISTENT?	DESKTOP COUNTS
PCoIP	Windows XP SP3	Persistent	25
RDP/PCoIP	Windows XP SP3	Non-Persistent	25

The Linked Clone creation process is the same as conducted in the previous section. You can configure the task based on your storage availability and virtual machine sizing.

Step 3: Connecting to Pool by Tags

Tag-based Entitlements
VMware View 4 provides the advanced entitlement to Desktop Pools not only based on current entitlement settings, but also on the Connection Server through which a user logs in. For customers who need perimeter identity (for example: Internal Connection Server or External Security Server access) at logon, VMware View 4 enables users configuring certain clients to go through a particular Connection Server. In this case, a tag is introduced to identify and route the client to the Connection Server. In a broker cluster at a large VMware View deployment. The tag or tags of a Connection Server are then compared to the tag specified in time of the desktop pool creation/edit.

If the tag required by the desktop pool does not match the tag of the broker in question, even if a user is entitled or assigned to a desktop pool, the desktop will not show up in the available desktop list. The Connection Server tags take precedence over the desktop or pool tags.

In this evaluation, you will set up two instances of Connection Servers where brokers have been classified to serve different networks (internal/external for example).

| VMWARE VIEW CONNECTION SERVER IP	NAME	TAG	DESKTOPS	OS
192.168.13.246	View 1	External	10	XP Pro SP3
192.168.13.245	View 2	Internal	10	XP Pro SP3

Use Case
The internal broker might not be visible to users connecting over a VPN. In a case like this, the two brokers could still be formed into a cluster. The external broker might be tagged "External" and the internal broker tagged "Internal" and then pools could be tagged so that some desktops are not visible when a user logs in externally but are visible internally.

For example, imagine a deployment of four Connection Servers where two of the Connection Servers have connected Security Servers. The two Connection Servers without Security Servers are used to support internal users and the two Connection Servers with Security Servers are used to support Internet (external) users. The first two could have a configured entitlements tag of "Internal" and the second two could have a configured entitlements tag of "External".

- The UI allows an administrator to specify one or more tag strings of up to 64 characters for each Connection Broker. You can then specify the tag string required for a specific Connection Broker to access the Pool. At runtime, when a user authenticates him or herself via a Connection Server, an extra step of tag matching is performed. The result will be a filter of the resulting entitled Desktop list.
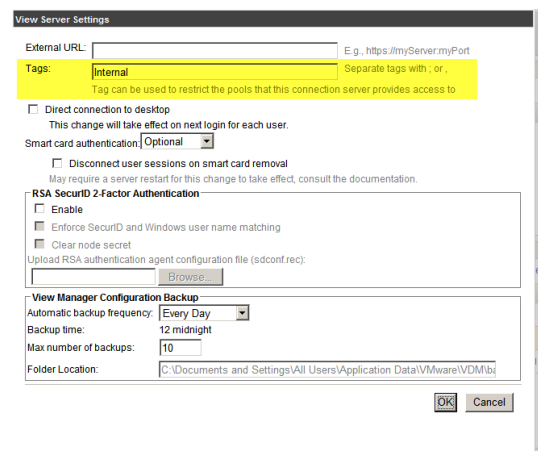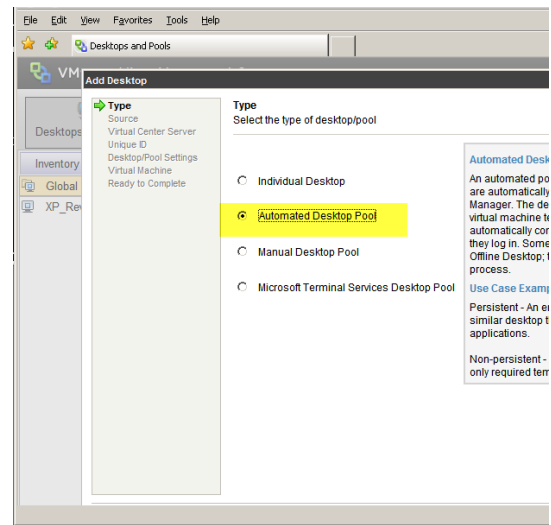

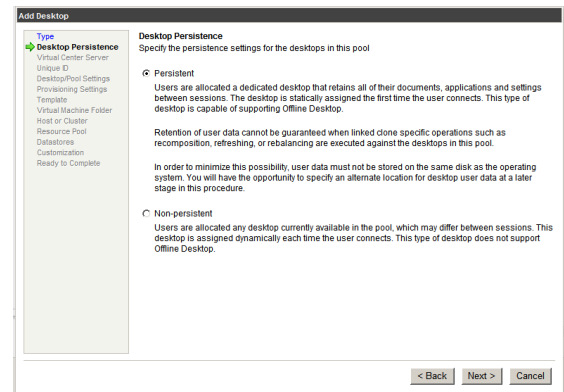- Set the replica server tag as External.
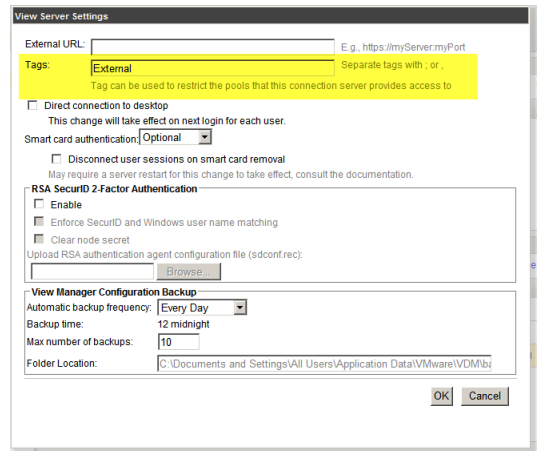
- Once the tags are set in the connection broker, you can see the tag column in the VMware View Manager console is filled with the Tag attributes.
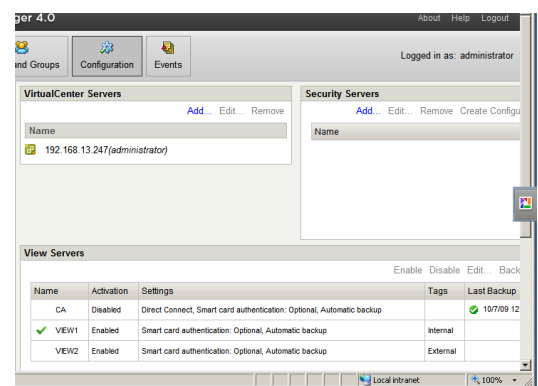
|	
• In the VMware View 1 Connection Server (192.168.13.246/admin), login to the View Manager console, click **Desktops and Pools** tab and select **Add**. You are creating 25 full clone and 25 Linked Clone desktops. Select **Automated Desktop Pool**.	
• Select **Persistent** for the desktop type. • Click **Next**.	
• Create the 10 Linked Clone desktop pools first and go through the same process again to create the full clone – only without checking the highlighted checkbox.	
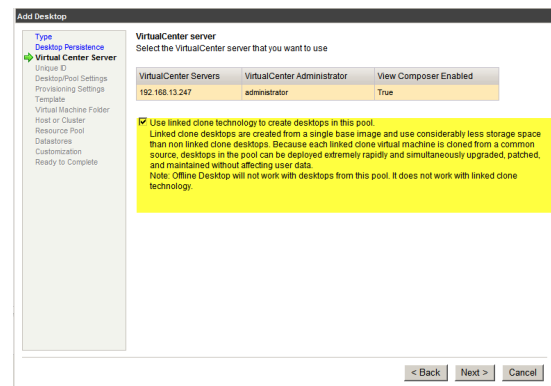
- Fill in the name attribute for the **Unique ID** and **Display Name**.
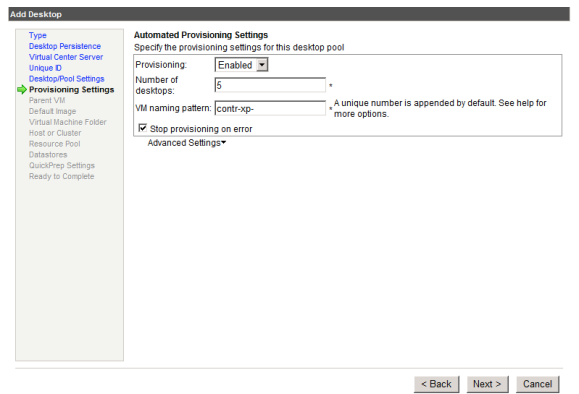
- This is same user interface as you used to create the individual desktop earlier. Leave the default setup as it is.
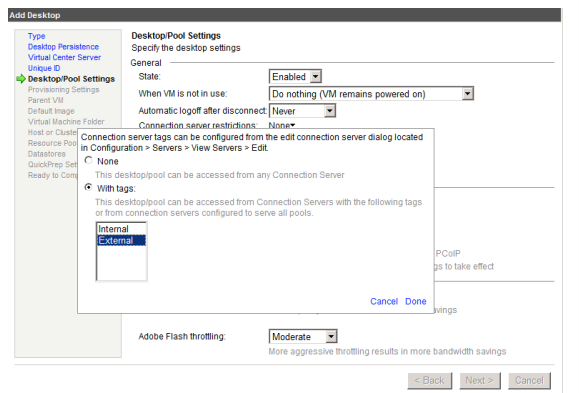

- Enter the number of the desktops that your storage allows you to create. The naming pattern for the desktop is the name vCenter will use to name the virtual machine, so create a unique and easily recognized name.
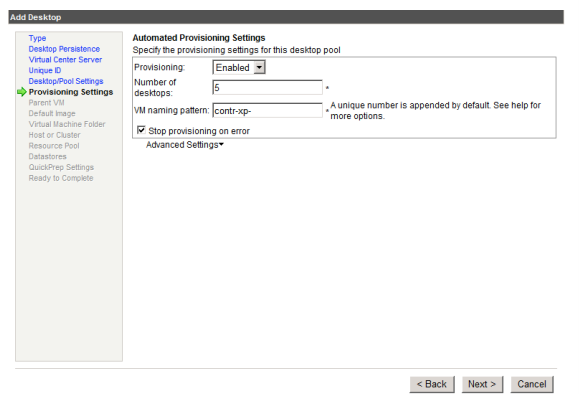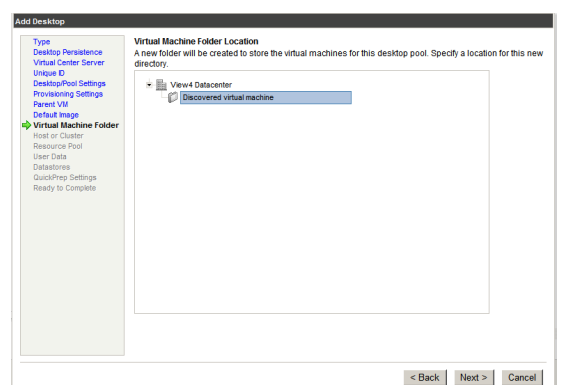
- Desktop cloning relies on the virtual machine template as the base. Previously, you created a template by selecting a clean base template and cloning it to template. Select that template and click **Next**.

- Linked Clone requires the template and snapshot as the golden image.
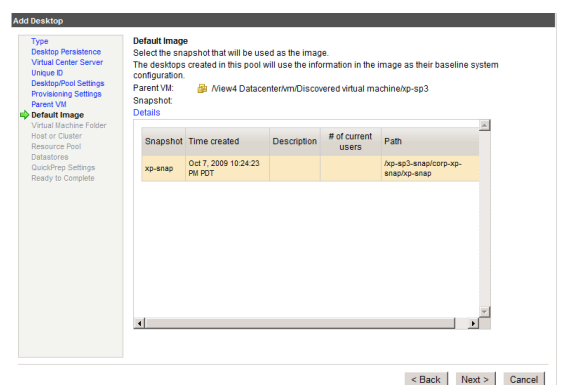
- Select the folder location where the desktops should be organized.

- Select the host or ESX server where the desktop is created. Note the vSphere mode for VMware View Composer option is dimmed and not selectable. It is because the host being used is running vSphere already. If you are using a previous version of ESX, this option will be available for upgrade use.
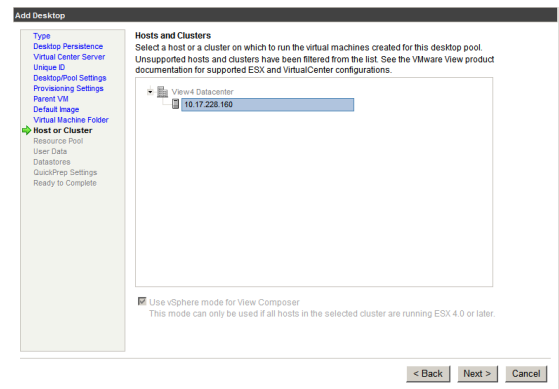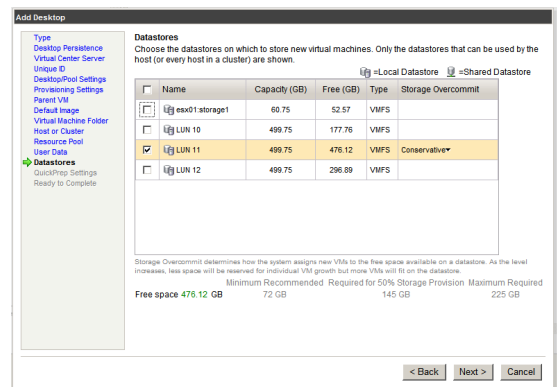
- Add desktops to the resource pool.
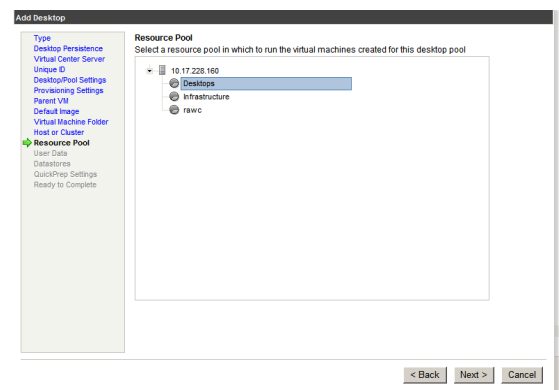
- Allocate user data disk for the persistent data. Keep the default value and select **Next**.
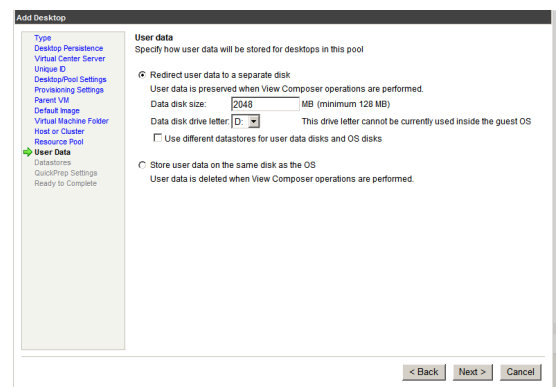
- In this setup, the storage LUN for the better demo effects is attached. You can simply use the local storage host:storage1 for your test.

- You can see that the default domain is filled in automatically by quickprep. This is set at the **Configuration Tab** > **Servers** > **Select View Connection** > **Edit**.
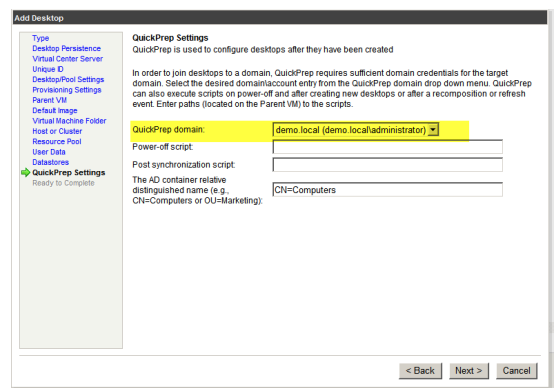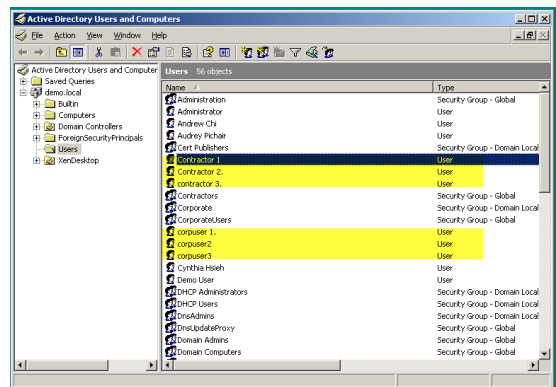

- Do a final review of the Linked Clone setup and click **Finish** to complete. It will take several minutes to create the clones.
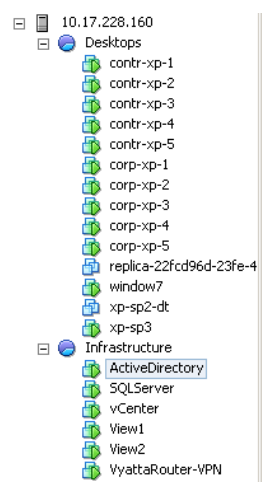
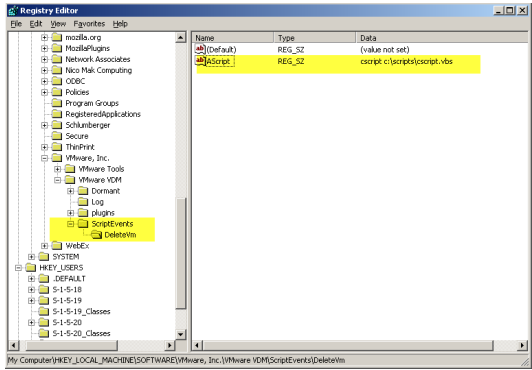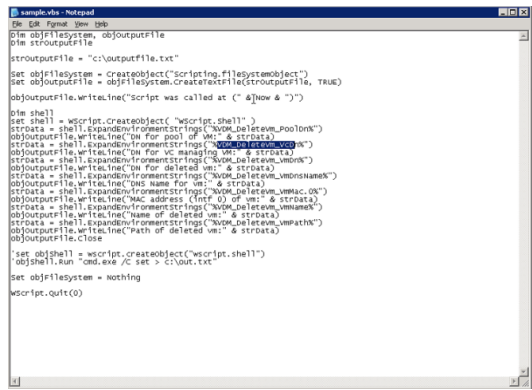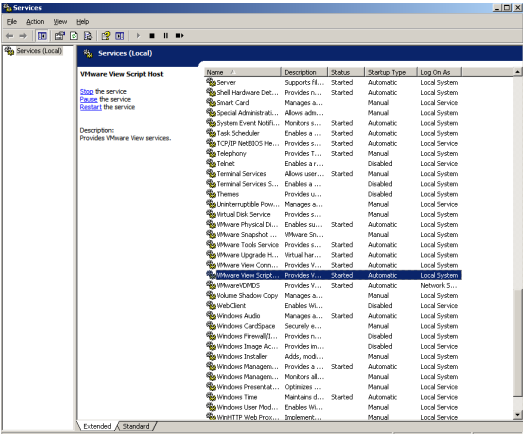|	
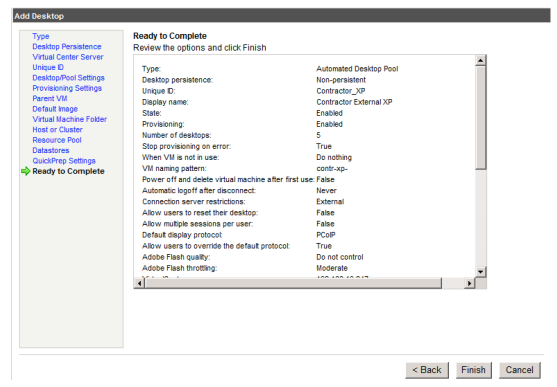
• Create additional users in Active Directory (ActiveDirectory:192.168.13.252)
  - Corporate 1-3 user for the Group Internal
  - Contractor 1-3 user for the Group External
• This will be used for the pool entitlement for users and groups.	

• Access VMware vCenter or ESX management by using the VMware vSphere client.	
• Login to View Manager console. You can see the Linked Clone pools are created and listed in the Desktop and Pool pane. Select **Entitlements** to grant right to access the desktop. • Assign the group you created in ActiveDirectory.	
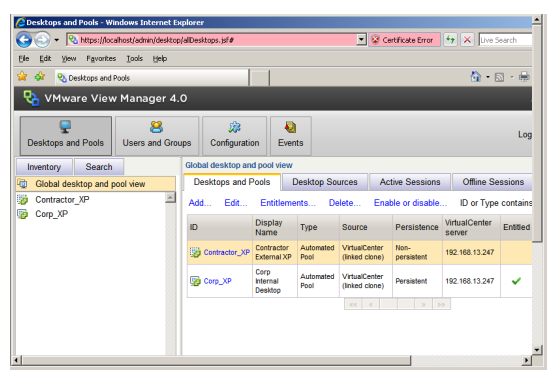
Repeat these steps for creating additional XP desktops with non-persistent and persistent use.

Step 4: Deleting the Clone Using Deletion Script

Provide the cleanup rule and scripting capabilities to enable administrators to perform further integration functions. In some environments, this can be achieved by removing entries from ActiveDirectory. In others, you may need to trigger other applications for a tighter integration.

• A new key needs to be created manually. Please refer to VMware View Administration Guide for further details.	
• The visual basic script can be used to clean up or trigger further application activities. This new feature offers the extensibility framework.	
• Run **services.msc** to access the Services console. Enable the script services manually. It is not started by default.	

- Login to VMware View Manager, Select **Delete the desktop**. Select **Delete from Disk** option. It will trigger the script set previously.
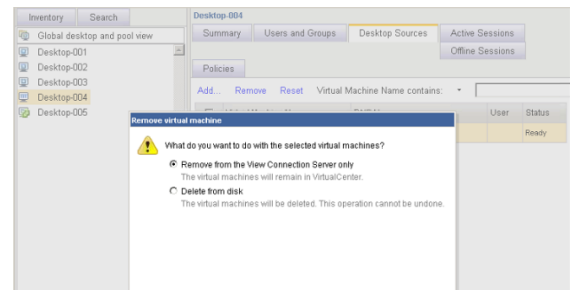
Scenario 2:
Configure PCoIP Full and Linked Clone in VMware vSphere

Create Full Clone with Thin Provisioning

Thin Provisioning in its simplest form means only using the disk space you need. Traditionally, with virtual machines, if you create a 500GB virtual disk it will use 500GB of your VMFS data store. With Thin Provisioning you can create a 500GB virtual disk, but if only 100GB is in use, only 100GB of your VMFS data store will be utilized.
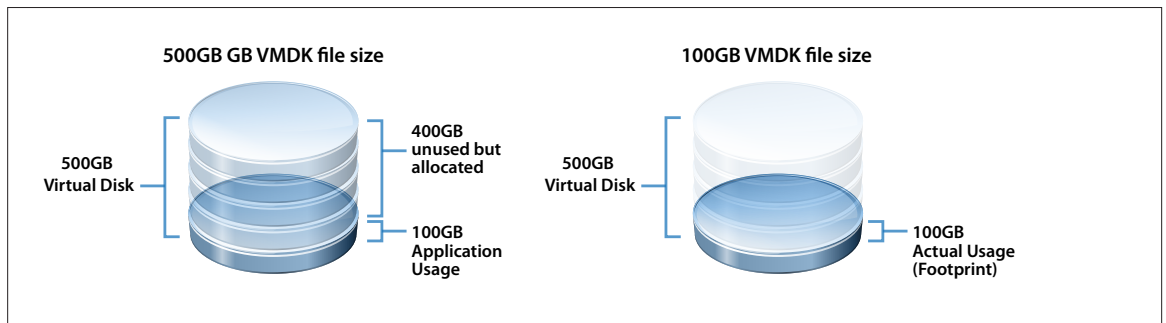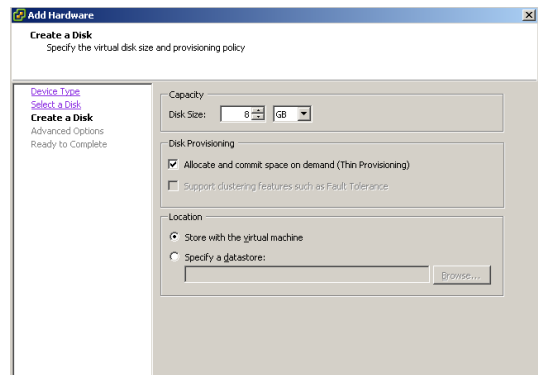

Figure 8.

You can create a five desktop XP pool using Full Clone from VMware View 4 and compare them with the Thin Provisioning option check. The features include increased storage utilization, reduced application downtime, and streamlined capacity management.

- When you create a virtual machine in VMware vSphere, the option to create Thin Provisioning settings is under **Settings** > **Add Hardware**.

- In VMware View 4, you can configure the Thin Provisioning while preparing the Linked Clone base template
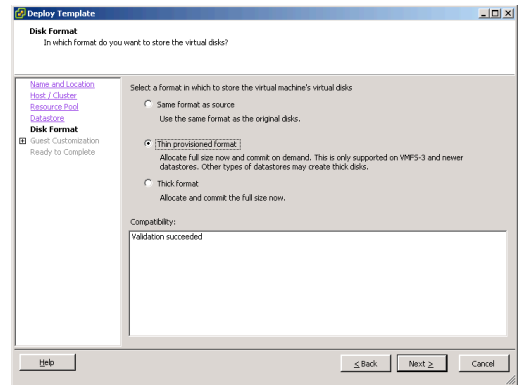
Now, in order to compare the storage usage difference with Thin Provisioning enabled in the virtual desktop deployment, the best approach is to provision them and perform storage comparison with the virtual machines without thin provisioning enabled. Considerations for storage provisioning fall in throughput needs to scale with an increase in capacity, i.e., multiple virtual machines per I/O path.
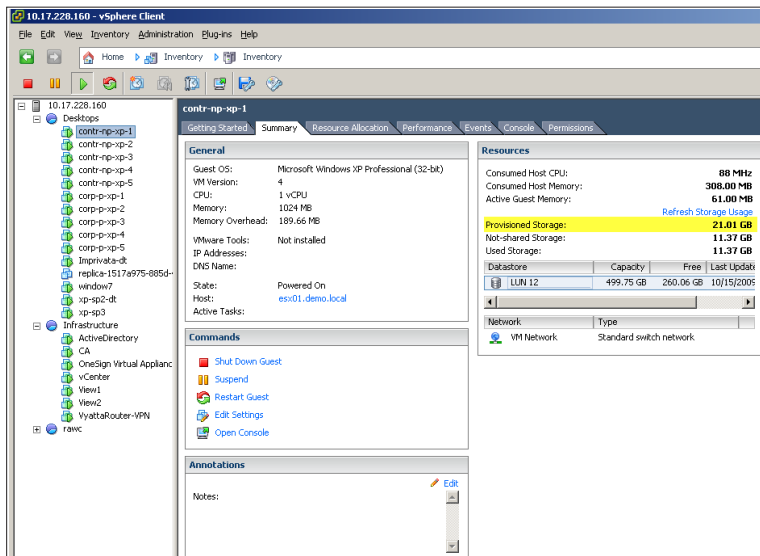

Figure 9.

In the meantime, *transient storage* on the swap space is used only when the virtual machine is powered on and delta disks are used by snapshots and linked to virtual machines.
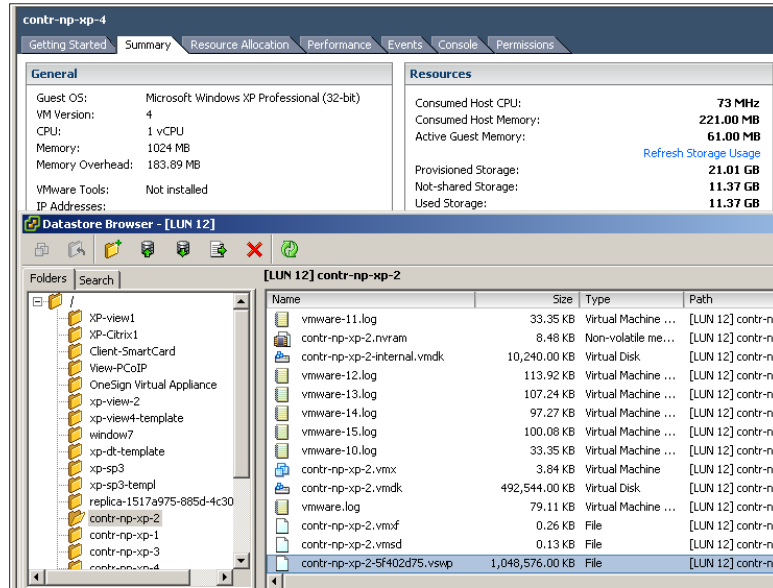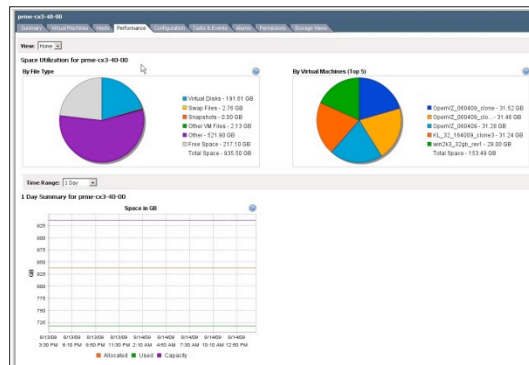

Figure 10.

Datastore View in vSphere
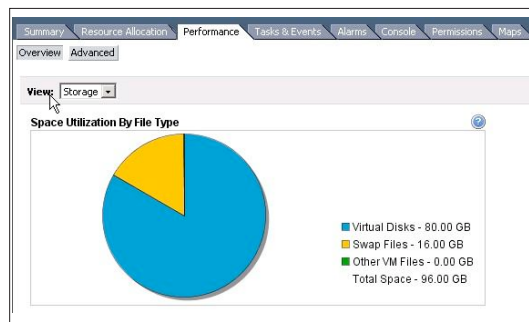

Figure 11.

VM Storage Performance View

Figure 12.

Anti-Virus Protection

The VMsafe API comes with VMware vSphere. VMware offers a number of VMsafe partner solutions that provide secure virtual machines with virus-scanning capability.

• Trend Micro Core Protection 1.0. This is an anti-virus product that performs offline and online scheduled virtual machine scans without an agent. It uses a smaller agent for on-access scanning or to clean up infections. The product is available at: http://us.trendmicro.com/us/solutions/enterprise/security-solutions/virtualization/virtual-machines/index.html

• McAfee Virus Scan for Offline Virtual Images 2.0. This is an anti-virus product that performs offline schedule virtual machine scans without an agent. It complements a regular virus scan agents' online scanning.
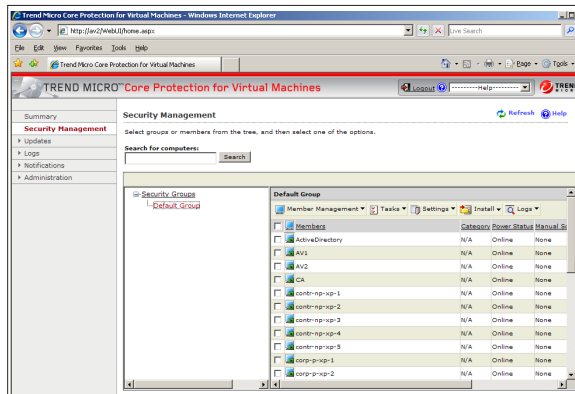
Figure 16.

VMsafe reduces high storage I/O and memory usage during scheduled and pandemic malware scan activities.
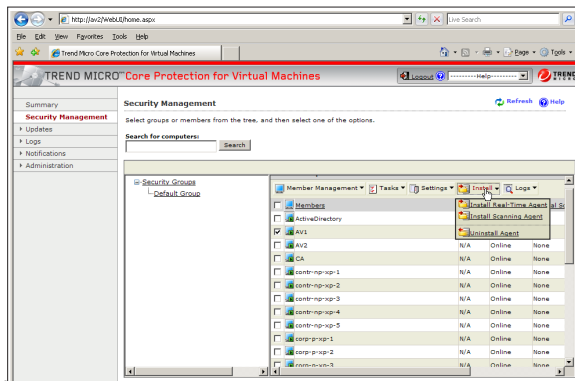

Figure 17.

The above figure shows the anti-virus server committing a real-time agent to an individual virtual machine. It also has the functionality of offline snapshot image scanning.

This is a VMware vSphere feature and is now available for VMware View 4. Please refer to the VMware View 4 Deployment Guide for further product demonstration.

Scenario 3:
Set up Triple Single Sign-On (SSO) in VMware View 4

Log in as Currently Logged-on User

This is a new option in VMware View Client that allows you to log onto the broker using currently logged on credentials. The standard sign up flow using AD credentials is:

• User connects to View Connection Server

• VMware View Connection Server compares a list of trusted AD domains to the client

• User authenticates with username and password

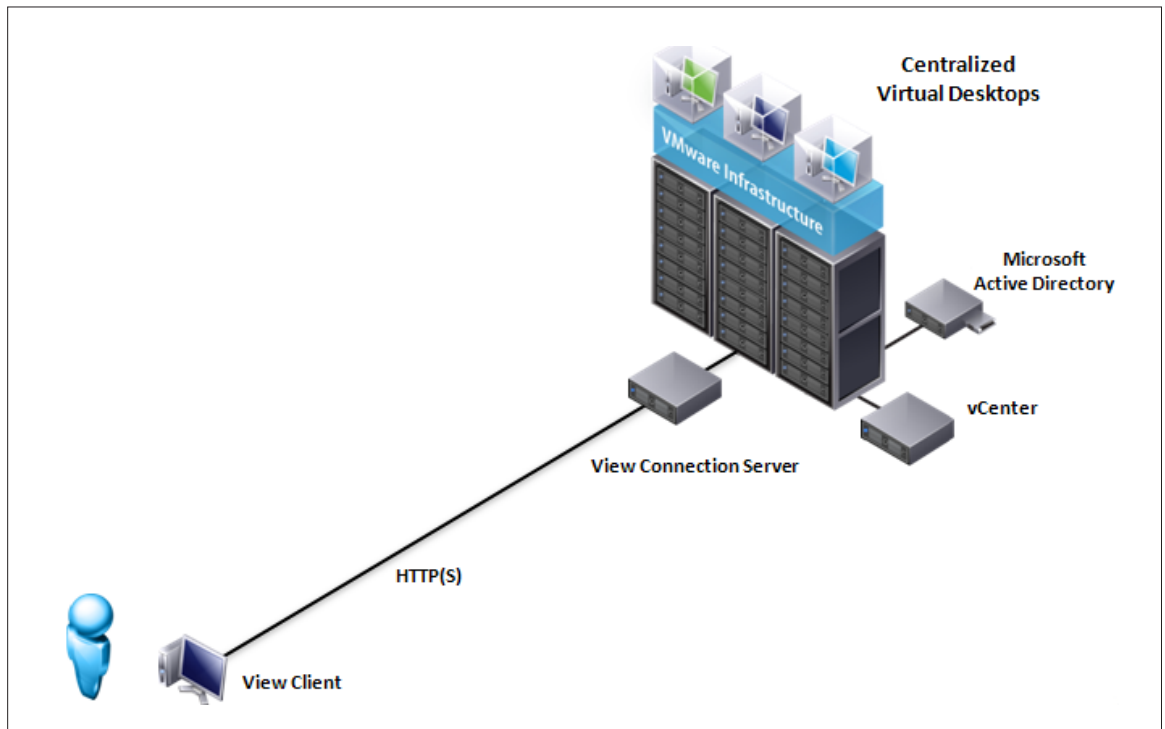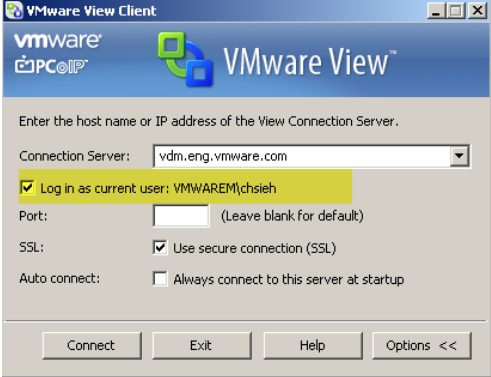• VMware View Connection Server delegates authentication to Windows/AD

Figure 13.

VMware View 4 continues to support the AD credential (username and password) login, smart card, and RSA securID token in RDP.

• During the View Agent installation, select the **Connect as Current Logon User** checkbox option to enable SSO.	
• Launch View Client at local desktop or thin client. • View Client has new **Log in as Current User: Domain User** checkbox. When a user's AD credential is authenticated on the client device using either password (RDP/PCoIP) or smart card authentication in RDP, the Connection Broker will use the same user identity. • This value can also be set using GPO policy or registry key setting. Please refer to the View Administration Guide. • You should be able to login to the guest desktop environment without being prompted to enter the credentials again.	VMware View Client Enter the host name or IP address of the View Connection Server. Connection Server: vdm.eng.vmware.com ☑ Log in as current user: VMWAREM\chsieh Port: (Leave blank for default) SSL: ☑ Use secure connection (SSL) Auto connect: ☐ Always connect to this server at startup Connect Exit Help Options <<

Support Information

For additional evaluation questions and installation support, please address your questions to desktop-tm@vmware.com.

About the Author

Cynthia Hsieh is a senior technical marketing manager in VMware Enterprise Marketing team. She focuses on application integration, proof of concepts, and security subjects.

Hsieh's previous background includes product management positions at Wyse, Trend Micro, Oracle, and Yahoo.

vmware®