

Administering VMware View™ 4.5

By Mike Laverick

© Mike Laverick Ltd

With Contributions and Assistance from

Rory Clements (nee VMware)
Alaric Davies (vExpert 2009/2010)



Report Errors: mikelaverick@rtfm-ed.co.uk

Follow on Twitter: http://twitter.com/Mike_Laverick

Mike Laverick Podcast: <http://www.rtfm-ed.co.uk/podcasts/podcast.xml>

Administering VMware View 4.5

Copyright © 2010 by Mike Laverick Ltd

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, or otherwise, without written permission from Mike Laverick Ltd. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Disclaimer:

The topic of creating a Virtual Desktop Infrastructure (VDI) using many different vendors is the subject of another book. This guide was written with VMware View 4.5 (Beta1/2 and RC) and Windows 7 Enterprise and Windows 2008 Server R2 with Service Pack 2. As such, some of the screen grabs and workflows may be slightly different in the final GA release. However, in the interests of having detailed documentation delivered in a timely fashion – I felt it was best to release this as is, with a view to QA the content as quickly as possible after the GA. Additionally, there may be some system times and dates which appear skewed. This is caused by me writing about a feature in January, and then coming back to the same feature in July. Often only part of the workflow needs changing, so I don't retake ALL the graphics ALL over again. It's a waste of my precious time!

If you do spot a graphic that is incorrect or workflow that seems disjointed please feel free to email corrections and suggestions to mikelaverick@rtfm-ed.co.uk

Author Statement:

This guide is *not* intended to be a complete guide to ALL the functionality of the VMware View 4.5 product. Instead it's intended to get you up and running with the core features of the technology. I would whole-heartedly recommend reading the official admin guide from VMware, as well as attending a training course on VMware View 4.5

Authors Edition

Table of Contents

What's New in View 4.5?	8
Chapter 1: Introduction to Virtual Desktops	9
Advantages of Virtual Desktops	10
Disadvantages of Virtual Desktops.....	11
How most VDI Systems Work	11
VMware View Architecture	13
Chapter 2: Install a Connection Server	15
Chapter 3: Post Configuration of Connection Server	18
Adding in vCenter(s).....	18
Enabling Event Database.....	21
Dashboard View	22
Users and Groups Node.....	24
Chapter 4: Install the Agent in the Virtual Desktop	25
Chapter 5: Install the Local Mode Client	29
Chapter 6: Publish an Individual Virtual Desktop.....	32
Chapter 7: Publish a Dedicated Virtual Desktop Pool	38
Chapter 8: Publish a Floating Virtual Desktop Pool	52
Managing Pools and Desktops	53
Pool Status	53
Unassigning Users from Dedicated Pools.....	54
Maintenance Mode – Taking a Desktop Offline	54
Resetting a Desktop.....	55
Remove a Desktop	57
Remote Session Management	58
Chapter 9: VMware Composer and Linked Clones	60
Install View Composer	62
Enable View Composer in VMware View	63
Prepare Parent VM.....	64
Create the Linked Clone Persistent Pool.....	65
The vCenter Environment after using Linked Clones	74
Fixing Linked Clones Errors.....	76
Chapter 10: Refresh, Recompose and Rebalance	78
Refresh Virtual Desktops in the Pool	78

Recompose a Linked Clone Virtual Desktop	81
Rebalance a Linked Clone Virtual Desktop	84
Chapter 11: Enabling Local Mode	85
Installing the Transfer Server	86
Enabling a Centralized Image Repository	88
Publish the Source Parent VM (Mandatory for Linked Cloned Desktops, Optional for regular desktop pools)	90
Check Out a Local Mode Desktop	91
Check In, Rollback and Backup to Server.....	93
Manage Local Mode Desktops with View Administration	94
Enabling Replication	95
Chapter 12: Enabling "Kiosk Mode"	97
Chapter 13: Publishing Terminal Servers (TS) /Remote Desktop Services (RDS)	98
Chapter 14: Microsoft Group Policies	102
Installing the Remote Administration Tools to Windows 7.....	103
Redirect the Desktop	104
Redirect the Start Menu	110
Removing the HomeGroup Desktop Icon in Windows 7	112
Remove the Libraries Desktop Icon in Windows 7	113
Remove the Control Panel Icon in Windows 7	114
Remove the Users Folder Icon in Windows 7	115
Remove the Network Location Dialog Box	115
Chapter 15: VMware User Experience	121
Global Settings	121
Global, Pool and User Policies	123
Chapter 16: Install a Connection Server Replica	125
Chapter 17: Install a Security Server	127
Chapter 18: Load Balance Security Servers.....	132
Enable Microsoft NLB Clustering for Security Servers.....	133
Test the Load-Balanced Configuration	138
Chapter 19: Create & Apply Certificates.....	139
Add Java Keytool to the System Path	140
Generate a Certificate Request File	141
Submit the Request to the Certificate Authority	143

Chapter 20: Virtual Applications with ThinApp.....	150
Advantages of Application Virtualization	150
Limitations and Requirements	152
Frequently Asked Questions.....	154
Install ThinApp – The “Build” Machine	155
Create a ThinApp Example - Acrobat Reader	155
Publishing a ThinApp	168
Configuring the ThinApp Repository	168
Adding ThinApps into View Server.....	169
Entitling a ThinApp to a Desktop Pool via an Application Group	170
Rebuilding a ThinApp with Custom Package.ini Settings.....	174
Other ThinApp Utilities	176
Chapter 23: Managing VMware View with View PowerCLI	177
Managing vCenter to View Connections	178
List vCenters	178
Remove vCenter.....	179
Add a vCenter to View.....	180
Creating Desktop Pools	180
Creating Pools	181
Creating Manual Pools (Personal Desktop)	182
Creating a Dedicated Pools	182
Creating a Floating Desktop Pools (with Automatic Deletes)	183
Creating Linked Cloned Pools	183
Updating Pool Settings	184
Deleting Pools.....	184
Managing User Assignments	184
Add & Remove User and Group Assignments	184
Viewing User & Group Assignments.....	185
Managing User Sessions.....	186
This is the End of the Book - Conclusions.....	187

What's New in View 4.5?

Below is a very quick bulleted list overview of what's new to the View 4.5 release. It's not intended for those new to the product or to be completely comprehensive.

- In the Beta/RC Programme, PCoIP was still NOT compatible with the VMware Security Server. Sadly, this appears to be still be the case in the final GA. I'm hoping that VMware with retrofit View4.5 with some kind of VPN solution sometime later
- The Virtual Profile (aka Persona Management) feature was withdrawn in the Beta2 version of View 4.5. As such I have removed it from this guide, but will re-instate as soon as VMware adds back in
- New ThinApp Integration which allows you to publish ThinApps to the pool and automate their installation or streaming to the virtual desktop
- New and Improved Administration tools based on Adobe Air
- Folder structures within the View Administration Console
- Integrated Backup of the View server configuration – with auto-backup enabled
- Full Apple Mac OS X Client (RDP only, as yet no support for PCoIP)
- Webpage download for the full client – the ActiveX based client has been discontinued
- Adobe Flash management to change both quality and bandwidth throttling to control the amount of bandwidth used for Flash video content in webpages
- Connection Server Restrictions to allow you to control which connection servers provide the desktop to specific pools
- New Transfer Server role dedicated to providing Local Mode (formerly Offline) desktops
- New Event Database configuration for storing all View events
- A new more streamlined and secure install process for the Security Server, so no need to edit and copy the locked.properties file
- Support for administration with PowerShell and the VMware PowerCLI
- Support for integration with Microsoft SCOM
- Improved controls over the location of the virtual disks that make up the virtual desktop, which allows you to put write intensive data on faster storage – referred to as tiered storage

Whether these enhancements and improvements will help VMware close the gap on their chief rival, Citrix – is a matter of debate. In the past I personally balked at writing a guide to View. I just thought the product was so simple, so basic, and so crude as to not warrant one. With the arrival of View 4.5 my position changed. Its becoming a much more flexible beast – and I felt it was product I could really get my teeth into without feeling I was patronizing my audience.

Chapter 1: Introduction to Virtual Desktops

Before I go any further I would like to outline my experience and some caveats. Firstly, I've been working in the area of thin client computing since the mid 1990s. Before I got into virtualization and VMware, I was a Citrix Certified Instructor (CCI) working initially with Citrix MetaFrame 1.8 on Windows NT4 Terminal Service Edition and more or less ending with Citrix Presentation Server 4.5 on Windows 2003. Before VMware came along and eclipsed my Citrix work – my main product was Citrix. Secondly, I don't believe in panaceas. There are things I still really love about the Citrix product range, and indeed I still continue to use a Citrix Presentation Server to connect to my remote lab environment, which is held in co-location in the UK. So my message is this – fully research the advantages and disadvantages of ALL the remote desktop and application delivery options now available. When I started if you wanted to deliver a desktop or application to a user down-the-wire there was only ONE real way to do it – Citrix. Now we are bombarded daily with complementary and competing solutions, for example:

- VMware View
- VMware ThinApp
- Citrix XenDesktop
- Citrix XenApp
- Microsoft Remote Desktop Services (RDS)
- Microsoft App-V
- Quest Software vWorkspace
- Xenocode Virtual Application Studio
- Sun Virtual Desktop Connector (VDC)
- HP Client Virtual Software (CVS)
- ThinPrint
- UniPrint

VDI is essentially the same as Terminal Services (TS) or Citrix XenApp (formerly MetaFrame/Presentation server). That is to say, you provide a desktop to the user via a "thin" protocol. The difference between server-based computing and virtual desktops is that rather than having many users connected to one shared TS or Citrix Desktop running a server OS, users connect to their own personal desktop running a desktop OS. By virtue of VDI making use of a non-shared desktop OS, application compatibility issues that can plague a TS environment are almost completely mitigated. A variety of protocols exist to deliver the remote desktop, including the older legacy Microsoft RDP, and the newer VMware PCoIP, Citrix HDX and Microsoft RemoteFX protocols. These new protocols attempt to address some of the persistent graphics rendering limitations of the older display protocols. The advantages of VDI are many, but

its key advantages beyond the benefits of Thin Client Computing generally lie in remedying some of the limitations presented by the shared desktop approach of TS and Citrix XenApp:

Advantages of Virtual Desktops

- One user's activity does not directly affect the performance of other users. Each user is limited to the resources within their VM
- Applications install natively to the Windows environment. There is no need for complicated installation routines and validation to make applications work in an environment for which they were never actually designed. However, many people also like to complement their virtual desktop environment with a virtual application solution like VMware's ThinApp or Microsoft's App-V
- Desktop Hardening. The process of locking down the desktop - whilst desirable in VDI - is not mandatory. In TS & Citrix XenApp you absolutely must lock down the desktop to stop one user affecting the stability of the environment for other users using the shared desktop
- VDI allows you to leverage your corporate license agreement with Microsoft at no additional charge depending on if you have a Software Assurance (SA) agreement in place with Microsoft - without it the fee is around \$100 per seat., whereas each Citrix XenApp end-user connection requires a license from Citrix. Indeed, Microsoft went so far as to introduce a specific licensing model currently called the VECD (Vista Enterprise Centralized Desktop) program to promote the use of Windows as the operating system in the virtual desktop. This has been since superseded by a new model called VDA. It's by no means mandatory that you must use Windows as the guest operating system in a VDI project. You could use a Linux desktop distribution if you prefer it or your needs require it. This said few VDI environments run with just the virtualization layer and a virtual desktop on its own. Nine times out of ten there will be some type of VDI Broker server that will also need licensing!
- VDI can be coupled with other application virtualization tools such as Microsoft's App-V or VMware's ThinApp to reduce the footprint of the virtual desktop (because less is installed to Windows) and also allow for advanced features such as being able to run many different versions of the same application (flavours of Microsoft Word and Adobe Acrobat, for instance) on the same virtual desktop
- Features such as VMware View's Local Mode Desktop that allows an end-user to take a copy of the virtual desktop from the ESX host and make it available on the PC/Laptop even when they are not connected to the corporate network. Local Mode Desktop uses deltas to make sure only changes are synchronized back to the server copy of the VM, and a TTL value that allows for the offline desktop to work only for a limited period. In years to come these Local Mode VMs will be available to a client-based hypervisor as well

- VMware View3 introduced View Composer to enable a linked clone feature. This allows for one single master VM from which many virtual desktops can be created (the linked clone). These linked clones contain only the changes the user makes during the virtual desktop session and, as such, massively reduce the disk space required to run virtual desktops. However, linked clones can introduce other complications around storage capacity management and performance.

Disadvantages of Virtual Desktops

- Printing is a huge challenge in the world of thin-client computing. By far the biggest challenge is the amount of bandwidth used to send a print job from the remote datacentre back to the end-user's physical printer. It's quite common to see Microsoft PowerPoint print jobs balloon in size to hundreds of megabytes. Some thin-client vendors have their own solution using some kind of universal PCL printer drivers. Some organizations prefer to buy in a third-party printing solution such as ThinPrint or UniPrint. In View 3, VMware acquired a license for the core ThinPrint product that they call virtual printing. This licensed version of ThinPrint should be good enough to address most printing needs
- The most common VDI protocol is still Microsoft RDP. RDP has been shown not to perform as well as Citrix's ICA Protocol – and to be especially weak in the realm of multimedia, flash-based web-pages and graphically intensive applications such as CAD. As I mentioned earlier, Microsoft, VMware and Citrix all include new protocols (RemoteFX, PCoIP, HDX) to improve the client protocols used to connect to Windows Vista and Windows 7.
- Storage is quite a significant penalty in VDI. However, with the advent of de-duplication technology from storage vendors such as NetApp, and the introduction of thin provisioned virtual disks in vSphere4, this becomes less significant. As I have already mentioned, VMware had effectively created a kind of built-in de-duplication process with View Composer. If you combine thin provisioning from your storage vendor with thin-provisioning from VMware together with the linked clones feature, you are really doing your level best to reduce the disk foot print of your virtual desktop environment. It's worth stating that for modest VDI solutions local storage is a viable option, but remember that storing a VM on local storage means you cannot use a whole host of VMware features you may take for granted such as HA/DRA/DPM and automation via VUM.

How most VDI Systems Work

Despite the variety of solutions that now crowd the virtual desktop space, as you might expect, they all work in very much the same way and offer very similar features. Most will have a broker component which acts as an intermediary between the user and their virtual desktop. The job of the broker is to provide a

logon process after which the end user can select their desktop. Very often this connection will be based around a certificates-based SSL connection rather than relying on Microsoft RDP Security. This broker will also integrate with the management system to allow you to create pools (groups) of desktops for different purposes – a Sales Desktop pool and an Accounts Desktop pool for example. It will also integrate with Active Directory to allow you to allocate the right virtual desktop to the right people.

At the end user's side, they can either use a webpage to log in or a dedicated client. Frequently, the full client will offer a higher level of features to the end user than an ActiveX or Java client can provide. There will normally be some kind of agent installed in the virtual desktop that allows the user to connect to the virtual machine. Frequently, this agent will support advanced features such as two-factor authentication with technologies such as RSA's SecureID, and the ability to redirect USB connections between the virtual desktop and the end user machine. This allows the user to login with very high security and, for example, still use a USB-hosted printer sat on their desk.

For "Dilbert" or call centre-style users, you might even want to go so far as replacing the physical desktop PC with a thin client sometimes referred to as a dumb terminal (I've often wondered why they aren't called Smart Terminals!) which only offers a screen, keyboard and mouse interface to the virtual desktop. However, advanced variants of these devices can also include 3d graphics cards which enable significantly improved local rendering of complex remote desktops. There are two main types of dumb terminals, the first type has some kind of low-level operating system embedded in the client such as Windows CE, Windows XP Embedded or Linux. These clients can be flashed with new firmware updates remotely. The other type of dumb terminal is the Zero Client - they are very similar to the first type, but Zero Clients have no operating system or firmware to manage.

There are many, many of these devices available. It's well worth asking an OEM Vendor for samples of their devices so you can test them against your VDI environment since they vary massively in quality, reliability and functionality. To be brutally honest, they can be rubbish and a downright PITA. Some popular vendors of smart terminals and zero clients include:

- Wyse
- ChipPC
- Pano Logic
- NeoWare (now acquired by HP)
- Sun Sunray
- OEMs – All the major OEMs such as HP, Dell, and HP have some kind of Thin-Client Device

VMware View Architecture

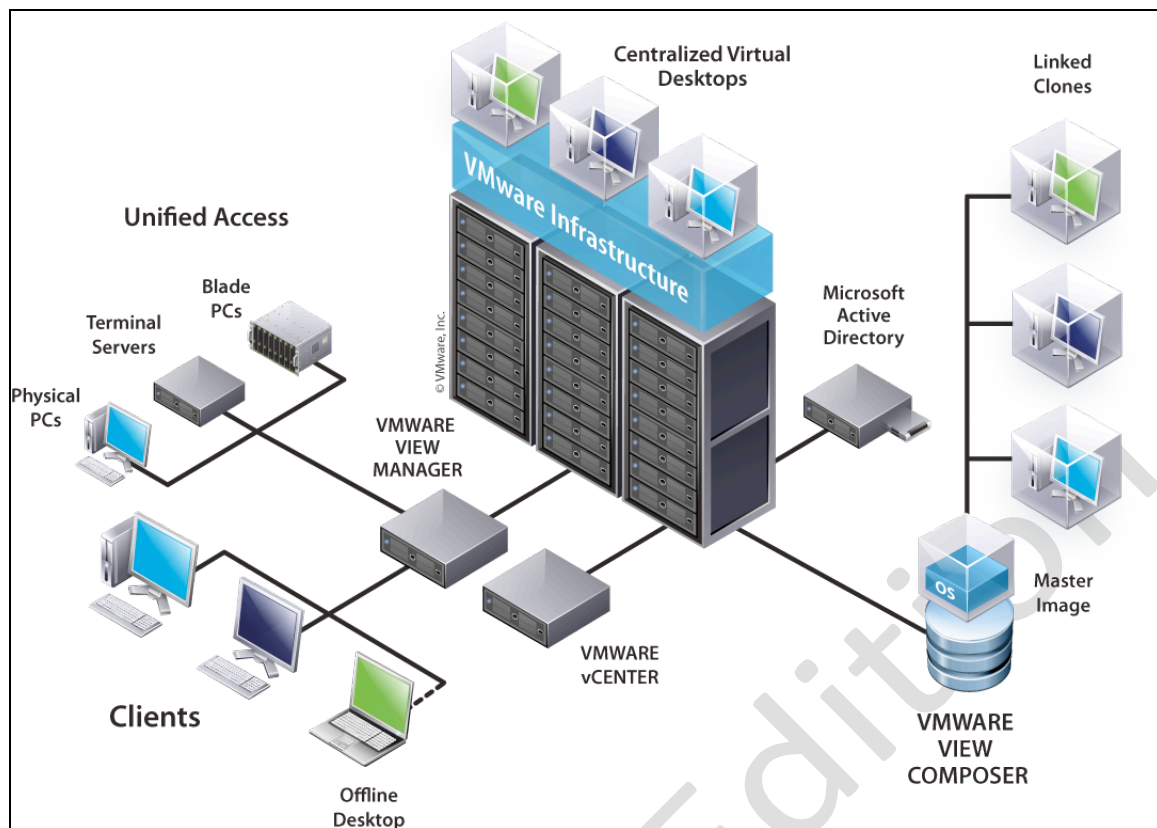
VMware View (formally called VMware Virtual Desktop Manager – VDM) ships as different .exe files when you download it from VMware’s website

- Connection Server (includes Connection, Replica, Security, and Transfer Server roles) – the broker
- Composer – the component which builds thin provisioned images
- Agent – installs in VM OS to provide additional VDI features
- Client – installs in end user OS
- Client (with Local Mode desktop support) – if available, enables Local Mode (aka offline) VDI

Since VMware View 4.5, these binaries are available in a 32-bit and 64-bit formats for both the client and server components. In this guide I’ve decided to use the 64-bit for the server components. As Windows 2008 is the last 32-bit operating system from Microsoft I’ve made the decision to move over to 64-bit in my environment.

The Connection Server is VMware’s term for a broker, and it actually comes as two types of server - a Security Server that can safely be placed in a DMZ, and the Connection Server which sits inside your private network and requires access to your Active Directory environment. The Security Server and Connection Server can be linked together to allow seamless and secure traversal of your firewall, while at the same time delivering corporate services such as email. Both Connection and Security Server roles encrypt the network link between the client and virtual desktop – essentially wrapping a SSL tunnel around the relatively insecure RDP communication. However, only the Security server is safe to be placed in a DMZ as it does not need to be a member of your Windows domain, and it can be hardened using standard procedures such as disabling unwanted Windows services. In VMware View 4.5, a new Transfer Server role exists which is used to manage and accelerate the download of Local Mode virtual desktops.

Below is a pretty typical diagram of the View 4.5 infrastructure. It’s missing some components such as the Security Server and the Transfer Server roles, so it is very much a LAN representation of the infrastructure. The main thing to say from a network perspective is that the Connection Server will need IP visibility of your client devices and the vCenter server in order to broker connections to your centralized desktops. Additionally, the Connection Server does need to be added into your Active Directory domain structure in order to correctly authenticate end users.



All in all, the experience for the end user is like sitting on a trusted network at the corporate office, but remotely. The VMware Composer is a piece of software that manages your templates that are used to create many virtual desktops. Specifically, the Composer enables the functionality of creating a Master virtual desktop from which all end-user virtual desktops are created. Changes to this Master virtual desktop may be proliferated to all its associated virtual machines.

It is possible to have more than one Connection Server and Security Server for fault tolerance. VMware uses Microsoft Active Directory Lightweight Directory Service (AD LDS) as the method of making sure that all the connection servers share the same configuration data by replicating this configuration information in a multiple-master model that is exactly like Microsoft's Active Directory service.

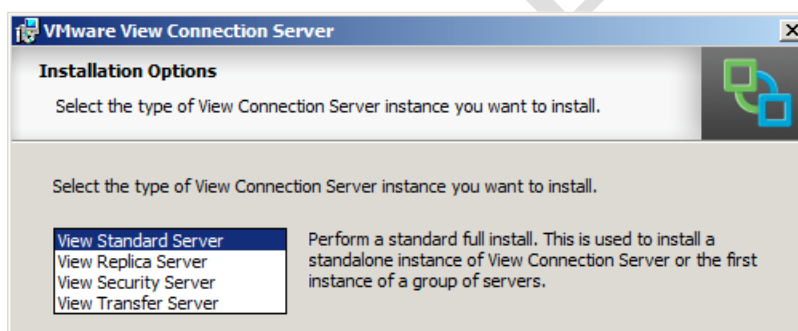
However, VMware do *not* currently offer a method to balance the load dynamically across the Connection Server and Security Server. This means you will have to invest in some method that ensures an even distribution of user connections across them. For example, in the old Virtual Desktop Manager (VDM) course, I used to use the free load-balancing virtual appliance called Hercules as a load balancer. In this guide, I am going to use Microsoft's Network Load-Balancing (NLB), however if you are really serious about IP-based load balancing then I would recommend sourcing a dedicated appliance for this role.

Chapter 2: Install a Connection Server

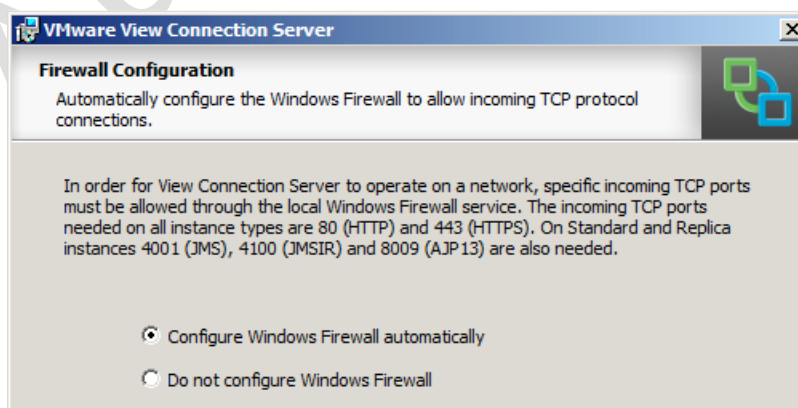
Installing the Connection Server is a breeze, and most of the real work happens in the post-configuration stage that is carried out using an Adobe Air-based administration tool. VMware recommends a minimum of at least 1 vCPU for the Connection Server, together with 2GB of RAM. At the time of writing the CS is available in a 32-bit and 64-bit edition.

1. Create a new Windows 2008 VM and join it to your Active Directory Domain
2. **Double click on the VMware-viewconnectionserver-N.N.N-NNNNNN.exe** file
3. **Accept** the usual suspects on **the Welcome Screen, EULA and the install path** for the software
4. Select 'View Standard Server' from the list

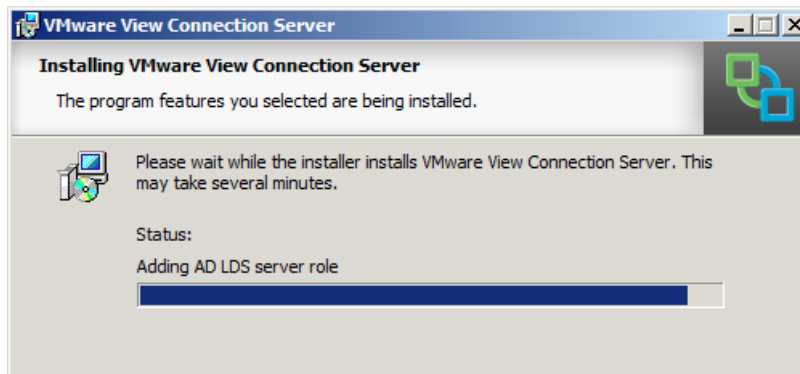
This choice is always used to create the first Connection Server, whereas 'View Replica Server' is used to add a second or third Connection Server. 'View Security Server' is used to add the Security Server role for the DMZ.



5. Next you will be asked if you would like the Windows Firewall configuration settings to be adjusted for VMware View to work correctly: Select this choice.

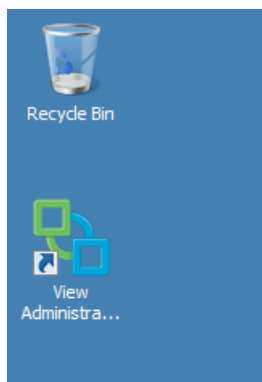


During the process the installation will create a Microsoft AD LDS instance, and you will receive messages about importing a schema using a .LDF file – at no stage is the Schema Master of the Active Directory Domain modified

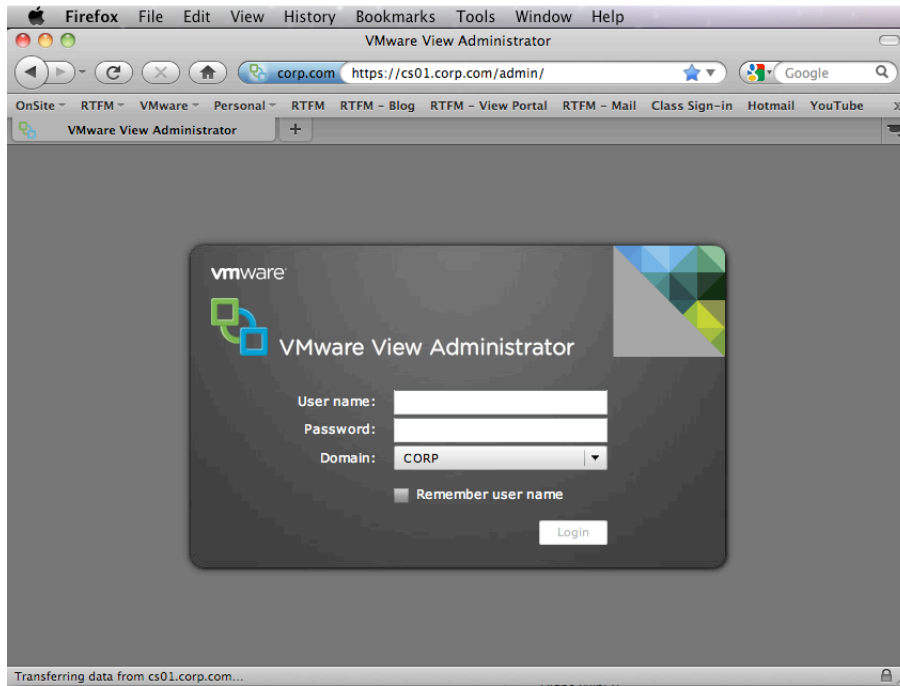


Note:

Once the installation has completed you are presented with a VMware Administrator Console icon on the desktop of the VMware View server. This icon merely opens a web browser at <http://localhost/admin>



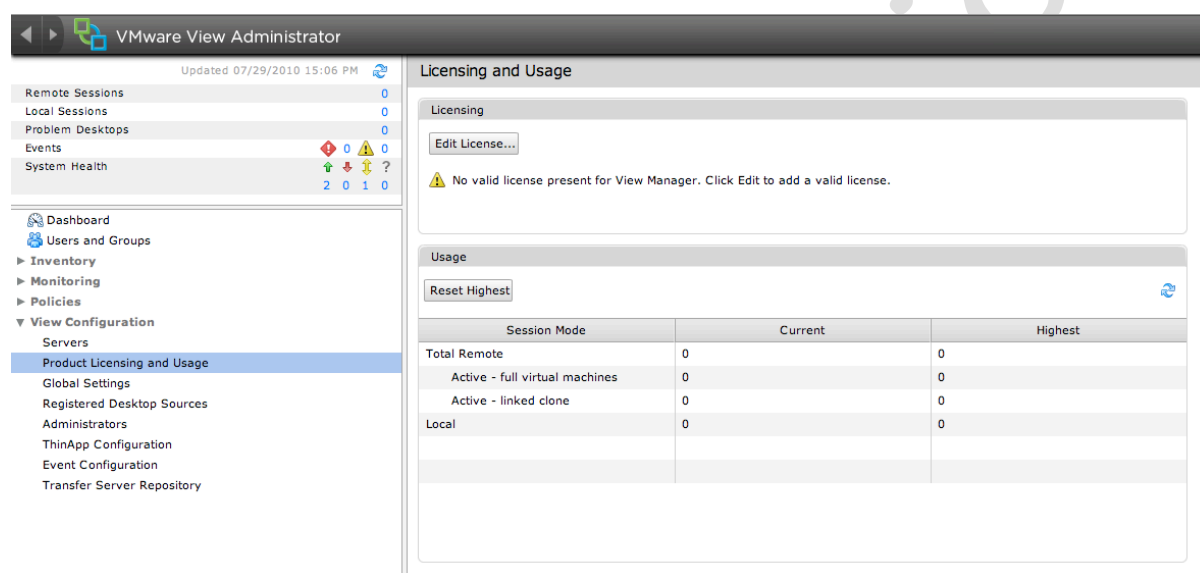
In a clean installation of Windows 2008 you will need to download and install the Adobe Flash Player. Be aware that there can be security implications to having Flash components present on a server. Be attentive to security bulletins, and patch promptly if advised of an issue. Once installed, you can reload the View Administrator Console and login with your administrator account:



Authors Edition

Chapter 3: Post Configuration of Connection Server

The Connection Server administration webpages are very simple and easy to understand. In many respects the management of the Connection Server could even be carried out by a very able desktop support person. If you are a VMware Professional, you could perhaps set up the system, but hand it over to desktop support personnel to manage on a day-to-day basis. Like many modern administration tools the webpage opens to a dashboard view. There are four main views - Inventory, Monitoring, Policies and View Configuration, as the screen grab below shows. The administration tool has detected that we are currently not licensed:



The screenshot shows the VMware View Administrator interface. The top bar indicates the application is updated on 07/29/2010 at 15:06 PM. The main content area is titled 'Licensing and Usage'. Under the 'Licensing' section, there is an 'Edit License...' button and a warning message: 'No valid license present for View Manager. Click Edit to add a valid license.' Under the 'Usage' section, there is a 'Reset Highest' button and a table showing session usage.

Session Mode	Current	Highest
Total Remote	0	0
Active - full virtual machines	0	0
Active - linked clone	0	0
Local	0	0

The Inventory node allows you to create virtual desktops and pools and assign them to appropriate users. The Users and Groups page simply allows you to see which users have access to which desktops – and manage their sessions. The Configuration Page is used in the primary set up of the system. The Events page, of course, is an event log of tasks carried out with the VMware View administration pages.

The post-configuration tasks contain two primary steps – firstly licensing the Connection Server, and then configuring it so it can communicate with your vCenter. Note: In a Production environment, it is recommended that the Connection Server component is not installed on your vCenter server.

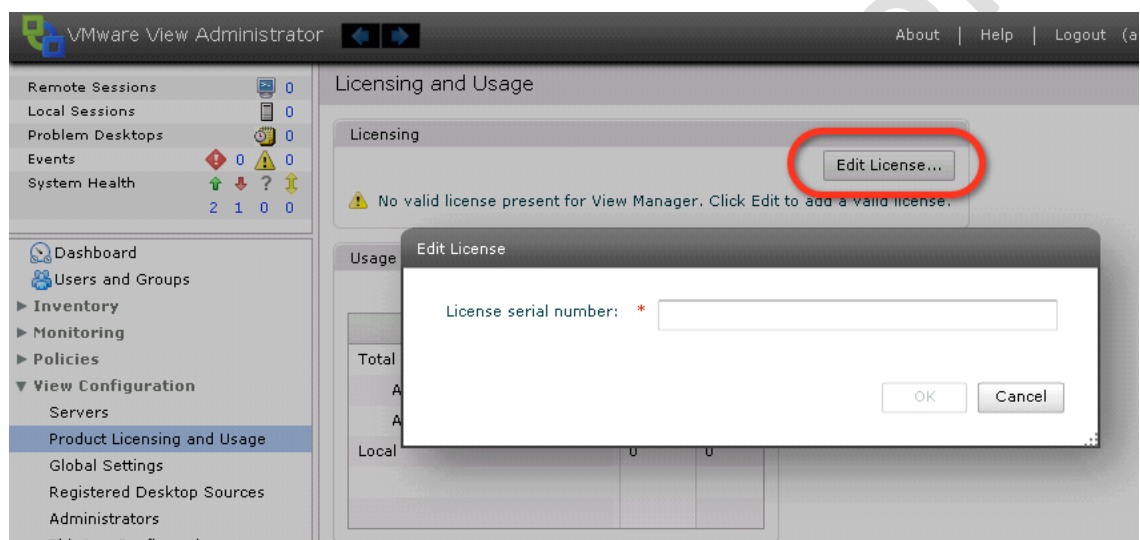
Adding in vCenter(s)

1. **Open up IE on the desktop of the Connection Server**
2. Type: **https://localhost/admin** and **accept the untrusted certificate warning message**

3. At the **login prompt type your administrator account and password** and click **Login**

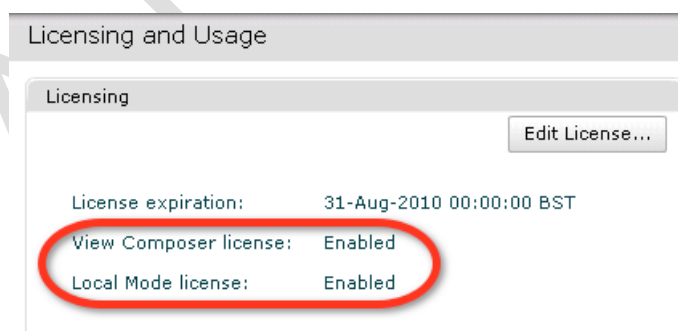
The default user group used in VMware View is the built-in Administrators group on the local server. As the Domain Admins group is added into the local Administrators group when you add a Windows server to a domain, this effectively means *any* Domain Administrator can manage the Connection Server until this is changed. In many respects this is just how vCenter handles default administration rights and privileges.

4. In **►View Configuration, Product Licensing and Usage**, select the link **Edit License**, as shown in the screen grab below:

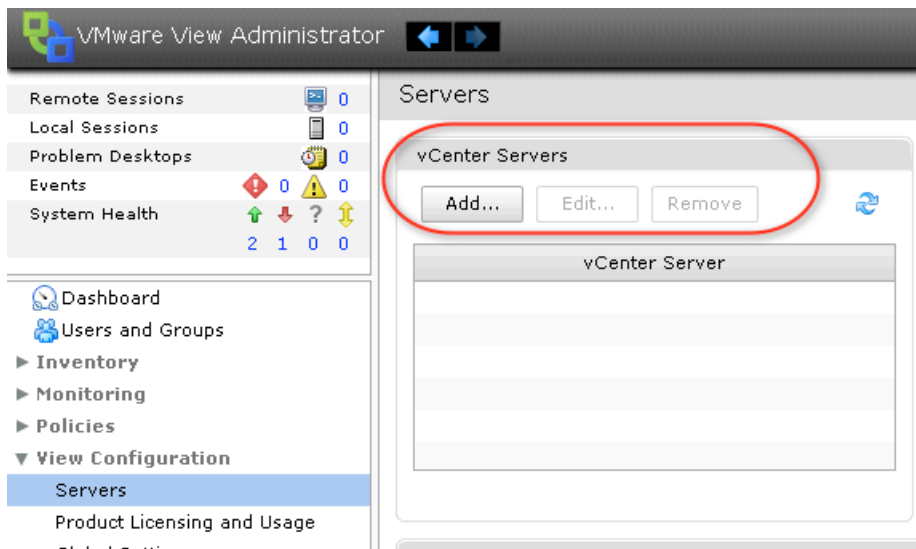


5. In the **Edit Licensing** popup, type in your license number

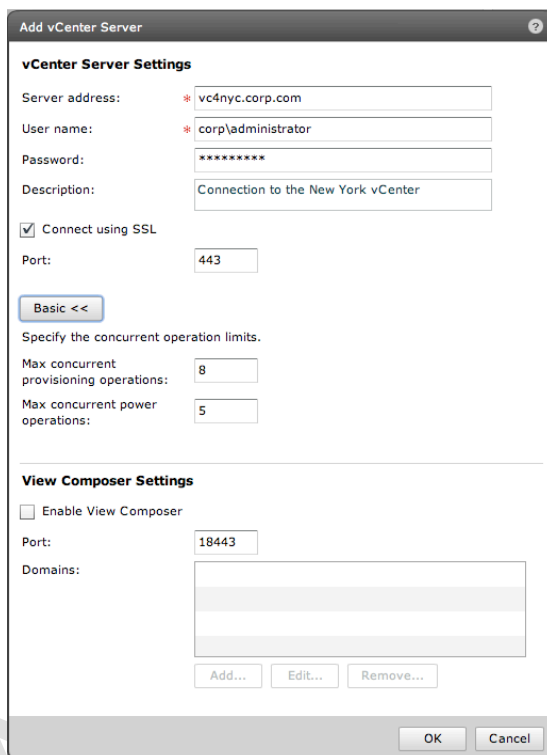
This license number also dictates whether advanced features are available to the system such as offline desktop and the composer feature.



6. Next supply the vCenter information by **clicking the Add button** in the **Servers** section under the **►View Configuration node**. This vCenter Settings page allows you to configure which vCenter system the connection server will use to locate virtual desktops



This page is fairly self-explanatory.

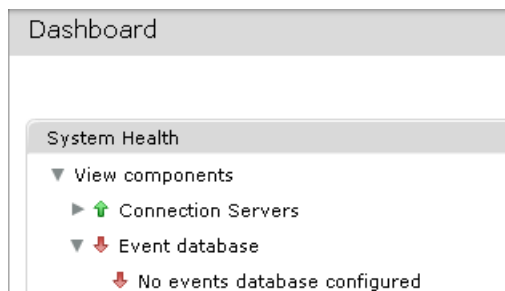


I would not recommend using a real administrator account for the Connection Server's communication with vCenter. This is required for the provisioning process and for the broker to validate the user login process and then select a desktop from the inventory. The "Enable View Composer" option does exactly what you think it would – it allows you to add in the details of the service that handles your "linked clones". As I have yet to install the View Composer service I will bypass it for the moment. Finally, clicking the Advanced button exposes some global settings that limit the number of simultaneous (concurrent) creation of new VMs and power on events. As you might suspect these are set to

stop the Connection Server overloading vCenter with more tasks than it can cope with.

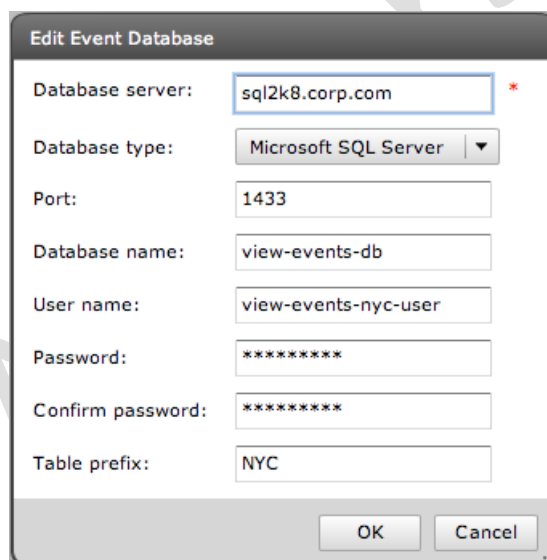
Enabling Event Database

The Event Database is new to View 4.5 and allows you to store events that occur in the product to an external SQL-style database. You can tell whether the Event Database is configured or not by checking out the new Dashboard feature in View 4.5



Unlike other VMware products, there is no need in this case to use the Microsoft ODBC Administrator tools to create a DSN configuration. The configuration is carried out entirely from within the View administration web pages. To configure your connection to the database carry out the following steps:

1. Open the **View Configuration**, and select **Event Configuration**
2. Next click the **Edit** button
3. Completed the dialog box like so:

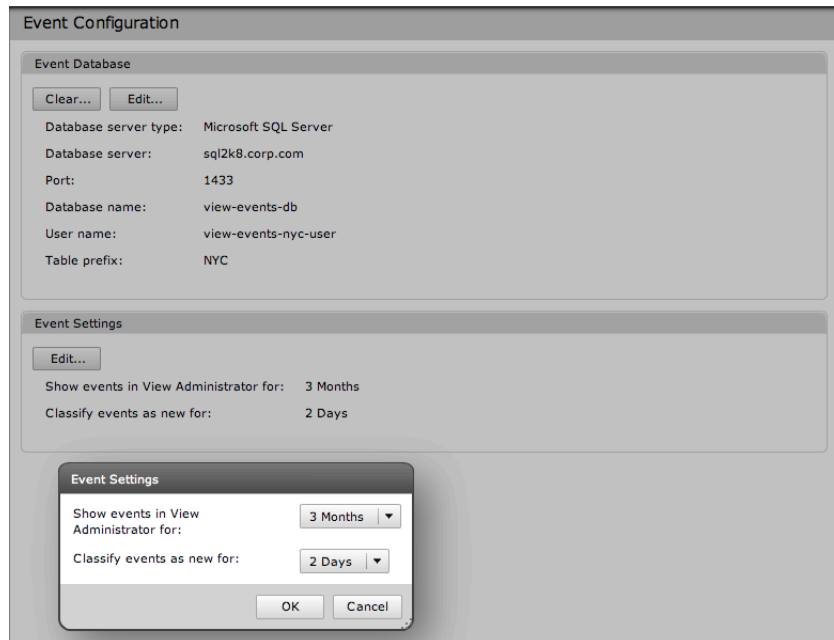


Note:

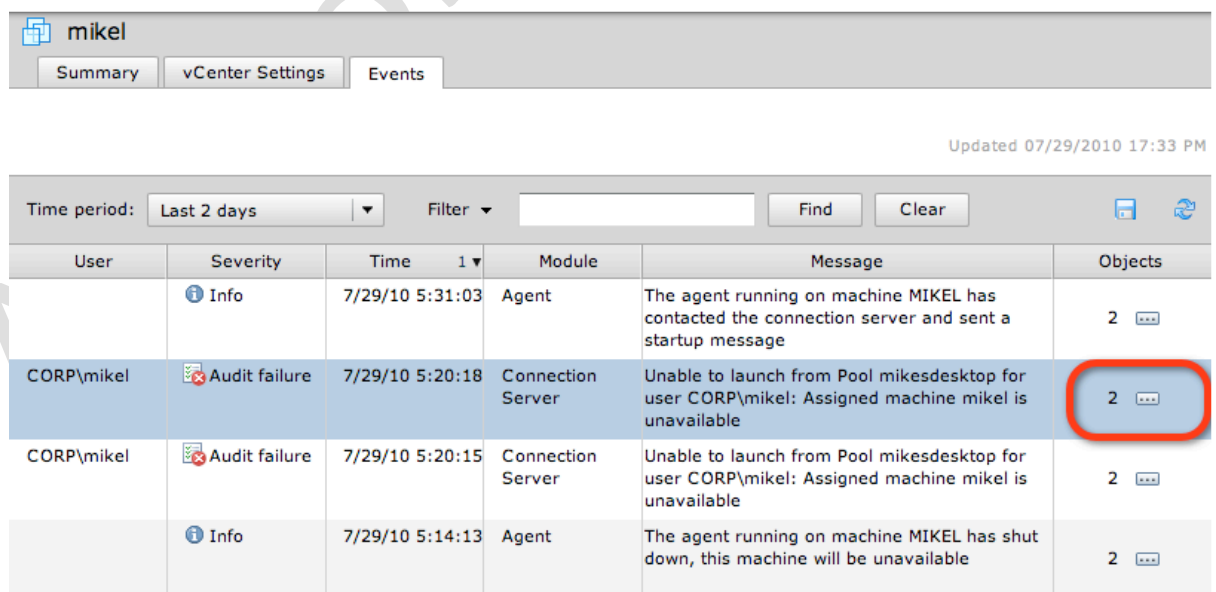
I think most of the information above is pretty clear, except the Table Prefix option. This allows you to have one Event Database shared by many deployments of View, this is achieved by inserting a string of

characters as a unique identifier. The Table Prefix is a required field even if you don't intend to use this functionality.

Once enabled, you are able to reconfigure the retention of data in the Event Database like so:



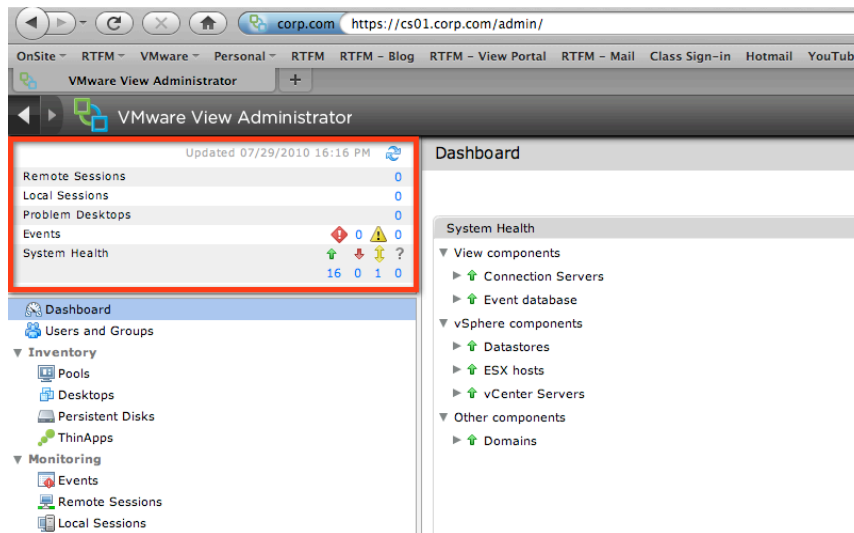
Once the Event Database is enabled you will see events in most locations in the management interface, as well as a dedicated events node in the inventory. There is a small icon that appears as an ellipsis that provides additional information:



Dashboard View

The main dashboard view is intended to be your overall window on how your View environment is behaving. This is an increasingly popular way for various

ISV's to display the core information they need to flag up to the administrator. When you first install View, many of these alarms, alerts and flags will be in red simply because the configuration has not been completed yet. Once the configuration of View is complete, it should look more like this:

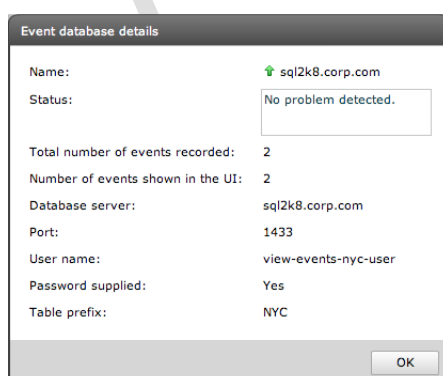


Note:

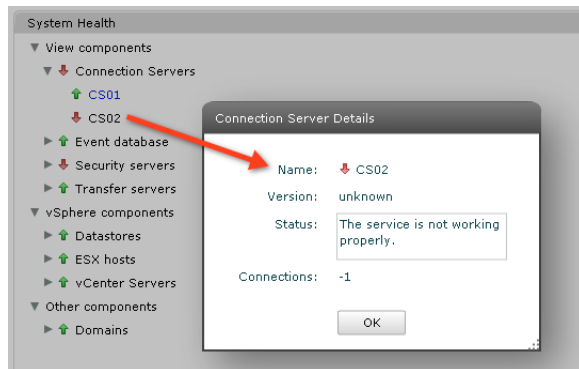
If you use VMware's DPM (Distributed Power Management) you will find you will get red alerts against the ESX hosts that have been placed in standby mode.

The main summary area highlighted in red shows you a running total of number of remote sessions, desktop problems and so on. Clicking on the blue links in this area will take you to the relevant location in the administration tools. So, if you clicked the number next to Remote Sessions, it would take you to the Remote Session node within Monitoring. As you have probably gathered, anything highlighted in blue is usually a link that leads you on to a more detailed set of properties or settings.

In the System Health areas, each node that makes up the components of View is listed. If there are any problems, these will be highlighted in red. Clicking on these links when they are red or green will bring up slightly more detailed data.



You will soon know if you have an issue with the components that make up View when these icons turn red. Sadly, there is no way at the moment to link these alarms to an SNMP Trap or email system.



In the right-hand corner of the Dashboard View, the Desktop Status panel gives us numerical data on the desktops being prepared, any desktop provisioning errors and desktops that have been prepared for use.

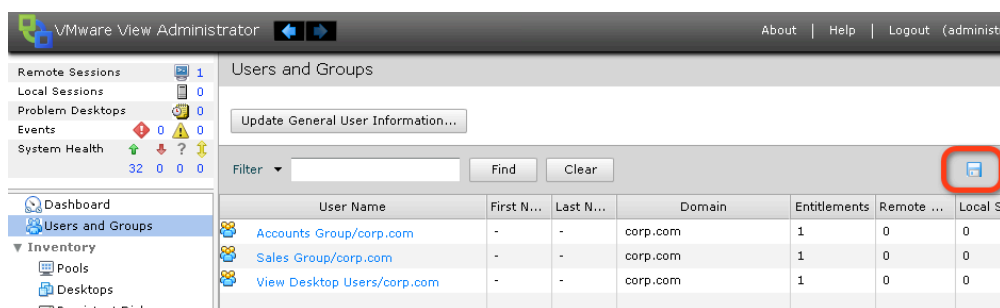
Finally, the Datastore panel enumerates your VMFS and NFS datastores, flagging up datastores that could potentially be over-committed from the perspective of the linked clone.

The screenshot shows the 'Datastores' panel with a table listing various datastores. A legend at the top right indicates that a green icon means 'Low on free space' and a red icon means 'Overcommitted'.

Datastore	vCenter Server	Capacity (GB)	Free space (GB)	Potential Pool Growth (GB)
virtualdesktops	vo4nyc.corp.com	99	72	24
netapp-srm-nyc	vo4nyc.corp.com	100	84	0
netapp-virtualmachines	vo4nyc.corp.com	100	86	0
fileservers	vo4nyc.corp.com	99	90	0
citrix	vo4nyc.corp.com	99	90	0
mail	vo4nyc.corp.com	99	90	0
media	vo4nyc.corp.com	100	93	0
rtfm_templates	vo4nyc.corp.com	300	151	0

Users and Groups Node

The users and groups node allows you to see the users and groups that have been entitled to use the system. Most of these list views also come with a small disk icon in the far right-hand corner, this allows you to export the information you see below in .CSV format:

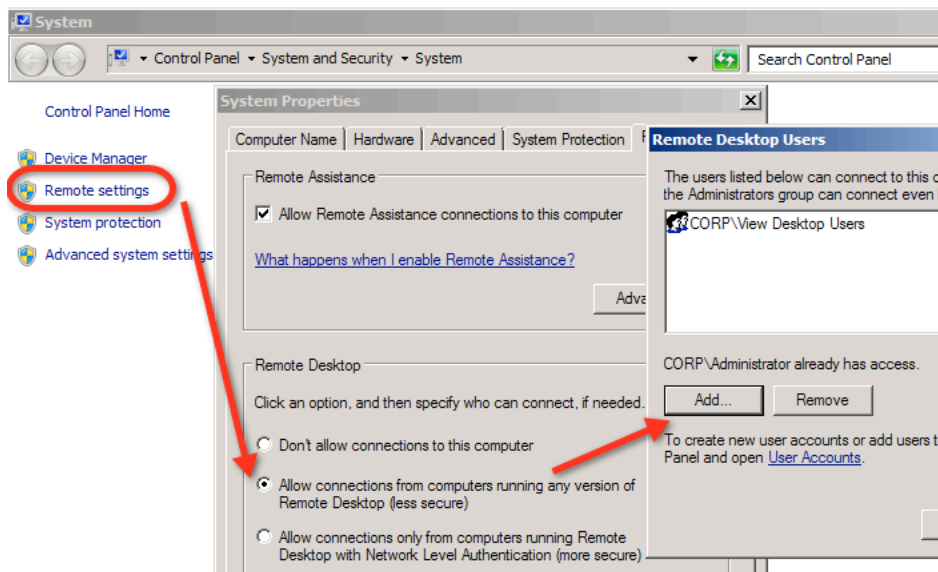


Chapter 4: Install the Agent in the Virtual Desktop

You will need to create a VM which runs either Windows XP Professional, or any of the non-Home editions of Windows Vista or Windows 7; you can do this using an existing template or manually. This virtual machine will be the one that end users connect with from their physical machine. The Home editions of Windows do not support RDP connections and cannot be added to the Microsoft Active Directory Domain. Both of these features are requirements for VMware View to work. As you can tell VMware View is really about delivering a corporate desktop to corporate users wherever they are on the network – be it at home or work.. Finally, it is possible to store virtual desktops on local storage, but doing so precludes features such as VMotion, DRS and HA. If you need to upgrade the ESX server software and you use local storage, you will be unable to move your virtual desktops to another ESX server without affecting the end users.

As you might expect, common problems normally exhibit themselves in the initial build of the Windows virtual desktop. Prior to installing the VMware View Agent, it's worth creating a checklist to confirm that the VM corresponds with your normal corporate build. For example I always confirm the following:

- The virtual desktop is **joined to the domain**
- **RDP has been enabled.** I would recommend that if you are using Vista or Windows 7 that you use lower security for RDP. This will mean any physical client will be able to connect without security errors occurring - it will allow a Windows XP physical client to connect to a Windows 7 virtual desktop. The higher level of security offered by RDP in Vista and Windows 7 is incompatible with older editions of the Remote Desktop client and may cause problems with dumb terminals. The screen grab below shows me enabling RDP on Windows 7 (Beta) and allowing the members of a group I called Virtual Desktop Users in Active Directory the privilege of Remote Access. When you first enable RDP on Windows 7 you will receive a pop-up message warning you to change the power settings to stop the hibernation and sleep settings from prematurely ending remote access:

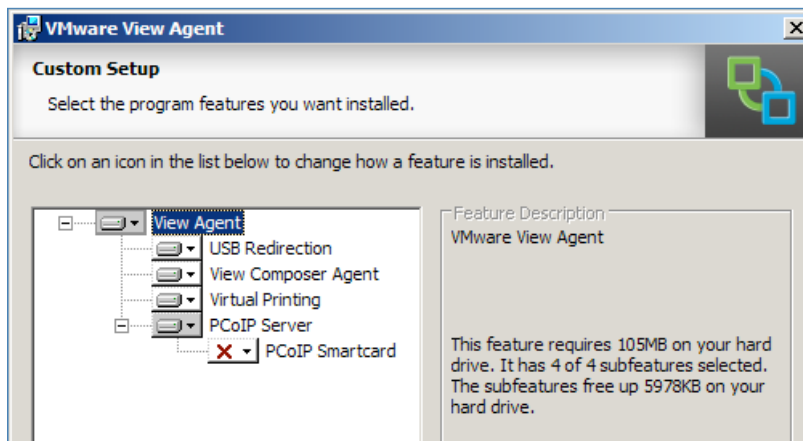


- **Confirm you can connect to the virtual desktop** by using the Microsoft RDP Client and an ordinary user account from the Active Directory Domain. The most common reason for this failing is simply forgetting to put the user accounts that will access the virtual desktops into the right group!
- **Turn off Sleep and Hibernate Settings** – Most modern editions of Windows come with power management settings that either sleep, suspend or hibernate the OS. This will stop all remote access as neither RDP or PCoIP have the APIs to control this power state functionality. If you do want to suspend or power off a virtual desktop when it's not in use, this can be controlled via settings on your desktop pools within View
- **Optimize your virtual desktop.** This book isn't really the place to discuss the perfect Windows XP/Vista/7 build. But before you make this virtual desktop a potential template to be used with your virtual desktop pools, you might want to think about how to harden and optimize your Windows builds for performance and security. This may include steps such as disabling services, running a defragment or perhaps using the shrink feature in VMware Tools to reduce the storage footprint of a VM. If you do intend to carry out a defrag process beware this cause problems with the "thin" virtual disk format, and cause the size of the VM to increase, as defrag reads and writes files across the disk to decrease fragmentation.

Some people go as far as using tools such as nLite and vLite to strip out unwanted or unneeded components from the source Windows XP or Vista CD. While these tools can be useful, they invalidate your support and if they are used too aggressively they can cause applications or services to fail because of missing components. Although you will hear people online singing the praises of such tools, beware the unforeseen consequences of

their over-enthusiastic use. As ever, there is a tension between optimizing Windows and breaking Windows. Personally, I've been quite impressed by the work done on slimming down Windows XP by folks on the Bold Fortune forum - <http://www.bold-fortune.com>

4. **To install the VMware Agent**, double-click the **VMware-viewagent-N.N.N-NNNNNN.exe**
5. After a short time, you will be presented with the **Custom Setup component for the VMware View Agent**



The custom installation allows you to control which sub-components are installed into the virtual desktop. The **USB Redirection service** allows users to plug USB devices such as memory sticks and webcams into the local client device, and have them appear in the virtual desktop. This installs a USB driver into the virtual desktop to allow this redirection to and from the client to the virtual desktop.

The **View Secure Authentication** component allows for the VMware View Client to pass through the logon details from the *client* directly to the agent. Incidentally, it does not pass through the credentials entered at the Ctrl+Alt+Del logon process on the physical client, which is a bit of a disappointment and a current limitation of the product.

The **View Composer Agent** is a part of the Composer feature and required if you want to use this VM to be the base of all your future VMs, acting as a master from which other VMs are created. Personally, I like to install ALL these features so I don't have any hardcoded limitations, and so there is no need to revisit the installer of the agent because of a missing component.

In View 4.0, VMware introduced the **Virtual Printing** feature. VMware acquired a license to the ThinPrint technology. ThinPrint still exists as independent company - VMware did not acquire the organization - so this is merely a technology exchange. Virtual Printing renders print jobs into a much smaller PDF format at the physical location of the virtual

desktop, and then redirects the PDF to the physical print device. It significantly reduces the size of print jobs within the virtual desktop environment. Your network teams will appreciate this too!

In View 4.0, VMware also licensed a new display protocol called PCoIP (PC over IP) – a protocol developed by a company called Teradici, and optimized by VMware engineers for implementation in software. Teradici have historically specialized in high-density graphics rendering using special hardware. The variant of PCoIP in View is essentially a software implementation. It may be the case that the thin terminals you use can be enabled with Teradici, so both the server and client are accelerated, and as you can see, there is a version that allows for the use of Smart Card authentication.

The Agent will enable RDP on the virtual desktop if you have not done already. However, the permissions and rights required to make it work will not be affective.

Authors Edition

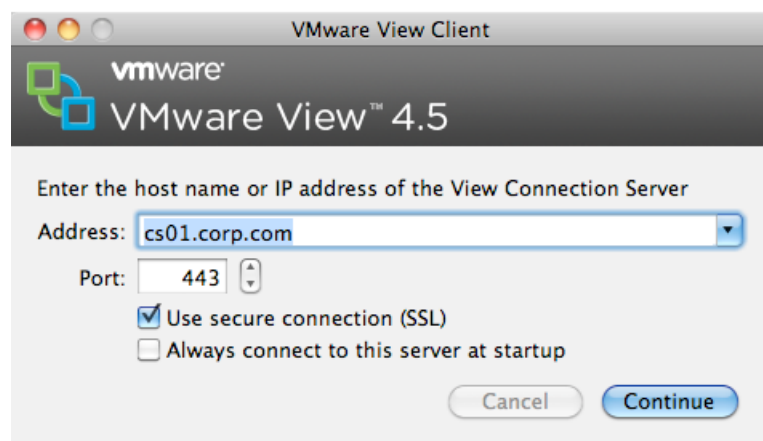
Chapter 5: Install the Local Mode Client

There are actually four different clients for VMware View currently available.

- Native Client (32/64-bit)
- Native Client with Local Mode Desktop (32/64-bit)
- Apple OS X Native Client

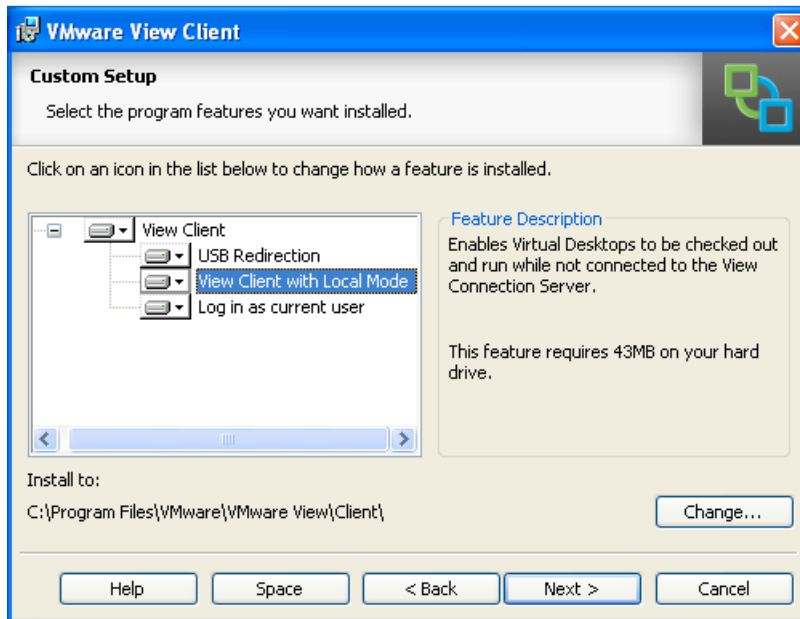
The new version of VMware View introduces 64-bit client support and includes a Apple Mac Client as well – previously Mac users like myself were forced to use a web page only. The Mac client currently only offers a RDP experience, and there is not yet a PCoIP client for the Mac. As such if you are on Mac as I am you will need to also download and install the RDP Client for Apple Mac.

<http://www.microsoft.com/downloads/details.aspx?FamilyID=cd9ec77e-5b07-4332-849f-046611458871&displaylang=en>



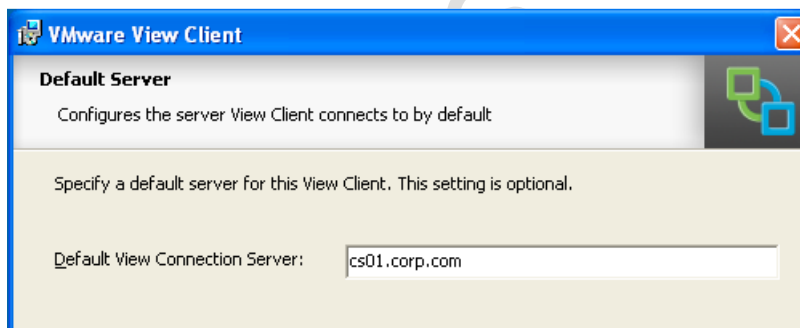
Additionally, you should know that the Local Mode client will NOT install into a virtual machine. It must be installed into a physical PC. As work around it possible to install the Local Mode client into a VM using some other virtualization platform, for example I was able to use the free version of VirtualBox to run Windows inside a VM and then install the Local Client. It seems a shame that VMware won't allow this for at least testing purposes.

1. On the end-user's physical machine, log in with your administrative account
2. **Install the VMware View Offline-Client** by running the **VMware-viewclientlocalmode-N.N.N-NNNNNN.exe**
3. **As with the VMware View Agent**, there is also a **USB Client and Local Mode Desktop Component** to the **Custom Setup dialog box**

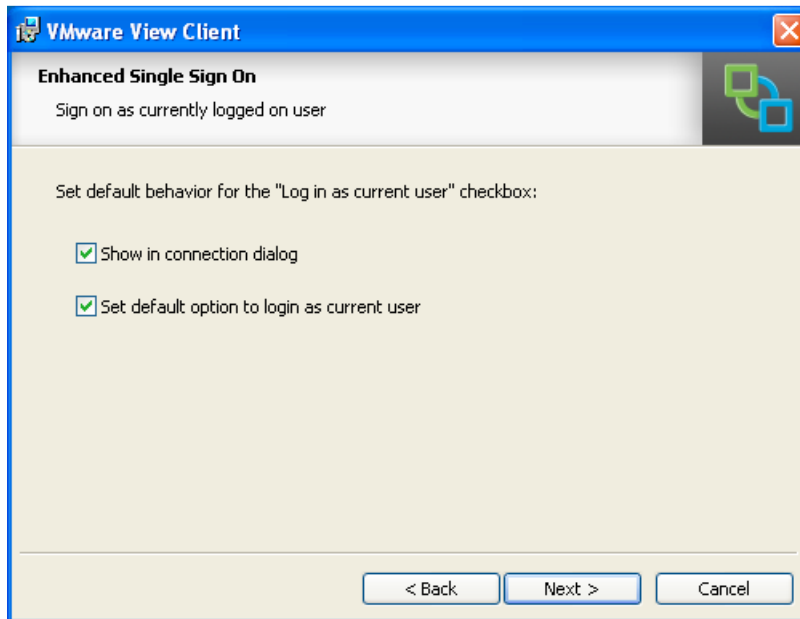


For testing purposes you can run the View Client inside a Windows XP/Vista/7 VM. However, the offline desktop feature *only* works with the Windows client on a *physical PC*. If you try to install the Local Mode feature into a virtual machine it will be deselected in the custom setup

4. Optionally, during the install **you are able to pre-set the Connection Server** that the client will use by default

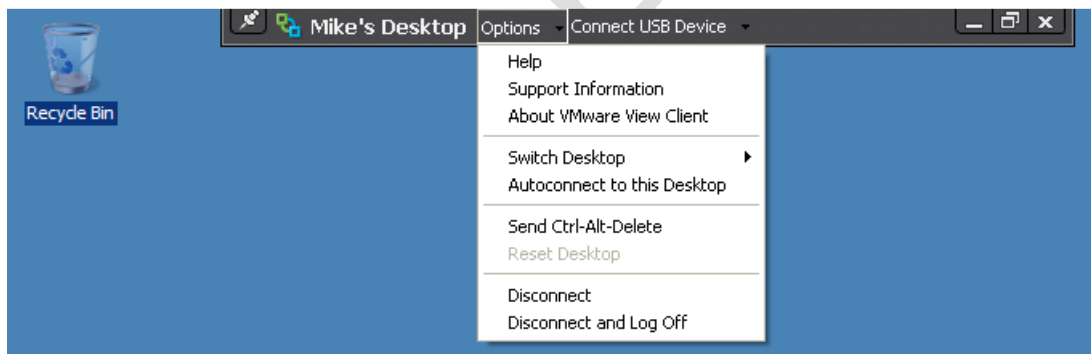


5. You can additionally set the defaults for the Enhanced Single Sign-on feature. This allows the user's credentials to the physical client to be passed through the View client, thus making the logon process more seamless.



Note:

Once the client has been loaded and users have connected to their virtual desktop – users see pull-down menu options that are similar to the Microsoft RDP Toolbar.



Chapter 6: Publish an Individual Virtual Desktop

With all the VMware View software installed, we are now in a position to publish our first desktop. I like to do this as soon as possible, so I can ensure that the View Client can connect to the Connection Server, and in turn connect to the Virtual Desktop running the View Agent. Once I'm satisfied that the virtual desktop works, I think about making a template out of it and create a larger pool of virtual desktops. After all, there's little point in creating a pool of 100 virtual desktops if the source of that pool is broken or doesn't work properly.

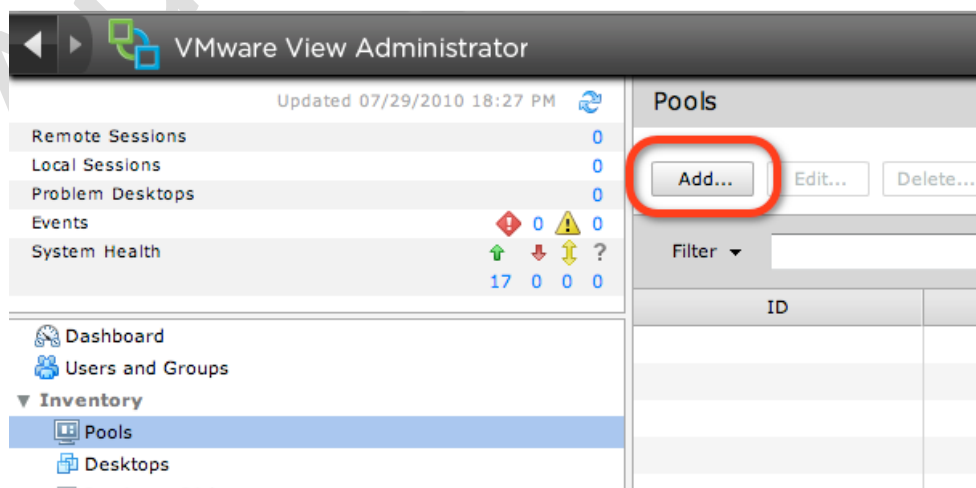
In View 3 it was possible to publish what were called Individual Desktops. These allowed one virtual desktop to be used per user, and ensured that only that user had rights to a particular virtual desktop. This feature is now deprecated, however it is still very easy to create a manual pool that contains only one virtual desktop and assign it to one user – which is essentially the same thing.

It is also possible to assign an individual virtual desktop to more than one person. On the surface this might seem an oxymoron. But, if you're looking for a usage case, I often see one PC being used by different people at different times in factories and production environments. Remember though, that unlike Microsoft Terminal Server or Citrix XenApp Server, only one person at a time can connect to a Windows XP/Vista/7 client desktop. In other words, these clients do not support the concept of "multi-win".

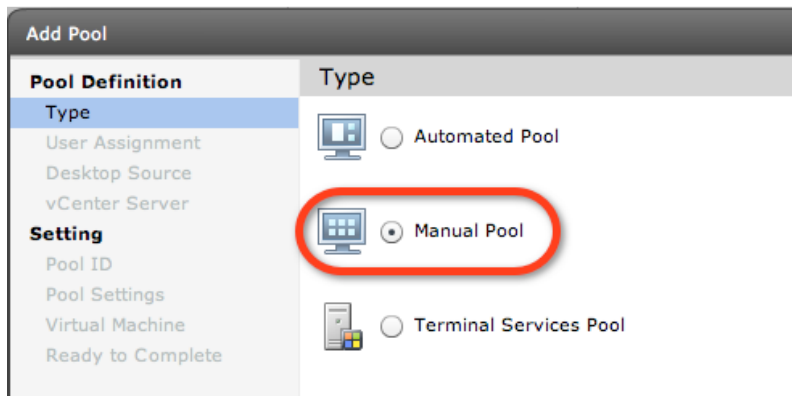
1. **Login to the Administrative webpage of the Connection Server** such as:

<https://cs01.corp.com/admin>

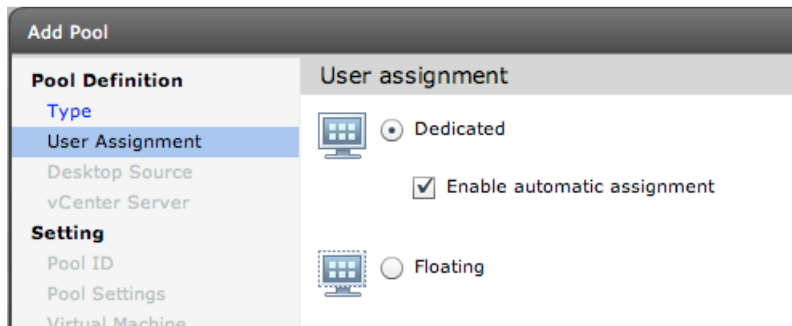
2. Open the ► **Inventory** node and click the **Pools** icon
3. Next click the **Add** button



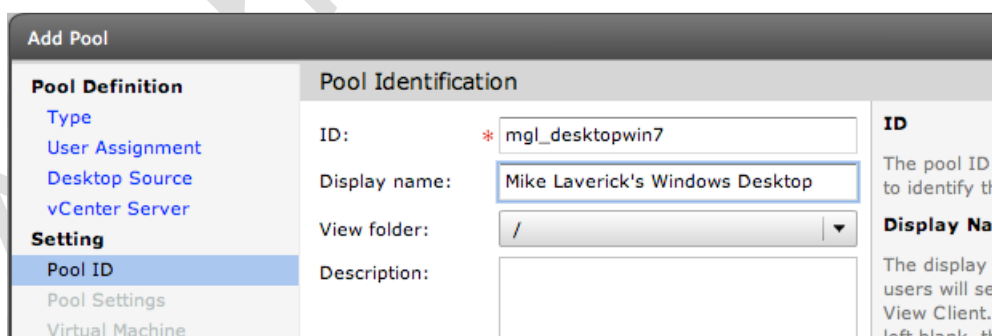
4. In the **Pool Type** page select **Manual Pool**



5. In the **User assignment** page, ensure the **Dedicated** option is enabled, and ensure the option to **"Enable automatic assignment"** is enabled



6. Choose the Desktop Source to be **vCenter virtual machines**
7. **Select the vCenter** which manages the virtual desktop
8. Next you must **specify a unique ID for this virtual desktop** together with **some friendly information by which the end-user will be able to identify the virtual desktop**.

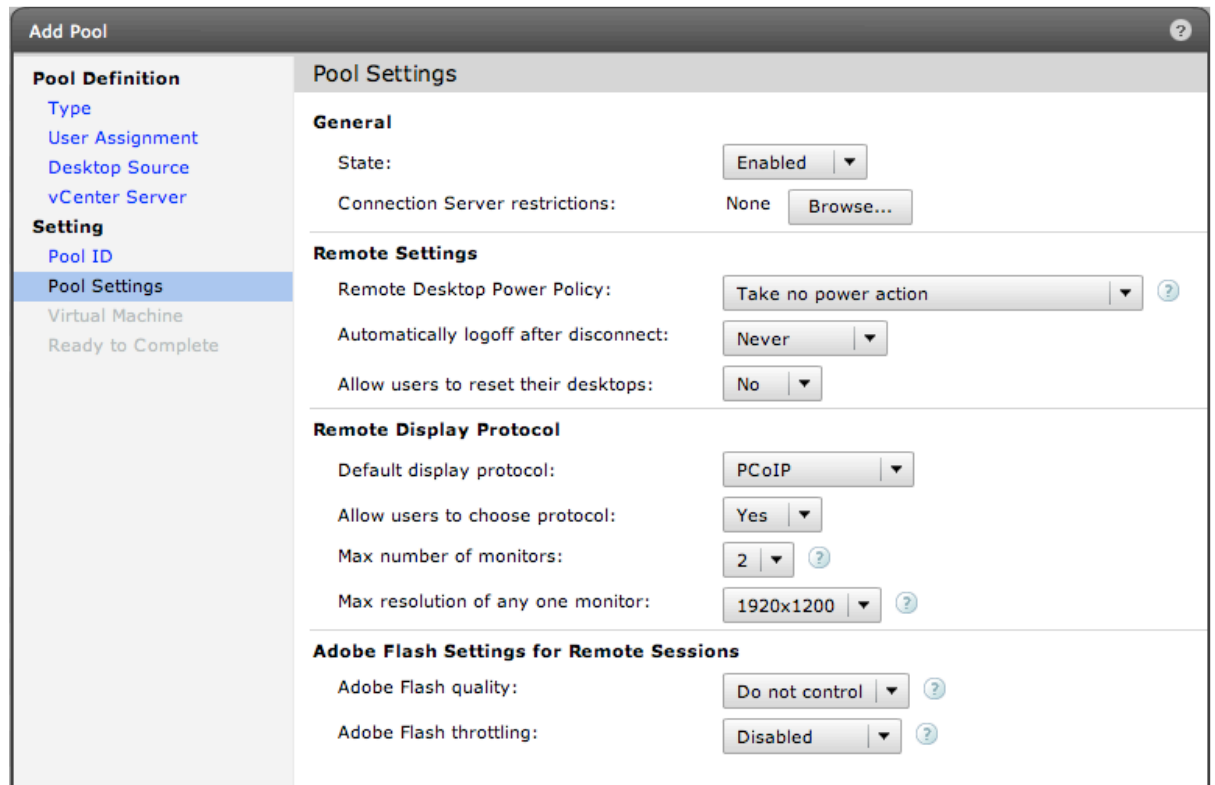


The ID must be unique to this instance of VMware View, and is stored in the Microsoft AD LDS system. It's important to know that, once set, the ID value *cannot* be changed, but the friendly information that the user sees can be changed at any time. New to View 4.5 is the ability to create folders within the View Administration console.

9. The **next page allows you to control some per-virtual desktop settings** that centre around the end user connection. I will be looking at

this page in more detail later on. For now we just want to confirm that the system works and that a client can connect to the virtual desktop

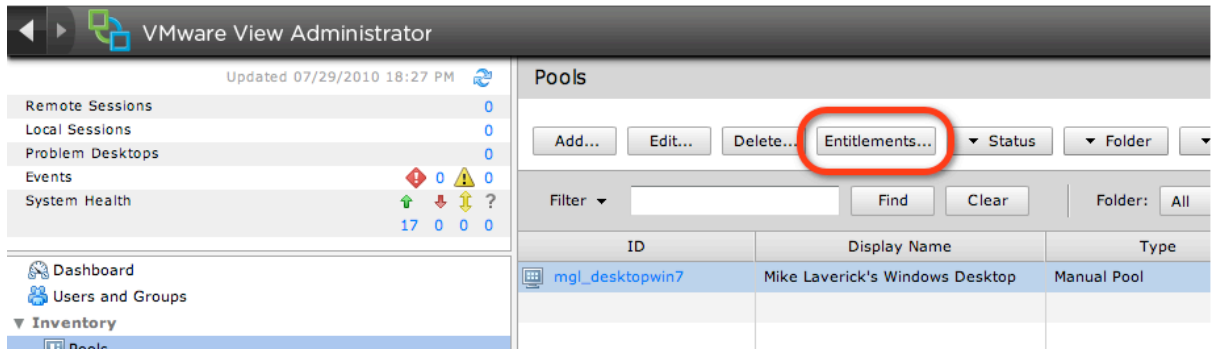
10. Next you select the virtual desktop that the end user will be allocated



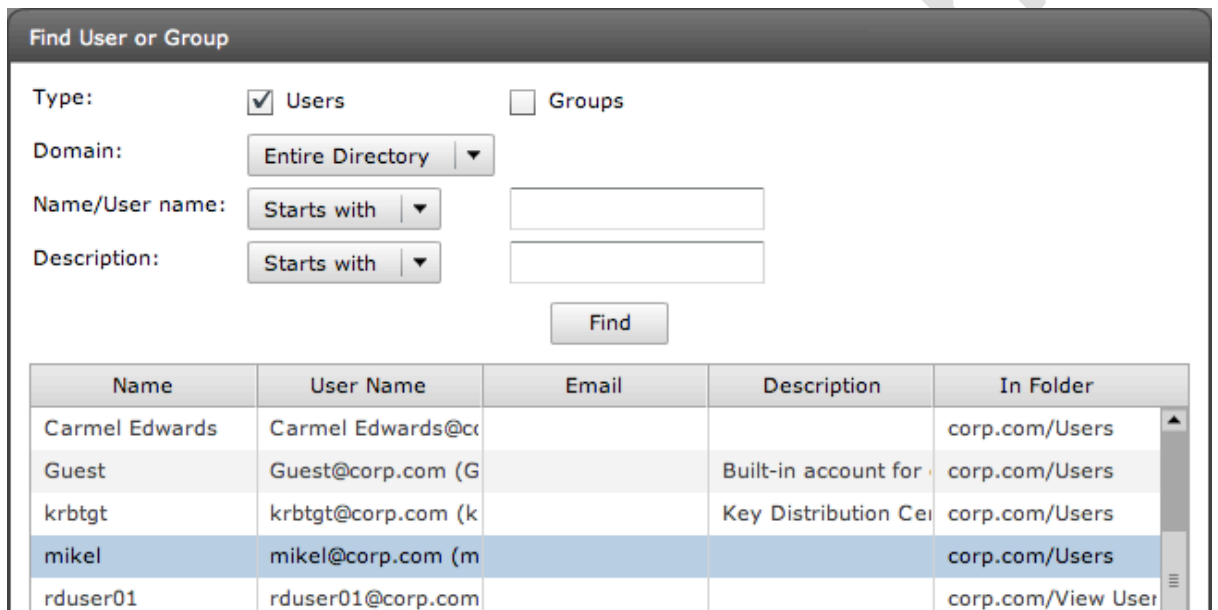
Next View will generate a lists which shows ALL Windows client operating systems within vCenter, regardless of whether they were virtual desktops with the View Agent installed or not. Due this, you may still want to prevent VMs from appearing in the View Admin tool by changing the account used by View, making sure that the account does not have access to these "test" VMs. *It's worth mentioning that once the virtual desktop is assigned in this part of the wizard, it cannot be modified from the webpage administration pages. Get the assignment right now, or you will be deleting this reference in View and starting again.*

After clicking Next and Finish, a desktop will be created in VMware View. The next step is making sure that only the right user has access to the desktop – VMware calls this process Entitlement. By default, no user has any rights to the virtual desktop until this step is carried out.

11. Select the virtual desktop in the list and click Entitlements

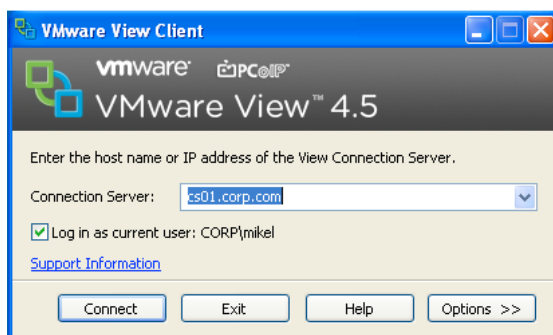


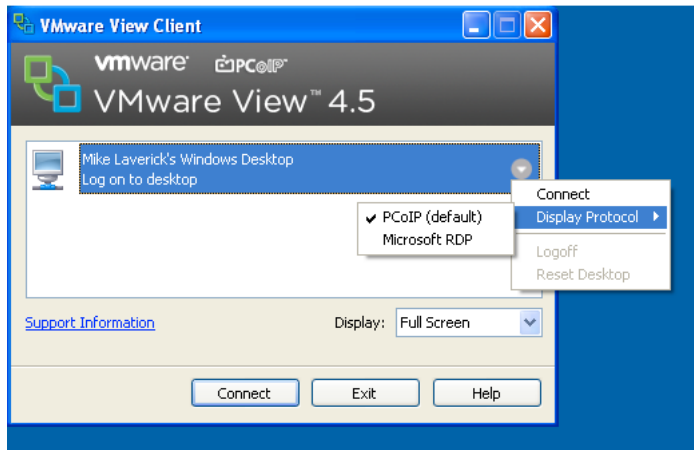
12. In the **Entitlements** pop-up page, click the **Add** button
13. Click the **Find** button and **locate the correct user**, in my case MikeL



Notice how the Find option defaults to locating just users and not groups as well. That's fine in this case, but when we come to create pools of virtual desktops, it's best to use Active Directory groups rather than users, so that the Sales group can be given access to the Sales Virtual Desktop, for example.

Now the virtual desktop is created and entitled, we can use the client to attempt our first connection to the virtual desktop. The screen grabs below show this process from the user's perspective





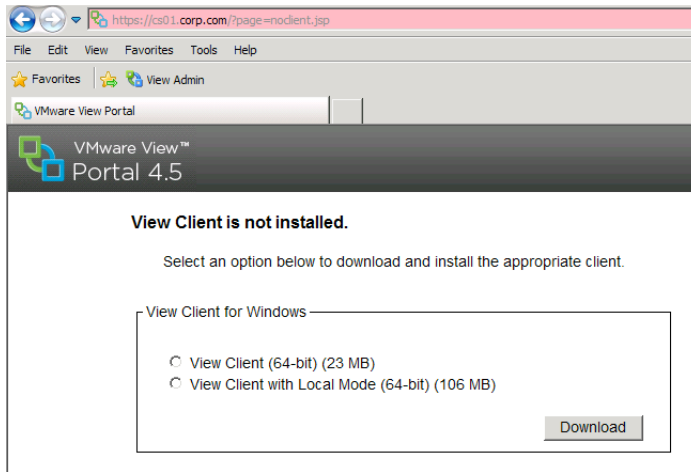
Note:

Notice how the dropdown arrow next to the desktop name allows the user to set which protocol they wish to use with View



For non-Windows clients (Linux or Mac), a Java based .jnlp file will be downloaded to the user's machine, which will start a tunnel session to the Connection Server (or Security Server) which will in turn, once opened, start the RDP engine.

Users who visit the Connection Server via web-browser will find they are asked to download and install the View Client, if it has not already been installed. If it has been installed the client is automatically started and loaded for them, when they visit the web page.



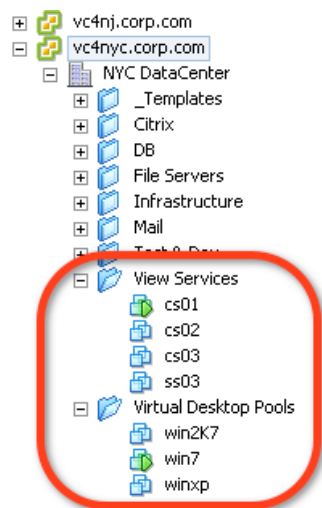
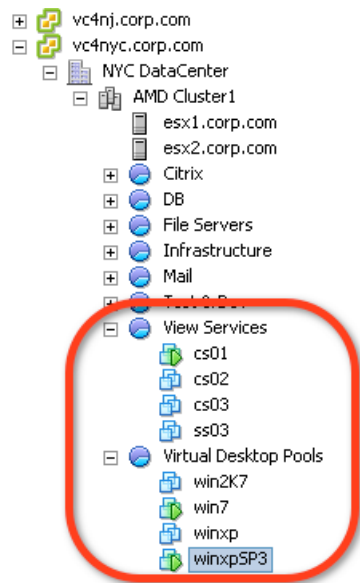
Authors Edition

Chapter 7: Publish a Dedicated Virtual Desktop Pool

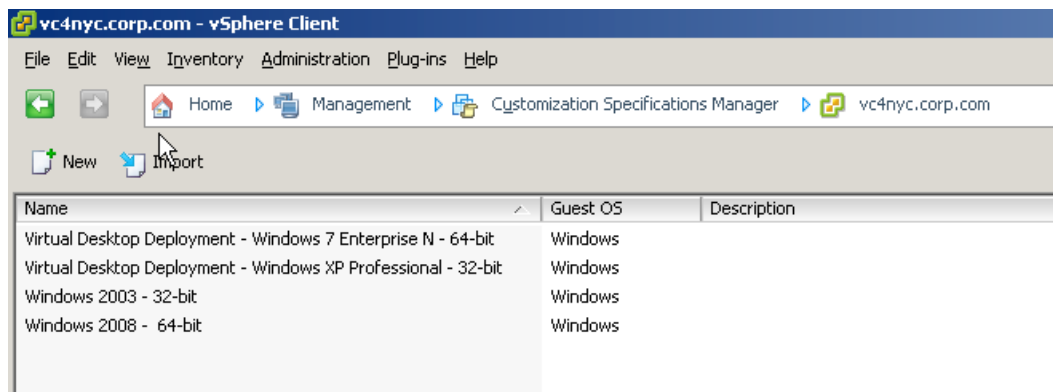
View has always had a concept of virtual desktop pools. At the simplest level, a pool is just a grouping of resources the user can access, these can be virtual desktops, blade PC or terminal servers. Depending on your settings, pools fall into two main types – an Automated Pool or Manual Pool. With an automated pool, virtual desktops are created upfront for a number of users, and then on-demand as more users access the desktops. Below is a bulleted list which outlines the pool types, and what features are supported with them:

- **Automated Pool** – For virtual desktops only and supports Local Mode, PCoIP and Persona Management – and critically supports the View Composer Linked Mode feature. With the automated pool there are two modes called Dedicated and Floating which used to be called Persistent and Non-Persistent mode. Although the terms have changed, they essentially mean the same thing. With Dedicated mode, the user grabs a virtual desktop from the pool, and it remains theirs forever. With a Floating pool, a user is still allocated a virtual desktop, but when the user logs out, the virtual desktop is handed back to the pool to be used by another user. Floating pools are closely aligned with a more concurrency-based perspective of providing virtual desktops – you only need the number of virtual desktops that match the total concurrent load at any one time. As you might expect, the desktop has to be locked down with policies and other tools, especially when the user is never returned to the same desktop. It's worth mentioning that you cannot switch a Dedicated pool to being a Floating pool, or vice versa.
- **Manual Pool** – For virtual desktops and physical computers such as blade PCs. Manual pools support all the features of an Automated pool except, critically, View Composer Linked Mode is not supported, however the local mode feature is supported.
- **Terminal Services Pool** – None of the advanced features are supported, so, critically, there is no PCoIP support for these legacy RDP-enabled systems.

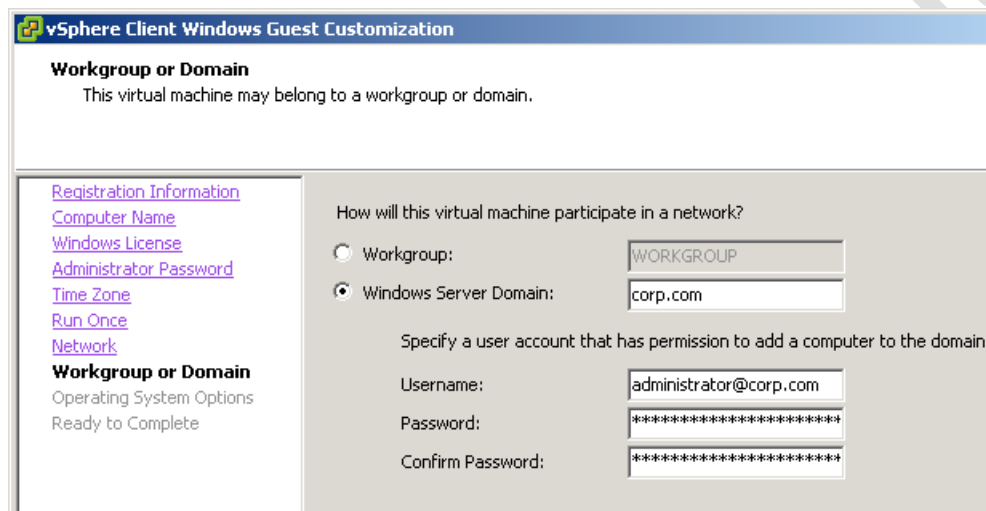
Before we begin to look at Virtual Desktop Pools, I want to discuss some of the requirements and best practices. Firstly, examine your group structures in Active Directory – you may wish to create a group structure specifically for assigning the right users to the right virtual desktop pool. Secondly, you might want to create a similar structure in vCenter of resource pools and virtual machine folders to keep your VMware View environment separate and distinct from the rest of your virtual infrastructure. The two screen grabs below show my configuration:



As you can see, I have both a resource pool and virtual machine folder structure for my VMware View environment. Win7 and WindowsXPSP3 are my test virtual desktops that I will convert into templates to form the basis of my virtual desktop pools. The desktop pool feature uses templates, Microsoft Sysprep and the guest customization configurations to automate the bulk creation of virtual desktops. As such, I always test my templates and the guest customization configurations to make sure they work before I even think about creating a virtual desktop pool.



The guest customization stored in vCenter must be DHCP based otherwise it will not be shown. VMware View assumes all your virtual desktops will be configured as DHCP clients. Additionally, I found with Windows 7 that I had to use the full FQDN values to make sure it successfully joined my CORP.COM domain:



Important:

One of the most common mistakes I've seen is folks forgetting that when they make a virtual machine into a template, everything about the VM is captured as part of the template – including connected CD-ROMs and floppy disks!

Additionally, in the Guest Customization Wizard it is possible to store a password to reset the Administrator password in Windows. These passwords are protected by encryption by using a public key. For this to function properly, the user account used by VMware View to communicate with vCenter must have rights to the Guest Customization Settings.

Finally, a word about the VMware Guest Customization wizard – currently it has no method to control where the computer accounts of the virtual desktops are located. This is especially important in the context of VDI as the correct location of computer accounts in your AD structure is necessary if you are using Microsoft Group Policy objects. VMware *does* have a method to achieve this, but only if you use the Linked Clones feature. If you are not using this feature from

VMware, you might want to investigate the use of Microsoft's sysprep.inf files. These sysprep.inf files *do* support the placement of the computer account into the desired Organizational Unit in Active Directory. If you are using Windows XP, you still create sysprep.inf files using the Setup Manager located in the \support\deploy.cab file on the Windows XP CD.

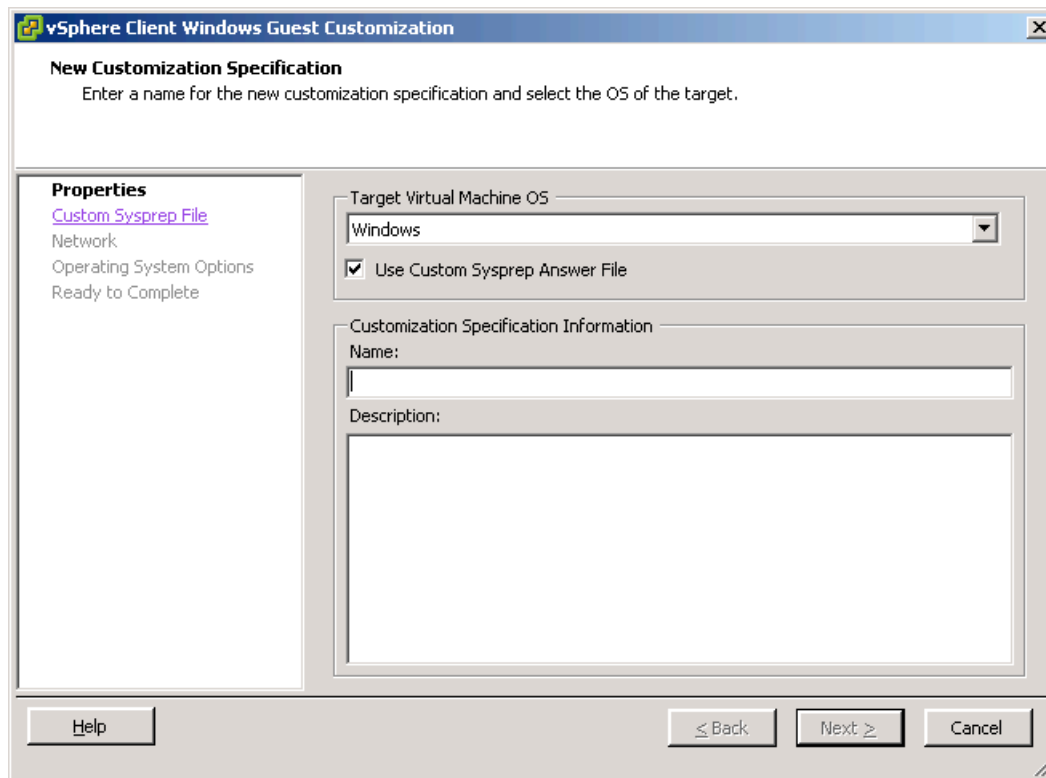
In Windows XP, the sysprep.inf file supports a MachineObjectOU parameter that uses the Distinguished Name syntax to indicate the location of the computer account. This is manually added to the sysprep.inf file in the [Identification] section beneath the details that outline how it will be joined to the domain:

```
[Identification]
JoinDomain=CORP
DomainAdmin=administrator
DomainAdminPassword=vmware
MachineObjectOU=OU=Accounts, OU=Virtual Desktops, DC=CORP, DC=com
```

If, on the other hand, you intend to deploy Windows Vista (sic) or Windows 7, you will need to download and install the appropriate Windows Automated Installation Kit (WAIK) for the client operating system. For Windows 7 you can find its WAIK here:

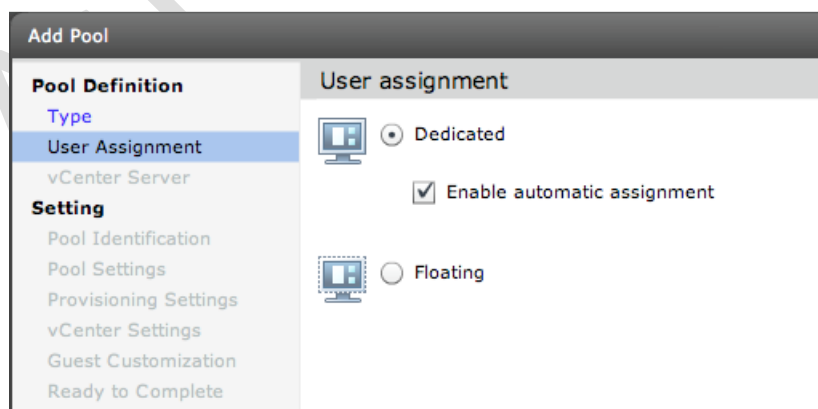
<http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=en>

Once you have created your sysprep.inf file and made the necessary changes, the file can be imported into vCenter by navigating to the Guest Customization manager in the Home location under the Management section



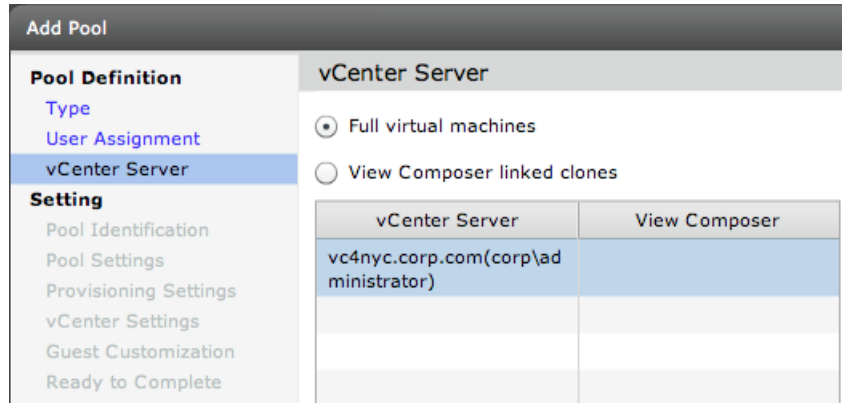
Once you are happy the above is in place, we're ready to publish the desktop. In this format, the desktops created will be assigned to a group of users. Once a user has logged on and acquired the desktop, it will belong to them and cannot be used by another person in the organization

1. **Login to the Administrative webpage of the Connection Server**
2. Open ► **Inventory**
3. Select the Pools node
4. Click the **Add...** button
5. In the pool type select the option called **Automated Pool**
6. In the **User Assignment** page, select **Dedicated** as the method, and leave "**Enable automatic assignment**" as the option



Remember, with the Dedicated desktop, the user is initially randomly assigned a virtual desktop from the pool, but subsequently always returns to the same desktop.

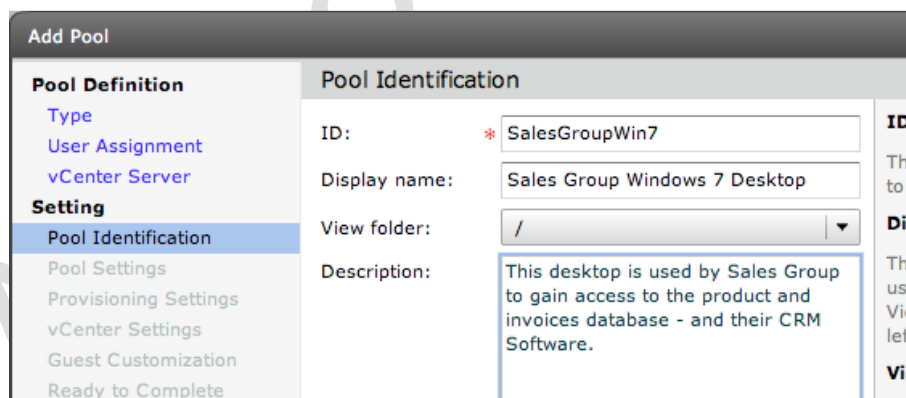
7. In the vCenter page, select the option called **Full virtual machines**



Note:

I will look at Linked Clone-enabled pools shortly. Notice how my vCenter is not yet enabled for the Linked Clone feature

8. **Select the vCenter(s)** which manages the virtual desktop
9. Next, you must **specify a unique ID for this virtual desktop**, together with **some friendly information by which the end user will be able to identify the virtual desktop**. In my case I set a unique ID of SalesGroupWin7, with a friendly name of Sales Group Windows 7 Desktop



10. The **next page allows you to control some per-virtual desktop settings** which centre around the end user connection

Add Pool

Pool Definition

- Type
- User Assignment
- vCenter Server

Setting

- Pool Identification
- Pool Settings**
- Provisioning Settings
- vCenter Settings
- Guest Customization
- Ready to Complete

Pool Settings

General

State: Enabled

Connection Server restrictions: None

Remote Settings

Remote Desktop Power Policy: Take no power action

Automatically logoff after disconnect: Never

Allow users to reset their desktops: No

Remote Display Protocol

Default display protocol: PCoIP

Allow users to choose protocol: Yes

Max number of monitors: 2

Max resolution of any one monitor: 1920x1200

Adobe Flash Settings for Remote Sessions

Adobe Flash quality: Do not control

Adobe Flash throttling: Disabled

Note:

I think many of these settings are self-explanatory. But in an effort to remain complete, the table below explains each setting, what it does and the consequences of each selection. You're welcome to bypass this table and move on to the next part of the wizard if you so wish

Option	Meaning
State	Enabled/Disable. Can be used to create a pool without users being able to access it at the end of the wizard. Additionally, allows you to temporarily take pool offline. Changing this option does not disconnect existing users
Connection Server Restrictions	It's possible to have replicas of Connection Servers. By default, any Connection Server could take the inbound user connection. This new option enables the ability to restrict users to specific Connection Servers
Remote Desktop Power Policy	This changes the power state of the VM when the user logs off. Options include Power Off, Suspend, and Always Turn On. If the last one is selected, if the user tries to power off their VM, it is

	always powered back on again
Automatically logoff after disconnection	Users can disconnect from a virtual desktop. The default action is that they are NOT logged out. This option enables the logging out of the desktop if the user disconnects, or logging out a disconnected session after a period of time. The default period is 120 minutes
Allow users to reset their desktops	By default, users have no method to reboot their virtual desktop, unless you give them access within Windows. Enabling this option adds a menu option to the View Client toolbar, which allows the user to force a hard reboot
Default Display Protocol Allow users to choose protocol	The first option allows you to set which of RDP or PCoIP is the preferred protocol. The second option controls if users have access to adjust this default from the View Client. If left unmodified, this setting can cause problems if some kind of network device such as an internal firewall causes PCoIP to be unavailable.
Max number of monitors Max resolution of any one monitor	As you might expect, View supports multiple monitor configurations from 2-3-4. Each monitor should be of the same resolution. The second option sets the maximum resolution allowed for 1 of the N monitors. Multiple monitor support is only available to the PCoIP protocol, and existing virtual desktops must be restarted for it to take effect
Adobe Flash Quality Adobe Flash Throttling	New to View 4 are options to control Flash video as it appears in webpages. Flash quality can be adjusted to Low, Medium and High, and Flash Throttling can be adjusted to Conservative, Moderate and Aggressive. Low and Aggressive will result in LESS bandwidth being consumed, but at the expense of quality

11. The **Provisioning Settings** page controls how the virtual desktops will be created in the pool.

The screenshot shows the 'Add Pool' configuration interface. The left sidebar lists navigation options under 'Pool Definition' and 'Setting'. The main area is titled 'Provisioning Settings' and contains three sections:

- Basic:** Two checked checkboxes: 'Enable provisioning' and 'Stop provisioning on error'.
- Virtual Machine Naming:** Three radio button options. 'Specify names manually' is unselected. Below it is a text input '0 names entered' and a button 'Enter names...'. 'Start desktops in maintenance mode' is unselected. '# Unassigned desktops kept powered on:' is set to 1. 'Use a naming pattern' is selected. Below it is a text input 'Naming Pattern: salesdesktop'.
- Pool Sizing:** Three radio button options. 'Provision desktops on demand' is selected. Below it are two text inputs: 'Max number of desktops:' set to 50 and 'Min number of desktops:' set to 5. 'Number of spare (powered on) desktops:' is set to 2. 'Provision all desktops up-front' is unselected.

Note:

The **Basic** options include "Enable provisioning". With this setting ticked, after clicking Finish in the web admin wizard, the creation of the virtual desktops in the pool will begin automatically. The "Stop provisioning on error" option will halt the creation of the pool if a significant error occurs, such as running out of space in the VMFS volume.

The **Virtual Machine Naming** options are used to set the base virtual machine name in vCenter and also the NETBIOS name of Windows as the desktops are created. This names and creates a folder in vCenter to contain the virtual desktops. I would avoid the "Specify names manually" option, as this means that each VM created has to have its NETBIOS name set by hand by interacting with the Sysprep Mini-Installation wizard. The option to "Use a naming pattern" is the one to go for, as it will take the text provided and serialize each desktop created in the form of salesdesktop1, salesdesktop2 and so on. Optionally, it is possible to include a unique number anywhere in the string with the {n} value to set this number – I could use sales{n}desktop to generate a pattern of sales1desktop, sales2desktop and so on. The maximum length of this field is 13 characters.

The “**Pool Sizing**” options allow you to set a Maximum, Minimum and Minimum setting. These are used to set a hard limit so you don’t get hundreds and thousands of desktops created. They also allow you to create a buffer (or idle pool) of virtual desktops ready to be connected to, so users don’t have to wait while a desktop is created when they log on – it will be ready and waiting for them.

In my case, the absolute maximum number of virtual desktops is 50, after clicking Finish, 5 virtual desktops will be created. Once these 5 desktops have been allocated, VMware View will create another 2. The idea of this is to create only the number of desktops you initially need (5). As your organization grows and employs new users, it will generate the additional virtual desktops needed (2). However, because you will run out of disk or memory you have capped this growth to a maximum of 50 virtual desktops. These fields contain validation so it is impossible to set something that is illogical; the screen grab below shows this. In this case I asked for a minimum that is larger than my maximum – with no spare or reserve virtual machines.

Pool Sizing

Max number of desktops:

Number of spare (powered on) desktops:

Provision desktops on demand

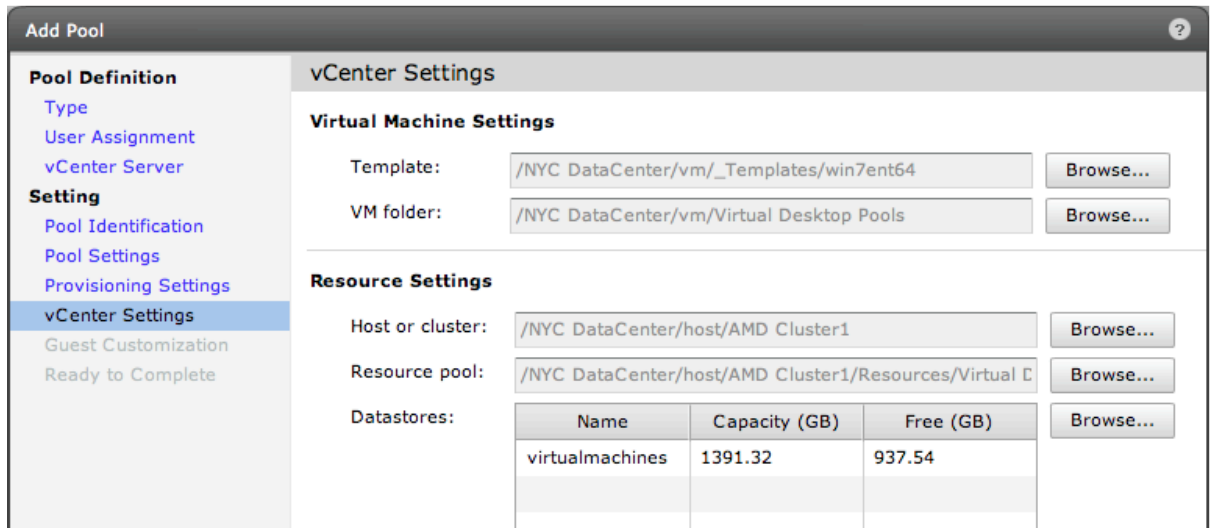
Min number of desktops:

Provision all desktops up-front

Minimum or spare number of desktops must be less than Max number of desktops

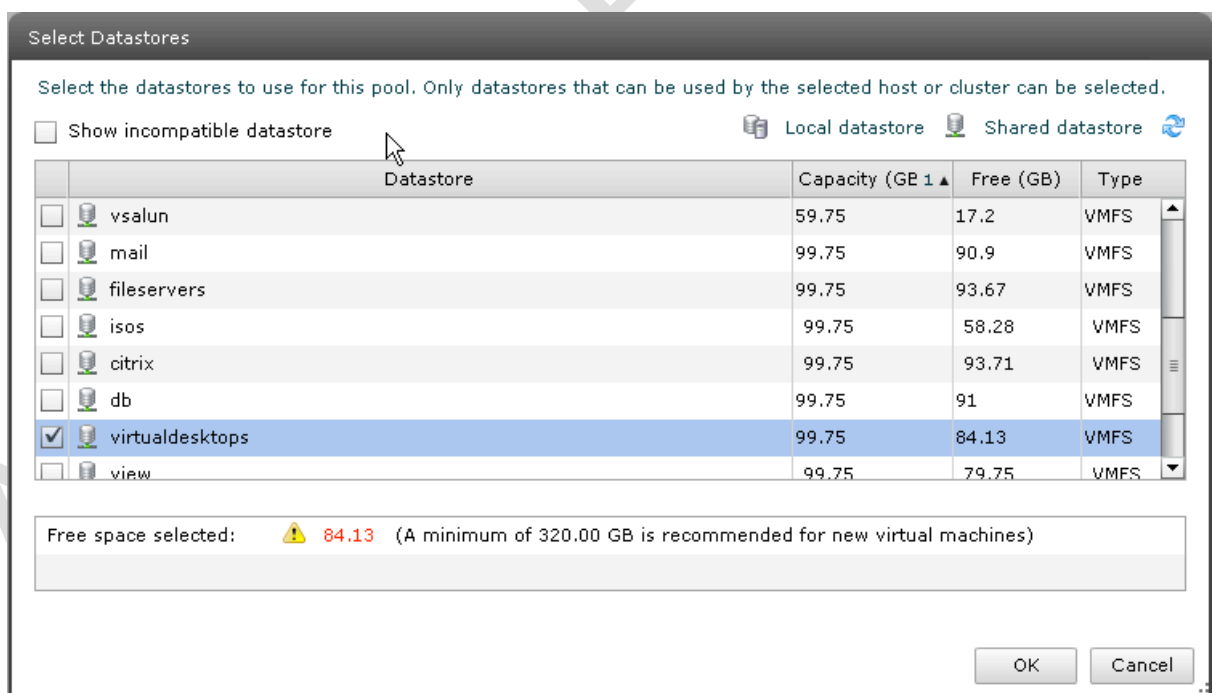
In my case to save disk space and time I actually used 10,2,2 for the settings. This meant I wouldn’t need too many clients (3) before I began to see the minimum and spare values spawn new desktops as my user-base grew.

12. Next, in the **vCenter Settings** page we can **select the template** that will form the basis of the Automated Dedicated Virtual Desktop pool. Each select button allows you to browse the vCenter specified earlier to indicate where the VMs should be located in terms of the vCenter Folders, Cluster and Resource Pool.



By far the most interesting select button is the datastore options.

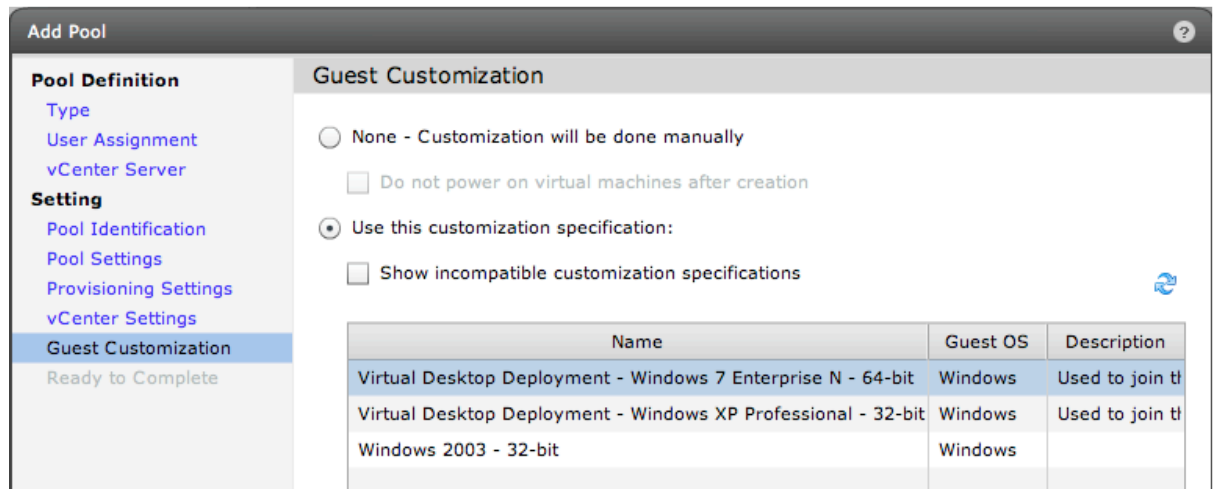
- Select a storage location.** The somewhat cryptic warning at the bottom of this dialog box is a reminder that you don't just need space for the virtual disks of the virtual desktops, but also their swap files as well. It is possible to select more than one datastore in this list, and if you do this, View will distribute the virtual desktops across the datastores selected



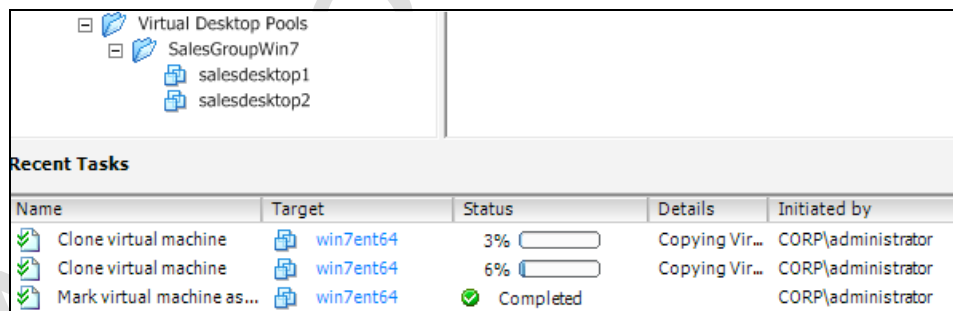
The option to "Show incompatible datastore" is best avoided, as this will expose local storage and other datastores which are not available to the entire DRS/HA Cluster. Shared datastores are recognisable by the cylinder with a pipe symbol. In my case, I've selected a VMFS volume on my SAN which only has 84GB of free space. View warns you that this

is less than the recommended minimum volume size of 320GB. This number has increased in View 4.5 compared with previous releases, most likely to accommodate the increased disk footprint of Windows 7. The "Select Datastores" window allows you to select more than one datastore simultaneously - the system interprets this by aggregating all the storage selected.

14. Finally, select a **Guest Customization** for the correct operating system that joins the virtual desktop to a valid Microsoft Active Directory domain



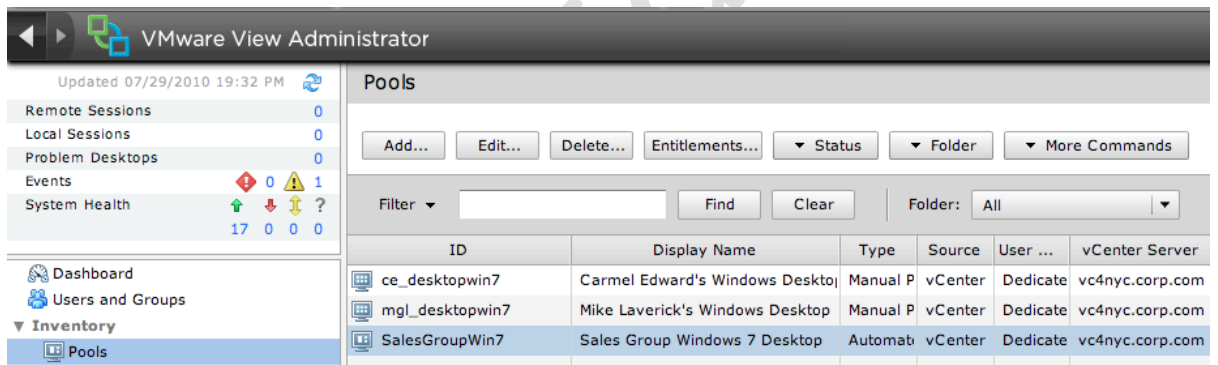
Clicking Finish will trigger the provisioning process and also create a folder to hold the virtual desktops created in the pool. So to be 100% clear View Pools will automatically create a folder, but does not automatically create resource pools.





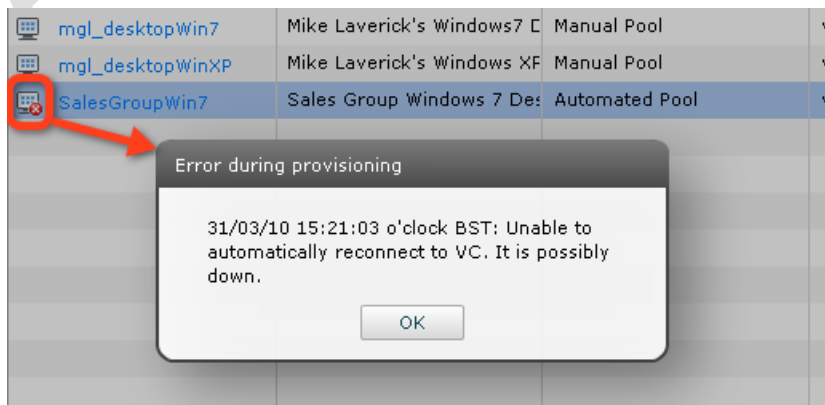
Finally, configure the VMware View rights to allow the Sales AD group to access the desktop.

15. Select the **virtual desktop pool** in the list and click the **Entitlements...** link



Note:

The icons in this view can give you an indication of possible problems in the wider environment. For example, if the vCenter server is unavailable for whatever reason, the View administration console will show a red X next to the affected pool(s):



Once the desktop has been added it should appear in the list, and will display with a solid line around the icon if it is a dedicated pool like this:



whereas the manual pool icons looks like this



16. In the **Entitlements** pop-up page, click the **Add** button
17. **Disable the filter on Users**, and **Enable the filter on Groups**
18. Click the **Find button** and **locate the correct group**, in my case Sales Group

Name	User name	Email
Sales Group	Sales Group/corp.com	
salesuser01	salesuser01@corp.com (salesuser01)	

In my group model, I used the Virtual Desktop User group to handle the Windows rights required for access to Microsoft RDP, and membership of a functional user group (Sales, Accounts, Distribution) to handle access to a particular desktop pool. Of course there are many, many different ways to handle the group structures depending on the size of your organization, and the complexity of the end-user base. As a test, I created a user called "salesuser0N" and added him to both the View Desktop User group and Sales User group. Fundamentally, membership of both groups is required in my case for this user to connect.

Caution:

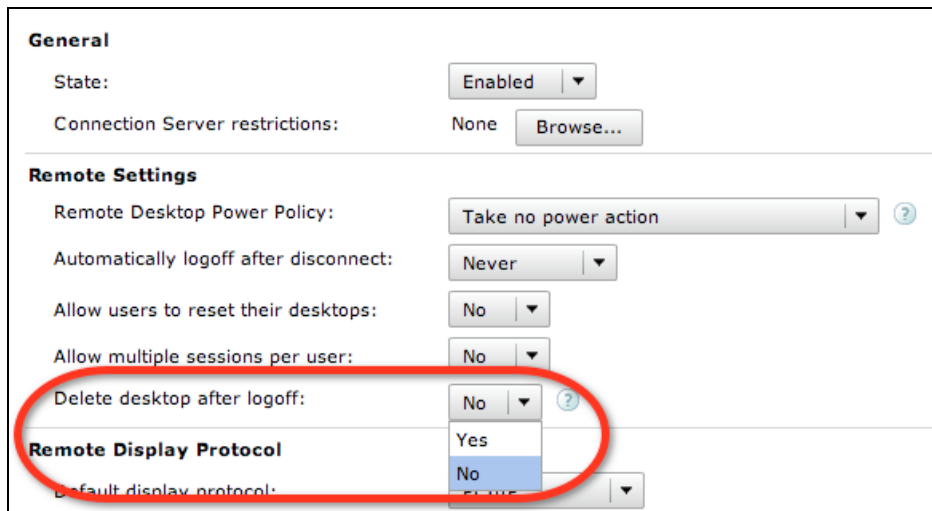
Occasionally, I found the dialog box above does not work with the Entire Directory option, and I've had to change the focus of the dropdown list to select the actual domain I wanted to search

Chapter 8: Publish a Floating Virtual Desktop Pool

Automated Floating Virtual Desktop Pools are set up in a very similar way to Automated Dedicated pools. They differ in one crucial respect – the user is merely allocated a virtual desktop when they log on, and when they log off we can optionally configure view to delete their old virtual desktop and create a new desktop. This has the net effect of giving the user a clean environment every time they login. This can be helpful in kiosk-style environments like a school or college, which are somewhat notorious for being meddled with by teenagers who think downloading screen grabs of Pamela Anderson and leaving them as desktop backgrounds is very funny! Of course, one way to defeat these miscreants is by locking down the desktop with policies to the degree that they can do next to nil to tamper with their environment. Due to its volatile nature, it is imperative that users of non-persistent virtual desktops are not able to save files on the desktop or on the C: drive. If they do, when they log off the data will be lost forever.

By now you are probably very familiar with the pages of VMware View web administration, so I will keep screen grabs down to an absolute minimum in the following instructions:

1. **Login to the Administrative webpage of the Connection Server**
2. Open the ► **Inventory**
3. Select the Pools node
4. Click the **Add...** button
5. In the pool type select the option called **Automated Pool**
6. In the **User Assignment** page, select **Floating** as the method
7. In the vCenter page select the option called **Full Virtual Machines**
8. **Select the vCenter(s)** which manages the virtual desktop
9. Next you must **specify a unique ID for this virtual desktop** together with **some friendly information by which the end-user will be able to identify the virtual desktop**. In my case I set an unique ID of Student, with a friendly name of Student Desktop
10. In the Pool Settings notice how a new option has appeared called **“Delete desktop after logoff”**



11. In the **Provision Settings** page, set your configuration as deemed appropriate for the levels of concurrency you expect to see in this pool. You may wish to dispense with setting a “Min number of desktops” and keep the option to “Provision all desktops up-front”. The choice is yours.
12. In the **vCenter Settings** page, select the Template, VM Folder, Cluster, Resource Pool and Datastore for this new pool
13. Finally, select a **Guest Customization Specification** suitable for your domain and operating system

Note:

Floating pools appear with dashed line around the icon for the pool like so:

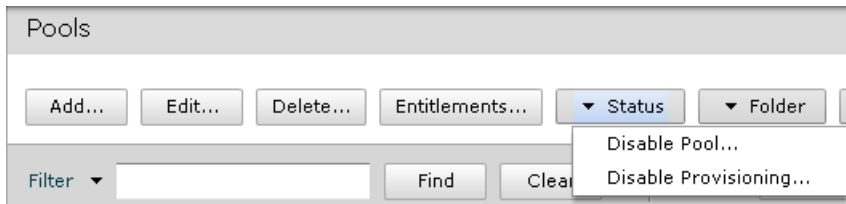


Managing Pools and Desktops

As we saw in earlier chapters, creating pools is a very simple process – and the main pool node will show you all the pools you have created. A simple Edit button allows you to modify some (but not all) of your settings generated by the Add pool wizard. The notable value that cannot be modified after the pool has been created is the pool ID parameter.

Pool Status

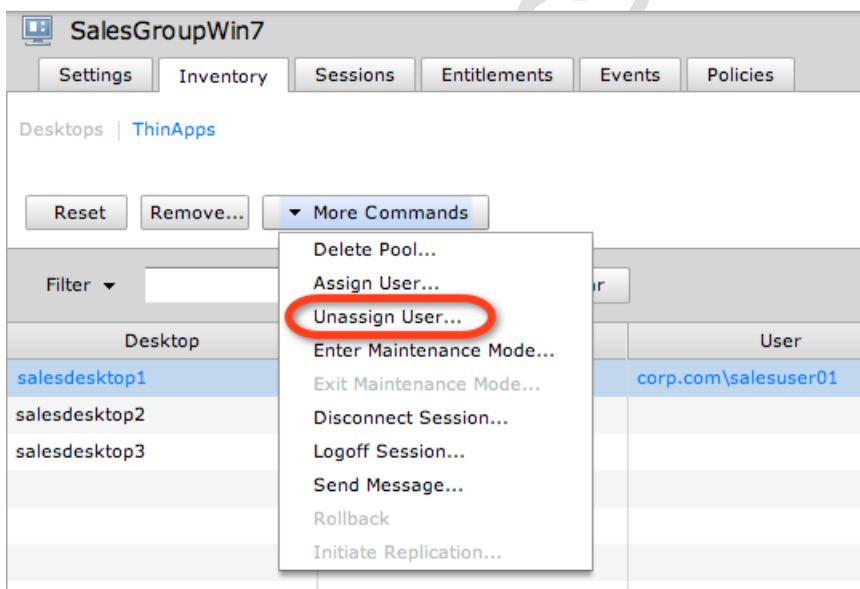
Every pool comes with a Status button with the options to both “Disable Pool...” and “Disable Provisioning...”.



These menus do change, especially if a problem occurs during the provisioning process. They can also be used to re-trigger the provisioning process if those issues have been resolved – you will see the status option change from Disable Provisioning to Enable Provisioning

Unassigning Users from Dedicated Pools

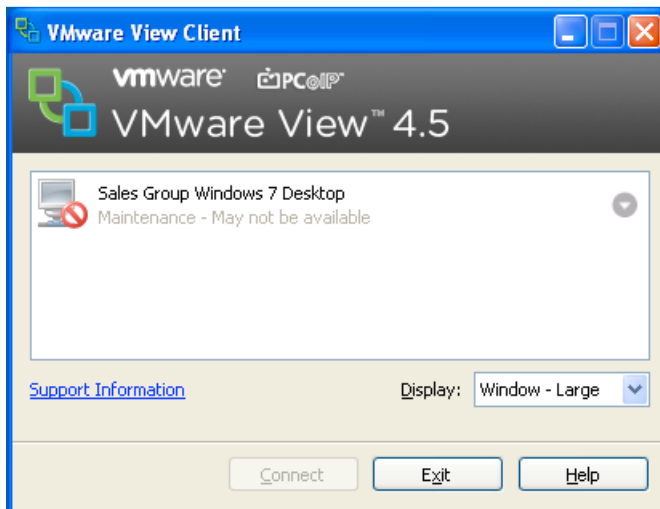
One of the management issues of dedicated pools is unassigning users. As you might recall, with a Dedicated Pool a user is randomly assigned a desktop from the pool when they first connect. This desktop then becomes their own desktop that they constantly reuse. This introduces a management issue – what if the user leaves the organization, or is reassigned to a different segment of the business where they need an entirely different virtual desktop for their work? This would leave the desktop assigned to the original user, with no other user able to access that desktop. Essentially, the desktop becomes a wasted and orphaned resource in the pool. In previous releases we had to resort to a command-line tool to fix this issue. In View 4.5, this process is now exposed to the GUI. If you select the pool and navigate to the Inventory tab, the “More Commands” button exposes this new option:



Maintenance Mode – Taking a Desktop Offline

As you can see from the screen grab above it is also possible to manually, on a per-desktop basis, disallow access to a specific desktop owned by a user on a dedicated pool. This does not disconnect and log out the user if they are already

connected, but if the user logs out and tries to log in again, the View client tells them that their desktop is unavailable:

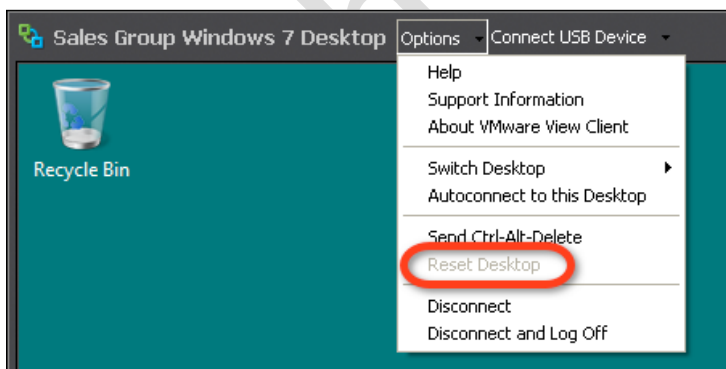


Resetting a Desktop

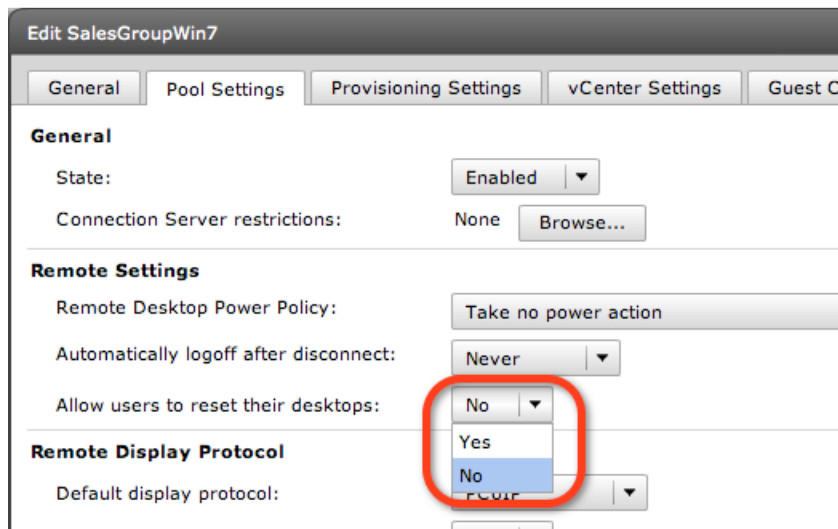
Warning:

This is quite a dangerous option as no prompt is sent to the user that this is about to happen.

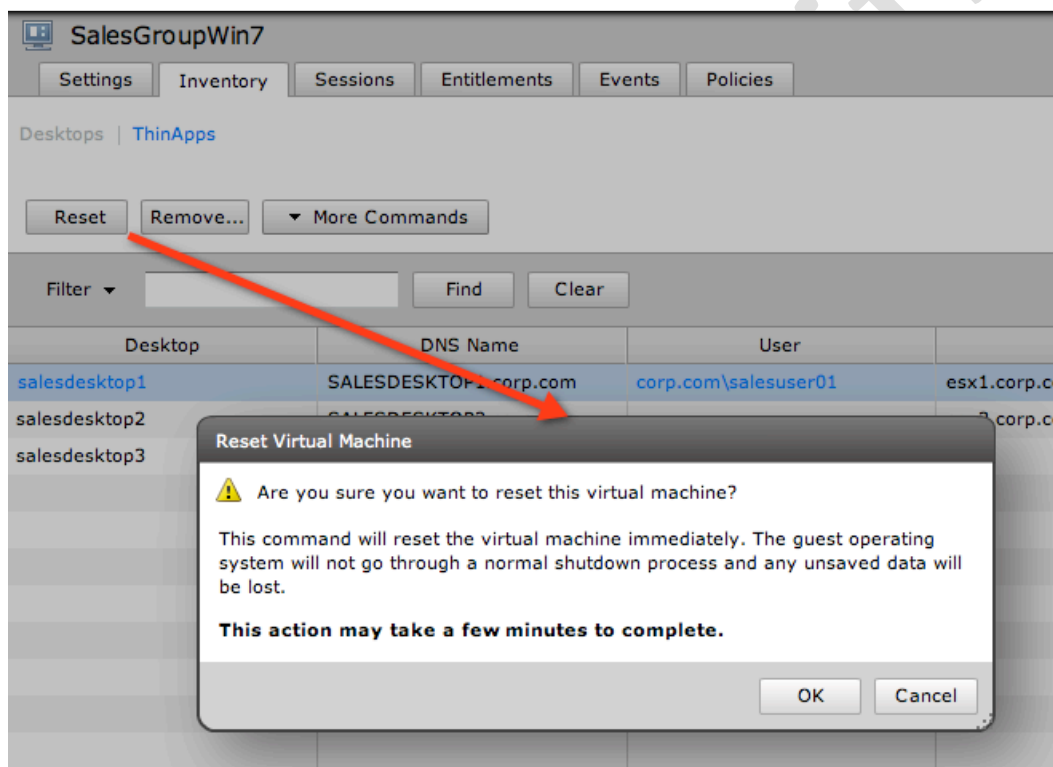
If a virtual desktop for whatever reason becomes completely unresponsive, such that the user cannot interact with it, it is possible from the View management pages to hard reboot the VM. This does NOT perform a graceful shutdown of the VM, and therefore any files the user has not saved will be lost. Remember, it's not a default pool setting that users can reset their own desktops unless you grant it. If you don't grant the permission, you will find the option to "Reset Desktop" in the View Client Toolbar will be dimmed.



Remember, to grant your users this privilege, you would edit the pool settings, navigate to the "Pool Settings" tab, and change "Allow users to reset their desktops:" to Yes.

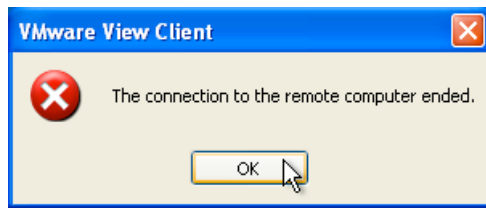


If you do decide to use the reset option from the View administration tools, you will see this message when you click the option:



The actual user experience is actually quite unpleasant. Here's what happens. When you perform a reset of the virtual desktop, the VM is rebooted hard. In Windows 7 this can be sometime detected as a fault, and cause Windows 7 enter its repair mode. From the end-users perspective for a short period the RDP session stays open. This is because remote display protocols work on a retry process that keeps the presentation on screen for a while in the hope that the connection will be re-established. If the user has any open and unsaved files, these applications will prompt the user to save their files. However, it will be too late. The user won't be able to interact with their session because it isn't there

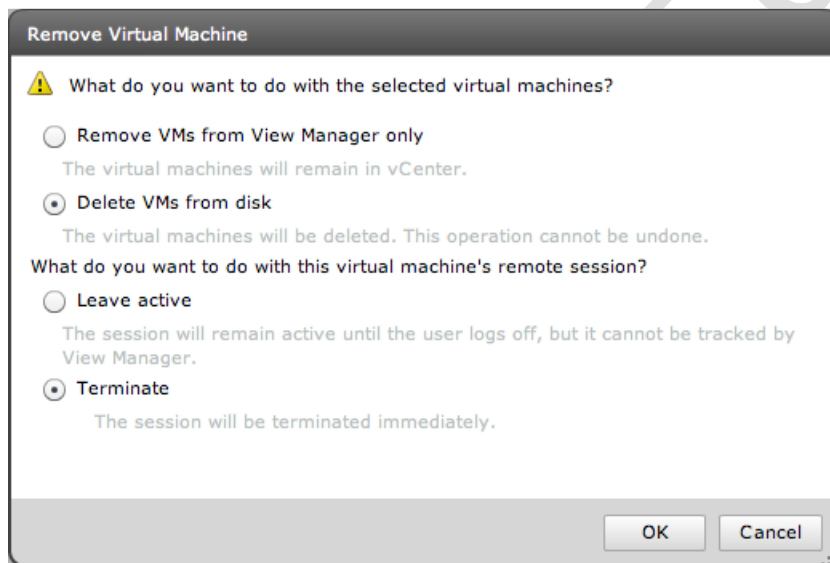
anymore. After a short period, the client session ends unceremoniously – leaving the user with this rather blunt message:



With the PCoIP protocol no such message is generated and the user is bombed out of the session without notification.

Remove a Desktop

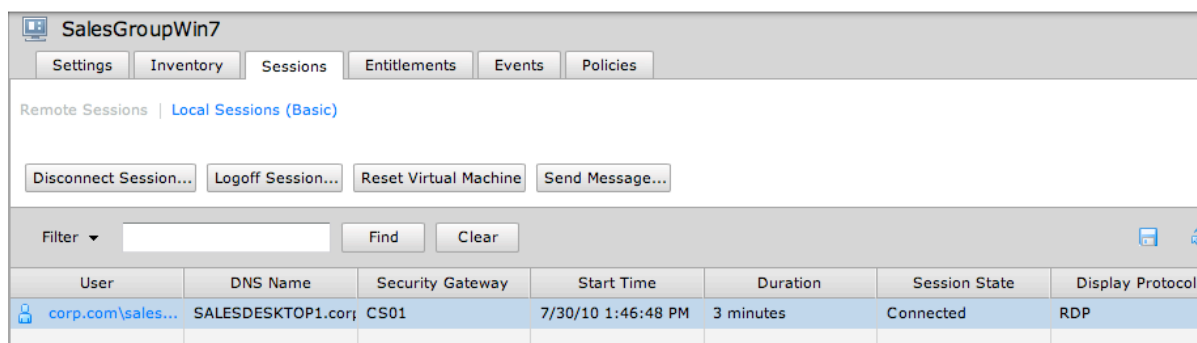
Right next door to the Reset button on a desktop is the Remove option. This can be used to delete a virtual desktop from the pool. It will cause the user to take a new desktop from the pool as their original desktop was destroyed. Additionally, because a desktop has been removed from the pool, it's likely to trigger the creation of a new desktop based on the pool's provisioning settings (max, spare and min). If you click the Remove button whilst a user is connected, View will display a dialog box like so:



In the screen grab I've actually changed the defaults to physically delete the virtual desktop from the datastore, and also destroy the user session. You could decide to be less intrusive and let the session carry on – in this case the desktop would be deleted only when the user finished their session and logged out. Again, as with the reset, this is very intrusive to users, as their session is unceremoniously ended without any opportunity to save data, and the VM is then powered off and deleted. If there is spare capacity in the pool, the user will be able to reconnect to View and will simply be allocated a new desktop from the pool.

Remote Session Management

More options exist for managing user sessions from the aptly named Sessions tab that appears on the pool's properties. The sessions are filtered by remote sessions (RDP/PCoIP), Local Sessions (Basic) and Local Sessions (Transfer). From the Session tab, it's possible to Disconnect, Logoff, Reset and Send Messages to actively connected users. From the screen grab below, you can see all these options. Notice how the Duration column can indicate that there may be a time problem with a VM if it comes up with the message "Clock Skewed", and that my user has connected using RDP rather than PCoIP.



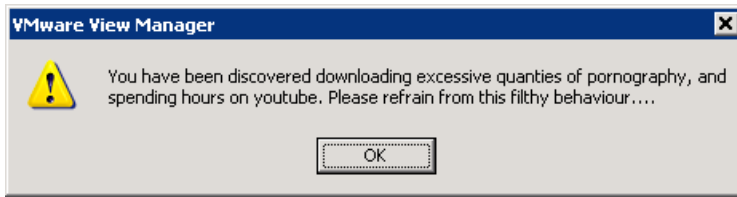
The screenshot shows the 'Sessions' tab in the 'SalesGroupWin7' interface. It features a navigation bar with tabs for Settings, Inventory, Sessions, Entitlements, Events, and Policies. Below the navigation bar, there are buttons for 'Disconnect Session...', 'Logoff Session...', 'Reset Virtual Machine', and 'Send Message...'. A search bar with 'Filter', 'Find', and 'Clear' buttons is present. The main area contains a table with the following data:

User	DNS Name	Security Gateway	Start Time	Duration	Session State	Display Protocol
corp.com\sales...	SALESDESKTOP1.corp	CS01	7/30/10 1:46:48 PM	3 minutes	Connected	RDP

Important:

As you have probably gathered, the View administration pages do not automatically refresh. So it's possible to try to disconnect, logoff, reset or send a message to a session that simply doesn't exist anymore. So, click refresh if you have been in these pages for a while

- **Disconnect** - Merely closes the user's window on their virtual desktop. The user is not logged out of their VM, and files remain open in the virtual desktop. No prompt is sent to the user that you are about to disconnect their session
- **Logoff** - Logs the user out of their VM. No message is sent to the user that they are being logged off, however they are prompted briefly to save any data. If they don't respond in a timely fashion, or are unable to, the session terminates the applications within the virtual desktop without saving their data
- **Reset Virtual Machine** - Covered earlier in this chapter
- **Send Message** - This sends a popup message to the user that appears within the virtual desktop. The UI allows you to categorize your messages into three types (info, warning and error). As with all messaging systems it's wise to engage your brain before sending messages to your management team. With great power, comes great responsibility risk!



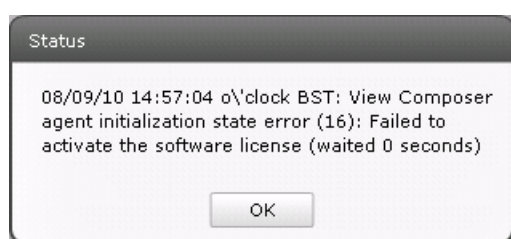
The major thing that is missing from View session management at the moment is some type of remote console feature, by which an administrator could view a user's desktop session and interact with it. This would allow helpdesk staff to at least see the user's desktop to guide them through a process or new system, and intercede on the user's behalf if they were really in a jam.

Authors Edition

Chapter 9: VMware Composer and Linked Clones

IMPORTANT:

If you are using linked clones with Windows 7, the new version of View Composer requires that you running license activation services in your environment. This will means you will either need a "Multiple Activation Key" (MAK) or "Key Management Service" (KMS), requiring a KMS key for the linked clones feature to work with Windows 7. Specifically, you will receive this error message in the View located in the "Inventory" tab of the affected pool.



This activation issue will be particular challenge to those people who need to demonstrate or train View 4.5 with Windows 7 as a guest operating system. A simple work around until Microsoft changes its activation routine might be to use Windows XP that still supports volume "corp" license keys.

As you can see, using conventional templates and virtual disks to create virtual desktops does come with some significant disadvantages. Firstly, even with thinly-provisioned virtual disks you can waste disk space on very expensive shared storage. Secondly, although the automated provisioning of virtual desktop pools is efficient, it can be a huge storage hit on the array. If you have many desktops to create in a short period of time, it can take some time to complete the build process. Thirdly, whilst Sysprep is fine as an engine to reset the Security ID and Domain parameters, it isn't the quickest of processes even when automated by guest customizations.

With this in mind, VMware View3 introduced the Composer feature and Linked Clones. The concept is a simple one. You create a single Master virtual desktop – very much in the same vein that we have covered so far. In VMware Composer, this is referred to as the "Parent VM". A snapshot is taken of this Parent VM, and then a replica is generated. From this replica, linked clones are created. The reason they are called linked clones is that fundamentally the source of a clone's information comes from the read-only replica.

The difference is that rather than using the template process to create a virtual desktop, only a file containing its delta (or differences) is created. Linked Clones

are called such because the clone is linked to a replica of the Parent VM. In this way we can significantly reduce both the storage costs and deployment time. Additionally, it means that when changes are made to the master, the changes are proliferated to each of the linked clones, in a process which VMware calls "recomposing". The virtual desktops are *not* linked to the parent VM but to the replica – this allows you to reuse the parent VM as the source for other linked cloned desktops. If you are using automated dedicated pools with linked clones, the replica disk is marked as read-only, all changes a user makes are sent to the VM's delta virtual disk. Additionally, there is an optional "disposable disk" that used to be called a "user data disk". This disposable disk holds a local profile for the user. The disposable disk is marked as being read-write, and the user is allowed to make changes to their profile and environment, albeit circumscribed by their Active Directory Group Policy settings. The user disk is automatically created and attached to the virtual desktop at first power on, and is assigned a drive letter that you choose when creating the linked clone. These disk types can be configured as what is called a persistent or non-persistent disk. The difference between them is that with a persistent disk, user profile changes are retained when the user logs out, and with a non-persistent disk, user profile changes are discarded. If your virtual desktop pool is automated and dedicated, I would recommend using the persistent disk type. On the other hand, if your pool is of the floating type I would recommend the non-persistent disk type. It's worth stating that there are innumerable methods of handling the troublesome user profile, and you might want to investigate those first.

Such savings in space and time have been around at the storage layer for some time from such vendors as NetApp with their SnapClone and De-Duplication technology. If you have these storage technologies already, you may wish to evaluate their effectiveness and cost before using the linked clones feature. It's worth noting that these so-called high-level storage features from the storage vendors are not always free and often require a license to function. With this said I think the future maybe that whilst VMware View may be the place where you create and define VMs, the instructions to carry out the cloning process will be sent directly to array to offload the copy process.

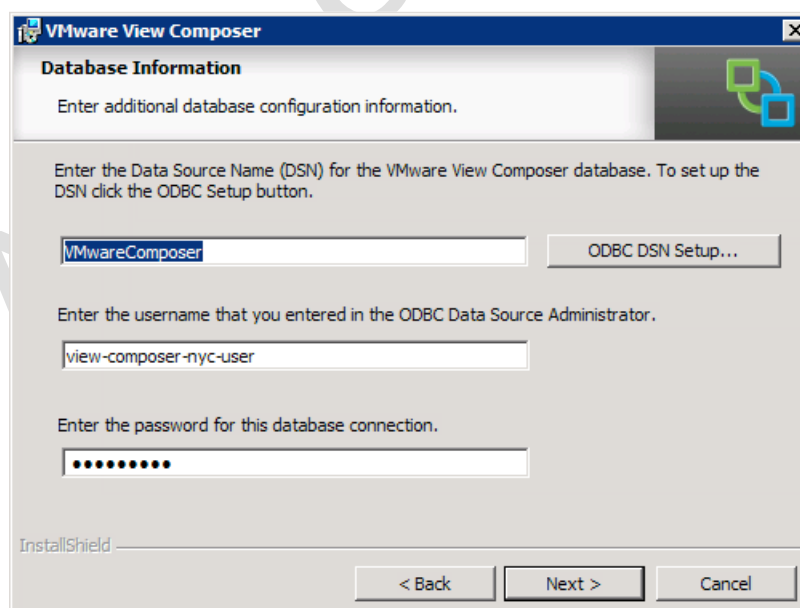
Perhaps the best analogy for Linked Clones is to compare their utilization of disk space with the way that ESX utilizes memory. In ESX, it is possible to allocate more memory to the VMs than is physically present on the ESX host. VMware call this memory over-commitment. Well, in a very similar way with View Composer, we can create more virtual desktops than we have physical disk space for. As with memory over-commitment, with disk over-commitment we must monitor very carefully the *actual* disk space used. View Composer comes with built-in settings that control what happens if we get close to using more disk space than we actually have available. In many respects, it's like having virtual storage on an expensive array which might not even possess this feature.

Finally, VMware have developed their only utility to replace Microsoft Sysprep, which is called QuickPrep. As the name suggests, the intention is to add a linked clone virtual desktop to a Microsoft domain as rapidly as possible. QuickPrep uses an account in Active Directory that you have configured with rights to join computers to the domain. It then pre-populates computer accounts in the domain, which significantly speeds up the deployment process. In addition, QuickPrep allows the administrator to specify where those computer account objects will be created using the Distinguished Name format (e.g. OU=Virtual Desktops, OU=Marketing), thus ensuring the right Active Directory Group Policy objects are applied. Additionally, if you delete linked clone virtual desktop pool it will automate the process of deleting the computer accounts in Active Directory, its worth noting that Dynamic DNS records can still be listed in the DNS database.

For linked clones to be possible, you must install the VMware View Composer Service onto your vCenter server. View Composer also needs a backend database and it is possible to create a new database on your existing database server that is used to hold other VMware databases for features like vCenter and VMware Update Manager.

Install View Composer

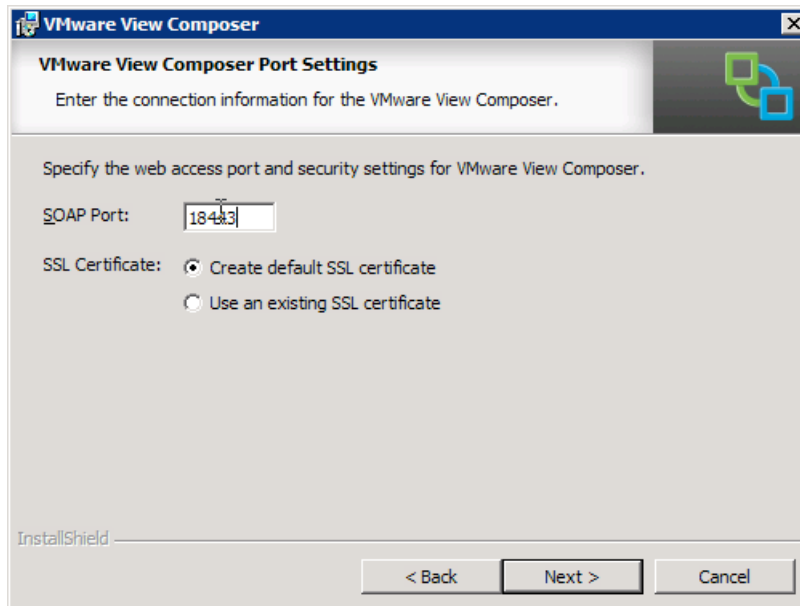
1. **Log on to the vCenter desktop**, and run the **VMware-viewcomposer-N.N.N-NNNNNN.exe**
2. Click your way through the usual suspects of Welcome, File locations and EULA
3. In the **Database Information** dialog supply your **vCenter DSN Settings**



Important:

During the beta programme I discovered that View 4.5 did NOT support the use of spaces in the DSN. This may change when the product becomes generally available. This was still the case at the time of the Release Candidate

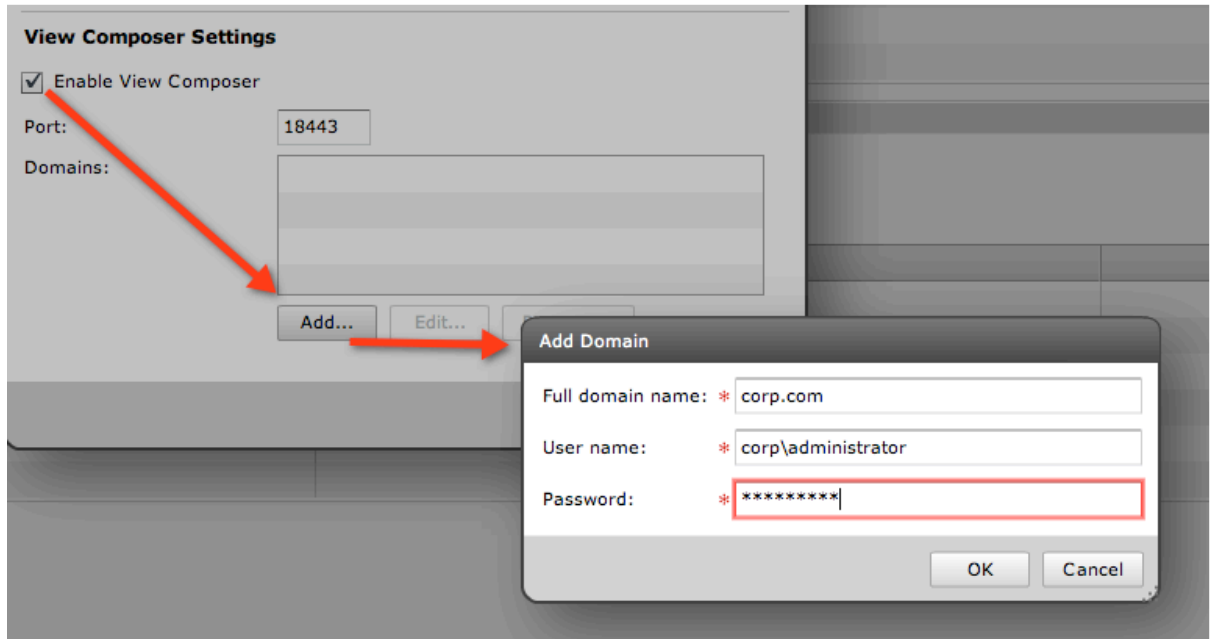
4. **Change the default port for View Composer, and allow it to generate the default certificate for it**



5. Choose **Next** and **Install**

Enable View Composer in VMware View

1. **Login to the Administrative webpage of the Connection Server**
2. Select the **►View Configuration** icon
3. Under the **vCenter section**, select **Servers**
4. **Select the entry for your vCenter and click the Edit... button**
5. Select the **Enable View Composer** option
6. Next click the **Add** button to set the service account for View Composer, under the **Domain Administrators Accounts** click **Add...**
7. In the **Add Administrators popup** complete the dialog box **using a DSN format for specifying the domain, DOMAIN\username format for the username field.**



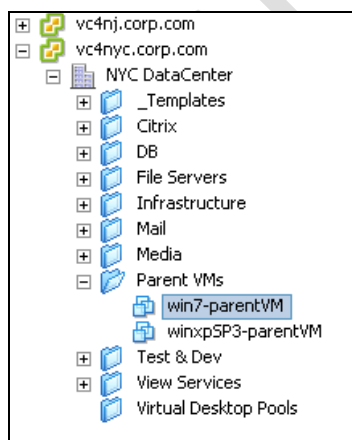
Once enabled you should find the icon for vCenter in the View Admin web page changes to to this:



Prepare Parent VM

The Parent VM forms the base of the virtual desktop pool using linked clones. It's probably a good idea to create a brand new VM from one of your templates that you know works without error. I would avoid re-using some existing VM for use as the parent - it might be claimed by View for a user. If a VM is chosen which has already been created and entitled, it will NOT appear in the list of Parent VMs in the wizard. It took me a day to work that out!

I like to create a special folder for my parent VMs before I begin.



1. Login to the **Parent VM**
2. Confirm it is joined to the domain

3. **Release its IP address** with `ipconfig /release`

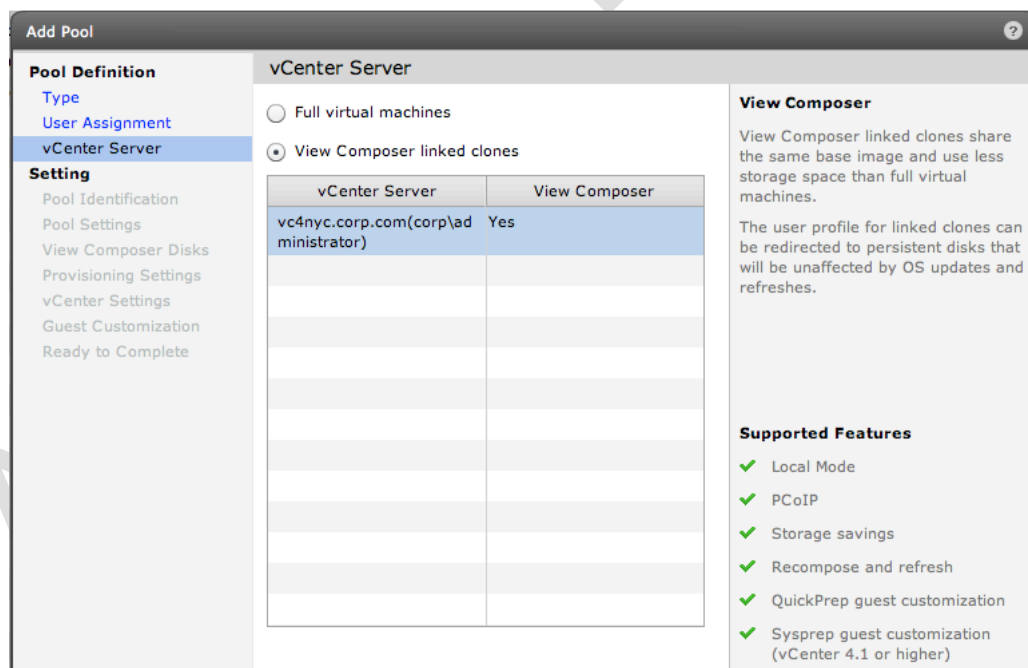
This is done to make sure that the clones do not retain the IP address settings of the parent VM.

4. **Shut down the Parent VM**

5. **Snapshot the Parent VM**, allocating a friendly name such as Baseline Snapshot or alternatively name your snapshot after a grouping such as "Accounts Baseline". A parent can be used multiple times by different pools. But I imagine many people will want to have one parent per pool to keep it nice and simple

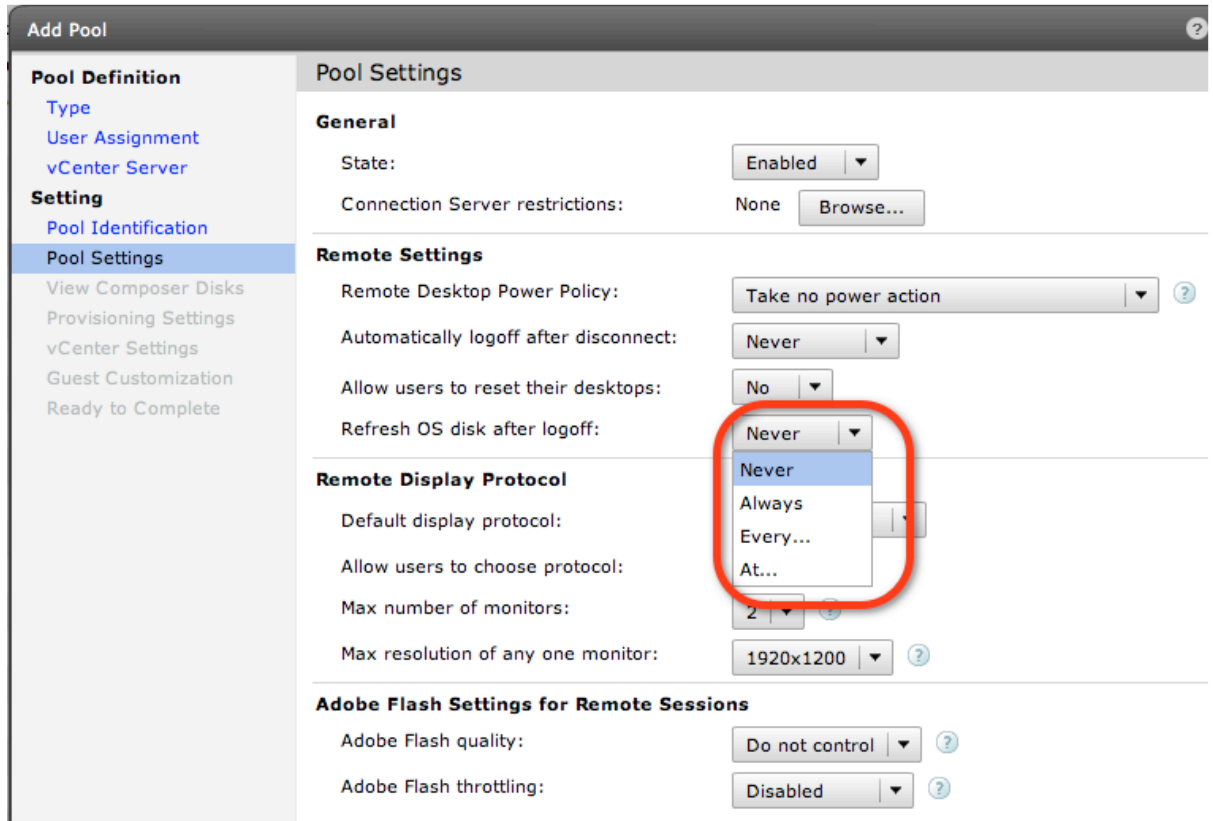
Create the Linked Clone Persistent Pool

1. **Log in to the Administrative webpage of the Connection Server**
2. Open the ► **Inventory**
3. Select the Pools node
4. Click the **Add...** button
5. In the pool type, select the option called **Automated Pool**
6. In the **User Assignment** page, select **Dedicated** as the method, and leave "Enable automatic assignment" as the option
7. In the vCenter page, select the option called **View Composer linked clones**

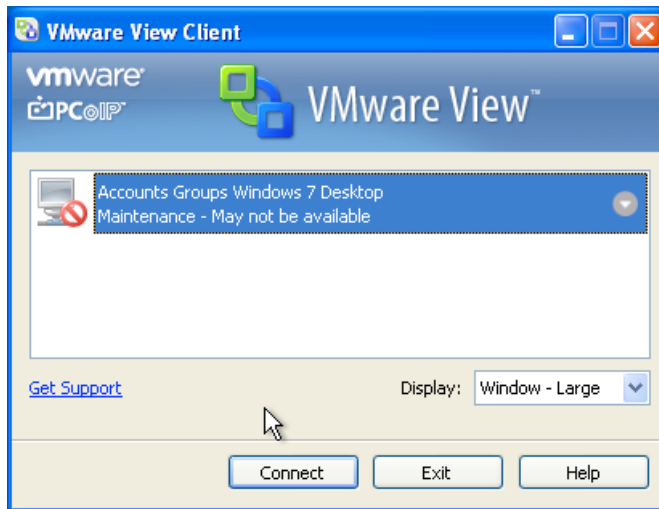


8. Next you must **specify a unique ID for this virtual desktop**, together with **some friendly information by which the end user will be able to identify the virtual desktop**. In my case, I set a unique ID of AccountsGroupWin7, with a friendly name of Accounts Groups Windows 7 Desktop

9. The **Pools Settings** page allows you to control some per-virtual desktop settings that centre around the end user connection. This part of the wizard remains the same, however a new option will also be displayed – allowing control over the use of the “Refresh OS Disk after logoff” option

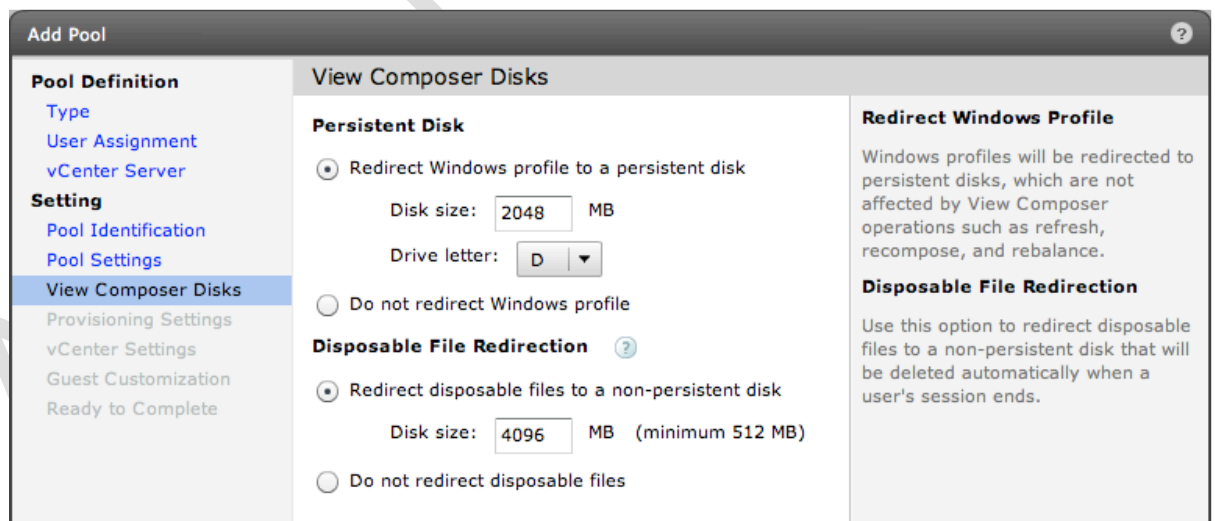


This refresh at log off causes the user’s virtual desktop to shut down, and the delta virtual disks to be discarded. New delta virtual disks are then created. The entire process can take some time and if the user attempts to log out and log in quickly they can find that the virtual desktop is not yet ready. If the user attempts to reconnect while this process is still ongoing, they will receive a message in their client indicating that their virtual desktop may not be available.



Personally, I've found users find this annoying, especially as log out and log in are sometimes used as a cure all for fixing problems in Windows. Personally, I would consider using "Never", and instead use the Connection Server's manual "Refresh" option which allows to you refresh the desktops at a given date and time. This would allow us to refresh the virtual desktops during the evening or weekend in such a way as to minimize the impact on end users.

10. The **View Composer Disks** page allows control of the user profile disposable disk. In my case, because I opted for the automated and dedicated pool type, I selected to "Redirect Windows profile to a persistent disk"

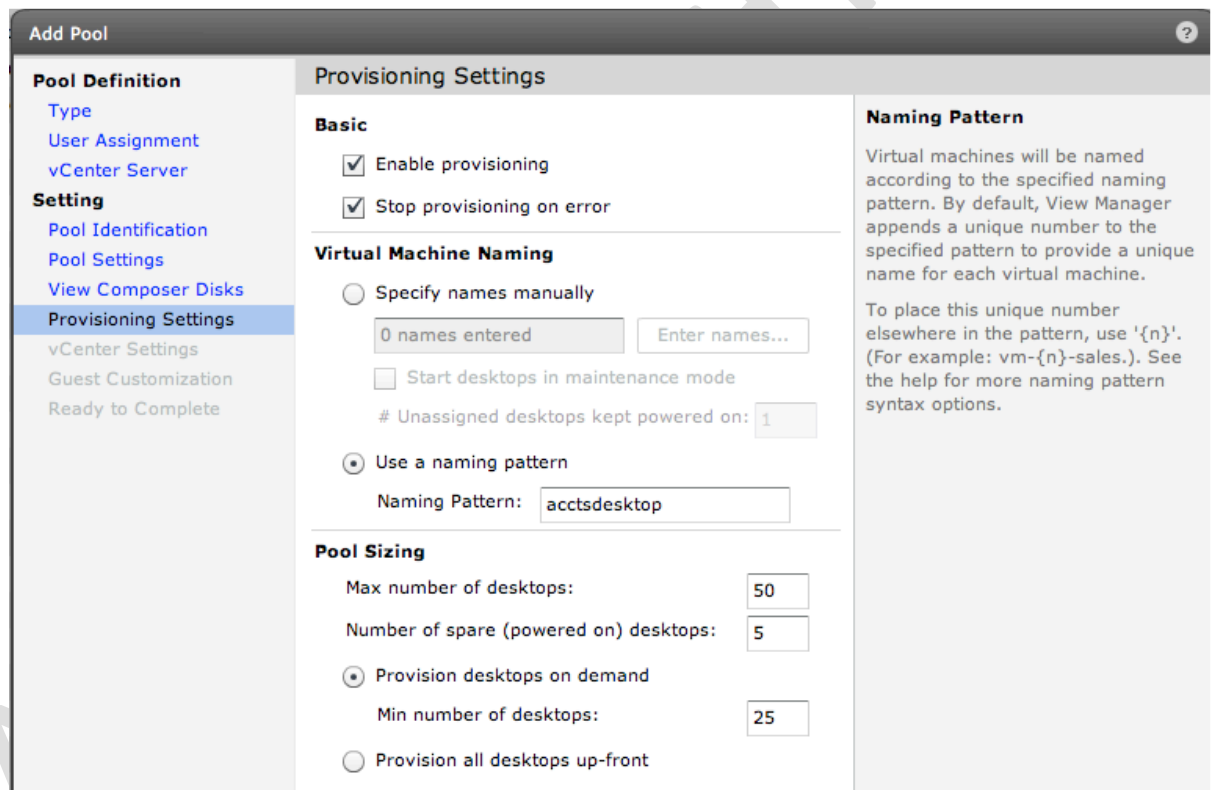


There are lot of options here which I think really need clarifying. If you choose "Redirect Windows profile to a persistent disk" you essentially abandoning the concept of roaming profile. Every time the user logs in they are returned to the same desktop with the same persistent profile. If you choose "Do not redirect Windows Profile" the profile remains in the C drive until you enable roaming profiles.

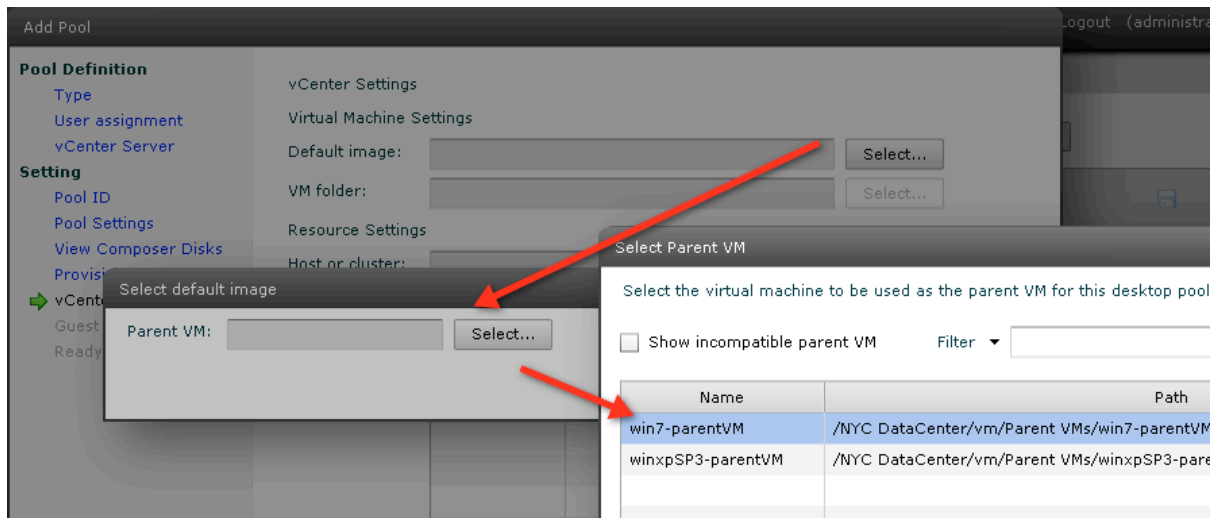
The “Disposable Disk” is used to handle the location of temporary files – a good example of this is the swap file in Windows. If this enabled these temporary files are relocated to the new location, and destroyed at log off. So if you think about it they’re four possible scenarios you could configure here.

It’s worth mentioning that you could choose not redirect the Windows profile, and use roaming profiles – but augment that solution with some kind “virtual profile” feature. It was hoped that VMware’s own virtual profile feature would ship with the 4.5 product, that sadly that isn’t the case.

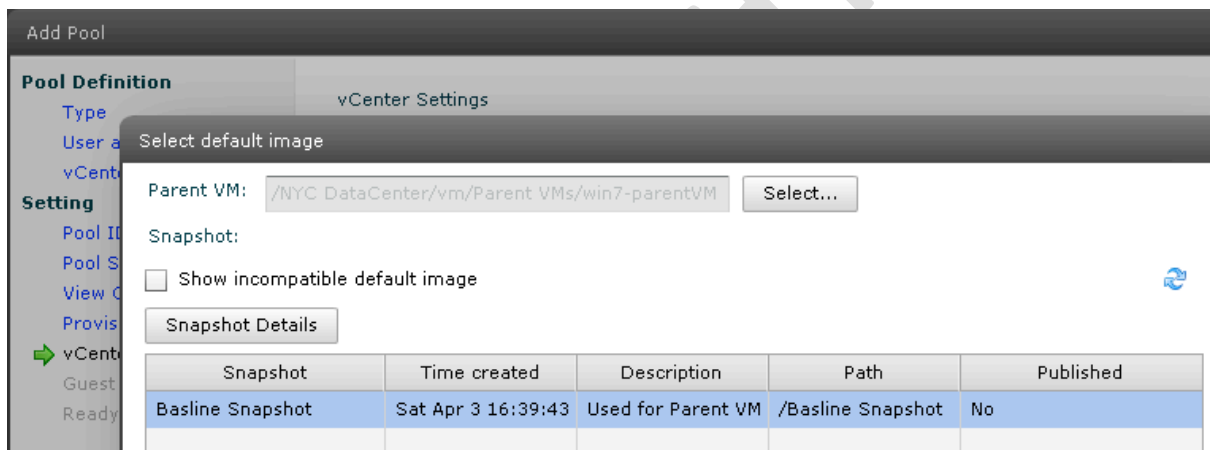
11. The **Provisioning Settings** page controls how the virtual desktops will be created in the pool. In this case I was able to use much larger values for max, spare and min because each VM will take up a fraction of the disk space used with virtual desktop pools created without linked mode.



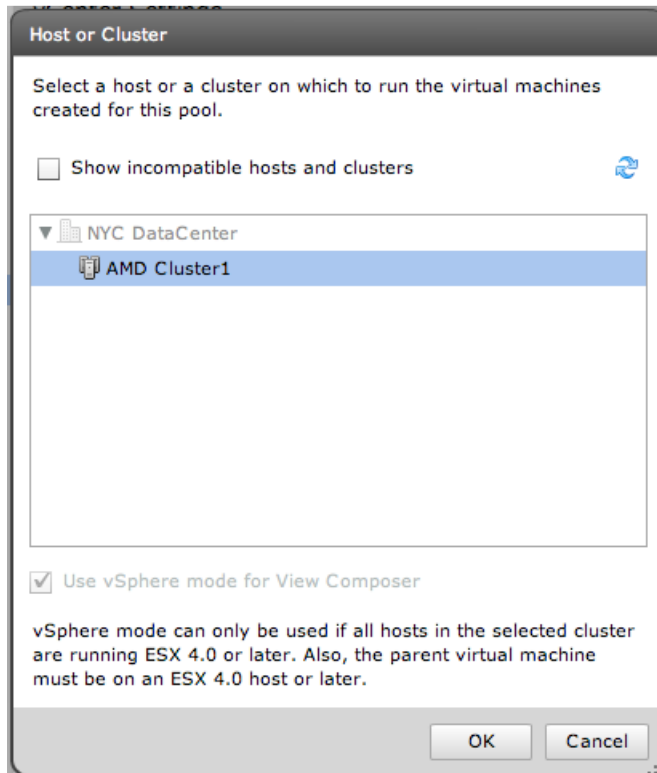
12. In the **vCenter Settings** page we can **select the Parent VM** that will form the basis of the linked clone. Each select button allows you to browse the vCenter selected earlier to indicate where the VMs should be located in terms of the VM Folders, Cluster and Resource Pool. In this case the wizard changes appearance to allow selection of the Parent VM



13. After **selecting the Parent VM**, you are then able to **select the snapshot** taken earlier:



14. Additionally, the **Host or Cluster dialog box is also slightly different**. It has an option to indicate whether you are using VM Hardware version 7 VMs on a pure ESX4 environment, or if you are using legacy VM Hardware version 4 VMs on the ESX3 platform. vCenter 4.0 does allow for both ESX3 and ESX4 hosts to co-exist in the same management context, but a VM Hardware version 7 virtual machine cannot run on an ESX3 host:



15. **Select a storage location.** Again, this dialog box changes once you are using linked clones. The interface allows you place the OS Disk, Persistent Disk and Master VM disks on different storage locations to improve either performance (say for the delta drives) or choose a lower tier of storage for components whose disk I/O will be less demanding. The emphasis in the dialog is on the space required for the linked clones, but remember that these different datastores could also be on different tiers of storage offering potentially different levels of both performance (SATA/FC/SDD) and fault tolerance (RAID5, RAID10 etc). Additionally, View estimates your storage consumption, and you are able to indicate how conservative or aggressive you are to disk over-commitment.

Select the datastores to use for this pool. Only datastores that can be used by the selected host or cluster can be selected.

Show incompatible datastore Local datastore Shared datastore

<input type="checkbox"/>	Datastore	Capacity (GB)	Free (GB)	Type	Use For	Storage Overcommit
<input type="checkbox"/>	rtfm_templates	200	41.32	NFS		
<input type="checkbox"/>	srm_new_york	49.75	18.89	VMFS		
<input type="checkbox"/>	templates	199.75	76.04	VMFS		
<input type="checkbox"/>	view	99.75	75.5	VMFS		
<input checked="" type="checkbox"/>	view-composer-disks	49.75	43.76	VMFS	Persistent disks	Conservative
<input checked="" type="checkbox"/>	view-master	59.75	17.2	VMFS	Master VM	Moderate
<input checked="" type="checkbox"/>	virtualdesktops	99.75	84.12	VMFS	OS disks	Aggressive

Use different datastore for OS disks and View Composer persistent disks

Use different datastore for View Composer replicas

Use For	Free (GB)	Min Recommended (GB)	50% utilization (GB)	Max Required (GB)
OS Data free space selected:	84.12	264.00	964.00	1,764.00
User data free space selected:	43.76	20.00	50.00	100.00
Master VM free space selected:	17.2			

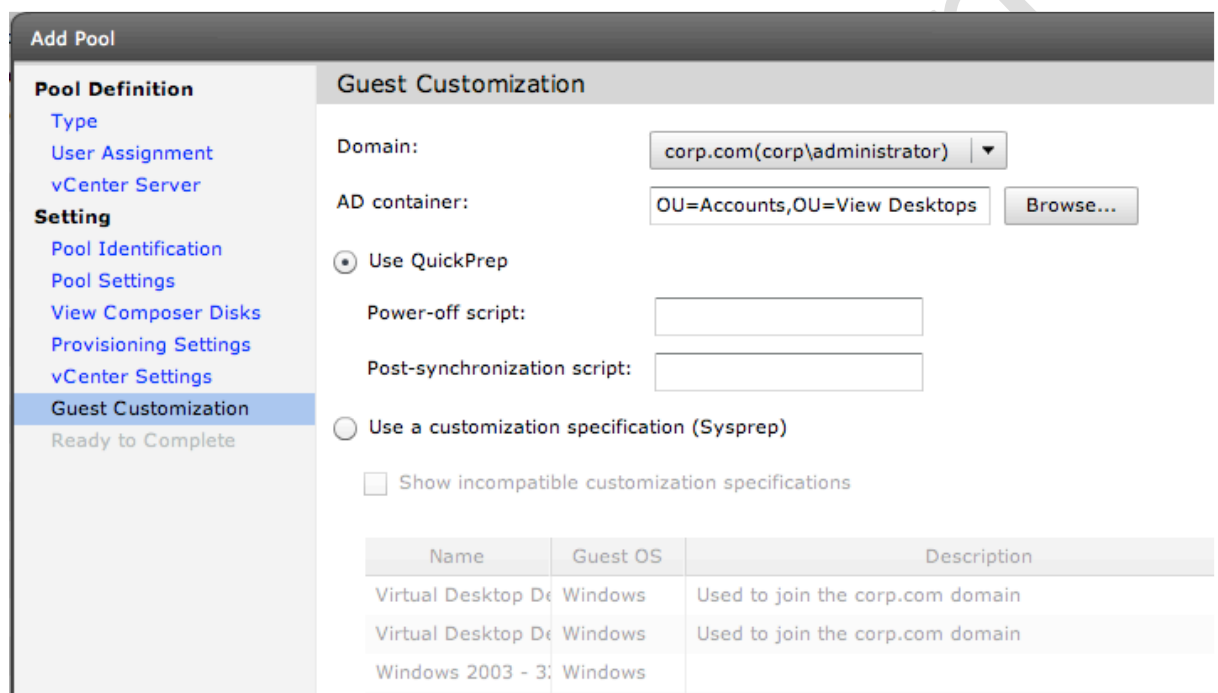
This screen grab has been constructed merely to illustrate the options available. If you enable the two options in the far left-hand corner (circled), this will allow you the most control over the placement of all the virtual disks or deltas that make up a linked clone.

With linked clones, it's possible to create perhaps 50 virtual desktops from a 10GB parent, but because the clones are merely deltas of the parent, they will not take up 500GB of disk space. In fact, they will take up much less. When I set up the storage, I hope that the VMs never actually need all the disk space I am assigning. The dropdown option allows me to set preferences of Aggressive, Moderate and Conservative as my estimate of how intensively I want to over-commit the storage used. If I select Aggressive, I'm indicating that I expect the delta files and the user data disk to grow in size very slowly – thus allowing me to create many virtual desktops with very little available storage capacity. By contrast, the Conservative option allows me to indicate that I expect the delta and the user data disk to grow rapidly. Clearly, if I have a policy to always "Refresh OS disk at logoff", the size of the deltas will be very small. The longer you retain the delta data, the greater the amount of free disk space you will need to hold that information.

At the bottom of the page, VMware do a good job of estimating the actual disk usage compared to the delta file usage. These numbers will turn red if you try to do something silly, like trying to create 1,000 desktops on a 10GB volume. This will happen if your datastores have less free space than the value represented in the Minimum

Recommended column. In the screen grab above, I selected different datastores which clearly have insufficient space for the volume of VMs I am creating, despite the space-saving properties of linked clones.

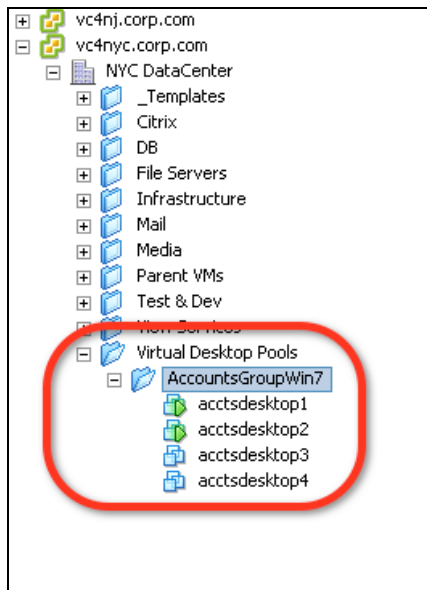
16. Finally, you will be able to specify options for **VMware QuickPrep**. The new browse button allows you to locate an OU where you would like QuickPrep to create the computer accounts. This is very useful for selective usage of computer-based Group Policy objects. After browsing the AD Structure, View automatically completed the DN (Distinguished Name) which reduces errors created by typos, not that I'd know anything about those!



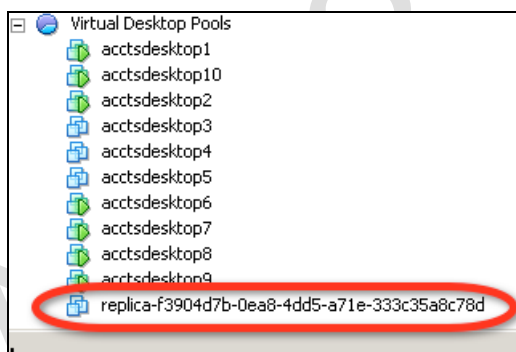
Whilst QuickPrep offers nothing like the level of sophistication that Microsoft Sysprep has, it does significantly decrease the deployment time caused by Sysprep's Mini Installation Wizard. In the example above, I decided to create a pool of desktops for accounts, and created an OU in Active Directory called Accounts to hold the computer accounts. As you can see, QuickPrep uses the Distinguished Name (DN) format for specifying the path to the OU using a comma to separate one OU from the next, such as "OU=Accounts,OU=Virtual Desktops".

It is also possible to call Power-off and Post-synchronization scripts for any additional desktop preparation work that needs to be carried out before the users access their desktops.

Once you click finish in the wizard, the deployment will begin. The process starts by creating a folder in Virtual Machines and Templates named after the unique ID for the pool – in my case this was AccountsGroupWin7. This holds the linked clones:



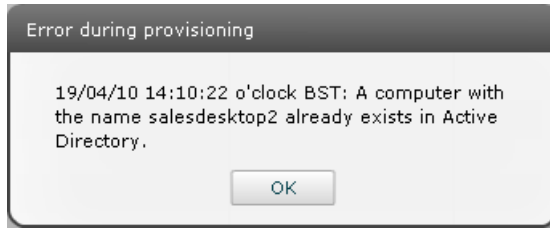
In the main Hosts and Clusters view you will see a “replica” VM. The Replica does take some time to be created, however, once completed you will find the system will very quickly begin to create your virtual desktops in the folder you selected with the wizard. One interesting aspect of the Replica and its linked clones is that it cannot and should not be deleted manually from vCenter. They can only be deleted by deleting the linked clone desktop pool in the View admin page. These objects are marked as being protected in this way to prevent accidental deletion of the source of the linked clones. If the Replica were deleted accidentally, the linked clones would be orphaned from the system. The Replicas are not given especially friendly names as you can see:



Note:

Warning:

Be careful if you delete and then recreate a pool. The deletion of a pool does not always delete (although with linked clones it should) the computer account objects created by either Sysprep or Quickprep. If Quickprep encounters a NETBIOS name that is already in use, the deployment will fail:



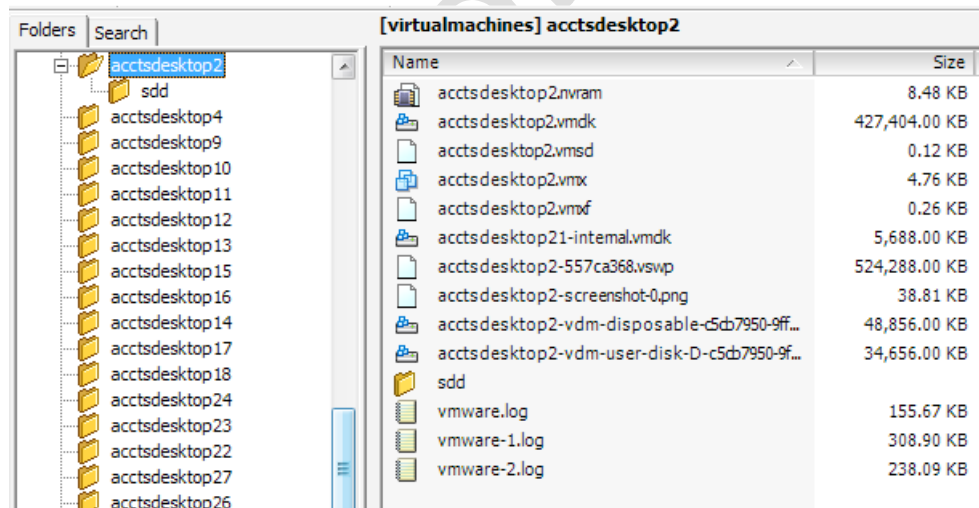
The vCenter Environment after using Linked Clones

In this section, I just want to very quickly tie up some loose ends in terms of the changes created by View Composer and the Linked Clones feature. I'm a firm believer in mapping abstract concepts to something tangible that you can see on screen. Most people learn by doing and seeing, rather than just listening to dry and abstract explanations based on pure theory!

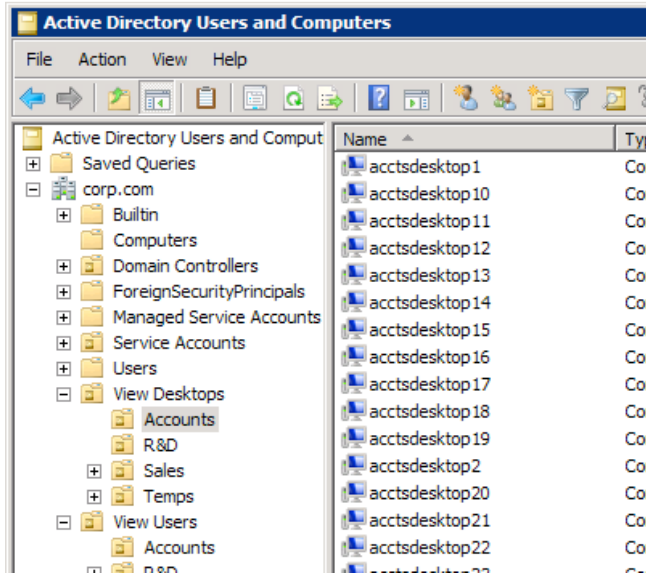
If I use the data store browser to examine the location selected for the virtual desktop (in my case I selected virtualdesktops), you can see that each of the linked clones' delta virtual disks takes up a very small amount of space.

As you can see, the linked clone called acctdesktop1 is only using 32MB of data; in fact its virtual machine swap file is larger than the virtual disk containing the desktop.

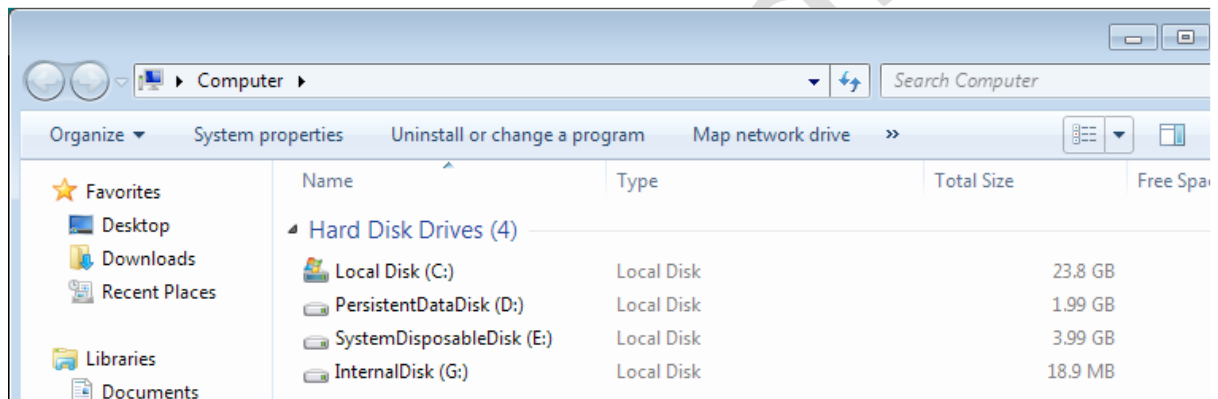
Similarly, the virtual disk which holds the Persistent Data Disk on the virtualdesktops VMFS volume is very small indeed, in this case around just a couple of KB in size.



Finally, in Active Directory, because I set appropriate values for QuickPrep, the OU called Accounts has been populated with computer accounts valid for each virtual desktop created.

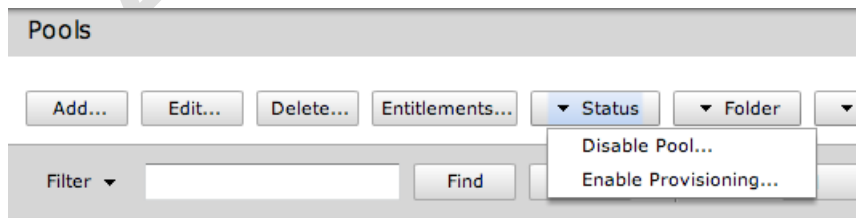


My last screen grab below shows the OS virtual disk and Persistent Data Disk, together with SystemDisposableDisk and InternalDisk in Windows Explorer in the VM.



TIP:

Occasionally, vCenter might not be available during the provisioning process, and this can cause the provisioning process to terminate unexpectedly, leaving a red X next to your pool. You can select the pool and restart the provisioning process from the status button once you have rectified your vCenter issue:



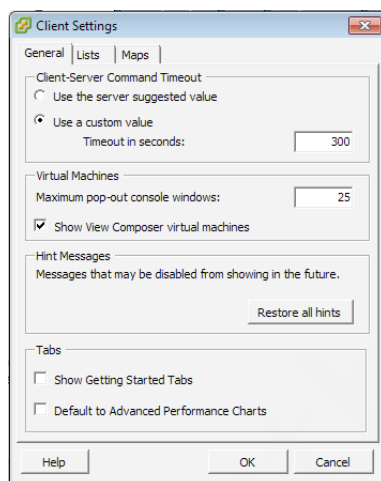
This option can be used to enabled and disable the provisioning process on demand.

Fixing Linked Clones Errors

Occasionally, (more occasionally than I would like) the removal of a linked clone enabled pool goes wrong. When you destroy a linked clone pool it should power down all the virtual desktops, and the finally delete the replica and the VM folder that was created in the deployment process. Sadly, this process doesn't always complete correctly, and it's often caused by a failure of communication between the VMware Composer service and the VMware Connection server.

Although the virtual desktops can be manually powered off, and deleted – you will find even as the administrator you will be unable to delete the replica from the system. This is because it is marked as “protected” object in the vCenter environment. The whole situation can very frustrating! Fortunately, there's a command-line utility that can be used to both unprotect the replica and remove it. The Replicas are stored in a hidden virtual machine folder called “VMwareViewComposerReplicaFolder”.

By default this fold is suppressed in the vSphere Client, but it can be made visible by changing the client options in Edit menu, Client Settings and enable the “Show View Composer virtual machines” option.



To remove orphaned replicas you can use the command `sviconfig`, and you will find it in `C:\Program Files (x86)`. The full command is documented in this KB article - <http://kb.vmware.com/kb/1008704>

Below is a sample syntax.

```
Sviconfig -operation=unprotectentity -VcUrl=https://localhost/sdk -  
Username=corp\administrator -Password=vmware -InventoryPath="/NYC  
DataCenter/vm/VMwareViewComposerReplicaFolder/replica-22bdbbed-  
fd79-45a1-b454-69be7ccc637b" -Recursive=true
```

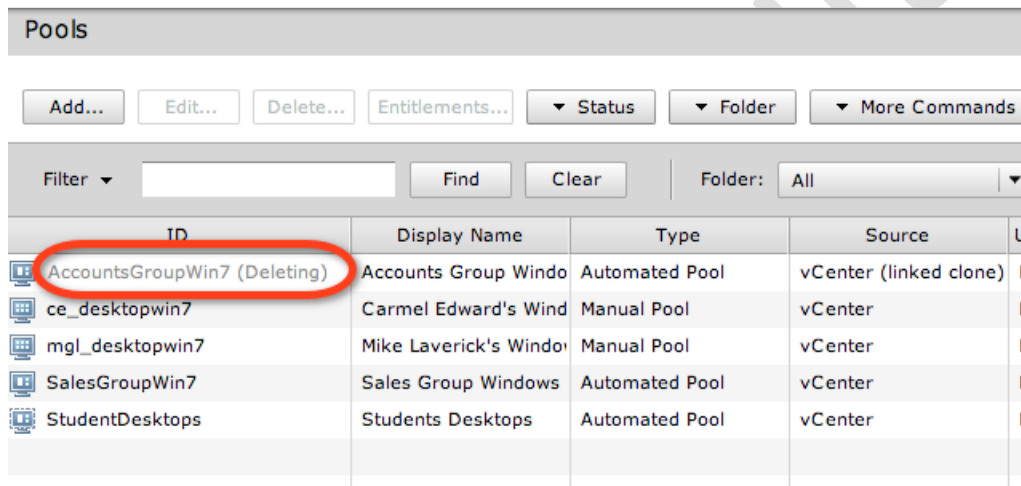
TIP: I use cut and paste to get hold of the long replica-NNNN value rather than typing it in manually.

The successful out come of this command will result in an output like this:

```
WARNING: Unprotecting UC managed entities will allow operations
(power on, delete, migrate) that can cause existing linked clones connected
to those managed entities to fail to work correctly.
Establishing connection to the UC server.
UC server connection established successfully.
Looking for the entity on the UC server.
VirtualMachine found.
VirtualMachine with MoId vm-820 successfully unprotected.
SvcConfig finished successfully.
Successfully unprotected entities: 1
Fail to unprotect entities: 0
```

Once this command has been running you will be able to manually delete the replica, and the other components that make up the linked clone desktop pools.

In addition to this I've sometimes found that linked cloned virtual desktop pools hang about in the web administration pages. They seem to hang in a (deleting...) process and won't complete. Normally, you can just click the refresh button in View, and then this entry will be removed – but sometimes it just appears to get stuck as process.



The screenshot shows the 'Pools' section of a vCenter web interface. It includes a toolbar with buttons for 'Add...', 'Edit...', 'Delete...', 'Entitlements...', 'Status', 'Folder', and 'More Commands'. Below the toolbar is a search area with a 'Filter' dropdown, a search box, and 'Find' and 'Clear' buttons. The main area is a table with columns for 'ID', 'Display Name', 'Type', and 'Source'. The first row, 'AccountsGroupWin7 (Deleting)', is circled in red. Other rows include 'ce_desktopwin7', 'mgl_desktopwin7', 'SalesGroupWin7', and 'StudentDesktops'.

ID	Display Name	Type	Source
AccountsGroupWin7 (Deleting)	Accounts Group Windo	Automated Pool	vCenter (linked clone)
ce_desktopwin7	Carmel Edward's Wind	Manual Pool	vCenter
mgl_desktopwin7	Mike Laverick's Windo	Manual Pool	vCenter
SalesGroupWin7	Sales Group Windows	Automated Pool	vCenter
StudentDesktops	Students Desktops	Automated Pool	vCenter

Restarting and rebooting the Connection Server does not fix this. I have however had some success with the new PowerCLI snap-ins. The new PowerCLI snap-ins contains a remove-pool cmdlets that can be used to remove desktop pools based on their Pool-ID parameter.

Remove-Pool -pool_id AcctsGroupWin7

Chapter 10: Refresh, Recompose and Rebalance

Once a linked clone desktop pool has been created, you have a few additional options or controls to manage them back on the main management webpage – VMware uses the terms Refresh, Recompose and Rebalance to describe the three main tasks that may need to be carried out on your linked clones. VMware uses quite neutral-sounding terms for these tasks – the words “refresh”, “recompose” and “rebalance” sound quite reassuring and non-intrusive. Don’t be fooled by the soft-sounding words, these changes have a huge impact on users and can take some time to complete, depending on the number of virtual desktops in the pool.

Refresh – This option resets the delta disks back to the original state. If you are familiar with VMware Snapshots, the process is analogous to reverting the VM back to its original state when it was first created. Any modifications the user has made to the virtual desktop will be discarded. Remember, this option can also be triggered by the logoff event (using the Pool Settings page), so every time the user logs off, the delta disk is discarded and regenerated. A refresh can be quite an intrusive task because if affected users are currently logged in, they will receive a message forcing them to log out of their environment. The virtual desktops are all powered off and new delta virtual disks are created.

Recompose – In this process, the linked clones are attached to a new replica. The net effect is that all the changes accrued in the delta disk are lost, and users get a brand new virtual desktop. The Recompose command can be used to roll out new software or a new service pack – effectively replacing the virtual desktop with a new build without having to re-create the virtual desktop pool and entitle it for the correct users. A recompose is a very intrusive task - if affected users are currently logged in, they will receive a message forcing them to log out of their environment. The next time they log in they may be receiving a very different desktop look and feel.

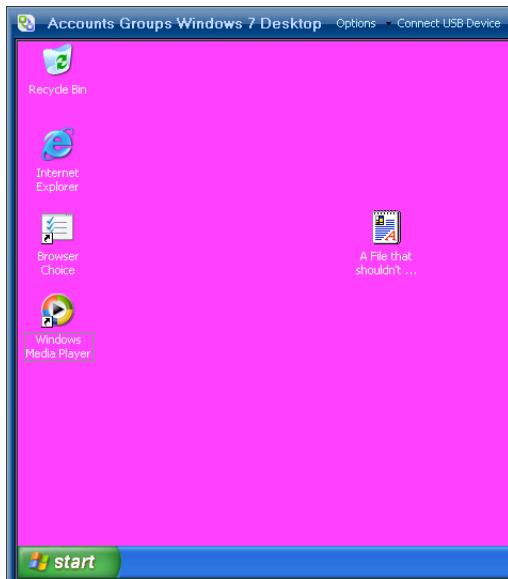
Rebalance – This option is there if you have selected different storage locations for your virtual desktops. It could be the case that you have more virtual desktops in one datastore than another. The Rebalance command attempts to redistribute the VMs evenly among the datastores. It’s essentially a storage management option.

Refresh Virtual Desktops in the Pool

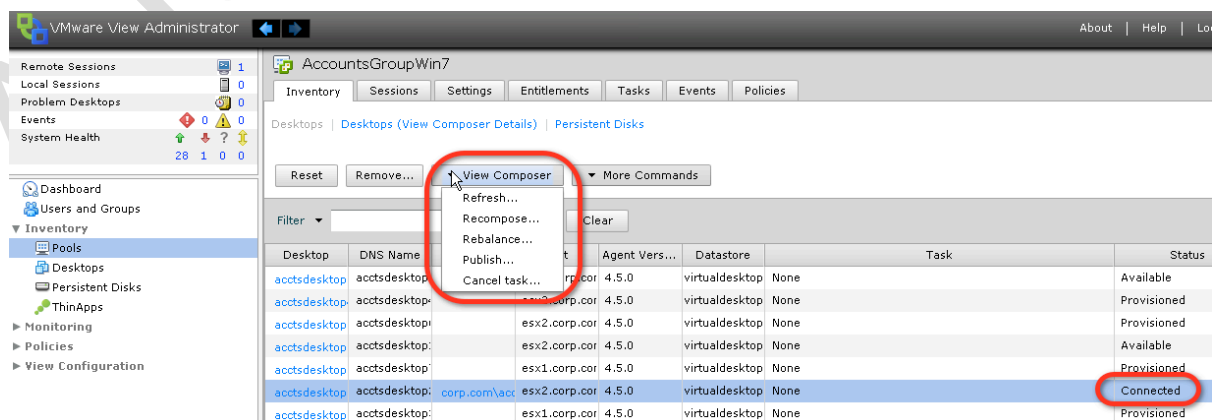
It is possible to refresh every virtual desktop in the pool, or by selecting individual virtual desktops in the list, refresh only those virtual desktops you feel need it. To test this and other features, I made a point of making changes to

the user's environment. So, in one case I made the desktop a bright pink and created a file that shouldn't have been there! NICE!

Remember that these changes go to the user's profile, and in the steps I outlined earlier I set a **persistent** disk. So, although changes in the operating system will be reset, the changes made to the profile disk will be kept. This means you can safely reset the operating system without losing the user's settings or data held in user profile locations such as their Desktop or My Documents folders.

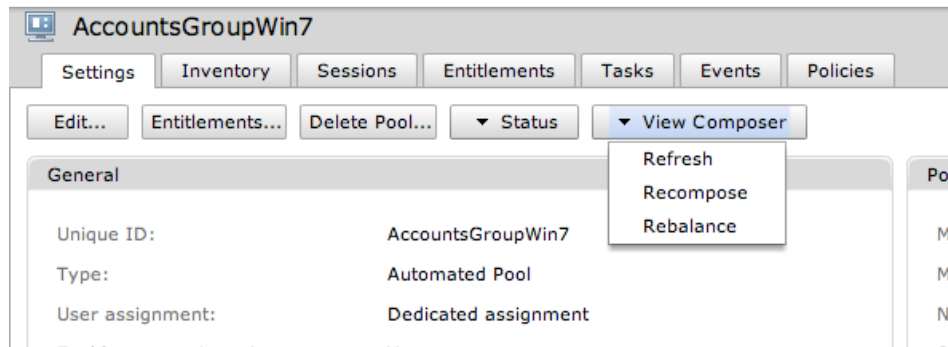


1. In the ► **Inventory**
2. Select **Pools** and **Select the Pool** you wish to modify:
3. **Select the desktop(s) you wish to refresh.** The system will allow you to use shift-click to bulk select desktops, and ctrl+click to select disparate desktops. Notice in the screen grab below, I have selected a desktop that I know has a user connected. Next click the **View Composer** button and select **Refresh**

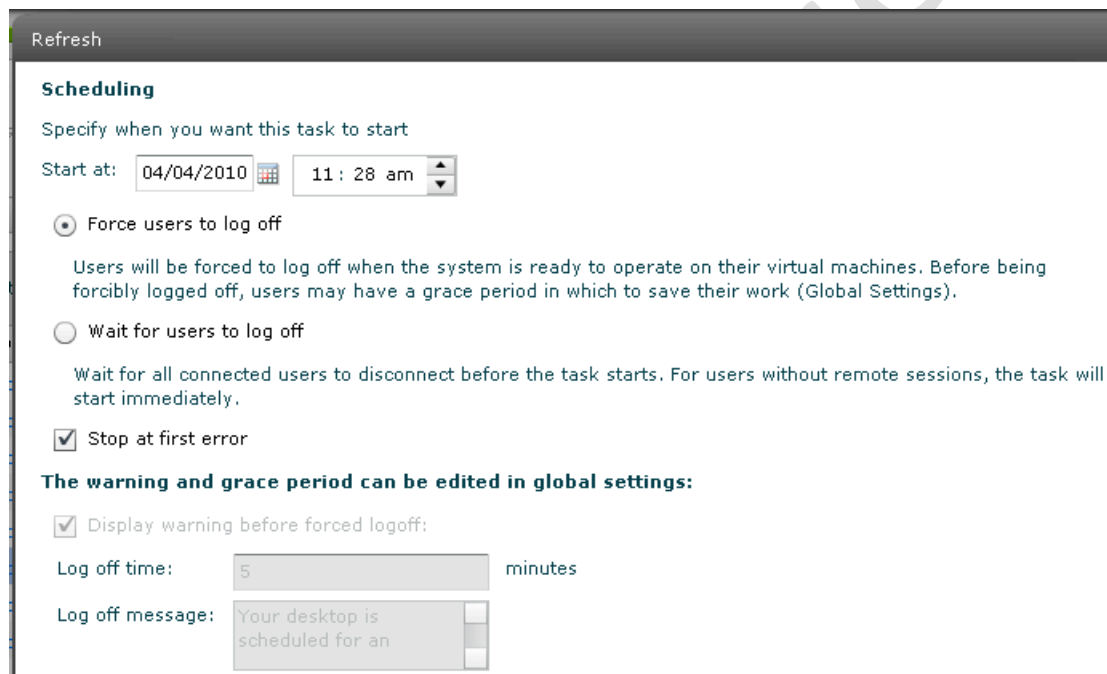


Note: I am aware that this graphic is shows an older version of the product whilst still in beta. However, it was too difficult to reproduce the exact same scenario using the GA product. The only difference is the icon next to the AccountsGroupWin7 pool name

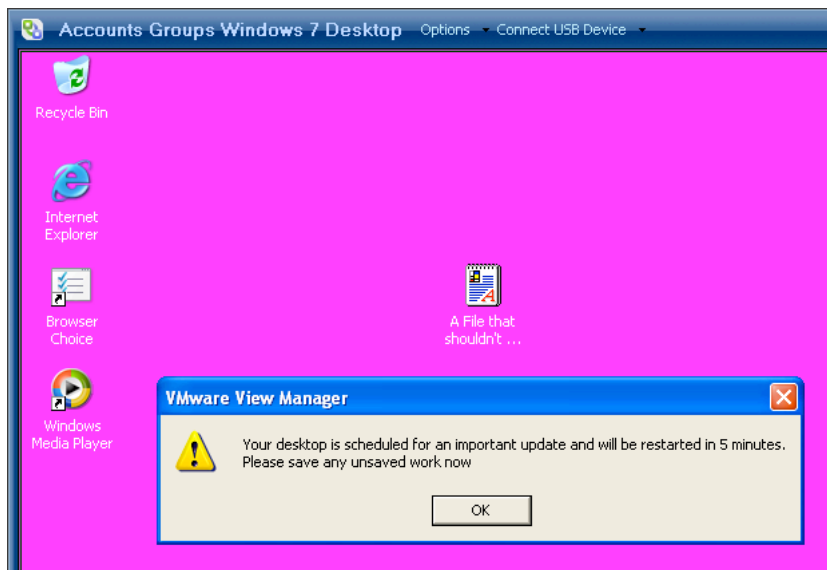
It is possible to refresh the entire desktop, from the **Settings** tab on the properties of the pool



4. This will bring up the **Refresh** page, which controls what will happen to users when the refresh occurs. I think this is fairly self-explanatory.



As you can see you set a time for the event, which allows you to defer the refresh until a more suitable and less intrusive time. You can force users to log off, which will send them a warning message (configurable under the global settings) and give them 5 minutes to save their work (also configurable). I think these are quite dangerous settings, given that users tend to leave themselves logged in whilst chatting around the water cooler. Alternatively, you can wait until users log off for the refresh event to take place. The dialog box looks like this:



Note:

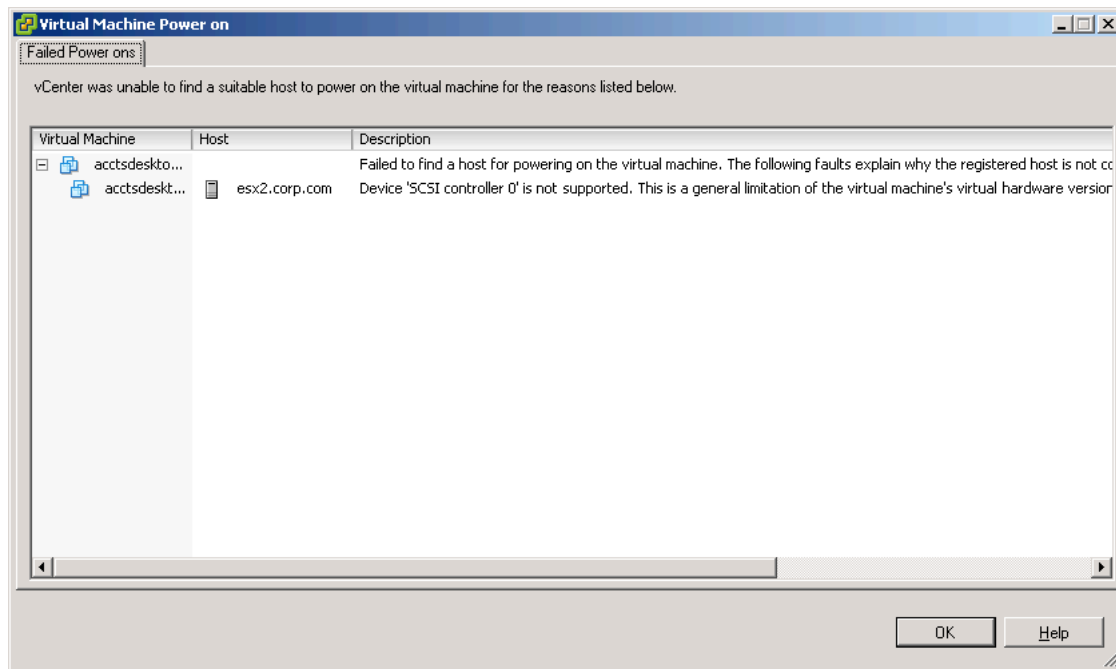
The outcome of this process should result in the user getting a brand new copy of Windows without losing their settings – as these have been stored in the Persistent Disk. Alternatively, if you redirect the Windows profile to the network (aka the roaming profile) then user settings should not be lost in this process

Recompose a Linked Clone Virtual Desktop

There are a number of ways to recompose a linked clone. You can either attach a brand new parent, or snapshot the existing parent with new changes. Remember, a recompose is essentially a quick way of pushing out a new build of the corporate desktop. I would recompose with a new snapshot if I was making a major change such as rolling out a service pack or upgrading the web browser from one version to another. In my example below, I'm going to upgrade Windows Media Player from version 9 to version 11 with my Windows XP desktops.

WARNING:

DO NOT use this feature to roll out a new operating system, such as switching from a Windows XP virtual desktop to a Windows 7 virtual desktop. You are far better off creating a brand new pool and assigning and un-assigning the users accordingly. Additionally, if you re-parent the VMs with a new parent of the SAME operating system type, ensure that the VM Hardware versions match. Otherwise you can anticipate fun and games when you try and power on the VMs after the recompose:

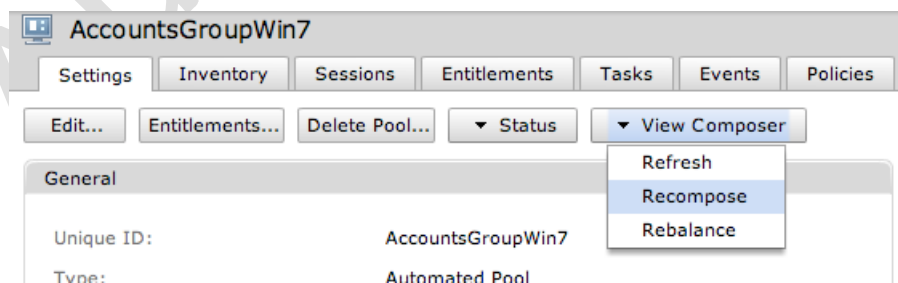


1. Power on the Parent VM

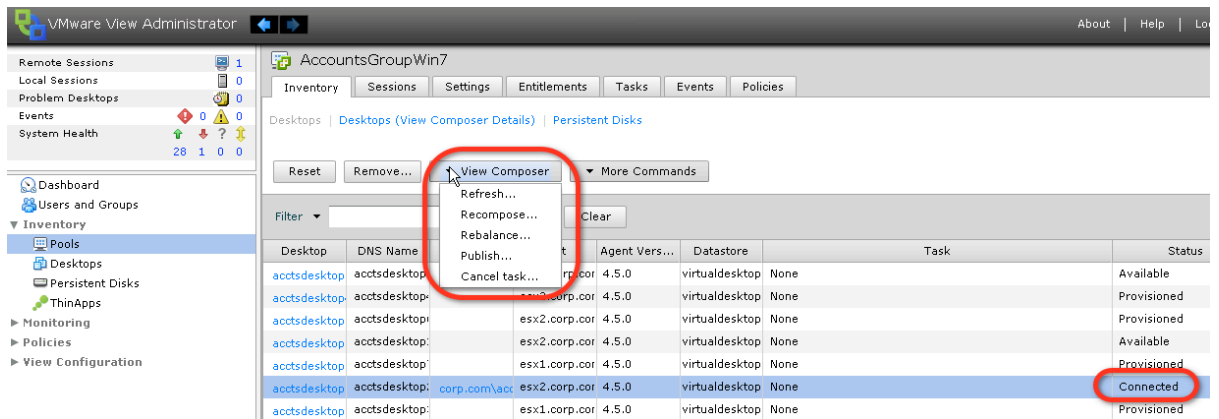
Note:

Remember you can make changes to the Parent VM at any time. The linked clones get their data from the replica of the Parent VM

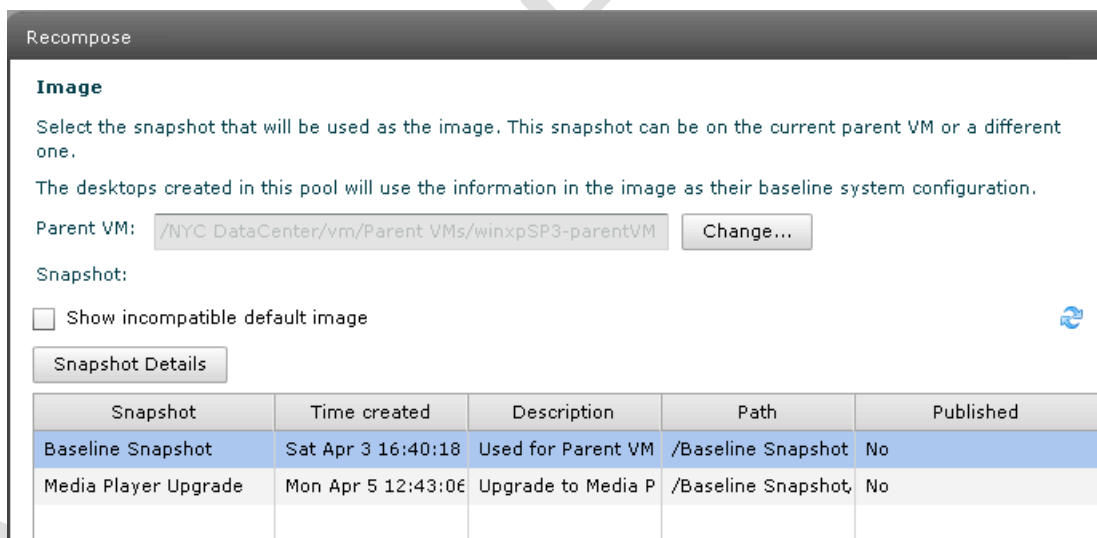
2. Log in and make your changes, in my case I downloaded and installed VLC Media Player
3. Once you have made your updates, **release the IP address of the Parent VM with ipconfig /release**
4. **Power off the Parent VM**, and **create a new snapshot**. In my case, I called it "Media Player Upgrade"
5. In the ► **Inventory**
6. Select **Pools** and **Select the Pool** you wish to modify:



Note: As with the refresh option you are able to select individual desktop for a recompose as well.



- The large change button allows you to completely alter the base image used for the linked clone. In my case however, I've only made a slight modification to the Parent VM. Remember, the Parent VM can have multiple snapshots used by multiple desktop pools. This means that you don't have to maintain a separate Parent VM for each different type of desktop pool you have – just a different snapshot for each desktop pool you maintain. However, its important to under the scalability limitations of a Parent VM with multiple snapshots – working numbers suggest in the region of 50 snapshots.



As with refreshing a desktop, you can schedule when this event will occur, View will then orchestrate the whole process of logging out users and will then proceed to power off each virtual desktop and delete it. Once all the desktops have been destroyed, View sets about creating a brand new set of virtual desktops from a new replica based on the new snapshot - in my case called Media Player Upgrade. During this process, you will see that the old replica files are unregistered and deleted.

This is clearly a very intrusive task to the end users, but saves time for administrators since you don't have to create a new pool with new settings every time you need to make a change to the OS. However, as

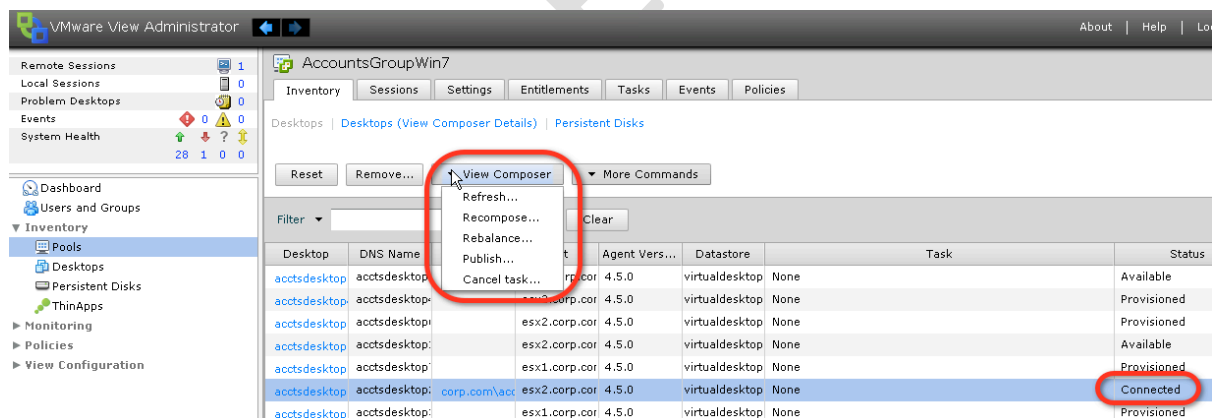
it effectively destroys the old pool and creates a new one, it's important to note that a recompose is not a trivial event.

The screen grab below shows the recompose in mid-cycle. An additional replica has been generated, with the older replica yet to be destroyed.



Rebalance a Linked Clone Virtual Desktop

1. In the ► **Inventory**
2. Select **Pools** and **Select the Pool** you wish to modify
3. **Select the desktop(s) you wish to refresh.** The system will allow you to use shift-click to bulk select desktops, and ctrl+click to select disparate desktops. Notice in the screen grab below, I have selected a desktop which I know has a user connected. Next click the **View Composer** button and select **Rebalance**



Rebalance

Rebalance

The rebalance operation evenly distributes desktops across the datastores available to this pool. Only desktops in the Ready, Error, or Customizing state with no schedules or pending cancellations can be rebalanced.

In order to rebalance the desktops it is necessary to refresh the operating systems to their base image, resetting the operating system disk to its initial state. User data will be unaffected if it resides on a separate disk.

Chapter 11: Enabling Local Mode

Very Important (Yes I mean VERY important. You should read this. You really should!)

*Local Mode uses a new role called the Transfer Server that is used to speed up the download and upload process. On Windows 2008 R2, VMware **ONLY** support the BusLogic or LSI Logic controller, unfortunately Windows 2008 R2 defaults to the LSI Logic SAS controller. Sadly, there is no safe or supported method to changing this if you have this in your default template for Windows 2008 R2. Even adding in second disk on different SCSI controller doesn't work, and renders the VM unbootable. This caused me to install Windows 2008 R2 all over again. I wasn't best pleased I could tell. You see I have better things to do with my life and time, than install Windows. That's why I got into VMware.*

*Finally, unlike the other server roles that make up View – the transfer server **MUST** be installed into a virtual machine running under vSphere. Well, at least they got that part right, eh?*

The Local Mode feature allows a user to carry on using their virtual desktop even when they are not connected to the network. Users now represent an increasingly mobile population who expect access to corporate services on the move – and not all of those services can currently be provided by handheld devices such as smartphones and PDAs. A Local Mode desktop is enabled by installing a special client onto the user's computer, and installing the Transfer Server component on the View back-end. The Transfer Server is a new component in View. Previously, offline desktops (as they were then called) were managed by the Connection Server. VMware have developed a more efficient Transfer Server role to improve the synchronization process. The main engine of the Transfer Server is the Tomcat web service. The Transfer Server is designed to run solely and only in a virtual machine, and it is possible to have more than one. All Transfer Servers connect to a centralized repository of virtual desktops (the Image Library) that have been checked out for Local Mode use. In a simple configuration its possible to store the checked out offline desktops inside a second virtual disks inside the Transfer Server rather than on an external file server on the network.

Local Mode desktops work by first downloading the user's entire virtual desktop to their local computer in a process called "Checking Out". This initial download can take some time, so it's best done from the LAN in this first instance. The Local Mode desktops essentially then become a synchronization feature that you might have come across in other technologies, with just the differences synchronized between the user's local computer and the View environment. When the user is disconnected from the network - say on a longhaul flight - the

locally-cached offline desktop is powered on and available. While the user works with the offline desktop, changes accrue in a snapshot delta file. This allows for further functionality such as:

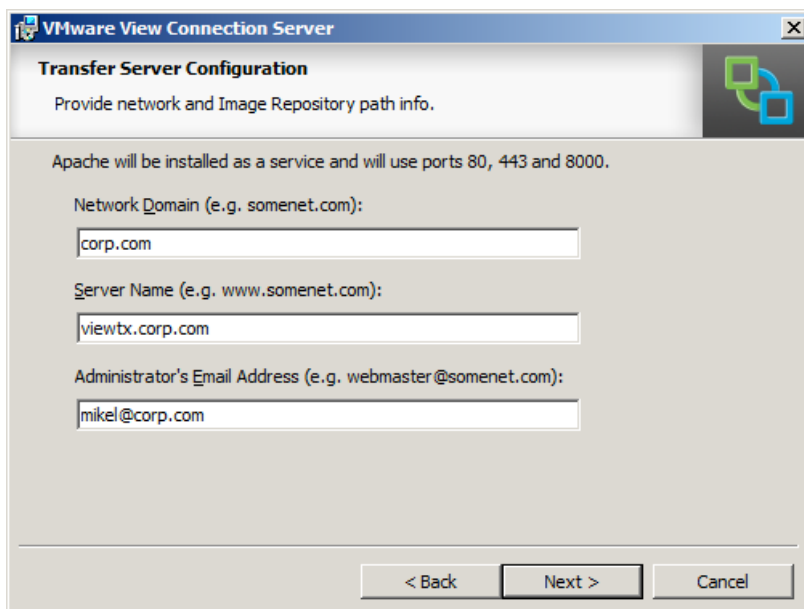
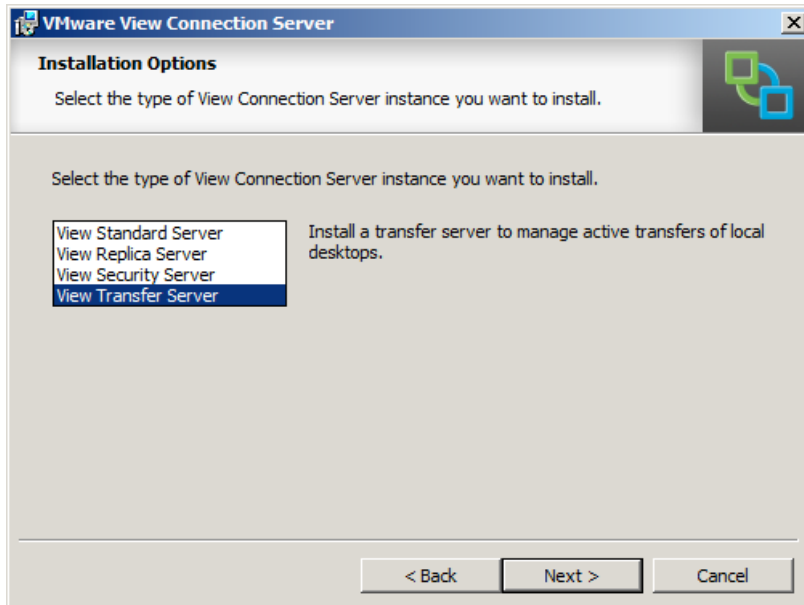
- **Check In** – when the user returns the corporate network the user Checks In the virtual desktop, and any changes (just the differences) are synchronized back to the vSphere4 environment
- **Rollback** – when the user decides to return the virtual desktop to its state *before* it is Checked In
- **Backup to Server** – when the user decides that the changes should neither be Checked In nor Rolled back but maintained, until such time as they choose to Check In or Rollback their virtual desktop

These privileges can be taken away from the end user by using the View administration web pages and adjusting the policy options.

During the transfer process the transfer server mounts the virtual disks used by the virtual desktop to additional SCSI controllers inside the VM. This speeds up the transfer process. Any VM can only have a maximum of 4 controllers, with 15 slots. This allows for a maximum of 60 transfers at any one time. As such the ESX host that the transfer server executes on must have access to all the datastores the virtual desktops reside on in order for the mounting process to be successful. The transfer process itself is carried out on a non-encrypted channel, as virtual desktops might contain sensitive data, you might wish to consider ways of encrypting the TCP sessions it generates or restricting transfer to LAN use only. Finally, once added to the View configuration the transfer server is isolated from DRS and set to be disabled for DRS. Watch out for maintenance modes that might “hang” at 2% because transfer server must be manually moved by the administrator of vCenter.

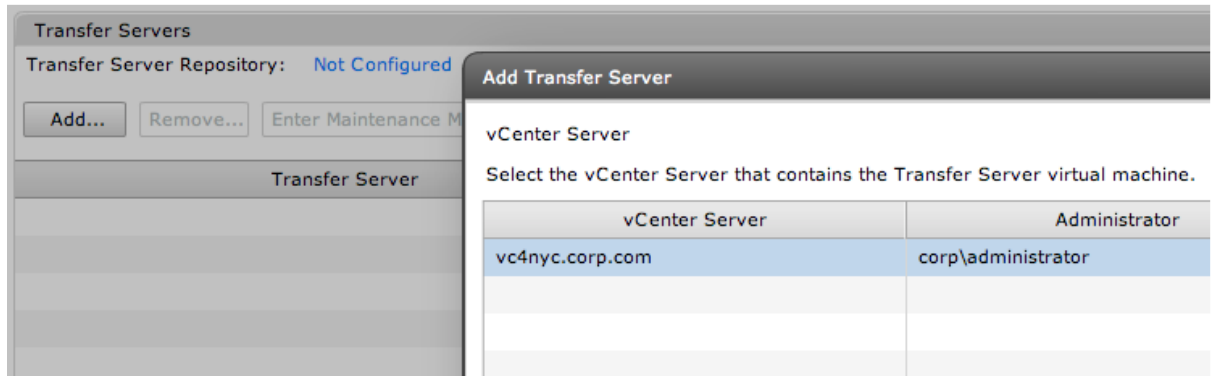
Installing the Transfer Server

The Transfer server component is contained in the same installer as the Connection Server.

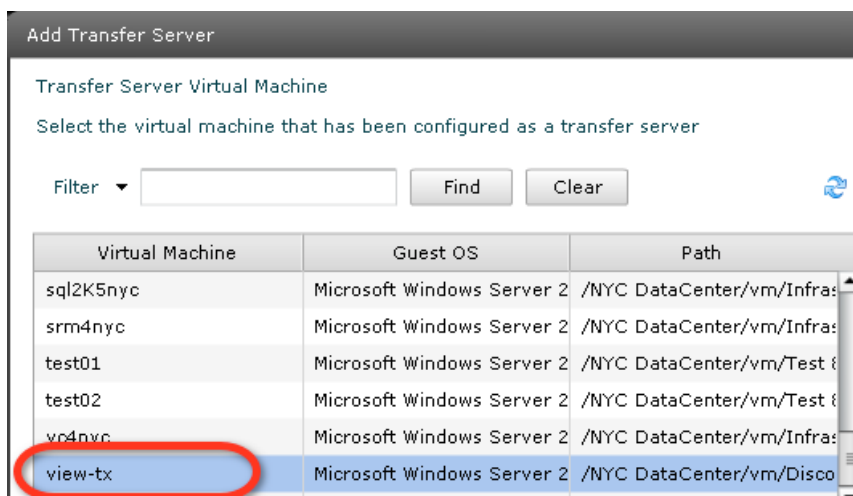


Once the Transfer Server is installed, you need to modify the Connection Server configuration to make it aware of the new server. This is very much like updating the Connection Server configuration when we installed the View Composer component.

1. Open the ► **View Configuration**
2. Click the **Servers** link
3. Scroll down to the **Transfer Server** pane
4. Click the **Add** button
5. In the **Add Transfer Server** page, **select the vCenter**



- Click next, and in the **Transfer Server Virtual Machine**, select the **Transfer Server**



After completing this process, you will see the status of the Transfer Server change from Pending, to Initializing Image Repository, to Ready. You may find that it fails with a message of "Missing Transfer Server Repository" if an Image Repository has yet to be configured.

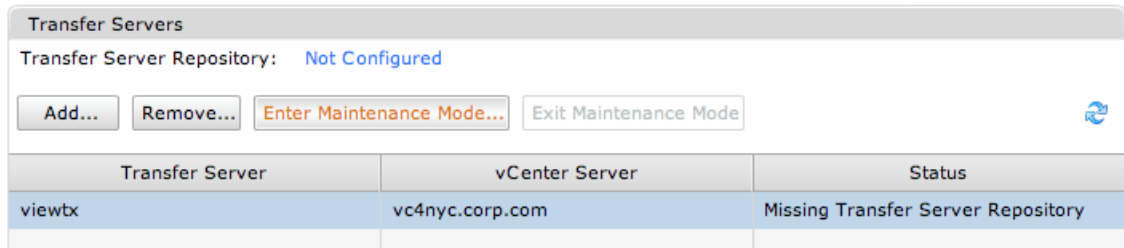
During this process the Transfer Server VM is rebooted, and additional SCSI controllers are added to it, these multiple SCSI controllers increase the amount of simultaneous disk transfers the Transfer Server can accommodate.

Enabling a Centralized Image Repository

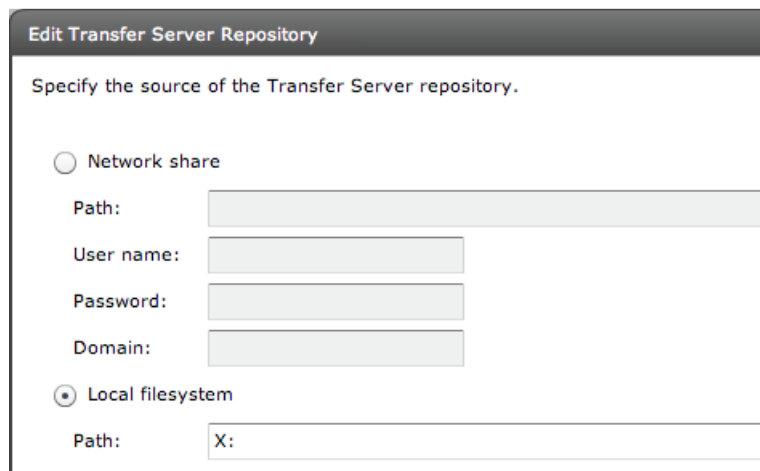
Before you begin using Local Mode, you will need to set up the Image Repository – the location which stores the Local Mode VMs either on a network fileshare or on storage local to the Transfer Server. The best location to use is a network-based one, this allows for scaling up the Local Mode feature by adding additional Transfer Servers which point to this central location for checking virtual desktops in and out.

- Open the ► **View Configuration**
- Click the **Servers** link

3. Scroll down to the **Transfer Server** pane
4. Click the **Enter Maintenance Mode** button and click **OK**



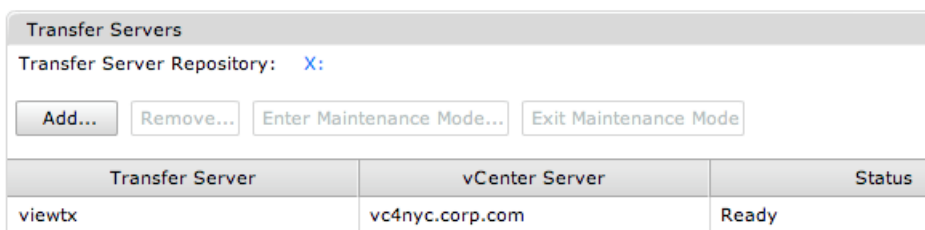
5. Click the **Transfer Server Repository** link (or click the Not Configured link for Transfer Server Repository, it will take you to same location)
6. Click the **Edit** button – complete the dialog box with the UNC path to the shared location and the credentials required to access it



Note: At this stage you have choice – to store the transfer repository on a network file share/SMB supported storage array – or inside a virtual disk on the Transfer Server. I opted to add a second virtual disk to my transfer server, and allocated an X: drive to it.

7. Once added, return to the **Servers** link
8. Scroll down to the **Transfer Server** pane
9. Click the **Enter Maintenance Mode** button and click **OK**

After a short while the status of the Transfer Server should update from Missing Transfer Server Repository to Ready.

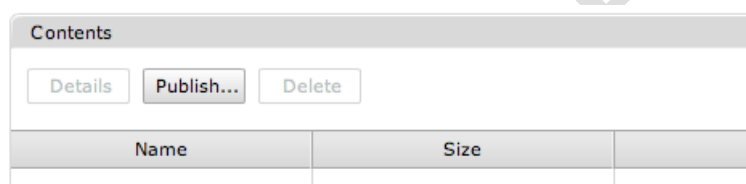


Publish the Source Parent VM (Mandatory for Linked Cloned Desktops, Optional for regular desktop pools)

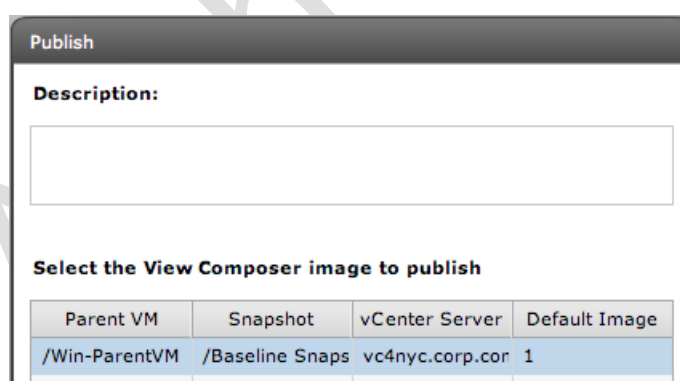
If you are using the Linked Clones feature, the final configuration step for enabling the Transfer Server with a linked clone desktop is to publish the Parent VM in the image repository. This is a relatively simple task, and is completed in seconds. The task does *not* need carrying out if you are not using linked clones. If you are working with conventional published desktops it is possible to skip this step.

This publishing process accelerates the download process for linked cloned local mode desktops. If you think about the link clones – each users desktop is only slightly different from another users. The publishing process stores a compressed and encrypted version of the View Composer image, so they can be quickly download by each user, together with the deltas that make up their own virtual desktop. You can see this as a kind of “caching” process

1. Open the ► **View Configuration**
2. Select **Transfer Server Repository**
3. Click the **Publish** button



4. Next select the **View Composer Image** you wish publish



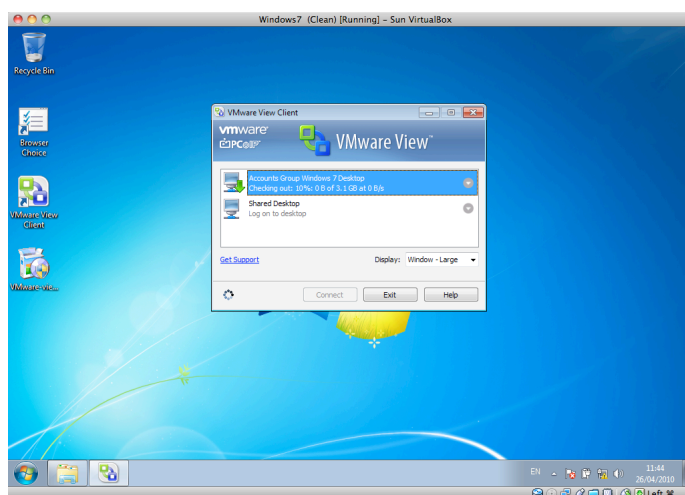
Note:

The system will then go through an initializing phase followed by a publishing phase with a % value, at this point the image is being transferred to the network location specified earlier. The information in the General pane will refresh to show you how much disk space your images are using.

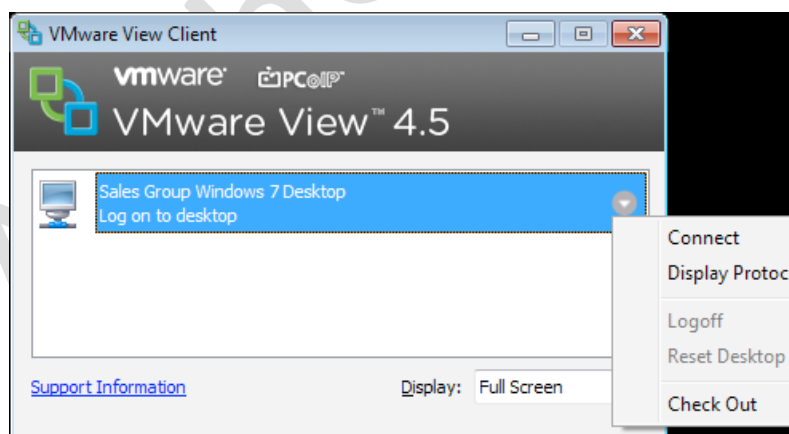
Check Out a Local Mode Desktop

Note:

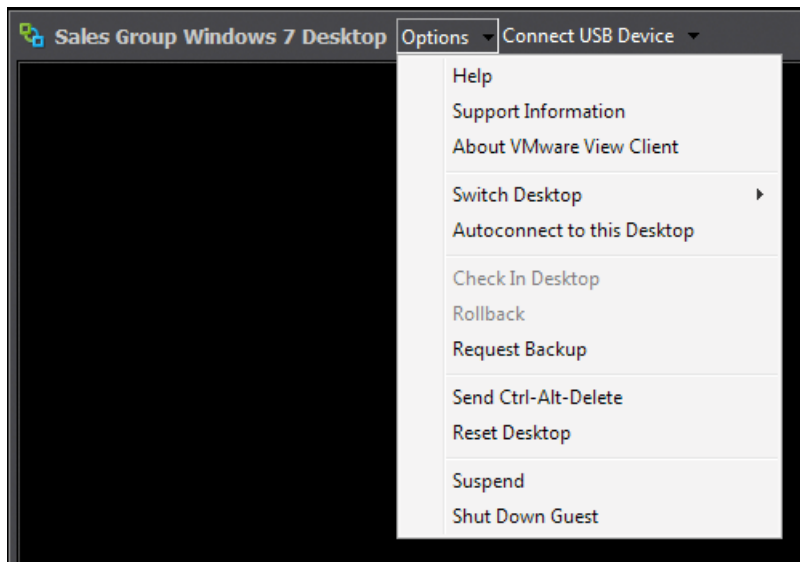
For testing purposes, you might like to run the Local Mode client inside a VMware Virtual Machine. Unfortunately, VMware won't allow it. They appear to use a registry setting inside the VM to detect that Windows is running inside a VMware virtual machine. My workaround to this limitation was to virtualize Windows on a different vendor's virtualization platform. I recently made the switch to Apple Mac, so I downloaded Sun's VirtualBox application that is free for both Windows and Mac, and used it to get the Local Mode client running from my home office. Madness, I know, but it beats the hell out of buying a physical Windows PC for a 10-minute test.



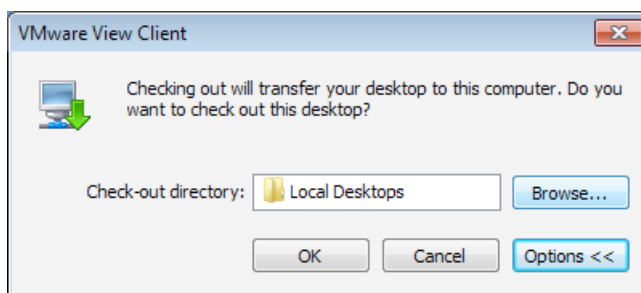
1. **Login using Local Mode Desktop client**
2. **Right-click virtual desktop listed, and choose Check Out**



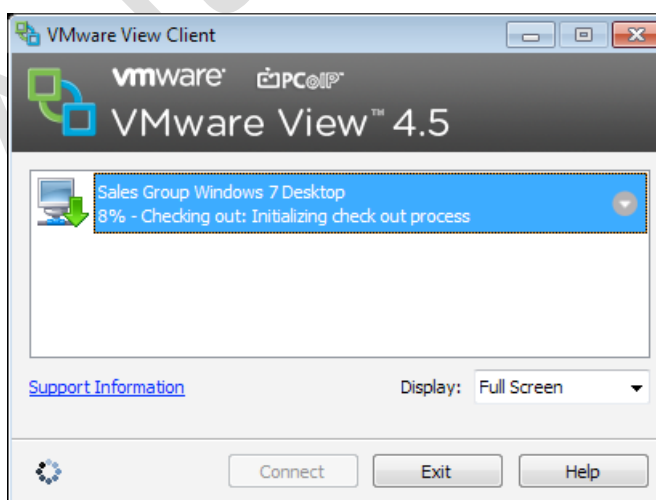
Remember, the Check Out option also appears in the menu in the end user toolbar if they have already connected to the virtual desktop



3. Before the download process begins, you may be warned that it is good practice to make sure the end user has logged in once to the virtual desktop

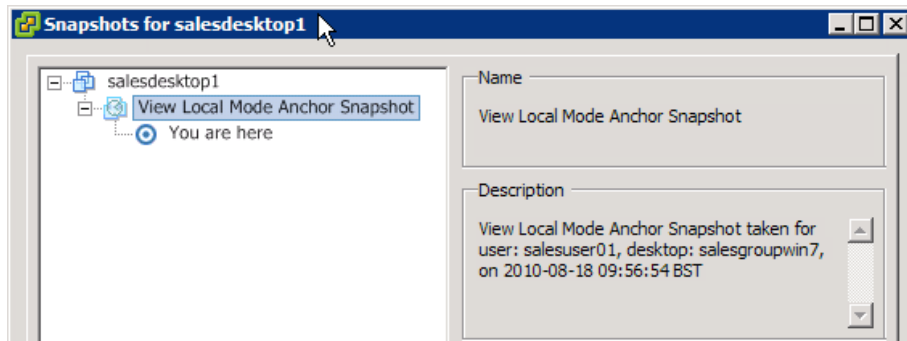


The files are downloaded to this path C:\<User Profile Path>\<Username> \AppData \Local \VMware \VDM \Local Desktops. Using the browse option, it is possible to change the location of the download. During this time the user will receive a percentage-based indicator of the progress of the download and the size of the virtual desktop.

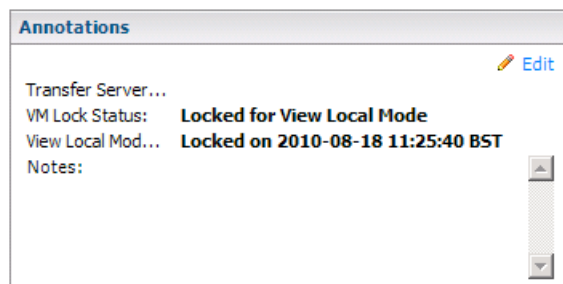


During this time the drop-down arrow will allow the user to either cancel or pause the Check Out process

Just before the download process begins, the virtual desktop is powered down and a snapshot is taken of the user virtual desktop.



Additionally, the Annotations on the virtual desktop are updated.



In the administration web pages you will see the following under the Monitoring and Local Sessions tab

Local Sessions

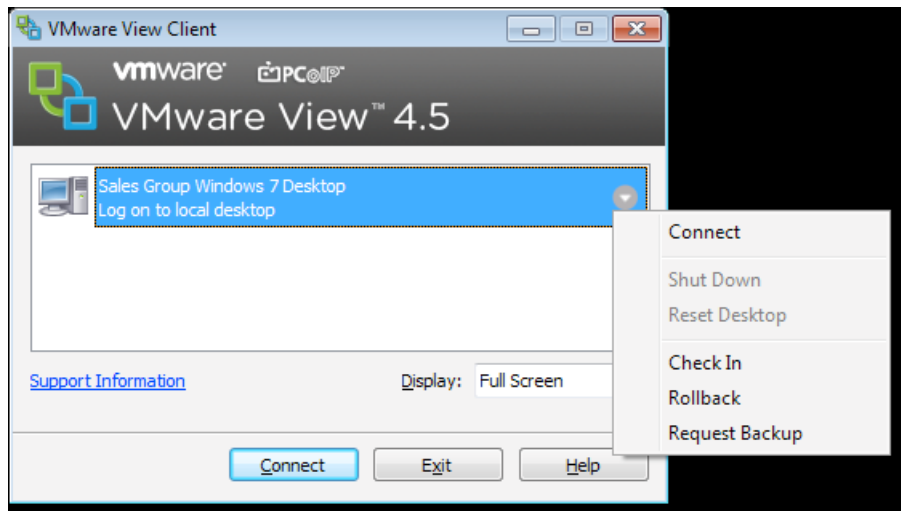
Details Rollback Initiate Replication...

Filter Find Clear

Desktop	Pool	User	Type	State	Check-out Time	Local Session ...	Last Server C...	Last Replication
salesdesktop1	SalesGroupWin7	corp.com\salesuser01	Local	Checking out	8/18/10 9:57:22	44 minutes	8/18/10 10:40:1	8/18/10 9:57:22

Check In, Rollback and Backup to Server

Once the user has used the offline desktop for the first time, new menu options appear in the window that displays the virtual desktop.



The time it takes to Check In or Backup to Server is dependent on two variables - the amount of bandwidth available, and the number of changes accrued in the delta file. Of course, the rollback option checks the virtual desktop back into View, but discards any changes accrued whilst in local mode.

Manage Local Mode Desktops with View Administration

There are surprisingly few options to control Local Mode desktops in the current edition of View 4.5. However it is possible to force a Rollback of the user's virtual desktop from the administrative webpages by

1. Log in to the Connection Servers administrative webpage
2. Under **Monitoring**, select the **Local Session** icon
3. **Select the end-users desktop**
4. Click the **Rollback...** button

Additionally, it's also possible to control whether users have access to the Local Mode desktop feature (by default, if they have the right client they do) and the Rollback option, as well as controlling for how long the Local Mode desktop will be allowed to function. It's possible for the administrator to set an expiration period describing for how many minutes, hours or days the Local Mode desktop can be checked out. After this period expires, the user's Local Mode desktop privileges also expire and they will find that the desktop will not power on after that time. You can adjust these settings so they affect every user, but is possible also have policy exceptions to allow for individual settings.

1. Click the ► **Global Policies** node
2. Select the **Global Policies...** icon under the Local Mode Policies pane

Local Mode Policies	
Edit Policies...	
Name	Global Policy
Local Mode	Allow
User-initiated rollback	Allow
Max time without server contact	7 Days
Target replication frequency	No replication
User deferred replication	Deny
Disks replicated	Persistent disks
User-initiated check in	Allow
User-initiated replication	Allow

I think these settings here are quite common sense. I think what might need some explanation is the replication options which is disabled by default in the policy

Enabling Replication

It is possible to enable a schedule of replication by which every so often the local mode desktop sends back its changes that have been accruing whilst offline. This guarantees that any deltas are being sent back to the virtual desktop in vCenter. By default it is turned off, which I think is kind of logical given that by definition a local mode user is well, running the virtual desktop locally and might not have any connectivity to sync back their changes. I think the reason for this feature is to allow for an automatic method for user to sync there changes, rather than relying on the end-user to do it.

To enabled automatic replication, and modify the frequency of updates – edit the global policy in the and set the desired replication frequency..

Edit Local Mode Policies

Set global policies for all desktops

Local Mode Policies

Local Mode: Allow

User-initiated rollback: Allow

Max time without server contact: 7 days

Target replication frequency: At a specified interval

User deferred replication: Deny

Disks replicated: Persistent disks

User-initiated check in: Allow

Target replication frequency details: 4 Hours

The View Administrator can initiate replication manually, by selecting a local mode desktop(s) in the Local Sessions node, and clicking the Initiate Replication button. As you can see in the screen grab above by default only the persistent

disk is replicated back to the system. It is possible to change this to be just the OS Disk or both the OS Disk *and* the Persistent Disk.

Authors Edition

Chapter 12: Enabling “Kiosk Mode”

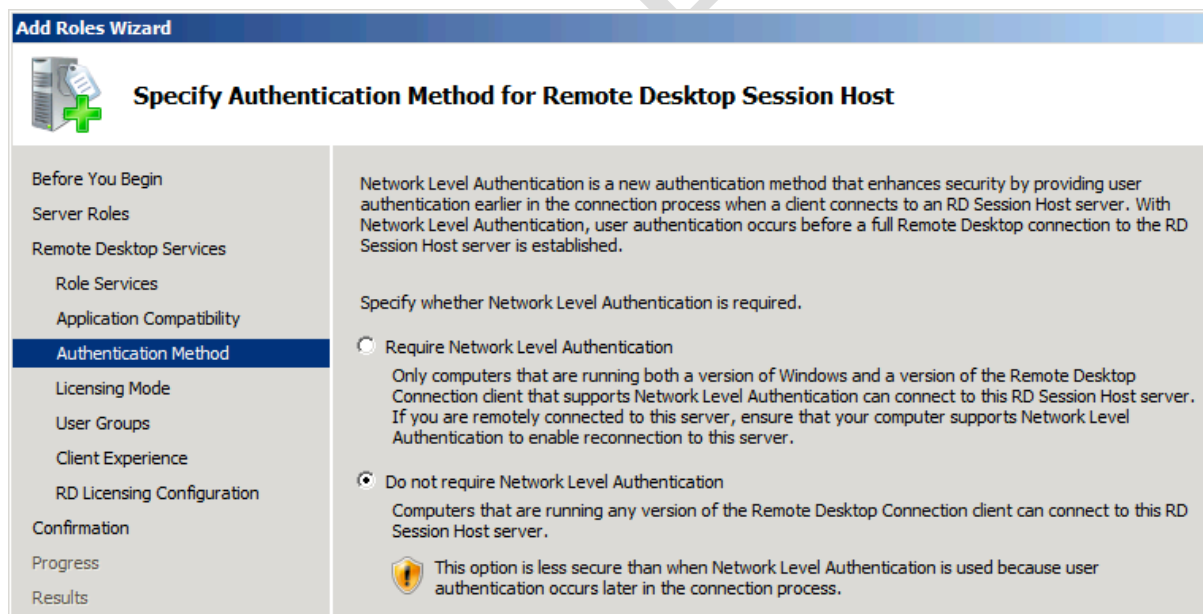
To Be Completed

Authors Edition

Chapter 13: Publishing Terminal Servers (TS) / Remote Desktop Services (RDS)

VMware View is not limited to merely allowing access to virtual desktops, it can also securely broker connections to other devices and systems such Terminal Servers now called Remote Desktop Services (RDS), Physical PCs (with RDP enabled) and PC Blades. This configuration begins with an installation of the View Agent that then registers the system with the Connection Server(s). Before you begin, it's worth confirming that the client(s) can connect to the external system using its normal RDP connection. The PCoIP protocol can only be used transparently with virtual desktops, the only way to use PCoIP with these non-virtual desktops is if they have Teradici hardware present.

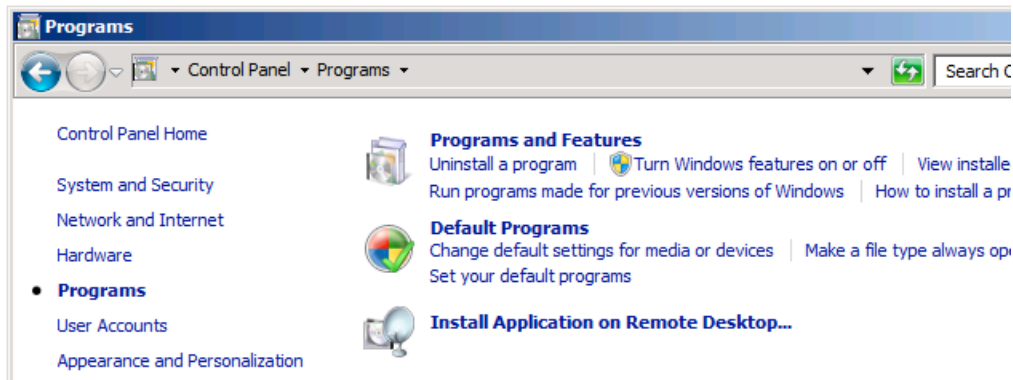
As with Windows Vista and Windows 7 there are two types of authentication supported in Windows 2008 R2 RDS. I would recommend using "Do not require NLA" if you are setting up a new RDS host. This will allow so called legacy clients like Windows XP and Apple Mac to connect without an error.



Remember on a TS/RDS server, it must be in "install mode" before installing any software. This can be achieved by using the command:

change user /install, followed when the installation is over with the change user /execute command.

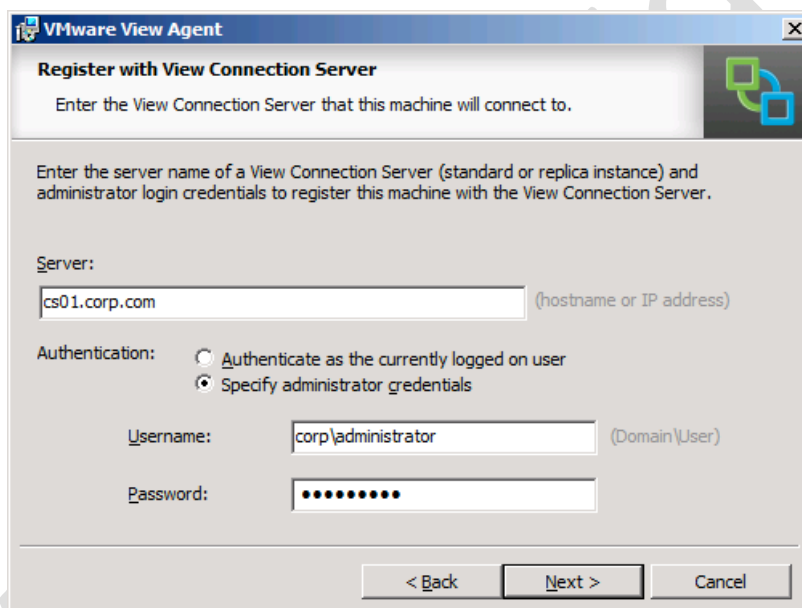
Alternatively, within Control Panel, Programs in Windows 2008 R2 you should see a "Install Application on Remote Desktop" link



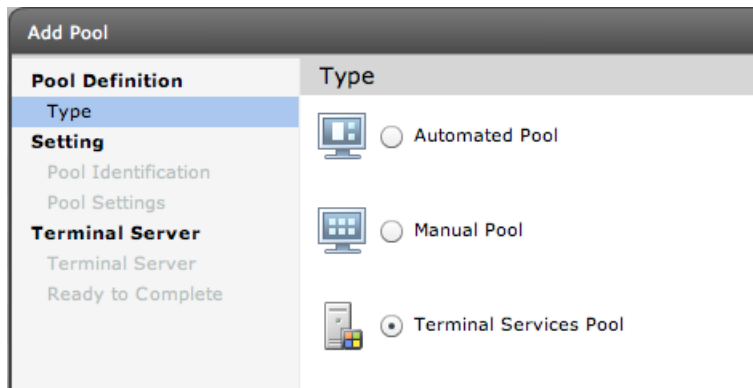
Note:

Remember to download the right version of the agent. If you running Windows 2008 R2 64-bit you will need the 64-bit version of the Agent

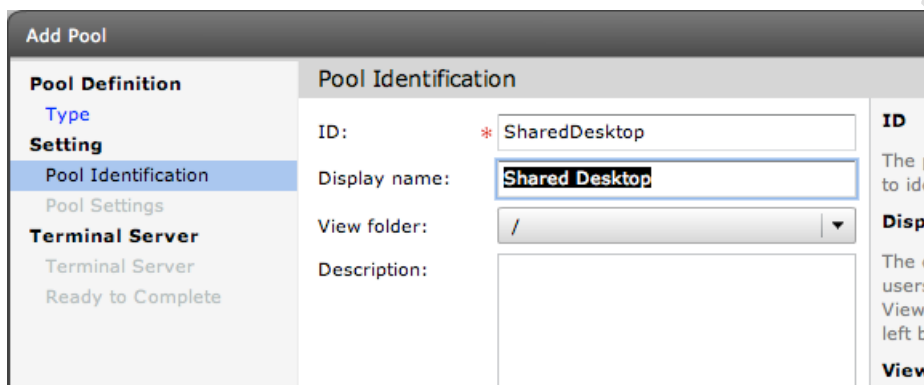
1. Run the **vmware-viewagent-xxxxx.exe**
2. In the **Register with View Connection Server** dialog box – type in the **name of the Connection Server**, together with your **credentials for the Connection Server**



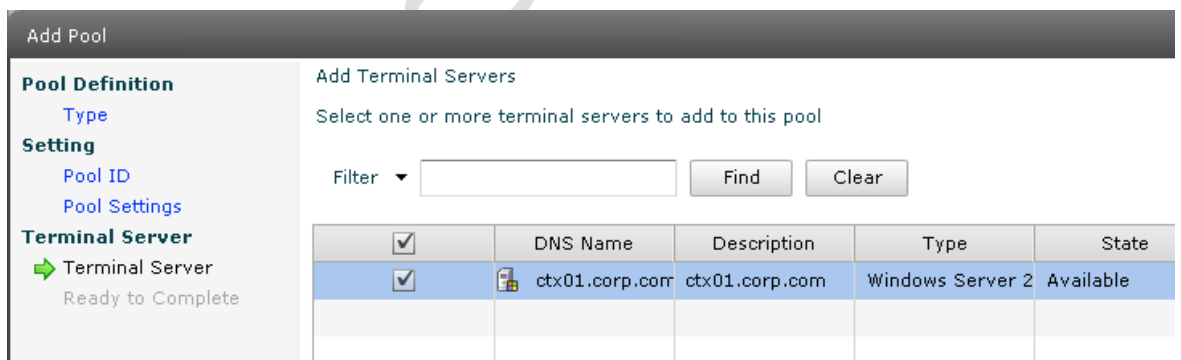
3. Click **Next** and **Install**
4. The next step is to publish the Terminal Server in the View administration pages. Begin by navigating to ► **Inventory** and **Pools**
5. Click the **Add** button and **Select Terminal Services Pool**



6. Type in a **unique ID** and **Friendly Name**



7. Configure the **Pool Settings** based on your own preferences
8. Select your **Terminal Server from the list** like so:



9. Click **Next** and **Finish**
10. Once the Terminal Server appears in the Pools list, **select it and then entitle** the shared desktop to your users

VMware View Administrator
Updated 08/18/2010 14:04 PM

Remote Sessions: 0
Local Sessions: 0
Problem Desktops: 11
Events: 44 (Warning), 2 (Error)
System Health: 19 (OK), 0 (Warning), 0 (Error), 0 (Unknown)

Navigation: Dashboard, Users and Groups, Inventory (Pools, Desktops, Persistent Disks, ThinApps), Monitoring

Tools: Add..., Edit..., Delete..., Entitlements..., Status, Folder, More Commands

Filter: [] Find Clear Folder: All

ID	Display Name	Type	Source	User Assi...
AccountsGroupWin7	Accounts Groups Windows 7 C	Automated Pool	vCenter (linked clone)	Dedicated vc
ce_desktopwin7	Carmel Edward's Windows De	Manual Pool	vCenter	Dedicated vc
mgI_desktopwin7	Mike Laverick's Windows Desl	Manual Pool	vCenter	Dedicated vc
SalesGroupWin7	Sales Group Windows 7 Deskl	Automated Pool	vCenter	Dedicated vc
SharedDesktop	Shared Desktop	Terminal Services Pool	Terminal Services	Floating
StudentDesktops	Students Desktops	Automated Pool	vCenter	Floating vc

The Terminal Server's shared desktop should appear in the list alongside any other virtual desktops that you have entitled the user to use.

Authors Edition

Chapter 14: Microsoft Group Policies

In the early days of VDI, there was much talk of a virtual desktop being this ultra-rich environment that the user could customize with impunity. There was frequently talk of a virtual desktop being your own computer or laptop which you could access and customize anywhere with an internet connection. When I heard this, I smiled wryly, knowing that corporate standards often decree restrictions over what users can and cannot do. In the current economic climate, it's a sobering thought that repeated studies show that end users waste time and are unproductive during working hours if they are distracted by a computing environment that permits work avoidance behaviour. Personally, I find this a rather cheerless view of working life, and I think to some degree these studies have taken a rather Dickensian view of the world of work. Nonetheless, the facts and studies speak for themselves, and if it was my company...

So, it would be somewhat remiss of me not to acknowledge in some way the significance of desktop restrictions within a VDI environment, despite the fact that this isn't a VMware issue or VDI problem, per se. After all, it's not VMware who puts Pinball and Solitaire on the Start Menu. I'm assuming you're probably already familiar with removing access to the run command or access to the registry tools in Microsoft Active Directory Group Policies. Indeed, you may have gone so far as abandoning the use of GPOs in favour of some other desktop lockdown tool such as Scriptlogic or PowerFuse. After all, there are some limitations with GPOs that reduce your ability to configure unique per-user settings for each application. That said, Microsoft GPOs remain popular because they are included as part of Active Directory. With those caveats and assumptions in mind, in this short section I want to explain and demonstrate some little known or used GPO settings. If I am forced to use Microsoft Active Directory GPOs, my goal is to use as few settings as possible - this speeds up the login process and users therefore spend less time reading the "Applying your personal settings..." message during the login process.

However, policies encompass a much wider remit than simply restrictions of the end user's Windows environment. VMware View ships with its own policy system, which allows control of the user's experience from a virtual desktop perspective too.

In this part of the guide, I have opted to use Windows 2008 Active Directory, in previous releases I was still using Windows 2003 Group Policies. With this said, if you have yet to upgrade you should still find the policies are more or less the same. Additionally, although I primarily used Windows XP during the testing process, in this section I opted to use Windows 7 as the target system - I consider this version of Windows to be the most likely guest operating system to be used in modern VMware View deployments. If you want to have access to the latest policy settings for Windows 7, you will need to run Windows 7 as the

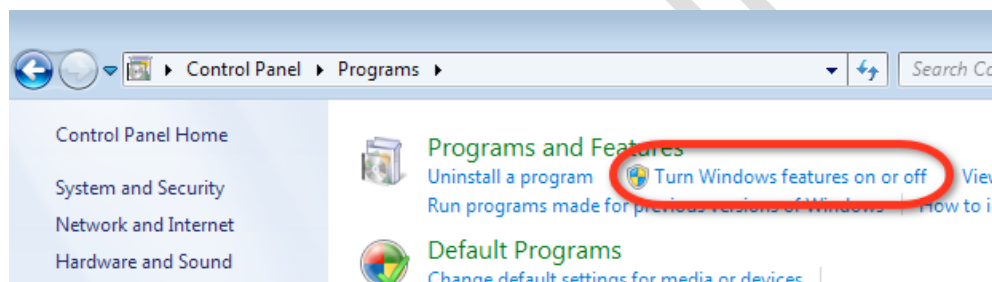
management system. In my humble opinion, the setup for this is quite convoluted, but there really is no other option, I'm sad to say.

Installing the Remote Administration Tools to Windows 7

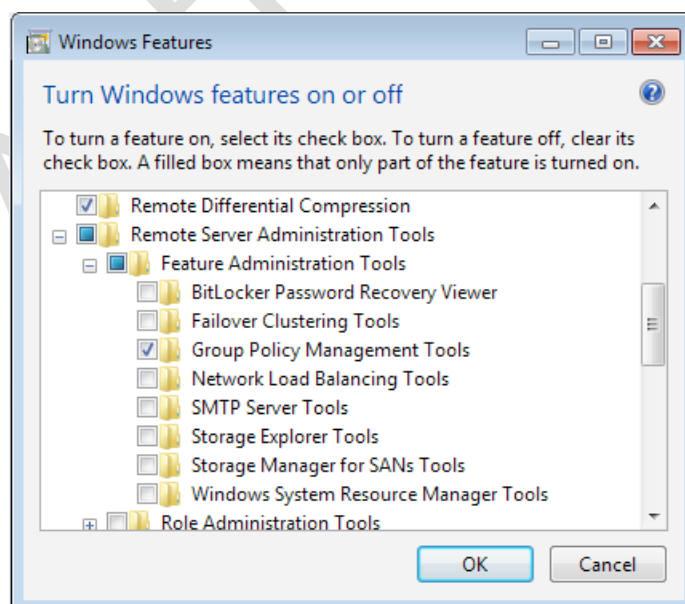
1. **Login into a Windows 7 system** which is part of the domain and connected to the internet
2. **Download the either x86/64 version of the Remote Administration Tools** from here:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=7D2F6AD7-656B-4313-A005-4E344E43997D&displaylang=en>

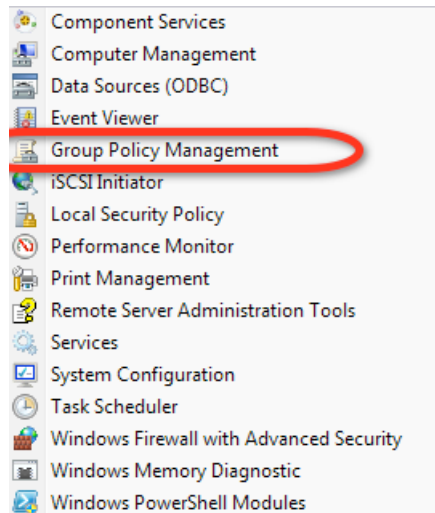
3. Install the package on a Windows 7 machine
4. Next, enable Remote Administration Tools (yes, you would think merely installing them would be enough!) by navigating to **Control Panel, Programs** and select the **Turn Windows Features on or off** link



5. In the **Windows Features dialog box**, scroll down to the **+Remote Administration Tools** node, and expand to see the **+Feature Administration Tools** and enable the **Group Policy Management Tools**



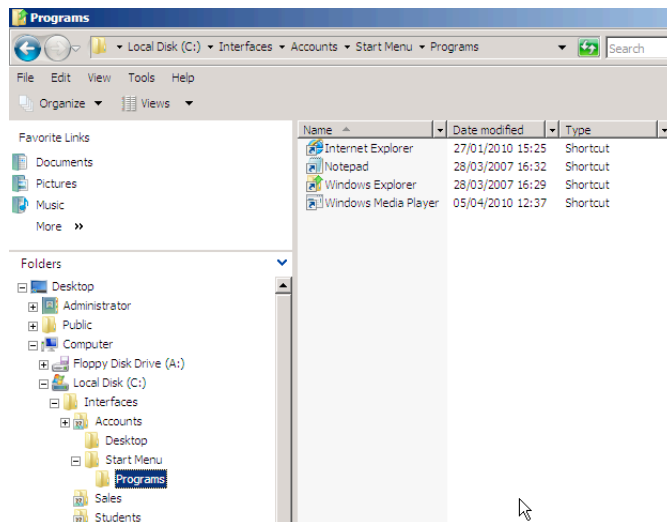
6. If you **enable the Administrative Tools in Windows 7** (Taskbar and Menu Properties, Start Menu Tab, Customize button, System Administrative Tools and enable the option to Display on the All Programs menu and Start menu), this should have added a Group Policy Management icon to your menu:



Redirect the Desktop

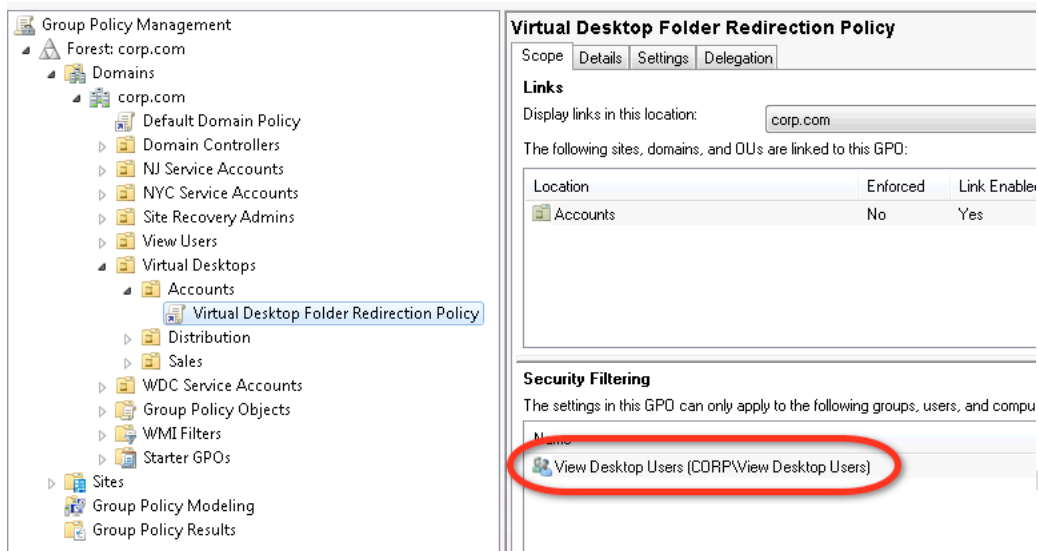
As you probably already know, redirecting folders that normally appear in the user's profile has a number of benefits, as it:

- Reduces the size of the profile
 - Ensures that user files are properly saved to a network location by setting My Documents to point to a network drive
 - Centralizes shortcuts that make up the Start Menu and Desktop, which allows for easy changes at the central location without the need to modify each user profile. These shared locations can be marked as read-only and this will prevent users right-clicking their desktop to save files. This is especially important in non-persistent pools, where the virtual desktop is deleted at log off.
1. **Start by creating some folders and shares on a file server. Create the folder structure you would like for the user's Start Menu and Desktop. Populate with shortcuts to applications associated with the user's virtual desktop.**



In the example above, I've created a folder structure for the Accounts, Sales and Students virtual desktop groups. Be careful when you create the shortcuts, if you take them from the server's Start Menu, they can often be hard-coded to a particular path, or not use variables like %SystemRoot%\system32\notepad.exe or "%ProgramFiles%\Windows NT\Accessories \wordpad.exe". Finally, allow that the folder called Start Menu is not hard-coded, while the use of the folder Programs is. If GPOs are set properly, you can replace the default Programs folder, which appears at the top of the Windows Start Menu, with your own. With policies you can either merge your shortcuts into an existing desktop, or remove the default Programs folder altogether. You want to be concerned about the availability of this share. Different versions of Windows client behave differently if the share is unavailable – some will load but you won't see the redirection, while others won't allow a logon to occur at all.

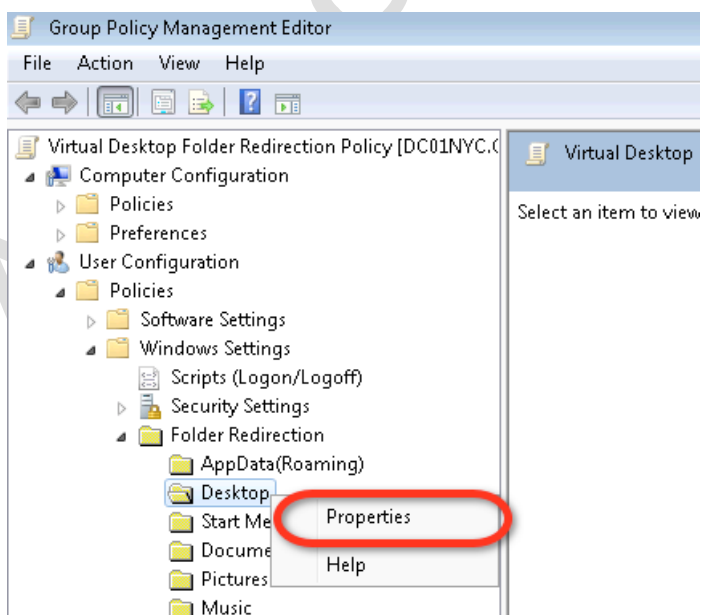
2. Next, in the Group Policy Management MMC, **create a GPO Object that will be used to restrict the user's virtual desktop**. This raises the issue of the best way to apply the restriction. I prefer to apply a GPO to the computer where possible, so the user receives one set of restrictions if they login to a virtual desktop, but an entirely different set elsewhere. This allows them to be heavily restricted in the VDI session, but perhaps less restricted on other computers in the domain. After all it's the virtual desktop I'm trying to secure from the end user. **Right-click the Organizational Unit, choose Create a GPO in this domain, and link it here.**



Note:

In this case, I've created a GPO called the "Virtual Desktop Folder Redirection Policy". By default, settings apply the restrictions to all authenticated users. The unintended consequence of this is that you could find yourself as the Administrator being unnecessarily restricted. To avoid this situation, I replace the default Security Filtering with the View Desktop Users group.

3. **Select the GPO** and Click **Edit**
4. Navigate to **+User Configuration +Policies +Windows Settings +Folder Redirection**
5. **Right-click the +Desktop** icon and select **Properties**

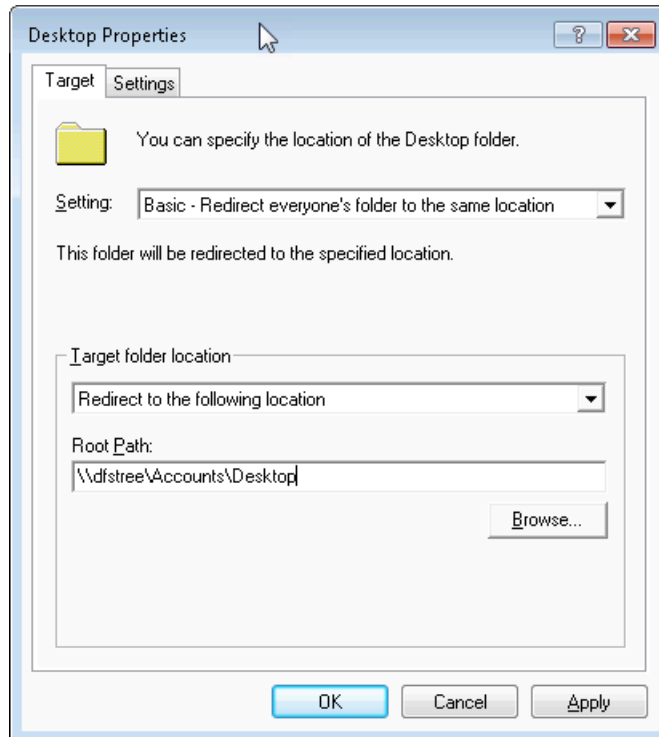


6. In the **Desktop Properties Dialog Box** select:

Setting: Basic – Redirect everyone’s folder to the same location

Target Folder Location: Redirect to the following location

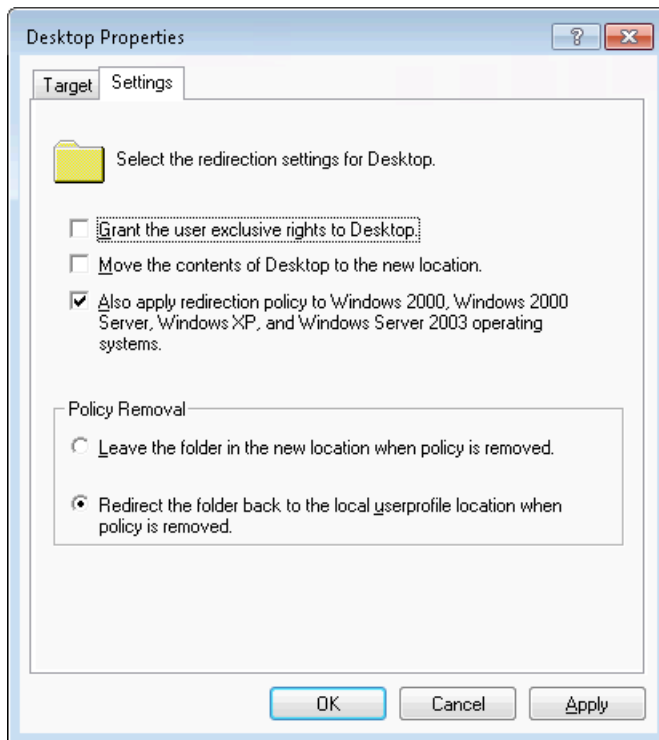
Root Path: Type or Browse to the location of the Desktop Folder in your share



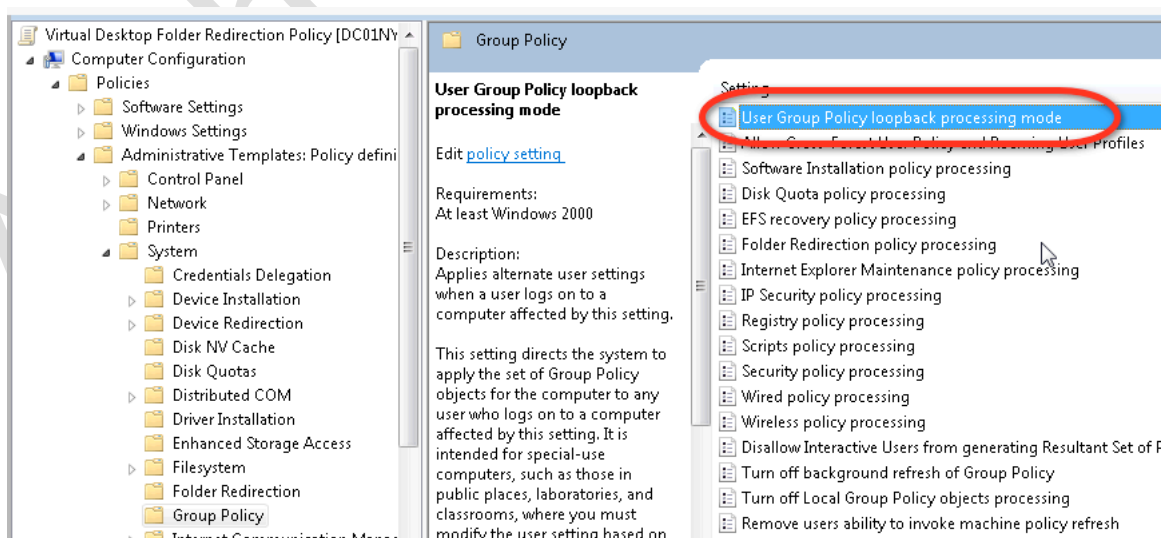
7. Before clicking **OK**, select the **Settings** Tab in the dialog box, and disable the option called “**Grant the user exclusive rights to Desktop**” and “**Move the contents of the Desktop to the new location**”. Leaving these settings would stop us from imposing our own desktop shortcuts over the end users. I would also select the option to “**Redirect the folder back to the local userprofile location when policy is removed**”, so should you delete the policy, the default location for the desktop folder is reset.

Note:

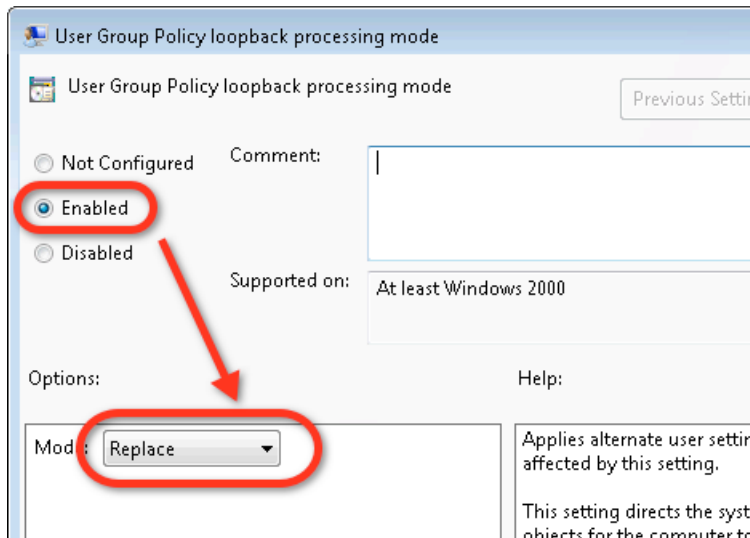
If this policy will also be set against Windows XP virtual desktops, enable the option to “Also apply redirection policy to Windows 2000.....systems”



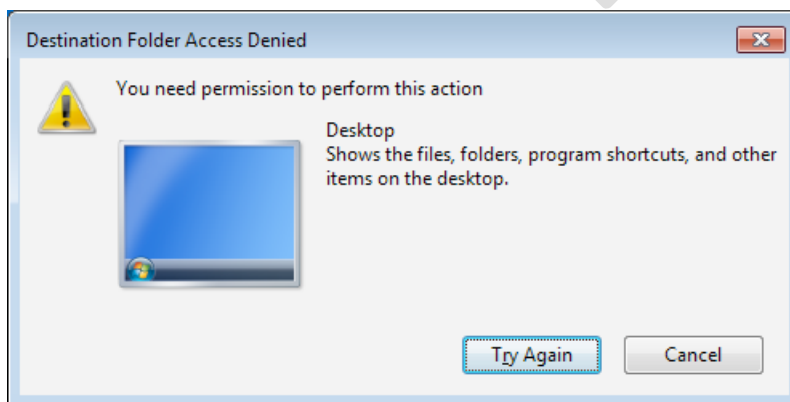
8. Click **OK** to apply this change.
9. Finally, **we need to make sure that this computer policy takes precedence over all other user policies.** So any settings that normally affect the end user on a standard computer are ignored, and our special virtual desktop settings are always applied. **This option is called "User Group Policy Loopback Processing Mode"** in Active Directory GPOs. Locate the setting at **+Computer Configuration +Policies +Administrative Templates +System and Group Policy**



10. **Doubleclick on the setting** called "User Group Policy loopback processing Mode", select the **Enable** option and set a mode of "Replace"



At this stage, you can test the policy by logging in as a user. In the shared location to which the desktop is being redirected, try hiding one of your shortcuts – you will find it disappears from the user view automatically, without a refresh. Additionally, try creating a new shortcut in the shared location – it should appear automatically. Finally, try as an end user to right click and save a file on the desktop. If you have set the permissions correctly on the share (read-only is all that is required), you should find that the user gets an Access Denied message.



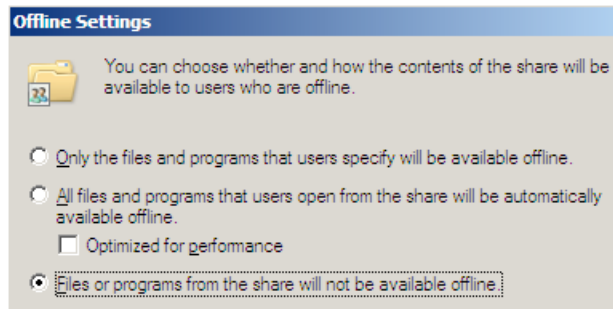
Caution:

Synchronizing offline files in Windows XP/Vista/7 often interferes with this dynamic functionality – I would recommend disabling the feature on this share. This can be done with the Microsoft GPO at this location:

+Computer Configuration +Policies +Administrative Templates +Network +Offline Files and set the option disabled on the policy setting called "Allow or Disallow use of the offline feature". I have to admit that this policy didn't seem to have the result I was hoping for, in the end I lost patience with Microsoft Policies and took advantage of all the disabling options associated with offline files. In fact I found the best way to stop offline files in their tracks was to make sure the share settings on

Windows Shares did not enable the feature. In Windows 2008, Offline caching is enabled by default by Microsoft, it can easily be changed with the Offline caching Settings dialog box on the properties of a share

(Windows 2008: Properties of the share, Advanced Sharing button, Caching button)



TIP:

By default, Windows 7 creates a Recycle Bin. If you would like a completely blank desktop with only your icons then enable:

“Remove Recycle Bin icon from Desktop” located at +User Configuration +Policies +Administrative Templates +Desktop

Additionally, if you want to stop users from accessing the Display Properties applet in the Control Panel, using the Desktop Tab or the Customize Desktop button which allows them to add icons to the desktop, then I would recommend enabling the following policy:

“Remove display in Control Panel” located at +User Configuration +Policies +Administrative Templates +Control Panel +Display

If you make a major change in the policy, rather than repeatedly logging in and out of the virtual desktop to check your work, issue the *gpupdate* command from the command line in Windows 7 for a refresh of the policy. Unfortunately, *gpupdate* in Windows 7 is not perfect, and will sometimes not update your changes - an example of this is doing any folder redirection work. So, you will sometimes need to log in and out to confirm your settings have taken effect

Redirect the Start Menu

Once you have redirected the Desktop, redirecting the Start Menu is very much the same. Many people prefer to enforce the classic Start Menu of Windows 9x/NT days, rather than the Windows 7 Start Menu. A word of warning, if you do this *after* redirecting the desktop it will add new icons to the desktop regardless of the settings we have previously outlined, namely My Computer and My Network Places. You might ask how these icons get created if we have made the desktop

share read-only. These new icons exist in the user profile that is also loaded along with our redirected desktop.

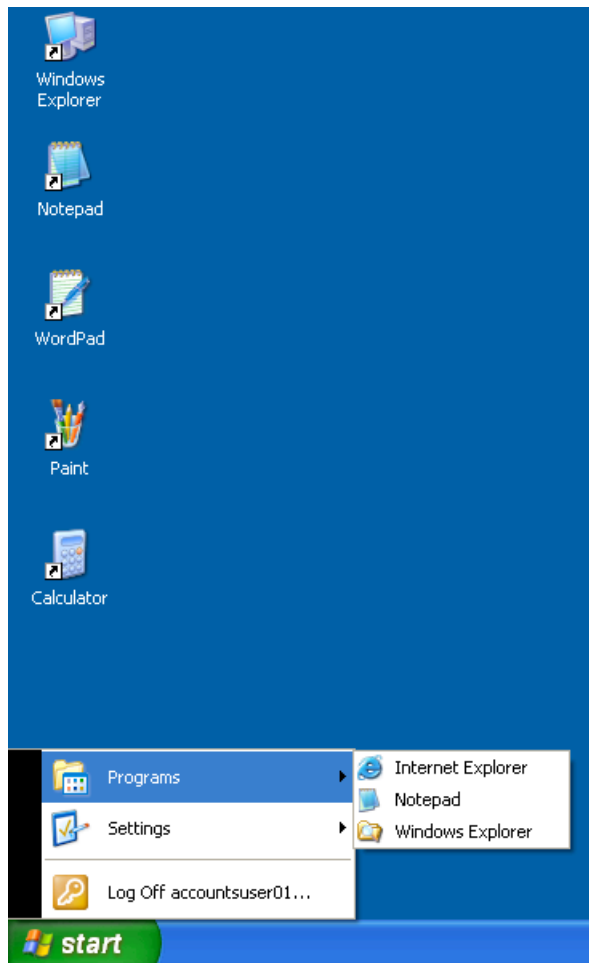
If you want to *completely supplant* the Windows Start Menu then you will have to engage a significant number of policy settings held in **+User Configuration +Policies +Administrative Templates +Start Menu and Task Bar**

Setting	State	Comment
Add Logoff to the Start Menu	Enabled	No
Remove drag-and-drop and context menus on the Start Me...	Enabled	No
Remove and prevent access to the Shut Down, Restart, Sleep...	Enabled	No
Remove common program groups from Start Menu	Enabled	No
Remove Search link from Start Menu	Enabled	No
Remove Help menu from Start Menu	Enabled	No
Remove Network Connections from Start Menu	Enabled	No
Remove Recent Items menu from Start Menu	Enabled	No
Remove Run menu from Start Menu	Enabled	No
Remove Default Programs link from the Start menu.	Enabled	No
Remove Documents icon from Start Menu	Enabled	No
Remove Music icon from Start Menu	Enabled	No
Remove Network icon from Start Menu	Enabled	No
Remove Pictures icon from Start Menu	Enabled	No
Prevent changes to Taskbar and Start Menu Settings	Enabled	No
Force classic Start Menu	Enabled	No
Add Search Internet link to Start Menu	Not configured	No

From **+User Configuration +Policies +Administrative Templates +Desktop**, I also engage these options as well:

Setting	State
Hide Internet Explorer icon on desktop	Enabled
Remove Computer icon on the desktop	Enabled
Remove My Documents icon on the desktop	Enabled
Hide Network Locations icon on desktop	Enabled
Remove Recycle Bin icon from desktop	Enabled

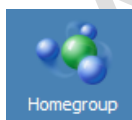
By enabling these options, and redirecting the Start Menu in exactly the same way as we did with the Desktop Properties, we can have complete control over the user's desktop. So, in Windows XP, the Desktop and Start Menu would look like this:



With Windows 7, this redirection of the Desktop and Start Menu will create some new icons on the desktop. So, to get the desktop looking clean and neat like the Windows XP one above, some work needs to be done to remove them.

Removing the HomeGroup Desktop Icon in Windows 7

The redirected desktop creates a Homegroup icon on the desktop. We can use this method to remove it.



This is caused by the new HomeGroup annoyance feature, which is meant to facilitate sharing of files between end users. To get rid of this icon:

1. **Logon as the administrator**, go to **Control Panel**
2. Select **Network and Internet**
11. **Select HomeGroup**, and click on the **Leave the homegroup** link to unjoin from any existing home group

12. Click on **Leave the homegroup to confirm leaving from the home group** and Click on **Finish** when done.

Note:

Next we will stop the service responsible for this feature by selecting Control Panel

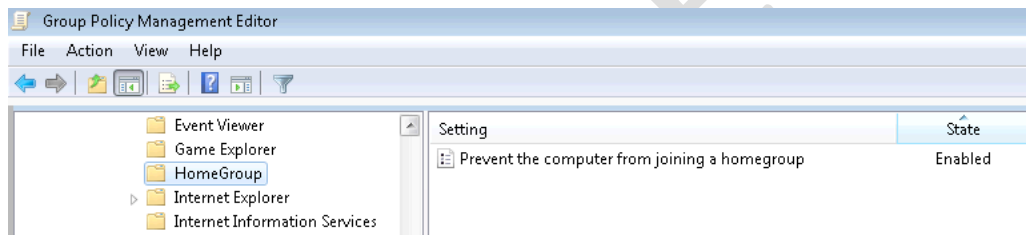
13. Open the **Service** applet, and **stop and disable these services - HomeGroup Listener and HomeGroup Provider**

Note:

It took me absolute age to find how to do this and I'm indebted to author of the blog - mydigitalife:

<http://www.mysdigitalife.info/2009/09/05/disable-and-turn-off-homegroup-services-to-hide-or-remove-home-group-from-windows-7-explorer/>

It is possible to manage the HomeGroup feature via the GPO system at this location - **+Computer Configuration +Policies +Administrative Templates +Windows Components +HomeGroup and modify the Prevent the computer from joining a homegroup setting.**



Remove the Libraries Desktop Icon in Windows 7

Another feature of this redirection process in Windows 7 is that you will find a Libraries icon placed on the user's desktop:



Currently, there doesn't appear to be a GPO method to remove this icon. Fortunately, I was able to locate a registry hack and the website mydigitalife.info came to the rescue. The code below is copied into a .reg file called *library.reg* using a text editor like Notepad.

Windows Registry Editor Version 5.00

```

[-
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
\Desktop\NameSpace\{031E4825-7B94-4dc3-B131-E946B44C8DD5}]
[-HKEY_CLASSES_ROOT\CLSID\{031E4825-7B94-4dc3-B131-E946B44C8DD5}]
[-HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{031E4825-7B94-4dc3-
B131-E946B44C8DD5}]
[-
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
\FolderDescriptions\{2112AB0A-C86A-4ffe-A368-0DE96E47012E}]
[-
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
\FolderDescriptions\{491E922F-5643-4af4-A7EB-4E7A138D8174}]
[-
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
\FolderDescriptions\{7b0db17d-9cd2-4a93-9733-46cc89022e7c}]
[-
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
\FolderDescriptions\{A302545D-DEFF-464b-ABE8-61C8648D939B}]
[-
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
\FolderDescriptions\{A990AE9F-A03B-4e80-94BC-9912D7504104}]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explore
r\HideDesktopIcons\NewStartPanel]
"{031E4825-7B94-4dc3-B131-E946B44C8DD5}"=-

```

I was able to login as administrator and use **regedit library.reg** to import the registry file to remove the offending Libraries icon. You can find this registry file on the mydigitallife.info blog.

<http://www.mydigitallife.info/2009/08/05/how-to-disable-and-remove-libraries-from-windows-7-explorer/>

Remove the Control Panel Icon in Windows 7

The Control Panel icon can be removed by another registry import, this time I found the solution on the sevenforums.com website:

<http://www.sevenforums.com/tutorials/919-desktop-icons-add-remove.html>

Save the following code into a .reg file and import in the same manner as we did with the libraries icon.

Windows Registry Editor Version 5.00

```

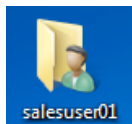
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Hi
deDesktopIcons\NewStartPanel]

```

```
"{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}"=dword:00000001
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\ClassicStartMenu]
"{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel]
"{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\ClassicStartMenu]"{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}"=dword:00000001
```

Remove the Users Folder Icon in Windows 7

Finally, this switch to a redirected desktop also leaves an icon to the Users folder on the desktop as well like so:



Save the following code to a .reg file and import as we did with the libraries icon.

Windows Registry Editor Version 5.00

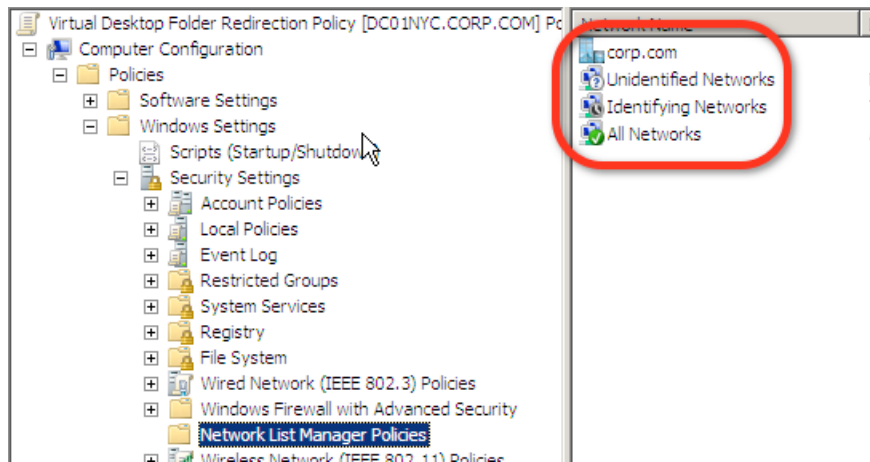
```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel]
"{59031a47-3f72-44a7-89c5-5595fe6b30ee}"=dword:00000000
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\ClassicStartMenu]
"{59031a47-3f72-44a7-89c5-5595fe6b30ee}"=dword:00000000
```

The Users folder icon is part of the User's profile, so you will need to make sure that your roaming profiles (if you use them) are updated such that the default is set to not include the Users folder.

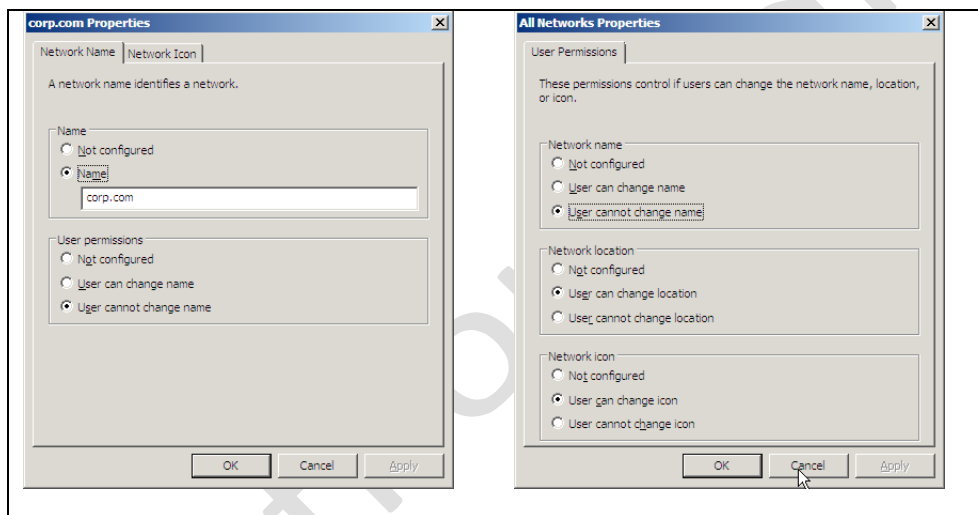
Remove the Network Location Dialog Box

One thing you will have seen with Windows Vista and Windows 7 is that with every new build virtual desktop created, the user will be confronted with a network location dialog box. This feature was designed for users who move their computers from one network to another, and need to be prompted for the level of security they desire. Clearly, with virtual desktops, the "computer" remains in the same datacentre, and on the same network in most cases. As such, the feature is more of an irritation than an advantage for our use case. In most cases, the end user will not have the privileges to set the correct value. The best way to handle this issue is by using the Group Policy settings located in:

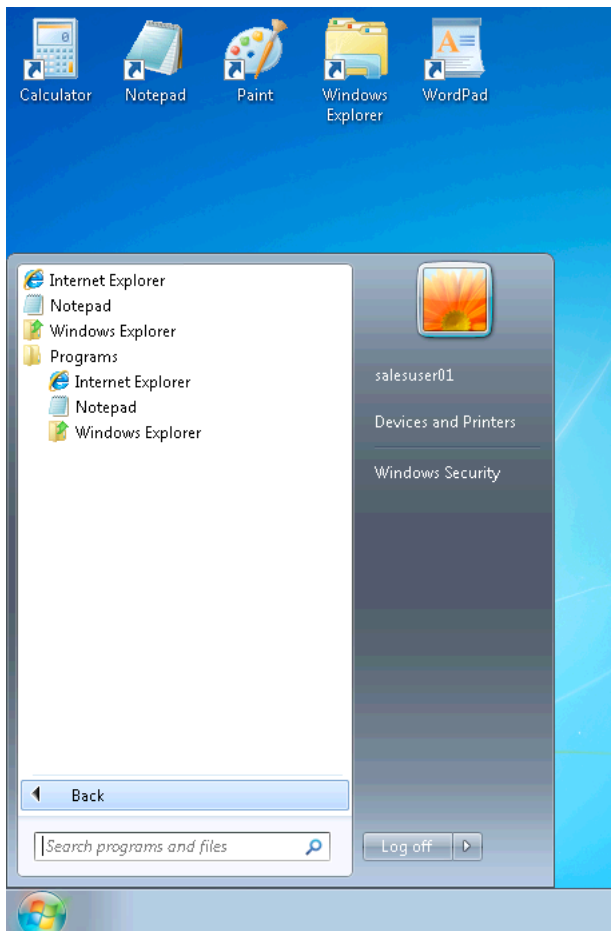
+Computer Configuration +Policies +Windows Settings +Security Settings and +Network List Manager Policies



A right-click on the network name icon (in my case corp.com) will open a properties dialog box where you can set the configuration on behalf of the user. Additionally, I also set the All Network Properties dialog box as well:



After completing these changes, we will have a desktop in Windows 7 similar to the one in Windows XP

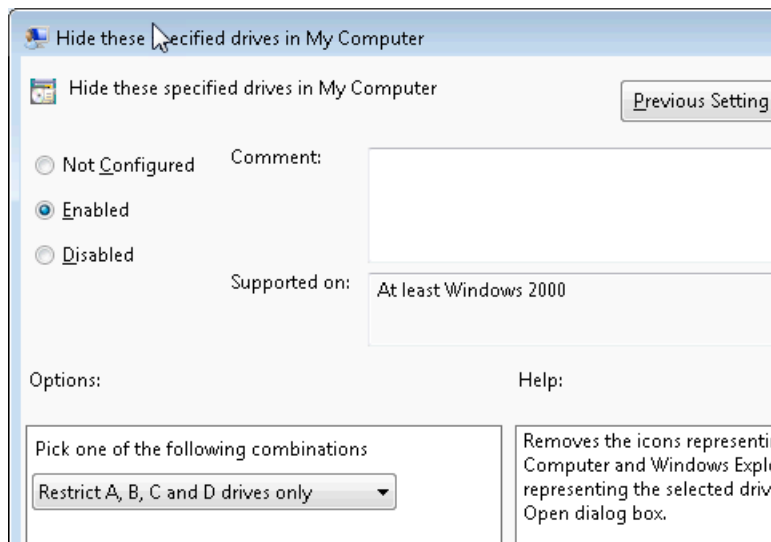


As you can see in the screen grab of the Windows 7 Start Menu, the quality of the menu is very rich and dense. This can lower performance (along with lots of other graphics enhancements such as menu animations, smooth-scrolling options etc.). If you wish you could change the theme for Windows to being the "Windows Classic" type, you may do so by enabling this option:

+User Configuration +Policies +Administrative Templates +Control Panel +Display +Desktop Themes and enable **"Load a specific visual style file or force Windows Classic"**. Enable the option but leave the path "Path to Visual Style" blank.

There are plenty of other loopholes in Windows that need closing. For example, while your users certainly need to see mapped network drives, they certainly don't need access to the C: Drive of the virtual machine. To hide drives in Windows you can use the following policy location:

+User Configuration +Policies +Administrative Templates +Windows Components +Windows Explorer and enable **"Hide these specified drives in My Computer"**.

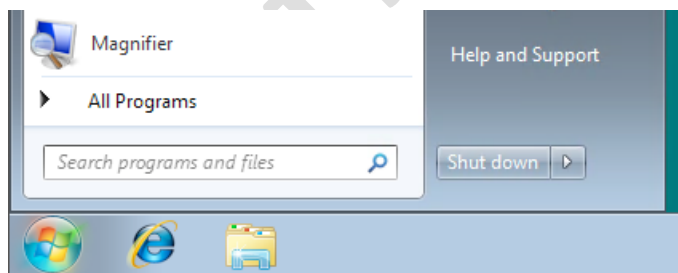


Additionally, the users still have access to the Windows Security dialog box via the Settings option on the Start Menu. So, perhaps some time spent disabling the Shutdown, Lock Computer and Task Manager options would be in order, too. The Windows Security dialog box can be controlled through the following policy location:

+User Configuration +Policies +Administrative Templates +System +Ctrl+Alt+Del Options

Whereas with **+User Configuration +Policies +Administrative Templates +Start Menu and Taskbar** there is an option where you can enable **"Remove and Prevent access to the Shut Down, Restart, Sleep, and Hibernate commands"**.

You might notice that in RDP sessions the default for the power button is to "logoff". This is fine, using PCoIP or Thin or Zero clients enabled with PCoIP you will these do allow users to shutdown their works stations.



So it's well worth covering you back, and ensuring that these power options are disabled.

Finally, I've not touched at all on some of the settings that inhibit the good performance of Microsoft RDP. These performance enhancements involve many changes and are beyond the scope of this guide, but there are plenty of locations on the internet that will help you with the settings you can change to improve performance. Here's a list of links to get you started:

<http://community.citrix.com/display/ocb/2010/01/15/Optimizing+Windows+7+for+FlexCast+Delivery>

<http://vmetc.com/2008/03/31/optimized-for-vdi-xp-virtual-machine-template-checklist/>

<http://virtuall.eu/blog/creating-a-vdi-template>

<http://whitepapers.techrepublic.com.com/abstract.aspx?docid=1680727>

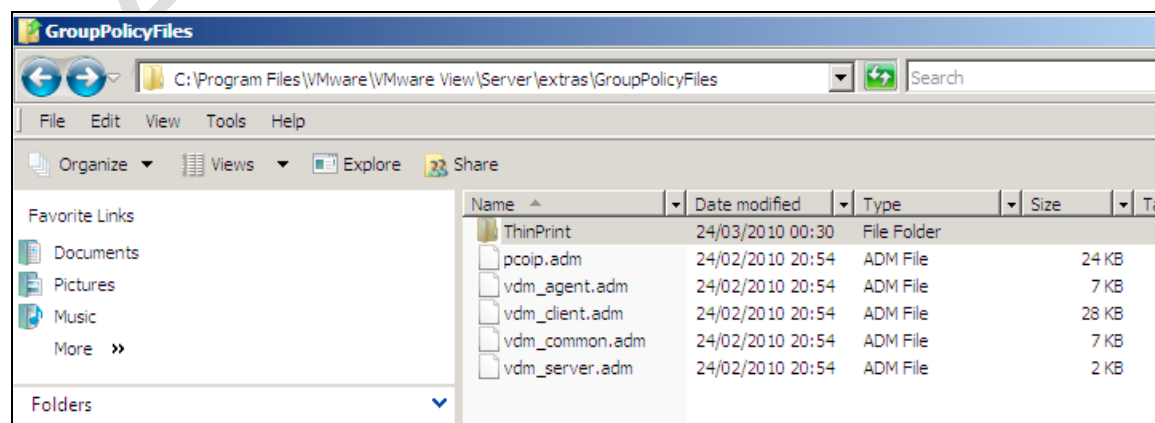
<http://support.citrix.com/article/CTX124239>

Obviously, given the fundamental importance of the remote protocol to the VDI experience, proceed with caution when making changes to this component.

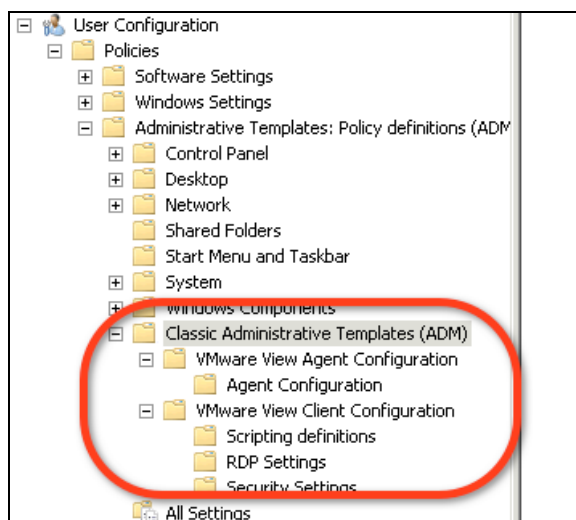
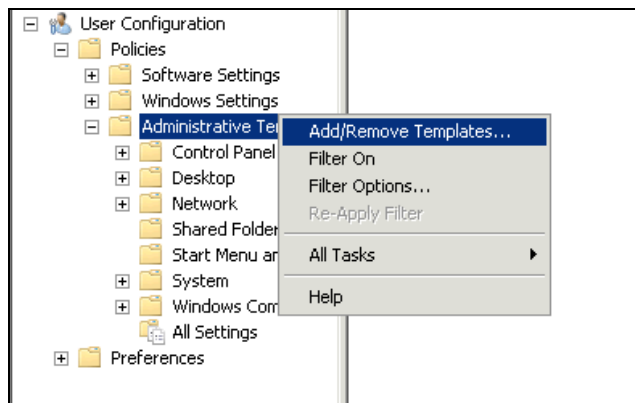
I think I've spent (wasted?) plenty of time on the subject already and perhaps made my point some time ago. I hope I haven't bored you too much! If you have been following this section to the letter, you will have a very restrictive desktop on which the user can do practically nothing but run the programs we dictate. It looks and feels very much like a TS or Citrix XenApp environment – I wonder if the users will notice the difference or even care!

There maybe some who find it a bit weird that I've used such an aggressive approach to the configuration of the users virtual desktop. Surely, one of the points of a virtual desktop is deliver a more "normal computing experience" akin to the end-users home PC. To be honest it's a matter of opinion and corporate standards. In terms of restrictions there sky is literally the limit – and you could go beyond Microsoft GPOs, and also consider removing components from the VM such as access to floppy, CD and com ports as well.

Anyway, as the final word on policies you, should be aware that the Connection Server holds a number of Microsoft GPO Template files (.ADM) which can be imported into the Administrative Templates part of a GPO. These custom ADMs allow you to set very popular Microsoft RDP preferences and also control the VMware View Client, Agent and some small Connection Server settings. You can find the .ADM files on the C: drive of the Connection Server at C:\Program Files\VMware\VMware View\Server\Extras\GroupPolicyFiles



These can be imported into Active Directory by right-clicking the + **User Configuration +Policies** and right-clicking +**Administrative Templates**



Chapter 15: VMware User Experience

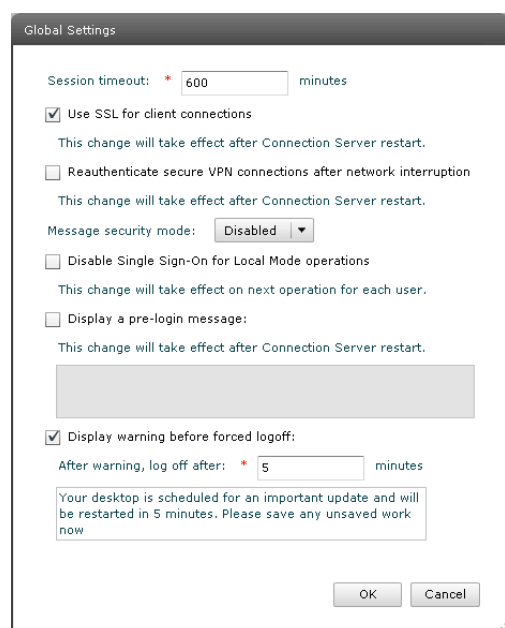
Note:

It will not have escaped your attention that the current version of View 4.5 lacks the "Virtual Profiles" feature that VMware acquired from RTO Soft. Virtual Profiles was in the Beta2 version of View 4.5, but was removed in the Release Candidate, and as a feature did not make the GA release. I imagine that some later this year or next, VMware will release an "Update 2" to View 4.5 which will add the feature back in. At that stage this chapter will be where I will cover the technology.

Global Settings


There are many locations where you can make changes to the way that VMware View functions.

Firstly, under ► **View Configuration** and **Global Settings** we have a dialog box that applies to all users connected via View to their virtual desktop.



Some of these settings I feel are self-explanatory, such as the Session Timeout values and the pre-login and forced log-off messages. However, for completeness I want to take you through each of these settings and explain the meaning, usage and impact.

Settings	Meaning, Usage and Impact
Session Timeout	Total length of sessions, regardless of activity. Default of 600 minutes is 10hrs. Warning: It's tempting to set a low tolerance on this value in effort to free up resources in the system, from users who leave themselves login for excessive time. Be careful. This can and does annoy users. My partner who works remotely via Citrix Presentation Server constantly moans about this being set in Citrix/TS/RDS. She literally has to hang around her computer waiting for the timeout message before she will take a coffee break! Getting logout often involves a length re-login process and wasted time loading up programs all over again...
Use SSL for client connections*	Turns off SSL for Connection Server – disable for local LAN connections where security might not be such a priority. However, it must be enabled for Smart Card Authentication. In the past, VMware has referred to this as a "Direct Connection"
Reauthenticate secure VPN connections*	Forces a re-login if you use a 3 rd party VPN connection to connect to the Connection Server. Setting has no effect if you disable SSL for Client Connections
Message Security Mode	Nothing to do with end-user messages! Concerns the security mode used between View server services. Enabling this will cause problems with older versions of View. If this is the case, either leave disabled or set the mode of mixed. In a pure View 4.x environment you can set "enabled" however, the View Security Servers config.properties file would need modifying for it to work
Disable Single Sign-on for Local Mode	Disables the single sign-on feature. Despite logging on to their corporate

	computer with domain credentials, users would have to supply login details to the View Client
Pre-Login Message*	<p>Displays (for mainly legal reasons) a message to a user prior to login to the system. A sample message appears below:</p> 
Display warning before forced logoff*	As we saw earlier in the recompose, refresh and rebalance of linked clones, users do receive messages when admin tasks affect the availability of their desktop
* Indicates that changes here require a restart of the Connection Server and any replicas	

Global, Pool and User Policies

Setting these global settings to one side for the moment, let's turn to VMware "Policy" settings. The use of speech marks is deliberate, as I think it's important not to see VMware Policies in the same light as, say, Microsoft GPOs. There's no VMware policy object that is attached to an OU, rather there is a global location where we can set our preferences. We can over-ride these settings by using policies that are created for each desktop pool you create; these in turn can be over-ridden by user policies. If set, User policies over-ride all settings specified globally or on pool policies.

As you might expect, the settings themselves are the same, all that changes is the scope of those changes – Global, Pool and User. These currently cover three main areas:

- View Policies (General Settings)
- Local Mode (Controls Local Mode - aka Offline Desktop - settings)
- Persona Management Policies

You can find global policies in the ► **Policies** and **Global Policies** – whereas Pool Policies can be found at ► **Inventory**, Select **Pools** then select the pool,

followed by click in the **Policies** tab. It's also in this location that you find the per-user policies or "Overrides". Notice in the screen grab below there is a "User Overrides" option. The important thing to note is that the overrides are to individual users, not groups in AD. I find that a little strange, but I assume VMware think the Pool represents a "group", although its perfectly possible for more than one AD group to be assigned to the pool. Sadly, that's where the logic of VMware Policies fail down – its been the case since VMware View first had a policy feature.

AccountsGroupWin7

Settings | Inventory | Sessions | Entitlements | Tasks | Events | Policies

Pool Policies | [User Overrides](#)

View Policies			
Edit Policies...			
Name	Global Policy	Pool Policy	Applied Policy
Multimedia redirection (MMR)	Allow	Inherit	Allow
USB access	Allow	Inherit	Allow
Remote mode	Allow	Inherit	Allow
PCoIP hardware acceleration	Allow - Medium priority	Inherit	Allow - Medium priority

Local Mode Policies			
Edit Policies...			
Name	Global Policy	Pool Policy	Applied Policy
Local Mode	Allow	Inherit	Allow
User-initiated rollback	Allow	Inherit	Allow
Max time without server contact	7 Days	Inherit	7 Days
Target replication frequency	1 Hours	Inherit	1 Hours
User deferred replication	Deny	Inherit	Deny
User-initiated check in	Allow	Inherit	Allow
User-initiated replication	Allow	Inherit	Allow
Disks replicated	Persistent disks	Inherit	Persistent disks

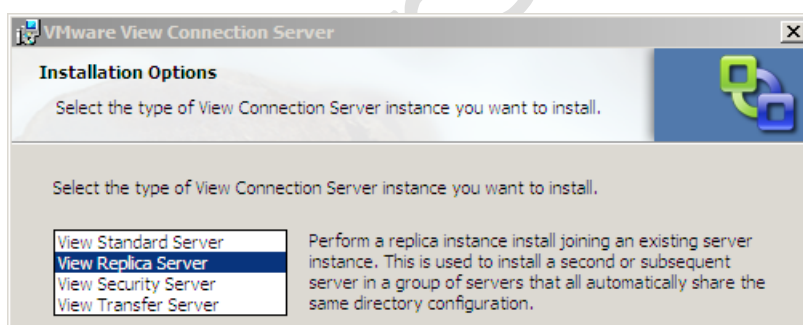
Authors EA

Chapter 16: Install a Connection Server Replica

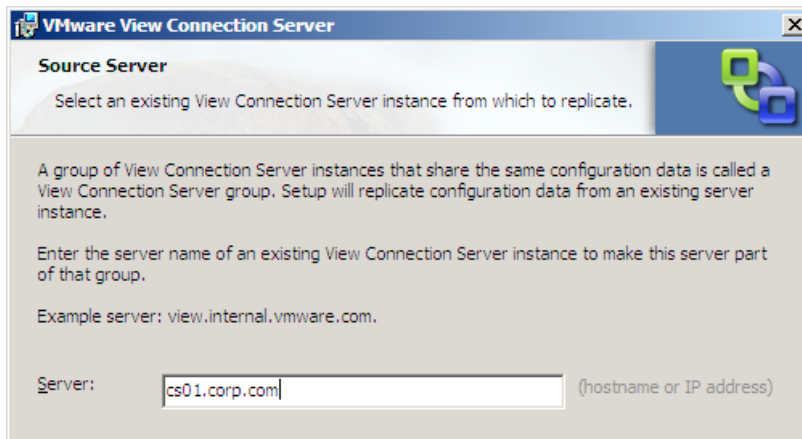
At the moment we only have one Connection Server, and if it went down or became unavailable, we would be in a heap of trouble. The solution to this single point of failure is to install a second Connection Server, referred to by VMware as a Replica. More than one Connection Server is referred to as a View Connection Server Group. It is a very easy task to carry out.

It's important to understand the limits of what a replica server can deliver. Replica servers are intended to offer availability, not fault tolerance. Once a user is actively connected to a Connection Server, if it becomes unavailable the sessions it is holding do not magically get moved to the replica. Additionally, there is no automatic load balancing built-in to the Connection Server software. You may need to rely on other third-party technologies to distribute the user load evenly between the Connection Servers.

1. **Create a new Windows 2008 VM and add it to Active Directory**
2. **Double click on the VMware-viewconnectionserver-N.N.N-NNNNNN.exe file**
3. **Accept** the usual suspects of **the Welcome Screen, EULA and the install path** for the software
4. Select **View Replica Server** from the list



5. **Type in the name of any existing Connection Server to make a View Connection Server Group.**



Note:

Allow the Connection Server software to configure the Windows Firewall.

If the installation has been successful, you will see the replica listed under "View Connection Servers" in the ►View Configuration and Servers page. Additionally, you should be able to load the View Client and configure it for the replica, and still receive the same desktop list.

View Connection Servers		
<input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Edit..."/> <input type="button" value="Backup Now..."/> <input type="button" value="More Commands"/>		
View Connection Server	State	Settings
CS01	Enabled	Secure tunnel connection, Smart card authentication: Optional, Automatic backup
CS02	Enabled	Secure tunnel connection, Smart card authentication: Optional, Automatic backup

Chapter 17: Install a Security Server

Despite the fact that Connection Servers offer an encrypted, certificates-based SSL Tunnel from the client to the virtual desktop, they are not appropriate for being patched to a DMZ. This is for two reasons:

- They are members of the corporate Active Directory Domain, and as such have domain privileges to a private network
- Ports are open to allow Active Directory communication which a hacker could utilize to facilitate other attacks

As an answer to the problem, VMware View has the Security Server role – it can be left in a workgroup and does not require domain access. It only responds to 443 requests and allows the firewall administrator to only open (inbound) secure ports to the external firewall. As with installing a second Connection Server, installing a Security Server is very easy. It is possible to have more than one for fault tolerance, however, a Security Server has a relationship with only one Connection Server at any one time. As you might recall, there is no built-in load-balancing feature for either the Connection Server or Security Server from VMware, as such you will need some sort of third-party load balancing solution.

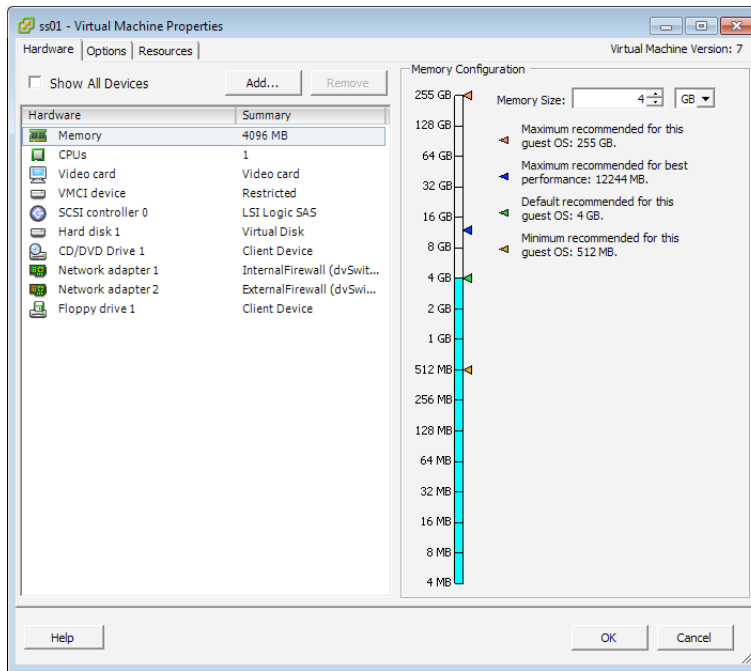
The installation of the Security Server differs quite a bit from both a Connection Server and a Transfer Server. Firstly, during the installation you will be asked for a pairing password. This is a one-off session-based password that expires after a configurable period, and is used to ensure that Security Servers and Connection Servers properly trust each other. However, no SSL Key exchange or SHA thumbprints are used in this process, unlike the case when you add an ESX host into vCenter, for example. Having successfully completed this verification process, you will be asked to set the “External DNS” name of the Security Server. This is to mask the true identity of the Security Server so, for example, my Security Server’s true FQDN is ss01.corp.com, but it will respond to the identity of view.corp.com. This external identity must be resolvable by public-facing DNS servers for it to work.

1. **Create a new Windows 2008 VM**

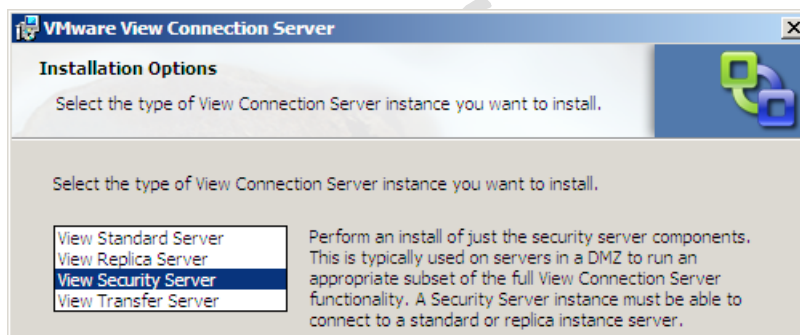
IMPORTANT:

DO **NOT** JOIN IT TO YOUR ACTIVE DIRECTORY DOMAIN

2. **Add a second NIC to the VM**, configure the first NIC to communicate to your internal firewall and the second NIC to communicate to your external firewall



3. **Double click on the VMware-viewconnectionserver-N.N.N-NNNNNN.exe file**
4. **Accept** the usual suspects of the **Welcome Screen, EULA and the install path** for the software
5. Select **'View Security Server'** from the list



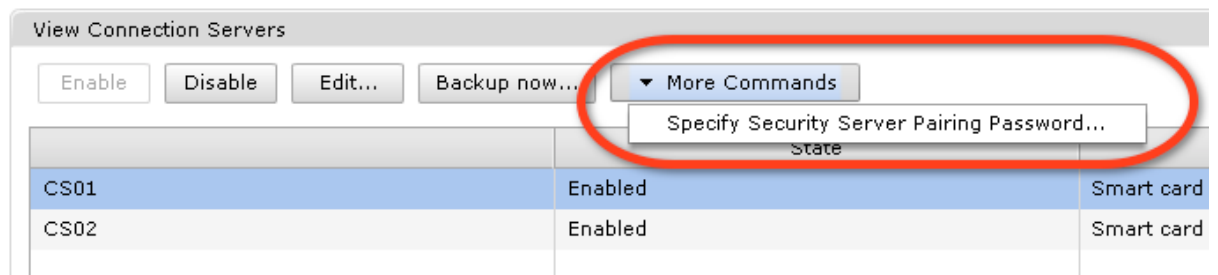
6. After the installation completes, you will be asked to **pair your Security Server to the Connection Server**



Note:

Given the Security Server's special role in the DMZ, you might find that internal name resolution fails for you. You can always use a hosts file for this purpose.

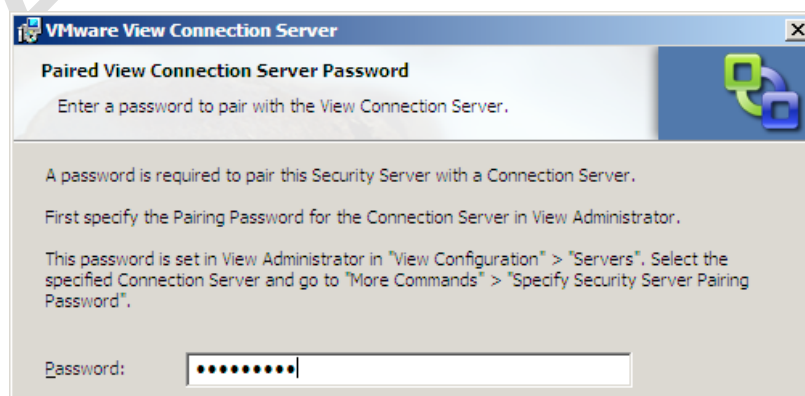
7. In the next step you will be asked to input the Security Server pairing password. To set a pairing password, navigate to ► **View Configuration**
8. Select **Server**, and then **Select the Connection Server** you will be pairing your Security Server to
9. Next click the **Commands** button – and select **Specify Security Server Pairing Password**



10. In the corresponding dialog box – **set your one-off pairing password – note the duration it takes before it expires!**



11. In the **Connection Server password dialog box** – type the password you set earlier



- The final step is to **set the External URL**. This is the name that external clients will use to connect to the Security Server. Critically, it must be resolvable by your external DNS environment. This URL can be changed once the installation has been completed



- As with the Transfer Server, the Security Server is added to the **View Configuration, Servers and Security Servers pane**

Security Server	Version	Connection Server
SS01	4.5	CS01

From this location the edit button can be used to alter the external URL.

As with the Connection Server, after the installation you should be able to connect to the Security Server using the View Client. Remember that as the Security Server is *not* joined to a Microsoft AD Domain there will be no automatic dynamic DNS update. As it is, the Security Servers are more likely to respond to external Internet IP addresses resolved by the public DNS system. If you wish to test the Security Server configuration you could use an IP address or a hosts file.

Secondary Security Servers are installed in exactly the same way, but two Security Servers are not allowed to be paired with one Connection Server. The pairing is a one-to-one relationship – one security server is paired with one connection server. In the case I have configured, ss01.corp.com is paired with cs01.corp.com and ss02.corp.com is paired with cs02.corp.com. Similar to the Security server, having more than one

Connection server is intended to deliver high availability to the environment, not fault tolerance. If a Security server goes down, the user's session to the virtual desktop will become disconnected.

Authors Edition

Chapter 18: Load Balance Security Servers

There are many options for load balancing your VMware View environment. Ideally, whatever solution you use should offer load balancing (as you might expect) but also be able to detect when nodes in the cluster become unavailable. Load balancers vary in quality and some do not handle this second requirement very efficiently. Of course, your availability issues could also be addressed with a combination of VMware High Availability and Fault Tolerance if your services were running in vSphere VMs.

Hercules is an IP-based load balancer that runs as a virtual appliance and is free to download from VMware's Market Place. I first came across this system from teaching the old VMware Virtual Desktop Manager (VDM) course, where we used it in the student labs. It does the job and simplifies the end user connection as they only need to connect to one IP address. True load balancing appliances - either physical or virtual - are likely to come in pairs to prevent them becoming a single point of failure but respond to one single IP address. You can download Hercules from here:

<http://www.vmware.com/appliances/directory/300>

The default login is *root* and the password is *root*, you will have to use the Linux text editor Vi to edit the `/etc/network/interfaces` file to modify its IP address. Once you have set the IP address of Hercules, you can use its PEN command to set the two Security Servers, and it will load balance like so:

pen 443 192.168.2.175:443 192.168.2.176:443

Alternatively, a cost-effective solution is to use Microsoft Network Load Balancing to create an NLB cluster of two or more Security Servers. Microsoft NLB is relatively easy to set up, and while it does handle load balancing successfully, I've found it somewhat lacking in detecting whether one of the nodes in the NLB cluster has gone down. It doesn't seem to have much awareness of the IP dependencies between the various components that it balances - additionally there will be scalability issues with NLB when you have a large enterprise deployment. The more I have investigated these options, the more I think how much simpler life would be if I only had one Security Server and Connection Server, and they were protected by VMware Fault Tolerance. However, the one thing that stops this configuration is patch management and upgrades. If you only have one Connection server and Security server, it becomes impossible to take down one of the roles to carry out maintenance of the server. Additionally, VMware FT does not protect a VM from service failure within the guest operation system.

What follows is very much a "Getting Started" guide to Microsoft NLB, it will not cover every single option or setting. My intention here is merely to show you an example of a load balancing system, and how it affects the configuration of the Security Server.

Before you head off to set up the Microsoft NLB Cluster, you can do a couple of checks at each Security Server. Firstly, can they ping each other by FQDN name? Secondly, can you run an nslookup test on the public FQDN and receive a positive response?

```
Mike-Lavericks-MacBook-Pro:~ MikeLaverick$ nslookup view.corp.com
Server:      192.168.0.1
Address:     192.168.0.1#53

Non-authoritative answer:
Name:   view.corp.com
Address: 216.250.183.109
```

If you cannot get name resolution working, you could use a hosts file on each Security Server. In my lab environment I often cheat and allow my Security Servers access to my DNS servers, which some people would regard as insecure. That said, a text file held on a local server in a DMZ could be regarded as less secure than accessing the DNS host. You pay your money and you take your choice. Technically, name resolution *between* the Security Servers is NOT required, but name resolution to the external/internet FQDN is.

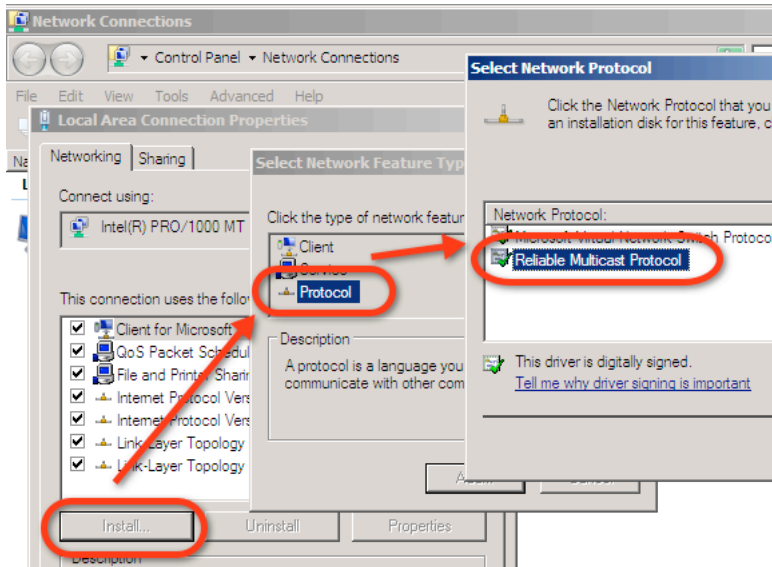
In the screen grab above, I have edited the image to not reveal the actual IP address that is the result. Successful responses to both of these questions will make the configuration of Microsoft NLB easier.

Enable Microsoft NLB Clustering for Security Servers

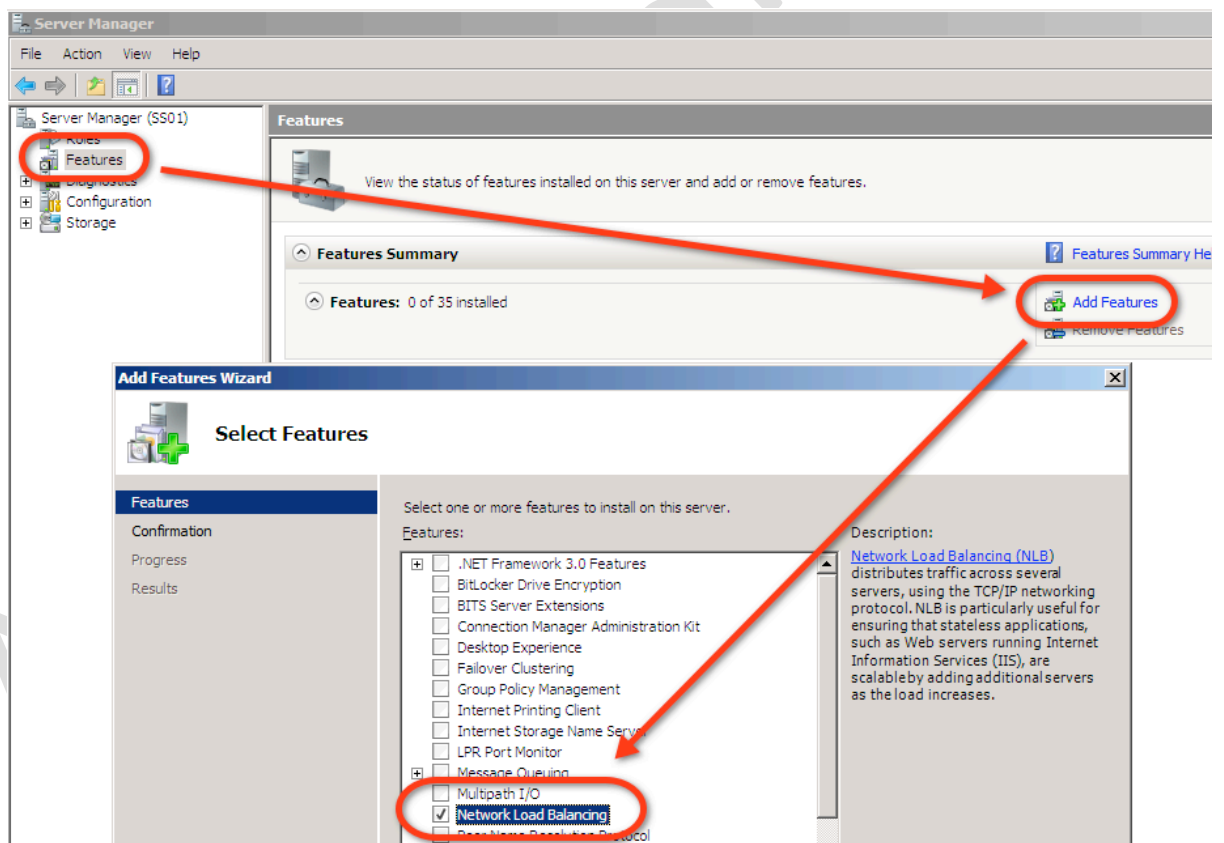
Microsoft NLB comes in two formats, a Unicast and Multicast method. I would strongly urge you to use Multicast as the method, for two main reasons. A Unicast Microsoft NLB is incompatible with vMotion, whereas Multicast is compatible. If you are forced to use a Unicast address you will have to modify the "Notify Switches" setting on the properties of a port group or vSwitch.

Secondly, a Unicast configuration is designed for when Windows has more than one network card. Since the way networking is configured in ESX is so different from the physical world, it's not necessary to add more than one NIC to the Security Server for NIC fault tolerance if it's running as a VM. However, you will still need more than one NIC in the Security Server so that it can communicate with the Connection Servers behind the internal firewall, and devices beyond the external firewall.

So for this configuration to work, you will need to install the "Reliable Multicast Protocol" for the Local Area Connection of each Security Server in the Microsoft NLB Cluster.

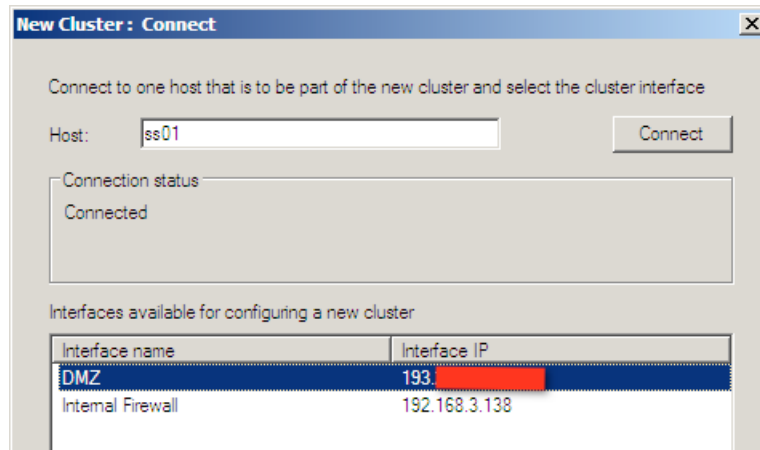


1. **Login to the Security Servers** and open the Server Manager MMC
2. Select the **+Features** node and click the **+Add Features** link
3. In the dialog box select **Network Load Balancing**



4. Click **Next** and **Install**
5. In the **Administrative Tools** menu - select the **Network Load Balancing Manager**
6. Choose **Cluster, New** in the menu
7. **Type in the name** or IP address that represents your DMZ network interface (in my case ss01 - 193.x.y.z) and click **Connect**. This should

enumerate the local area connections on the Security Server. I've renamed my interfaces to make them more meaningful in the dialog box:

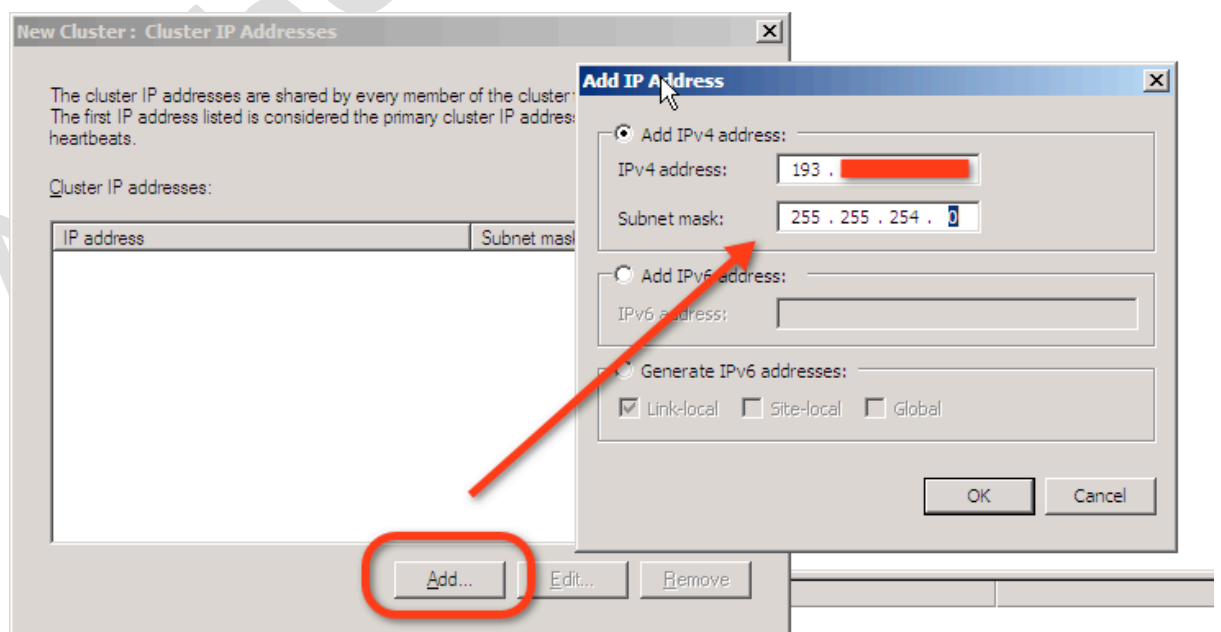


8. **Select the interface which is connected to external firewall or DMZ, and click Next**
9. In the **Cluster Parameters** dialog box, **accept the defaults** and **click Next**

Note:

Notice how this first host in the NLB cluster has a unique host identifier of 1, the second and third nodes added to the NLB cluster will each be given unique host identifiers of 2, 3 and so on. After you have waited a while, the cluster will be created with the first node joined to the cluster.

10. In the **Cluster IP addresses** dialog box **type in the external IP address used to access the cluster**



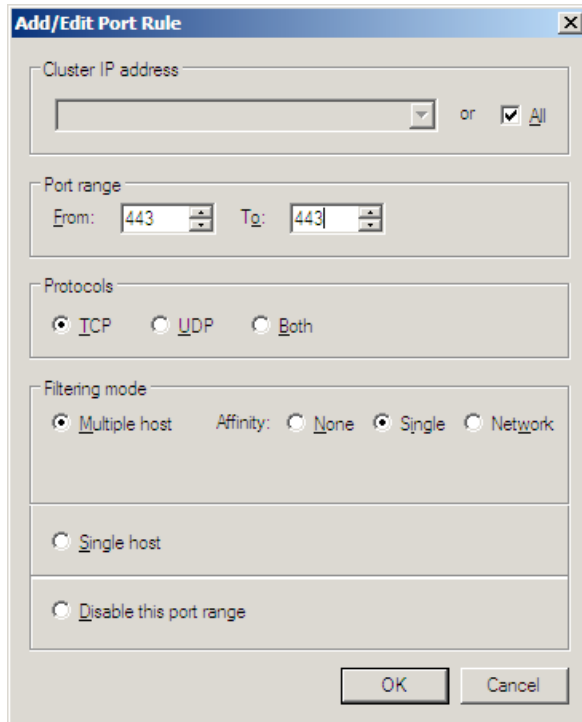
11. **Type in the FQDN that will be the public external URL** for the Security Server cluster, and select **Multicast** as the type:

The screenshot shows a dialog box titled "New Cluster: Cluster Parameters". It is divided into two main sections. The first section, "Cluster IP configuration", contains four fields: "IP address" with a dropdown menu showing "193", "Subnet mask" with the text "255 . 255 . 254 . 0", "Full Internet name" with the text "view.corp.com", and "Network address" with the text "03-bf-c1-c8-50-7d". The second section, "Cluster operation mode", contains three radio button options: "Unicast", "Multicast" (which is selected), and "IGMP multicast". At the bottom of the dialog box, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

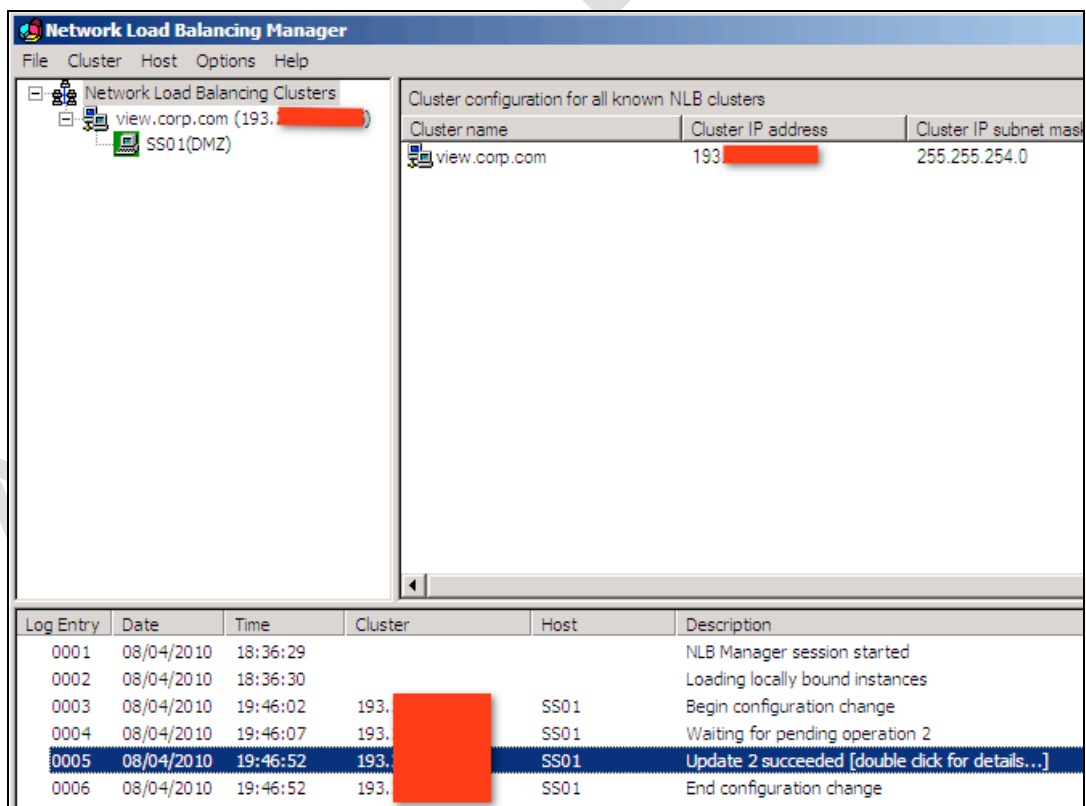
Note:

Be very careful with the IGMP Multicast as it can generate a significant amount of broadcast traffic. For this reason, it can be a good idea to place the Security Servers in a VLAN of their own, so their traffic does not adversely affect other systems. Additionally, you might find your network(s) does not support Multicast. I found this to be the case in my co-location. I was forced to opt for Unicast to simply make the configuration work.

12. In the **Port Rules** delete the default rule and **create a rule which is limited to listening for inbound 443 connections on TCP**

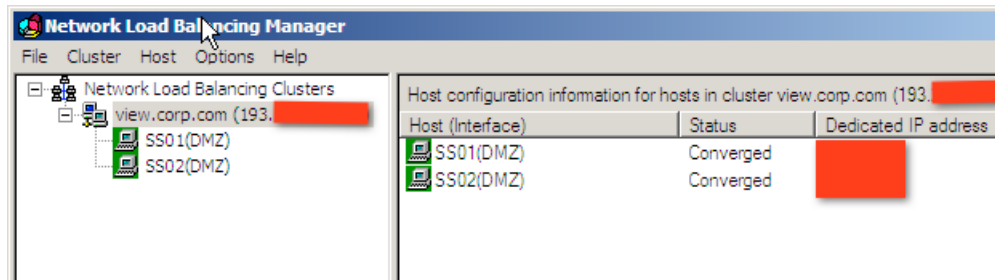


During this initial setup phase you can only add one server to the cluster. This server builds the cluster that then allows other servers to be added to it once it has completed its tasks.



- To **join additional servers to the cluster**, right-click the **cluster name**, in my case view.corp.com, and select **Add Host to Cluster**. In this wizard you can just click next..

After adding the second NLB host, there is a converging process before both nodes become active:



Test the Load-Balanced Configuration

Before you fire up a VMware View Client and try to log in to the VMware View NLB Cluster, first confirm that the client can resolve the external/internet FQDN to the correct address – in my case view.corp.com to my 193.x.x.x/23 address. My ISP does allow ICMP packets (which surprised me) so I can even ping my cluster from the Internet because my hosting provider allows ICMP packets as well (which surprised me even more!)

In my case I had to manually set the appropriate gateway settings on the properties of the Local Area Connection of the Security Server for this to work. Additionally, I had to adjust the metrics for my gateways (because I have more than one) to set the external/internet-based gateway address to be the preferred one.

VMware have a document that describes your options for load balancing in more detail. Although this document was originally written for VMware Virtual Desktop Manager 2, the load balancing technologies sit independently of the broker and therefore should work for any broker.

<http://www.vmware.com/files/pdf/vdm20-load-balancing-guide.pdf>

Chapter 19: Create & Apply Certificates

Now we're getting very close to a completed solution – all that is left to consider are those pesky things called certificates. In previous releases this was an important consideration. That's because in previous releases we had a fully-fledged 'web portal' which users could access via Internet Explorer, rather than using the fully blown client. VMware has now depreciated this functionality. As such the web portal now only acts a page to download the View client(s). However, to be complete I've opted to keep this in my guide. I also hope that VMware might reconsider the removal of the web portal and re-instate it in future releases.

I've been dealing with certificate technology for nearly ten years, and while they have come down in price since the days that Verisign and Thawte charged the earth for them, the generation and enrollment process is still fraught with administration, not least because each software vendor seems to prefer their own tools. There seems to be a bewildering array of certificate types, and in some cases the documentation seems to be decidedly lacking, precisely because there are so many different ways of managing the process. For this reason I'm going to assume you only have a passing understanding of certificates, and I hope I don't patronize too many people along the way.

In the main, certificates are used to prove or validate the identity of the server or service you're connecting to, with the intention of reassuring the user or customer that they have connected to a genuine website. The lynchpin of certificates is the concept of trust. You trust the certificate offered up by <https://www.hotmail.com> because an Authority created it that you trust. Specifically, your web browser has a list of trusted "root" certificate authorities (the people who issue certificates) built-in, including companies like VeriSign and Thawte. These authorities are meant to check out certificate applicants and revoke certificates that have been abused by rogue operators. The trouble is, they charge fees for their services, and there have been occasions in recent memory where the checking hasn't been as rigorous as it should be. The sad reality is that you can still go to a secured website that takes a payment, and then promptly shuts up shop the day after. Despite the rise and rise of e-commerce and a global financial system (are those terms sounding a bit hollow in Q2 of 2010?) consumer protection law seems to vary greatly, even from one part of the United States or the European Union to another.

The process of applying for certificates could be considered analogous to the way the passport system is generally managed. The root CA authority is like the national government, this body allows for the existence of the passport office (the Certificate Issuing Authority or sub-ordinate). The authority receives applications for passports from individuals who need to prove their identity to others (the certificate for the website). An application process is made by the

individual, and then the authority (the passport office) decides whether to allow or deny the application. The application process creates a private key that is used for encryption purposes. This private key is like a passport application together with all the other supporting documents required to validate the request (like your birth certificate and driving license). Until it is stamped or trusted by a recognized authority, it remains just a fancy piece of paper. These components need to be secured because if they were intercepted it would undermine the whole application procedure.

Occasionally, a certificate can be revoked if this relationship breaks down. The certificate authority can publish what are called revocation lists denying the authority of the certificate in question. You can liken this to when an individual commits a crime, and their freedom to travel is deliberately limited.

Alongside confirming the identity of the web server in question, the certificate also allows for encryption of data packets to and from the client and the server using the Secure Sockets Layer (SSL) originally developed by Netscape. SSL is the S you see in https://. Many web browsers now check the authority and validity of certificates which you will have seen countless times in iLO/DRAC/RAC boards and indeed in VMware products, which use internally self-signed certificates for Web Access and the vSphere Client. Indeed, nowadays the most common reason to generate certificates that are valid, is to prevent users over-reacting to various warnings and error messages generated when a certificate is not trusted. In the main, this is caused by lack of knowledge of what a certificate is, and the general paranoia about security of all web servers and sites – even intranet portals. Anyway, that's the end of the Sesame Street view of certificates, I'm now putting my bright yellow chicken suit to one side.

As you have seen, the process begins with a request for a certificate, and VMware use a Java utility called *keytool* to make the initial request file. Despite both the Connection Server and Security Servers being Windows-based, VMware has chosen not to use Microsoft utilities for the certificate enrollment process itself.

Add Java Keytool to the System Path

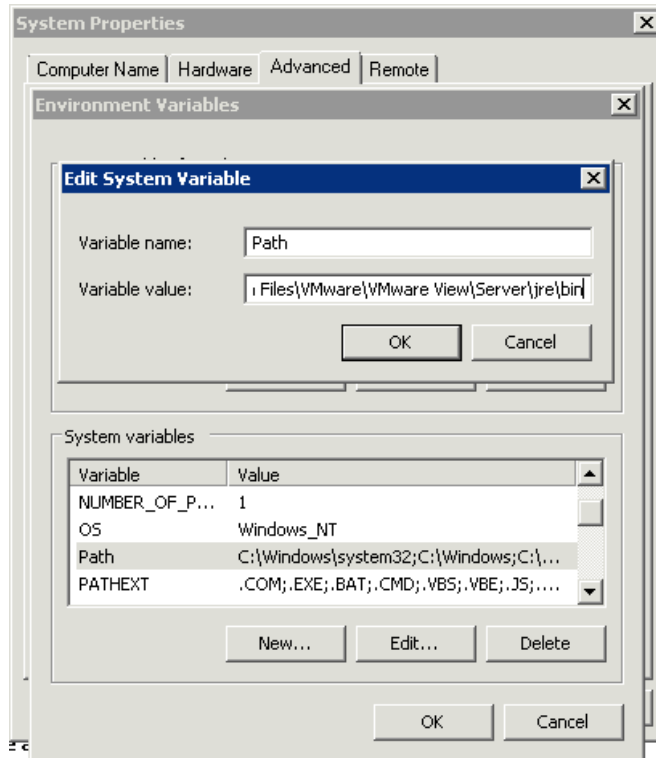
The Java Keytool is available on both the Connection and Security Server. It doesn't really matter which, I decided to use the Connection Server as it is on my internal network and trusted. Once the certificate request has been approved and the certificate downloaded, I will manually take it to each of my Security Servers and make sure it is installed and trusted. Unfortunately, the install of neither the Connection Server nor the Security Server sets up the necessary Path statements to the Java binaries to make them work:

1. Open the **Windows System Properties** dialog box
2. Under the **Advanced** tab, click on **Environment Variables** button.

3. In the **System variables group**, select **Path** and then click the **Edit** button.
4. In the **Variable value field** add the path to the JRE installation directory

;C:\Program Files\VMware\VMware View\Server\jre\bin

The semi-colon merely allows you to add one path after another



5. Click **OK** multiple times to confirm your changes and exit the dialog boxes

Generate a Certificate Request File

Next we need to use the *keytool* command to create a private key which is used in the identification and encryption process. This file on its own does not have authority from the higher body - it would be like printing your own passport. It is never transmitted across the network and is secured by encryption and password. If the private key were compromised then the whole chain of trust and authority would be compromised.

The private key is generated by using the *keytool* command together with some parameters. The *keytool* command will also run a wizard to ask you to identify information such as:

- The FQDN of the URL used by the end users to connect, in my case I've been using `view.corp.com`. Confusingly, *keytool* suggests using your "first and last name" when actually you should type the URL of your View virtual desktops environment

- Your department and organization
- Location (such as your town or city), State, and Country. The latter must be in the form of a two-letter country code that corresponds to the [ISO standards](#). For example in the United Kingdom you would not use UK, but actually GB for Great Britain. My country has many names, and we still haven't really decided what to call ourselves. If you're in the US, double-check your state name is in the correct format – I screwed up by initially typing New York State, rather than New York. I guess I should have remembered "New York, New York - so good, they named it twice!"

1. **Open a command prompt on the View Server** and use **cd** to locate yourself at the root of C:
2. Type the command:

```
keytool -genkey -keyalg "RSA" -keystore keys.p12 -storetype pkcs12 -validity 360
```

```
C:\>keytool -genkey -keyalg "RSA" -keystore keys.p12 -storetype pkcs12 -validity 360
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]: view.corp.com
What is the name of your organizational unit?
  [Unknown]: The Security Team
What is the name of your organization?
  [Unknown]: Corp Inc.
What is the name of your City or Locality?
  [Unknown]: New York
What is the name of your State or Province?
  [Unknown]: New York
What is the two-letter country code for this unit?
  [Unknown]: US
Is CN=view.corp.com, OU=The Security Team, O=Corp Inc., L=New York, ST=New York, C=US correct?
  [no]: yes
```

This command generates a private key using the RSA algorithm using the format of PKCS12. It is recommended that you secure and backup this file in case you ever wish to recreate the certificate files again. After hitting the enter key you will be asked for your identifying information – notice how the key file is itself encrypted and password-protected to prevent it being intercepted.

3. **Next we will create the certificate request file.** This is a file we can *safely* send to a root CA to request that our private key can be trusted by the root CA authority. This means that we must at no stage transfer the private key to anyone external to the organization. See the CSR file as a helper file that assists in the process of having our private key stamped for approval.

```
keytool -certreq -keyalg "RSA" -file mycertrequest.csr -keystore keys.p12 -storetype pkcs12 -storepass vmware
```

This command basically states you are creating a certificate request file (-certreq) using the RSA algorithm (-keyalg "RSA") calling the request file mycertrequest.csr, and using the private key created earlier, which is used to prove the identity of the server or services held in the keystore

file called keys.p12. The -storetype indicates we used the PKCS12 format, and the password used to access the private key data is *vmware*.

We should now have two files created in this process – one called keys.p12 which is protected and not human readable, and the mycertrequest.csr file which is text based and is viewable using a Microsoft *type* command

```
C:\>type mycertrequest.csr
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBxzCCATACAQAwwYYxCzAJBgNBAYTA1UTMRcwFQYDUQIEx5OZKcgWw9yaYBTdGF0ZTEWMBQGA1UEBxMNIU3IFlvcmsqQ2l0eTESMBAGA1UEChMJQ29ycCBJbmMuMR0wGAYDUQQLExFUaGUgU2Vj
dXJpdHkgUGUhbTEWMBQGA1UEAxMNdm1ldy5jb3JwLmNoLmNpbzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAkDPLnP057o8r2fDJYTOngSRsrwDQ3h9Tu09e18TaLRNHxSWG6y+zb055YL2QLUb8mwv
tRkJ5GBYDEgfRSMAknEZMSicJD+DRa88CsC1yghqW0T8HAsgYQ4Zduod/AfHBH7U0hcsMhdZgrEu
rj5BBtkTl13wPz9MozEGxsVFyiECAwEAaAAMA0GCSqGSIb3DQEBAQUAA4GBAENaGkC2qbT76S5e
34xwJ00YozevBTLCaU6p19oaiLYdNPLkfHrtefH7N9Z72Cu2U9wKef9eUHFu147YUnmmfzuKrIxp
lXg0WiAM/CRhPgHJb1i/jJjCbUFL3bZi3DyFYUz7wY5B0xbto07tcKQMGvF1WEcDhpTotmYGML5Y
g1x1
-----END NEW CERTIFICATE REQUEST-----
```

Submit the Request to the Certificate Authority

There are a number of places where you could submit this certificate request – either externally to a commercially available certificate authority which will be highly trusted by nearly every web browser and internet café on the planet, or alternatively, you could submit it to a certificate authority internal to your organization, which effectively limits your certificate to internal end users only. The request file can often be uploaded using HTTP forms, or you can frequently copy the text from -----BEGIN NEW CERTIFICATE REQUEST----- to -----END NEW CERTIFICATE REQUEST----- and then paste the string into an edit box on a form. Personally, I feel a file upload process is neater, but I have used both; it depends what the certificate authority supports. Many of the commercial certificate authorities allow you to generate a temporary test certificate which expires within a couple of days in the hope that you will later buy their services. These include:

Thawte:

<http://www.thawte.com>

VeriSign:

<http://verisign.com>

GlobalSign:

<http://globalsign.com>

In this example, I used Thawte to generate a certificate

1. In the cmd prompt, use the Microsoft **type** command to output the contents of the CSR file

2. **Select all the text** from including the words -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----
3. **Right-click** and **Choose Copy**
4. Open your web browser at:

<http://www.thawte.com>

5. In the **Thawte website**, click the link that says **"Free SSL Certificates"**
6. Next fill in the **Technical Contact page** and click **Continue**
7. From the **Select Server Platform** list, select the option **"Server not listed"**, and in its edit box type the string **"VMware View 4.5"**
8. Finally in the **Paste Certificate Signing Request (CSR)**... erm, press ctrl+v on your keyboard. I hope that isn't too bloody patronizing!

Note:

I don't intend to be funny here, but if you can't cut and paste a string into a web page then, Houston, we have a problem!

9. **Accept the Terms of the Agreement** and click **Submit**
10. **Thawte will then generate your certificate and send it to the email address provided earlier.**

Important:

When the email arrives it will contain two certificates – one identifying your FQDN for your View deployment (in my case view.corp.com), and


```

Your Thawte trial SSL certificate Download
-----
From: Thawte Customer Support Department <support@thawte.com>
To: Mike Laverick <mikelaverick@rtfm-ed.co.uk>
-----
an opportunity to experience the installation process as well as
determine your required server configuration.

-----
Your Thawte trial SSL certificate:

-----BEGIN CERTIFICATE-----
MIID0jCCArqgAwIBAgIQM2jh4cWZSR8/RpVdONDjnJANBgkqhkiG9w0BAQUFADCB
rTELMAkGA1UEBhMCVVMxFTATBgnVBAoTDHROyX0ZSwgS5jLjEoMcyGA1UECmFm
Q2Vydg1maWNoZG1vb1B7ZXJ2aWN1cyBEaXZpc21vbjEwMm4GA1UECmNmRm9yIFR1
c3QgUHVycG92ZXN0Z25seS4gIE5vIGFzc3VyYW5jZXMUMSswKQYDVQDEyJ0aGF3
dGUgVHJpYyYwZjU2VjdxJ11FNlcnZ1c1B5b290IENBMB4XDTEwMDQxNDAwMDAwF0x
DTEwMDUwNTIzNTk1OVowga0xZCAJBgNVBAYTA1VTMREwDwYDQ0IEhwO2Xcgw9y
azERMABGA1UEBmQlTmV3IFlvcmsxEjAQBgnVBAoUCUNvcnAgS5jLjEaMBGGA1UE
CxQVRVgh11FNlY3VyaXR5IFR1Yw0xMDAwBgnVBAUj0Zvc1BUZXRh11F1cnBvc2Vz
IE9ubHku1CB0byBhc3NlcmF1Y2VzLjEwMBQGA1UEAQNldy5jb3JwLmNvbTcB
nzANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEA1jySdsUtDu3e0bF9jummntBTxtt5
jCC6GZhw8doj+3jXABJ08/UoB6A0M224AJAHV3NcrttiNLcogmu3qXsItpUo3whf
++ZFRc1a3pAAym/QuAb3xjv1i5Fo/D9BgvwmQdJ+Jz4210vCyht+TBFV0z1gKk+
WtnBj4ewKymSgscAweAAANMG4wDAYDVR0TAQH/BAIwADA/BgnVHR8EODAM2D5G
MqAwh15odHRw018vY3JSLnRoYX0ZS5jB20vdGhhd3R1VHJpYXkxSb290Q0Eu
Y3J5SMB0GA1UdJQQMBOGCCSQAQFwBwMBGgrBgEFBQcDAjANBgkqhkiG9w0BAQUF
AAOCAQAFax5c1PFNNP8VZg6tdDM/1286aEB5nyZY1iQ9NhsLgtjoMhg8xvkD2k7
f14dyUytd7jGsiCNkpufo1PJM0nbz7xyNySCL3DEROerj+Hwxh1k7gtAUvraX
Ux7hA1Zxxqz2m0EneXbk7bwnNyVDEJca/Fvnp8vU3xa7q1275UHC/ZFFLPobfjqv
6C9bGUNPKgFER8ggACA7b+hvHU7rCySU6gNEJseH7ScbNdlJu2zaGF0xsRzdWL8b
amhZgBj3kHuxPq1/IDRG3uLw80rv+W2X/OD6sw4ZzhXhg9e7LCnPetmHua3vhjv
Za4iBudoPSyZt20YiAPg3UBkXPzkVw==
-----END CERTIFICATE-----

```

```

testcertificate.p7 - Notepad
-----
-----BEGIN CERTIFICATE-----
MIID0jCCArqgAwIBAgIQM2jh4cWZSR8/RpVdONDjnJANBgkqhkiG9w0BAQUFADCB
rTELMAkGA1UEBhMCVVMxFTATBgnVBAoTDHROyX0ZSwgS5jLjEoMcyGA1UECmFm
Q2Vydg1maWNoZG1vb1B7ZXJ2aWN1cyBEaXZpc21vbjEwMm4GA1UECmNmRm9yIFR1
c3QgUHVycG92ZXN0Z25seS4gIE5vIGFzc3VyYW5jZXMUMSswKQYDVQDEyJ0aGF3
dGUgVHJpYyYwZjU2VjdxJ11FNlcnZ1c1B5b290IENBMB4XDTEwMDQxNDAwMDAwF0x
DTEwMDUwNTIzNTk1OVowga0xZCAJBgNVBAYTA1VTMREwDwYDQ0IEhwO2Xcgw9y
azERMABGA1UEBmQlTmV3IFlvcmsxEjAQBgnVBAoUCUNvcnAgS5jLjEaMBGGA1UE
CxQVRVgh11FNlY3VyaXR5IFR1Yw0xMDAwBgnVBAUj0Zvc1BUZXRh11F1cnBvc2Vz
IE9ubHku1CB0byBhc3NlcmF1Y2VzLjEwMBQGA1UEAQNldy5jb3JwLmNvbTcB
nzANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEA1jySdsUtDu3e0bF9jummntBTxtt5
jCC6GZhw8doj+3jXABJ08/UoB6A0M224AJAHV3NcrttiNLcogmu3qXsItpUo3whf
++ZFRc1a3pAAym/QuAb3xjv1i5Fo/D9BgvwmQdJ+Jz4210vCyht+TBFV0z1gKk+
WtnBj4ewKymSgscAweAAANMG4wDAYDVR0TAQH/BAIwADA/BgnVHR8EODAM2D5G
MqAwh15odHRw018vY3JSLnRoYX0ZS5jB20vdGhhd3R1VHJpYXkxSb290Q0Eu
Y3J5SMB0GA1UdJQQMBOGCCSQAQFwBwMBGgrBgEFBQcDAjANBgkqhkiG9w0BAQUF
AAOCAQAFax5c1PFNNP8VZg6tdDM/1286aEB5nyZY1iQ9NhsLgtjoMhg8xvkD2k7
f14dyUytd7jGsiCNkpufo1PJM0nbz7xyNySCL3DEROerj+Hwxh1k7gtAUvraX
Ux7hA1Zxxqz2m0EneXbk7bwnNyVDEJca/Fvnp8vU3xa7q1275UHC/ZFFLPobfjqv
6C9bGUNPKgFER8ggACA7b+hvHU7rCySU6gNEJseH7ScbNdlJu2zaGF0xsRzdWL8b
amhZgBj3kHuxPq1/IDRG3uLw80rv+W2X/OD6sw4ZzhXhg9e7LCnPetmHua3vhjv
Za4iBudoPSyZt20YiAPg3UBkXPzkVw==
-----END CERTIFICATE-----

```

Save the file and close Notepad. Finally, we will import our test root CA certificate and the view.corp.com certificate with keytool, and then configure our Security Servers to use it

13. To import the test root CA certificate type:

```

keytool -import -trustcacerts -keystore "C:\Program Files\VMware\VMware View\Server\jre\lib\security\cacerts" -storepass changeit -alias Root -import -file c:\Trustedcaroot.txt

```

Note:

When the prompt finally shows, type yes to accept the certificate being imported into the trusted root certificates store

```

C:\>keytool -import -trustcacerts -keystore "C:\Program Files\VMware\VMware View
\Server\jre\lib\security\cacerts" -storepass changeit -alias Root -import -file
c:\trustedroot.txt
Owner: CN=thawte Trial Secure Server Root CA, OU="For Test Purposes Only. No as
surances.", OU=Certification Services Division, O="thawte, Inc.", C=US
Issuer: CN=thawte Trial Secure Server Root CA, OU="For Test Purposes Only. No a
ssurances.", OU=Certification Services Division, O="thawte, Inc.", C=US
Serial number: 3F5329E27132B209ebf37a189a378d8
Valid from: Fri Oct 09 01:00:00 BST 2009 until: Tue Oct 09 00:59:59 BST 2029
Certificate fingerprints:
MD5: FB:8B:B4:59:96:74:32:7A:95:91:3A:E5:5D:24:52:53
SHA1: B9:32:B9:15:44:8A:C4:60:71:82:B0:2B:3E:B0:A7:37:61:09:2E:BF
Signature algorithm name: SHA1withRSA
Version: 3

Extensions:
#1: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
  CrL_Sign
]
#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints [
  CA:true
  PathLen:2147483647
]
#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
  0000: 05 42 68 03 E9 C9 65 C1 27 B3 D9 9B D4 0F F7 ..Bh...e.'.....
  0010: 7F F5 05 40 ...e
]
]
]
Trust this certificate? [no]: yes
Certificate was added to keystore

```

14. Type the keytool command:

keytool -import -keystore keys.p12 -storetype pkcs12 -storepass vmware -keyalg "RSA" -trustcacerts -file testcertificate.p7

This instructs keytool to import the private key held in keys.p12, once it is verified as being correct by the testcertificate.p7 file from the authority. Despite the appearance of trustcacerts in the string, frequently these "test only" certificate authorities are not live root CAs. This is done to prevent fraud and misuse of trial certificates, so when the import takes place you may well see the message "... is not trusted. Install anyway? [no]: yes". This message should not appear if you are carrying out the enrollment process with a proper commercial root CA or if you have already imported the test root CA certificate as I have done in this example.

15. Next **create the locked.properties file on the first Security Server**

Notepad C:\Program Files \VMware \ViewManager \Server \sslgateway \conf \locked.properties

16. **Add these two lines to configure the Security Server for the Private Key together with the password to access the file correctly**

keyfile=keys.p12

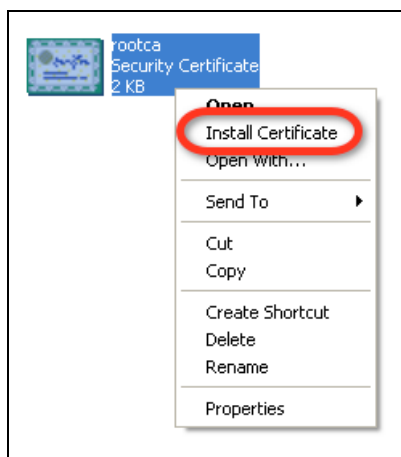
keypass=vmware

17. **Save the locked.properties file**

IMPORTANT:

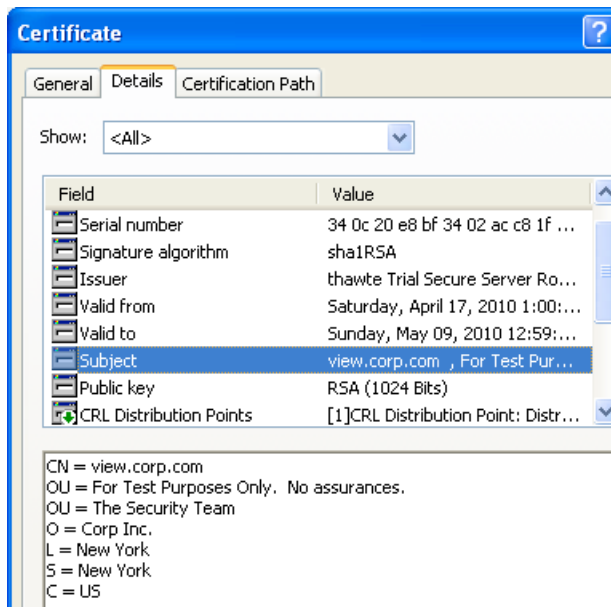
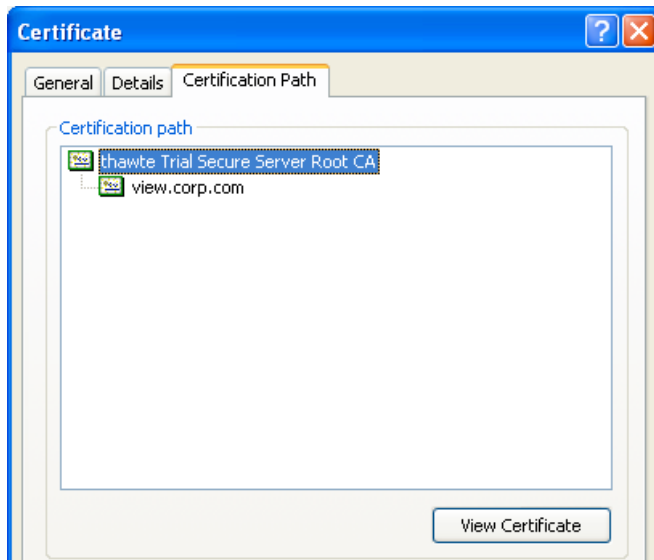
Copy the keys.p12 file to the C:\Program Files \VMware \ViewManager \Server \sslgateway \conf directory

18. Restart the **View Security Service** with either the Services MMC or using **net stop wsbroker** and **net start wsbroker** from the command prompt
19. Next **copy the keys.p12, testcertificate.p7 and locked.properties file to the companion Security Server**. Remember to copy the locked.properties file to the **C:\Program Files \VMware \ViewManager \Server \sslgateway \conf**. Then repeat steps 13, 14 and 18 on the second Security Server.
20. The next step is to **optionally install the test root CA certificate on one of your clients**. On the client, use Notepad to create a .CER file to hold the certificate data with **notepad c:\testrootca.cer**
21. Then copy the text **-----BEGIN CERTIFICATE-----** and **-----END CERTIFICATE-----** into the testrootca.cer file and save
22. Next **right-click the testrootca.cer file** and select **Install Certificate**



From this point you can simply next your way through the dialog boxes accepting the defaults

23. From the client where you just imported the test root CA certificate, open a web browser to your external URL, in my case <https://view.corp.com>. Your web browser should allow you to see the certificate to verify its content. Most web browsers like Internet Explorer support viewing the certificate by double-clicking the padlock icon in the status bar - you can use this dialog box to confirm that the Security Server is no longer using its own internally-generated certificate:



Chapter 20: Virtual Applications with ThinApp

We are now moving on to a whole other aspect of VDI, and that's the virtualization not just of operating systems but the applications as well. There are many benefits to application virtualization including:

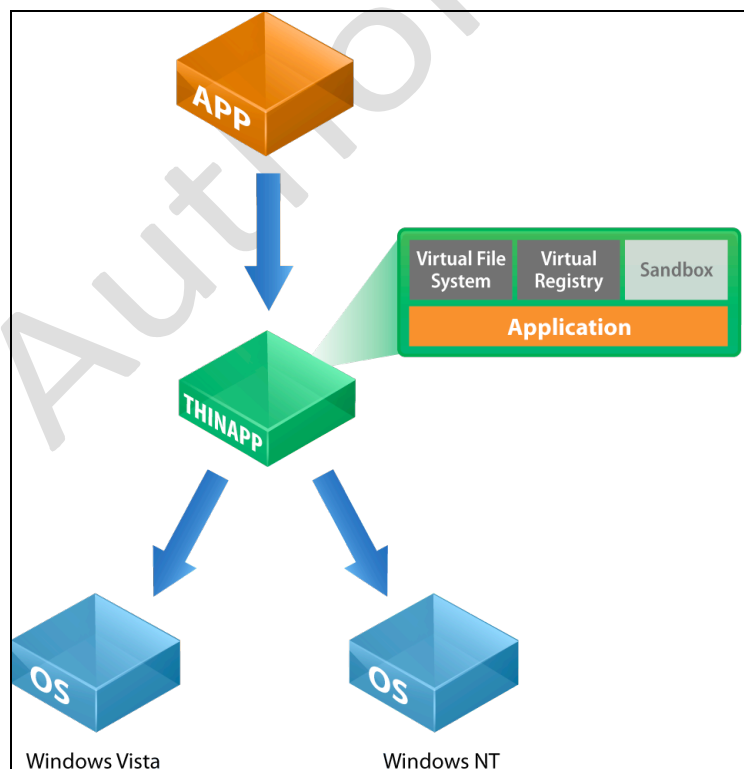
Advantages of Application Virtualization

- **Less conflicts** between one application and another
- **Same App, Different Versions:** The ability to run different versions of the same application in the same Windows environment
- **Keeping the Virtual Desktop Lean and Mean:** Keeping your virtual desktop as an environment to merely execute programs rather than store them locally in C:\Program Files
- **App-on-a-stick:** Application Virtualization is not limited to virtual desktops. Often you carry your applications around on a memory stick and execute them anywhere as they work within their own sandbox
- **ThinApps:** One key advantage of ThinApp is that the virtualization allows for total encapsulation - in other words, there is no need to install a special client at the destination where the ThinApp will run. A ThinApp is an entirely separate and independent .EXE in its own right. The ThinApp runtime uses a Primary Data Container to hold the ThinApp runtime itself - a read-only virtual file system and virtual registry. ThinApp is popular because unlike some application virtualization it is agent less and clientless. This is seen as being more portable than other solutions. It allows the application to be ported to virtual desktops and terminal service without rebuilding or recompiling the application
- **Network Streaming:** Most application virtualization products will "stream" apps if delivered over the network - in other words, the client just downloads the files it needs as it needs them. Often these can be configured to be cached - just like a web browser - to speed the application's launch when it is next loaded by the user
- **ThinApp the View Client** - If you think about it, one of the challenges of deploying View is that fact a client needs to be installed on the endpoint device. A simple remedy to this situation is to create a ThinApp of the client. It also means that when the client needs upgrading, you can simply publish a new version of the ThinApp
- **Play in your sandbox** - Most application virtualization tools have a sandbox concept, and ThinApp is no different. The idea is that all the changes a user makes to an application are directed to this sandbox location. So, unlike a conventional Terminal Services environment where end user customization can be difficult, the sandbox allows the user to customize the application to suit their needs. The sandbox is normally

included inside the user's roaming profile, but it can be redirected to a USB location for local use, or to a network location - the choice is yours. Additionally, the sandbox can be made read-only - while a user can open the application in their ThinApp session and make changes to their preferences, once the user logs out, the ThinApp returns to its default settings. If something goes wrong with a ThinApp, you could delete the sandbox associated with it, and this would force the re-creation of the sandbox as if the user had yet to run the ThinApp for the first time

- **All this and more** - You can do all this and more - ThinApp itself is in part a ThinApp, and the installer is just 7MB in size. How's that for efficient programming!

The diagram below shows a typical architecture overview of the ThinApp system. Each application sits within the ThinApp runtime that provides a virtual file system and virtual registry. As with server and desktop virtualization, the ThinApp-enabled application believes it is running in an unmodified environment - in most cases, applications should work happily within ThinApp. This virtual file system and virtual registry is given the collective name of the sandbox. The sandbox is a read-writable environment by default. As long as users have read-write access to their user profile (where the sandbox is stored), then any changes the users make to the application will be saved. Using the ThinApp "package.ini" file, it is possible to make the sandbox destroy itself every time the application is closed - this effectively makes the sandbox a read-only container, which discards any changes that the user made when the ThinApp was loaded.



When ThinApps are created everything that makes up the ThinApp is held in what VMware call the "Primary Data Container". This container holds a virtual file system and Windows Registry – when loaded the ThinApp thinks it can see a real C:\ driver when in fact it sees a virtual C: drive. The whole thing once loaded is referred to as the "Virtual Operating System" or VOS. If you like your ThinApp is running a virtual operating system, inside an operating system which is contained in a virtual machine!

Limitations and Requirements

It's worth acknowledging that some of these issues are a pain point whether you use application virtualization or not. The Licensing and Activation process can be a royal pain in the rear, and you could argue that any large corporate with a dedicated application packaging and deployment team would look at these issues and say "Well, yes we have to manage these with or without application virtualization, and anyway, application virtualization is one tool that helps us deal with those crummy installers."

- **Application is *not* installed natively:** One of the selling points of virtual desktops compared to the shared desktop model is that applications can be installed natively to the client operating system. By definition, if we use application virtualization this is no longer the case. One of the downsides of application virtualization is the inevitable fact that, sooner or later, an original software vendor will not support the use of ThinApp or other tools of its ilk.
- **Software with Drivers:** Software that installs or requires some kind of kernel mode driver will in most cases be impossible to capture in the application virtualization software. For example, you cannot create a ThinApp of VMware Workstation. When VMware Workstation installs, it adds drivers to the underlying Windows OS and modifies the underlying network infrastructure as well. This limitation also extends to scanner software and webcam software. Previously, I described creating a ThinApp of the View Client. If you do this, I recommend that you do not include the virtual printing or USB redirection service – both of these install kernel-mode drivers.
- **File Associations:** Although you can have three different versions of Acrobat Reader or Microsoft Word simultaneously running happily on one OS, only one of them can "own" the file associations of the application. So when you double click on a PDF file, the question would be which ThinApp would be used as the default application? Most application virtualization vendors have a method of setting a preference. In the case of View, it uses an .INI file
- **Support Politics:** If you think running an application or service inside a VM with source code totally unmodified can be political in the sense that an application vendor may not be officially support it, how do you think

these same application vendors respond to virtualizing their client applications? Expect to see comments like “re-engineering” and “not by design”. A bit like with service providers, these client application guys need to catch up. As with virtual appliances, distributing a client application which runs preconfigured and independently of the windows OS without an installation routine is the way to go. In fact, a virtualized application is likely to create less problems and conflicts due to using a sandbox

- **Licensing and Activation Processes:** As with virtual machines and the guest operating system, you will really want to hunt down and use so-called “Corp” editions that often allow for bulk activation, or even bypass the activation process altogether. However, ThinApp obviously doesn’t change your application vendor’s license policy, it merely captures the install you would have done if you didn’t own some kind of application virtualization software. So, if you want to run 20 copies of an application, and the vendor says you need a special unique TXT file for each application that runs, the same restriction would apply to a ThinApp. The last thing you want to do is to have to create 20 ThinApps; that kind of defeats the object of the exercise.
- **Dependencies Captured:** You will need a clean or “base” Windows install every time you capture an app, so that there are no dependencies present during the capture process. This avoids a situation where a .NET application refuses to function because the source OS had .NET installed before the capture process, and it was therefore ignored. When the virtual application is loaded on the destination it might fail because .NET is not installed. To get round this issue I install the ThinApp software to a clean “Build” machine and share out its directories. Then I take a snapshot of my Parent VM, and run the ThinApp software remotely while I install the new software. Once the build process is over, I can then revert the snapshot on the Parent VM so it is returned to a clean state – ready for my next ThinApp
- **Application Updates:** Most software comes with its own “Hey, I see you’re busy working right now. But we’ve released a new version of this software which fixes all the problems we knew we had in the beta program, would you like to download it to fix it – and then have a whole new bunch of bugs introduced that no-one knows the workarounds to?” Seriously, when an application tells me it has a new version, I sit there and think, “Am I tempting fate here?”. As an end user who manages his own single PC, I take that decision and live with the fact I’m not patched to the hilt. The same cannot be said for those in the corporate space. It’s important to switch off these application updates because they will most likely waste space in the end user sandbox, while at the same time failing because they are not aware they are running in the ThinApp sandbox
- **ThinApp Every App?:** Some organizations decide that large multi-app application suites like Microsoft Office are best installed locally to the

virtual desktop, leaving application virtualization to deliver strategic applications. This is not dissimilar from how many corporates use Citrix XenApp to deliver mission critical services like email and database access, but still continue to install applications locally. It remains to be seen whether such approaches remain popular as application virtualization technology matures. As with server virtualization, we might move to an "Application Virtualization First" policy with ThinApp or one of its competitors

Frequently Asked Questions

A. Can you build 64-bit applications and run them on 32-bit operating systems?

Q. No. A 64-bit ThinApp still makes calls to the processor looking for 64-bit attributes. So just as 64-bit virtual machines could not execute on 32-bit processors (in the days of ESX 3.x), the same applies to application virtualization.

A. Would a 32-bit application built-in Windows XP 32-bit run in Windows 7 64-bit?

Q. Yes, application virtualization insulates you from the operating system differences, and 64-bit processors and operating systems still support 32-bit applications. In fact, application virtualization is a good way of allowing legacy applications that won't install on new operating systems to continue to function. This is similar to how we P2V'd legacy Windows NT4 operating system servers into virtual machines in the last decade to extend their life beyond the hardware support period.

A. If I publish ThinApps, or groups of ThinApps, to a linked clone desktop, and then I refresh, recompose or rebalance the pool what happens then?

Q. View will reinstall the ThinApp for you.

A. If I packaging something large like Microsoft Office. What's the best practice? One large ThinApp – or a ThinApp for each component – Word, Excel and so on?

You could make office part of you default build installed locally. I use ThinApp to deliver strategic applications in an on-demand basis. If you do wish to ThinApp a large suite of applications like Microsoft Office – then general recommendation is to great one ThinApp for the suite. This will preserve the interoperability and productivity enhancements where one application acts as a "helper" for another. Splitting out the applications could create incompatibilities and lost functionality.

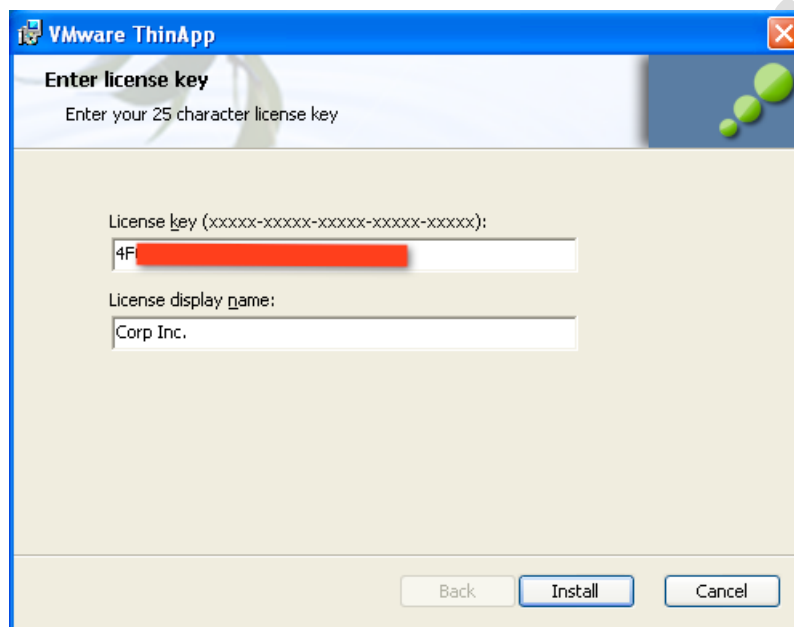
TIP:

If you want to see a ThinApp in action without the need to create yourself. It is

possible to download some free applications that have been already made into ThinApps. You can find these on the website - thindownload.com

Install ThinApp – The “Build” Machine

1. **Download and Install ThinApp** by executing the **VMware-ThinApp-N.N.N-NNNN.exe** on an ordinary virtual machine. View supports the configuration of a file server known as the ThinApp Repository. You could install ThinApp on this Repository server and only share out the Capture directory where your ThinApps are compiled. This will save you the hassle of copying the ThinApp from the Build machine to the Repository server
2. **Accept the EULA**
3. **Input your License String and License Display name**



The “License Display Name” is shown whenever a ThinApp is loaded. When a ThinApp is loaded, a small tray icon appears with the name of the application and the License Display Name. This is used in lieu of the vendor’s own “splash” or welcome screen. It may be required in order to meet the terms and conditions of some EULAs.

4. Next **share out the directory of C:\Program Files \VMware \VMware ThinApp**

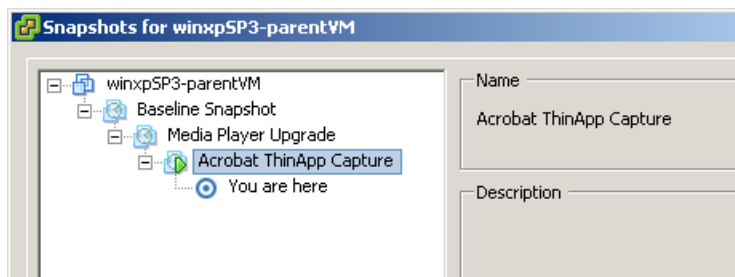
Create a ThinApp Example - Acrobat Reader

ThinApp is very easy to use – and if you have ever used some type of application capturing tool before, they feel very much the same – although the quality of them varies. So, if you have used Veritas WinInstallLE or Citrix Application Packager, it is very similar. The difference is that the output is a self-contained .EXE. Most packaging systems have a four stage process:

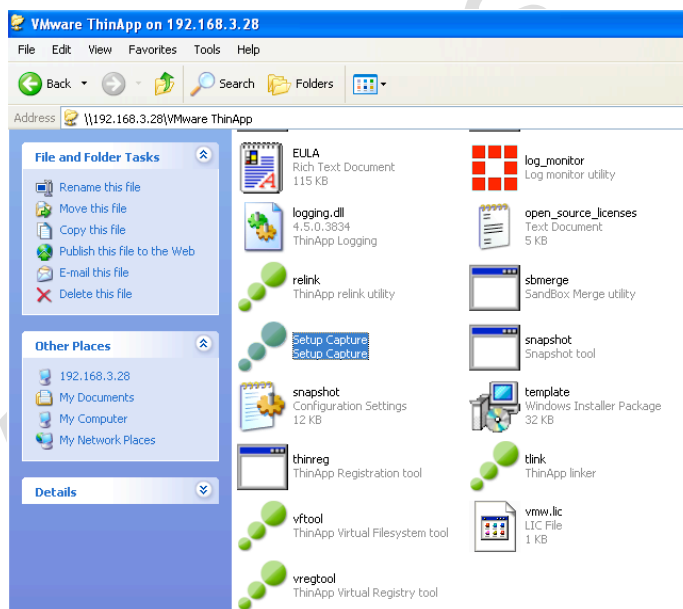
- Pre-analyze the clean environment (Pre-Scan)
- Install the Application Software (Install)
- Capture the Differences (Post-Scan)
- Output Package to default location (Build)

During the Pre-Scan and Post-Scan stage, ThinApp creates its own virtual registry and file system to capture all the changes being made. There is a snapshot taken both before and after, and by comparing the two, ThinApp can then begin the build process.

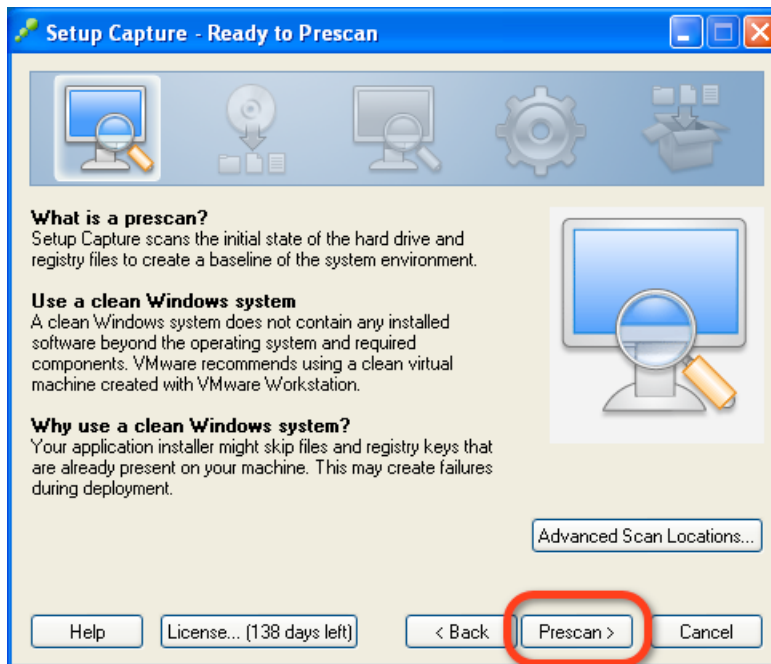
1. **Login to your Parent VM and take a snapshot** – in my case, I named the snapshot after the application I intended to install



2. **Locate and Download the Acrobat Reader** installation package
3. Once the download has completed, **Run the ThinApp Setup Capture** program by browsing the network for the build machine on the network

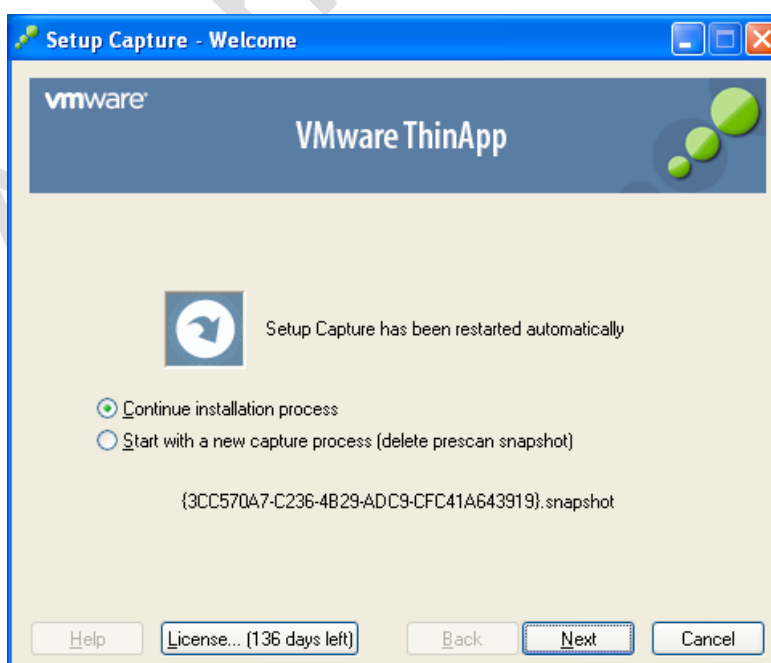


4. Click Next at the **Welcome Screen**
5. **Notice the warnings** about the significance of having a clean PC
6. **Click the Prescan button.** ThinApp will start the initial Prescan of the virtual desktop



Note:

The Advanced Scan Locations option allows you to select which virtual disks will be scanned, and also which parts of the registry. ThinApp always scans the HKEY_CURRENT_USER hive (which is, in fact, the user's profile), and you can optionally choose not to include HKEY_LOCAL_MACHINE (Windows system settings) and HKEY_USERS (the default user profile). This scanning process creates a snapshot of the machine's state prior to installing the application. If you subsequently cancel the Setup Capture wizard and then restart the process, a dialog box will appear asking how you want to manage the existing snapshot:

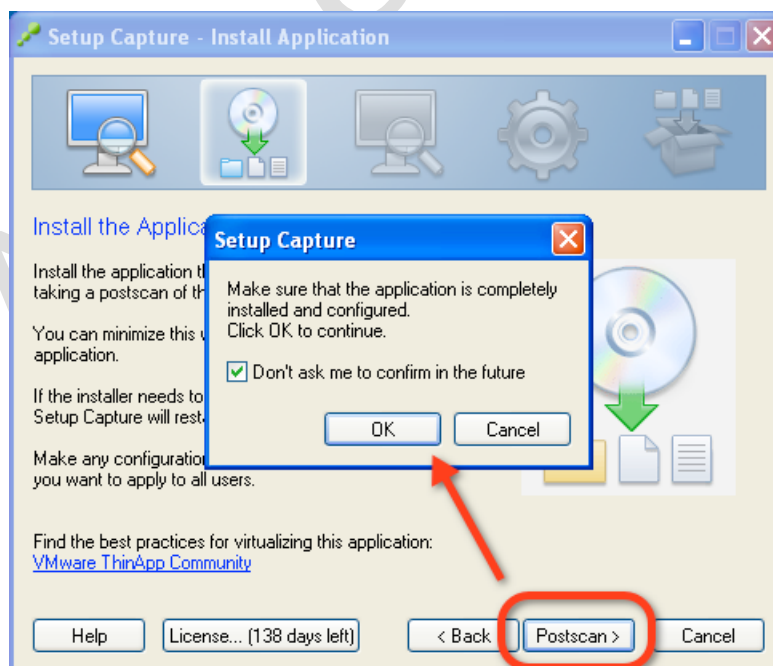


7. At the end of the Prescan, when you see the "Install your application now!" prompt, **minimize the ThinApp Window** and **start the install of the application, in my case Acrobat 9**

Naughty Tip:

Most application recording packages allow for a nifty hidden advantage. During the recording process, it is possible at the end of the install to load the application and modify the settings. If you do this before the post-analysis, these modifications (in our case to Acrobat Reader 9) will become global defaults for all users who access the ThinApp. This is handy, as some application vendors do not support Microsoft GPOs and sometimes are very tight-lipped about the registry locations for various options that might not be desirable in your environment. For example, I like to load Acrobat Reader and accept the Adobe Acrobat EULA on behalf of my end users. I also like to enable the option "Do not download or install updates automatically" in Edit, Preferences, Updater. The general recommendation is that if an application has its own (annoying) auto-updater facility and that you disable it were possible for ThinApps. The update is likely to fail, and will definitely fail if you have made the "Sandbox" read-only. If you do need to update an existing ThinApp with a new version, patch or plug-in you can use the "sbmerge" utility to facilitate this process.

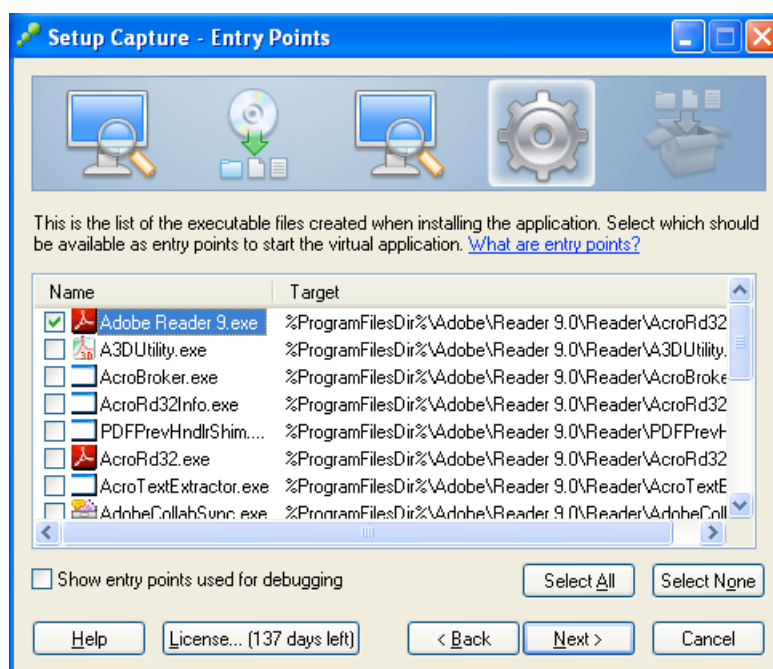
8. Once you have **finished with the installer, close the application** and **restore the ThinApp Setup Capture window. Click the Postscan button** and **this will trigger the Postscan phase**. Click **OK** in the Setup Capture dialog to indicate the install has completed



9. After the scan has completed, **ThinApp will list the “User-accessible entry points”**. These are EXEs that the user can trigger or have loaded once the main application has loaded.

The problem with most application recorders and packagers is that they quite frequently get confused. Frequently they cannot detect the difference between an installer .EXE and the application it is installing; in contrast ThinApp makes a good job of this. However, I noticed that this dialog box didn't include all the executables.

ThinApp detects these as Entry Points - the multiple executables that make up a single installer. It is possible to de-select these multiple executables to just select the .EXE you wish ThinApp to build.

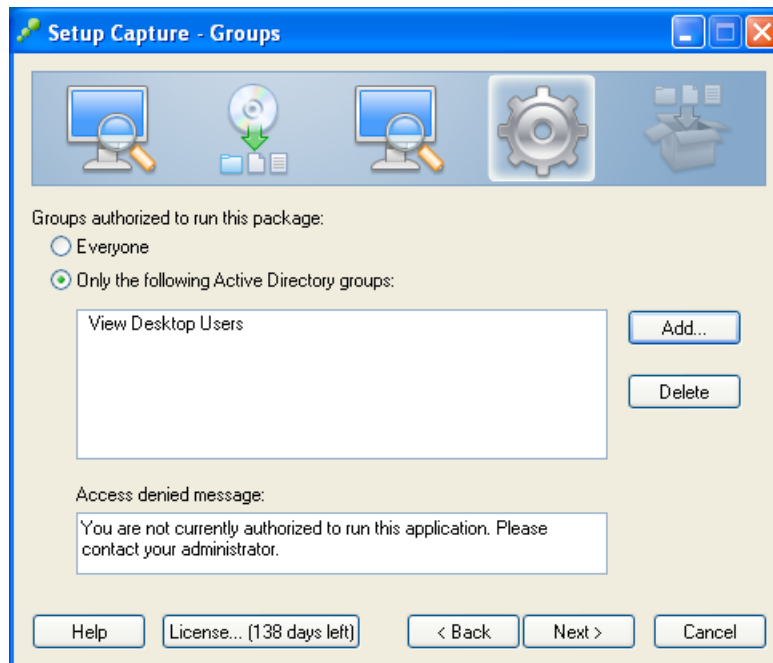


It's worth mentioning that my testing and validation won't be *anywhere near as rigorous as yours*, or will it? I think the general point I want to make about this dialog box is that every single application will produce different results, and I think you would have to know the application *very well* before considering deviating from these defaults. For example, the default selection didn't include AdobeARM.exe. Why not? I doubt anyone in VMware OR Adobe could answer that question. My best bet is to ask Adobe what AdobeARM.exe does, whether it's required for the main Reader to work, and what the implications would be if it wasn't included.

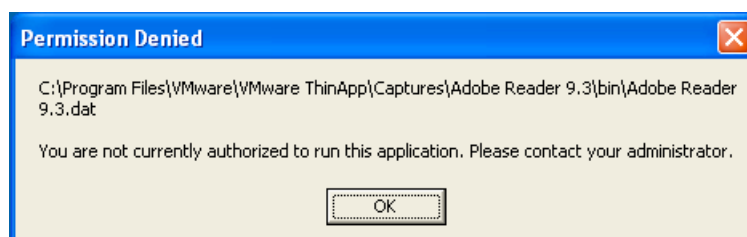
The best way to do describe an "entry point" as see it as "door" into an application, so for example when you install many files and ancillary applications are copied but the main "entry point" from the end-users perspective is winword.exe, excel.exe, powerpnt.exe and so on. In my discussion with VMware they recommended keeping the .dat file selected

during the build process, but then to publish the entry points the end user needs. The .dat often is merely the holder for the icon cache of the application. There can be cases where failure to included means that .exes a copied across but they lack their application icons.

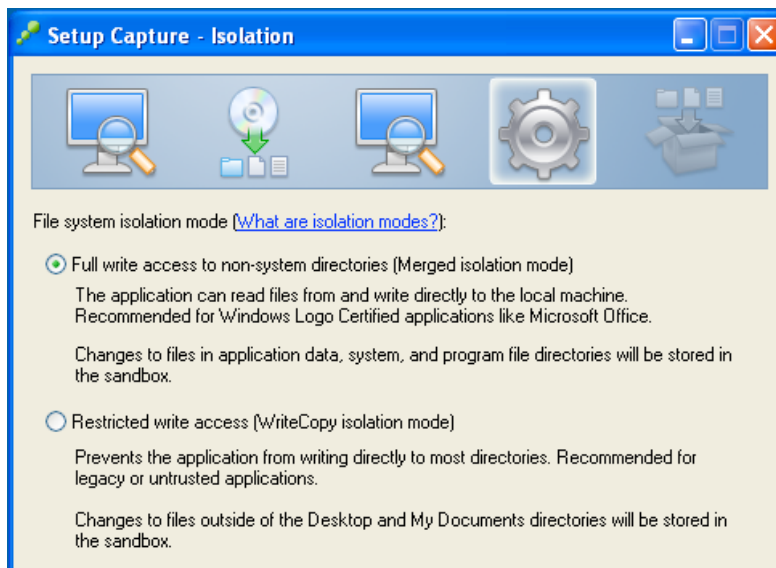
10. In the next window you can control how the ThinApp will be built



You can encode Active Directory controls that define the parties able to run the application. The idea is to restrict the portability of VMs, such that if a ThinApp leaks out of your organization, no-one will be able to run it without first authenticating to your private, internal and firewalled domain. ThinApps are very, very portable and without these sorts of controls, it is straightforward for a virtual desktop user to upload an entire application to the internet. Obviously they are still potentially able to do this, but the file cannot be executed from outside the organization. There are many virtual Internet drives which offer very cheap storage - a user could use these to upload applications out of the organization, and then download them for use at home. You have been warned. Notice how I have only included my core Virtual Desktop Users group, this means that even if I was full administrator of the domain, I would not be able to run the ThinApp unless I was a member of this group. If you do try run the application without the appropriate rights you receive this message:

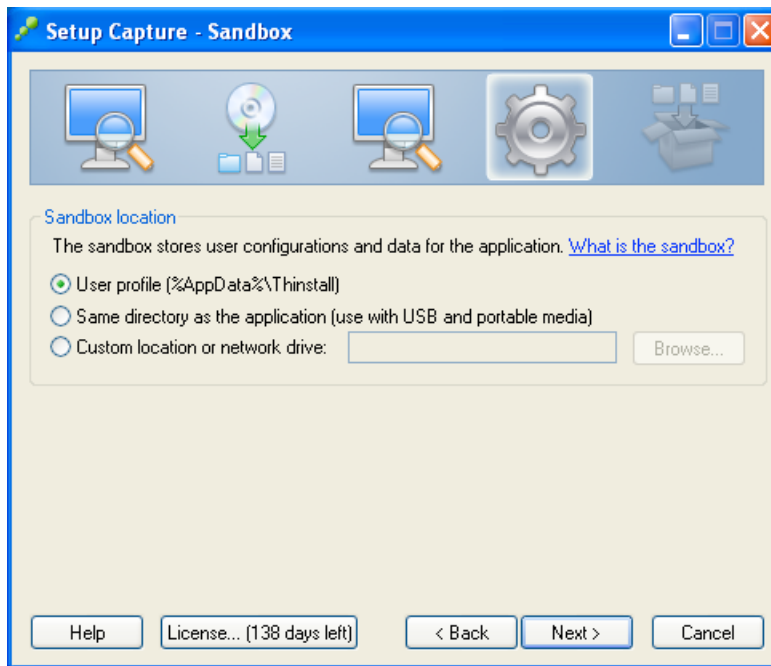


11. The next dialog box is a difficult one, as it is difficult to know 100% in all cases which option to select. There is something to be said for experimentation and rigorous testing



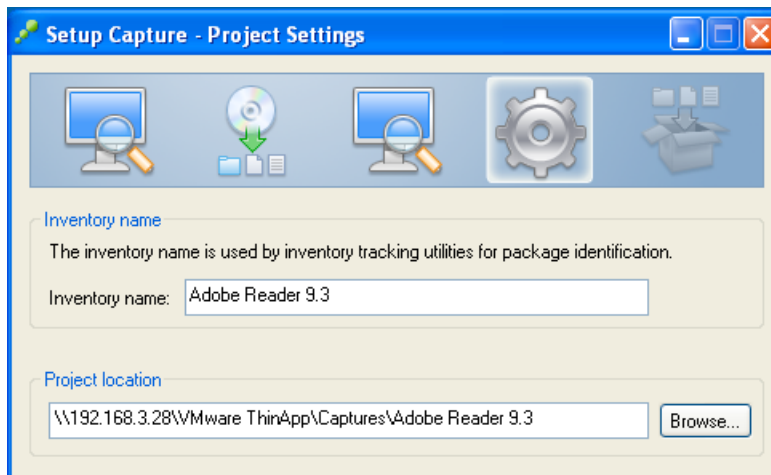
Merged isolation mode is very close to how applications normally behave when they are installed in a conventional desktop. However, in our virtual desktop, we can either disable or redirect many of the locations that are referred to here. The recommendation is to select this option for Microsoft Office and Windows Logo Certified applications. WriteCopy isolation mode is recommended for legacy or untrusted applications, and results in a more isolated or sandboxed ThinApp. This isolation appeals to me, and don't worry about users trying to locate local directories – I hide the A: C: and D: drives. However, I don't regard Acrobat Reader 9 as a legacy application, so I'm going to go with Merged isolation mode. After all, I don't want the isolation to be so complete that it stops the application from working altogether. The reality is that I think you will have to experiment and test the application beforehand. As there are often no recommendations from the application vendors themselves, another option is using the VMware ThinApp Forums for other people's experiences. Here, there are step-by-step accounts that describe how many commonplace apps have been successfully virtualized with ThinApp by other users.

12. The next option allows you to control where the user sandbox will be held

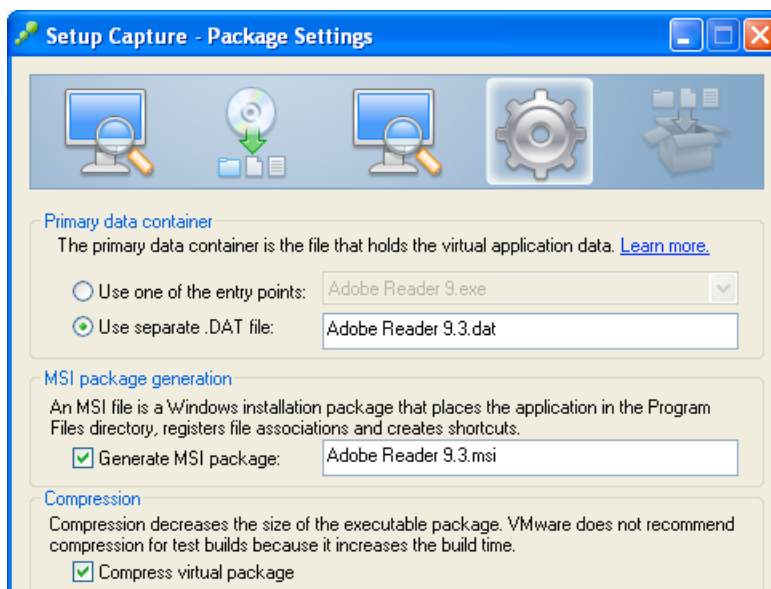


To maintain a per-user setting, ThinApp allows you to save per-user settings in three different locations – the User Profile, a USB device or a Network location. As we saw earlier, folder redirection can relocate the Application Data part of a user profile to a network location (such as the user’s home directory) so a network drive and user profile location could be effectively the same. The USB location is clearly not aimed at a virtual desktop environment but for a more stand-alone mode. This is popular with IT staff who can carry a memory stick of their favourite management applications. I’ve decided to stick with the User Profile option as I redirect this to the network anyway.

13. Next, select your **Inventory Name** and **Project Location**. The Inventory Name is the friendly name used by ThinApp when using VMware View or Microsoft GPOs to publish the ThinApp to the end user’s virtual desktop. The Project Location will be the destination of all the files discovered during the postscan stage, together with your ThinApp held in the \VMware ThinApp \Captures \<Your Inventory Name> \bin directory



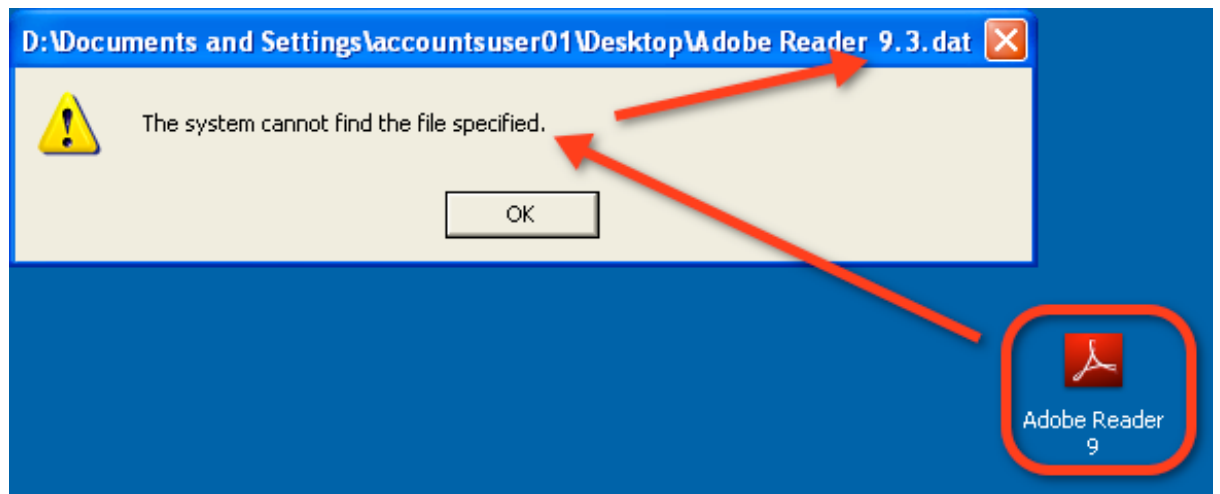
14. **Next, select your build options** – this allows you to set where the project files will be located (this is where you will find the ThinApp)



As you can see here, by default "Adobe Reader 9.3.dat" has been selected as the Primary data container. The Primary data container is the file that will contain the ThinApp "runtime". The ThinApp runtime loads within the virtual desktop, and in turn loads a virtual file system and virtual registry. As I stated earlier in this guide, the key advantage of ThinApp is that no special software (such as a ThinApp client) needs to be installed on the virtual desktop for the ThinApp to function – it is all contained within the Primary data container extracted and loaded by the ThinApp runtime engine.

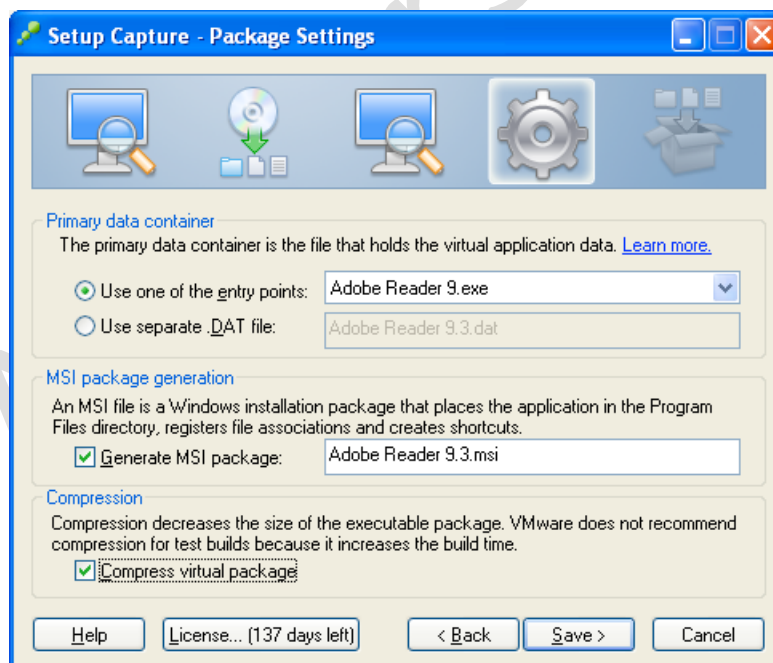
Selecting this option ("Use separate .DAT file") can have a significant impact on the ThinApp. For example, if I accept the default of Adobe Reader 9.3.dat, then I would need both the Adobe Reader 9.exe ThinApp AND the Adobe Reader 9.3.dat file to make the application run. If I

accepted the default data container and tried to run the Adobe Reader 9.3.exe ThinApp on its own, it would result in this error:

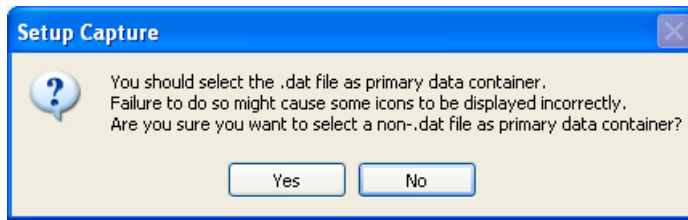


As you can see, the ThinApp on my desktop cannot load because it has no relationship with the data container (Adobe Reader 9.3.dat) and cannot find the file required to function. If the ThinApp Adobe Reader 9.3.exe was run from a network share, and in the same path the data container (Adobe Acrobat Reader 9.3.dat) was also present, then the ThinApp would load without a problem.

In my case, I selected "Use one of the entry points", and selected the only entry point available – Adobe Reader 9.exe



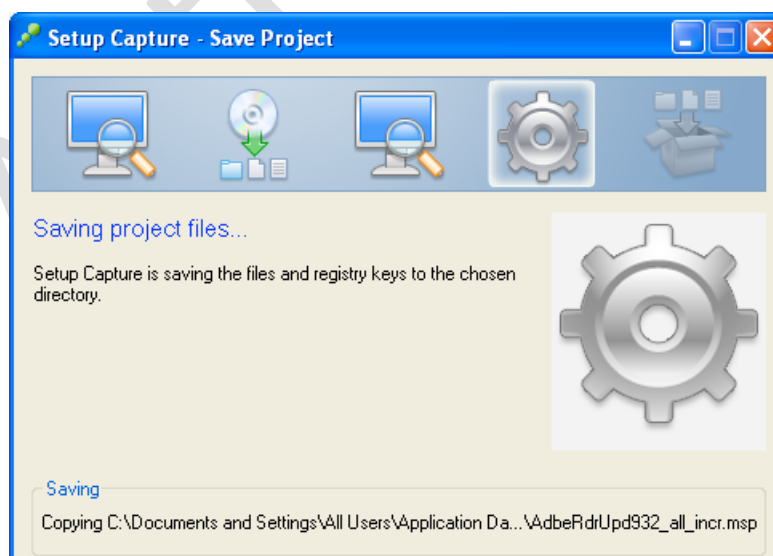
Deviating from the default .DAT container generates the warning shown below. So, as I said earlier, even that decision is not without consequences, as the dialog box below indicates:



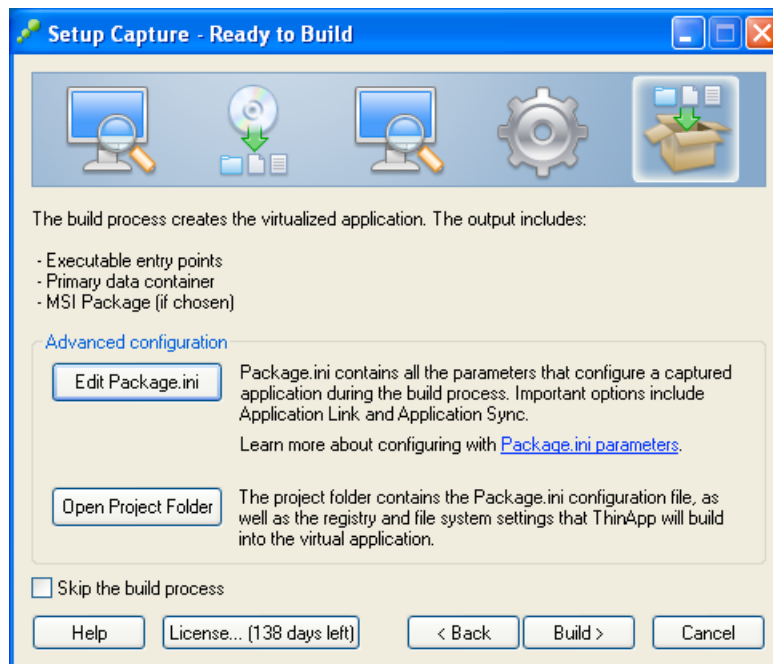
In my testing, I was able to select the Acrobat Reader 9.exe as my Primary Data Container and did not have problems with icons. As ever, you mileage may vary, depending on the application.

In addition to the Primary Data Container option – we have both MSI package generation and compression options too. The “Build MSI package” option will create an MSI file that you can then use to copy the ThinApp to the system – use this if you intend to have the ThinApp running from within the virtual desktop’s virtual disk. If you are just testing the application, use the option “Non Compression” which is generally much quicker. When you’re ready to build the application for Production use “Fast Compression”, as this reduces the time it takes to stream the application to the end user – but takes significantly longer to build. If you’re looking for a feel as to how long, large applications like Microsoft Office can take a couple of hours. Fast Compression does reduce the size of the package significantly (in some cases by as much as 50%) but the compression does come with an overhead for the actual load time of the ThinApp. In general, if the ThinApp were being hosted on a network share I would choose compression, but if the ThinApp was being “installed” in the virtual desktop and run locally or run from a removable drive, I would not.

15. At the end of the post-configuration stage of ThinApp, first save your **Project**



After this has completed, you will be offered additional configuration options just before the ThinApp is built.

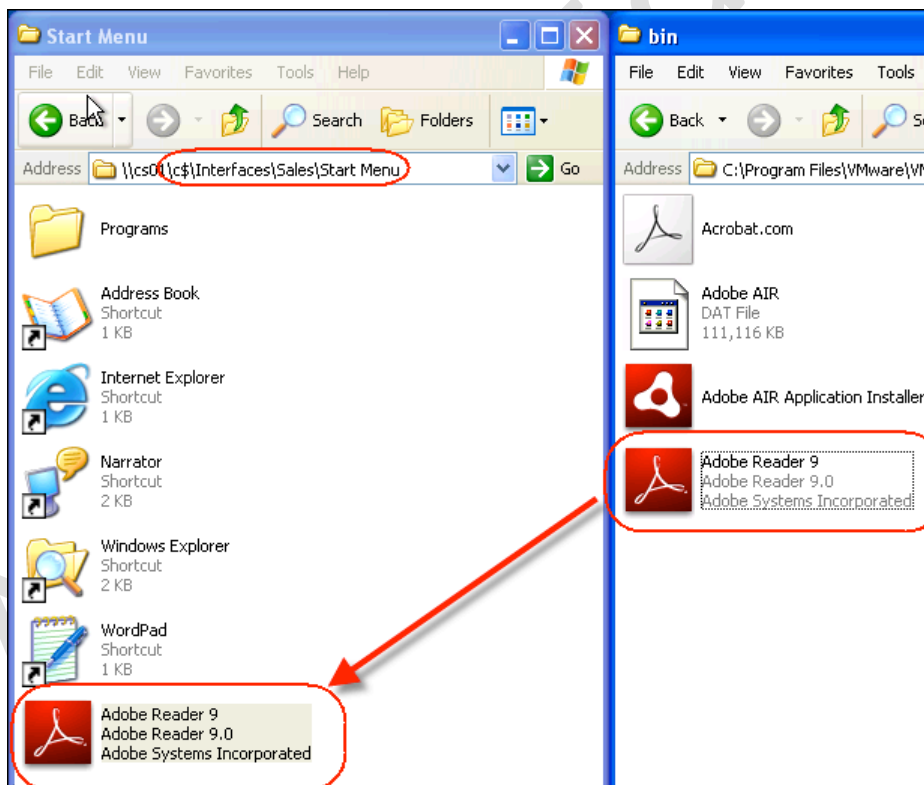


“Open Project Folder” button will allow you to modify various .INI and .INF files for advanced configuration. Once you are finished, you can return to the Build Now option. Buried inside the ThinApp is a batch file (build.cmd) which you can run to re-execute the build process located in the capture project directory. If you make changes to .INI files after the build, this allows you to re-build the ThinApp without going through the whole capture process again. For a complete list of all the package.ini settings, visit this location: <http://www.vmware.com/info?id=906>

16. Click the **Build** button
17. **At the end of the build process**, ThinApp should open a window showing the ThinApp and other ancillary executables. The core files for me are the Adobe Reader 9 ThinApp and the Adobe Reader 9.3.msi file. The MSI file was created for me by the option “Generate MSI package” selected earlier in the wizard



18. **As a quick test, you may copy the files to a location accessible to your user's virtual desktops.** I decided to copy them to my redirected Start Menu.



Notice how I only needed the ThinApp .EXE. I would recommend testing the application in the View Client with a test account.

IMPORTANT:

Once you have finished with your "capture" Parent VM, remember to revert the snapshot and then delete the snapshot to undo your changes

Publishing a ThinApp

There are many ways by which you can either publish or deploy a ThinApp. As you saw a moment ago, you could using a redirected desktop GPO system to advertise the ThinApp on the user's Start Menu. Alternatively, you can install the ThinApp using the MSI file created during the build of the ThinApp itself. This MSI installer could be triggered using GPO and Software Installation Policies. These methods are very much Microsoft-orientated and probably well understood by most people.

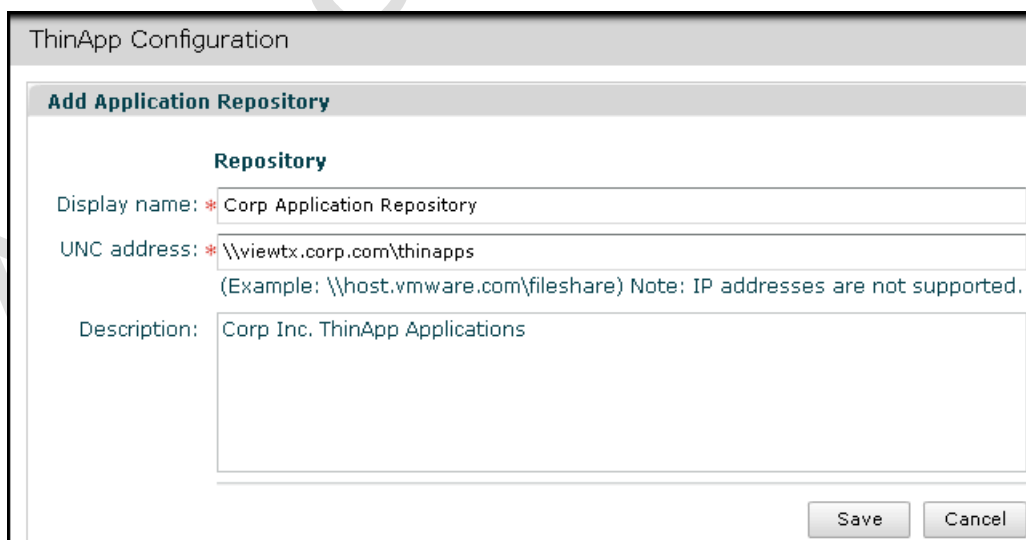
Beginning with View 4.5, it's also possible to publish ThinApps via the View Server Administration tool. As with Local Mode desktops, you can configure a file server that centrally holds your ThinApps, and then you select which desktop pools receive the ThinApps from the central library. First, configure the file server you wish to use, then copy all your desired ThinApps to the share on your file server. In my case, I decided to use my View Transfer Server as the file server to save on the number of VMs needed in my lab environment.

IMPORTANT:

When you share out the ThinApp directory, ensure that you add the Domain Computers group to the share, allocating Read permissions.

Configuring the ThinApp Repository

1. In View Administration select ► **View Configuration**
2. Select **ThinApp Configuration**
3. In the **Add Replication Repository** page, **type a friendly name** for the ThinApp Repository such as Corp Application Repository, followed by a **UNC path to the file server** which will store your ThinApps



The screenshot shows the 'ThinApp Configuration' dialog box with the 'Add Application Repository' tab selected. The 'Repository' section contains the following fields:

- Display name:** Corp Application Repository
- UNC address:** \\viewtx.corp.com\thinapps
(Example: \\host.vmware.com\fileshare) Note: IP addresses are not supported.
- Description:** Corp Inc. ThinApp Applications

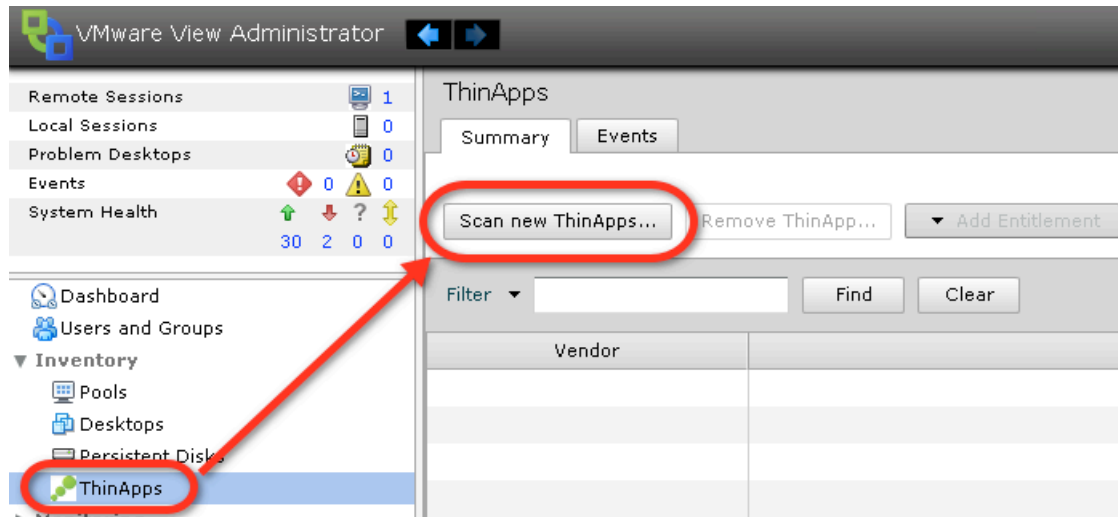
At the bottom right, there are 'Save' and 'Cancel' buttons.

4. Click the **Save** button

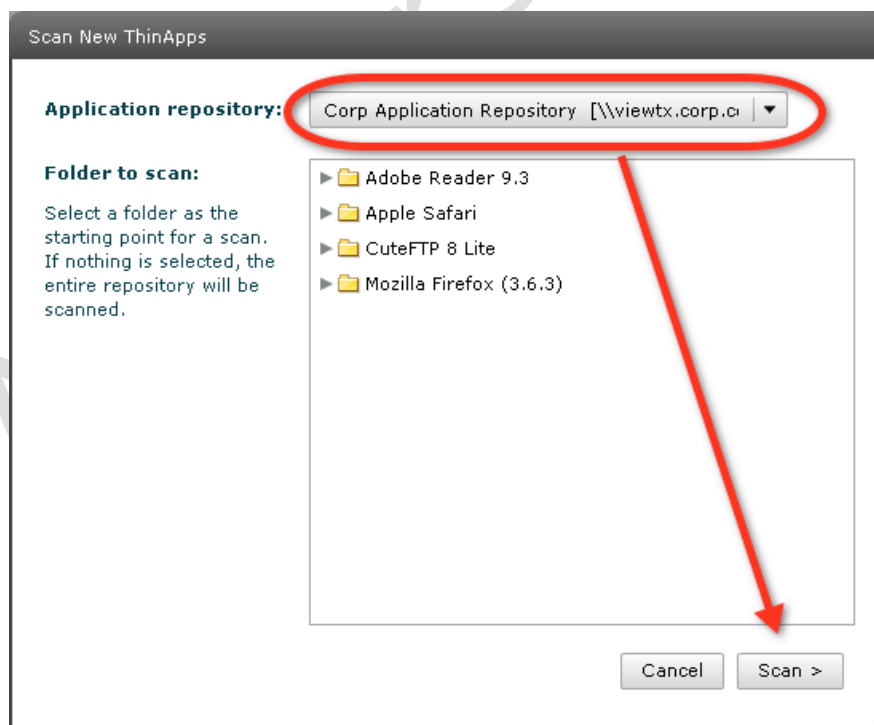
Adding ThinApps into View Server

The next stage is to set the View Connection servers to scan for the ThinApps held in the repository.

1. In View Administration select ► **Inventory**
2. Select the **ThinApps** node, and then click the **Scan new ThinApps...** button



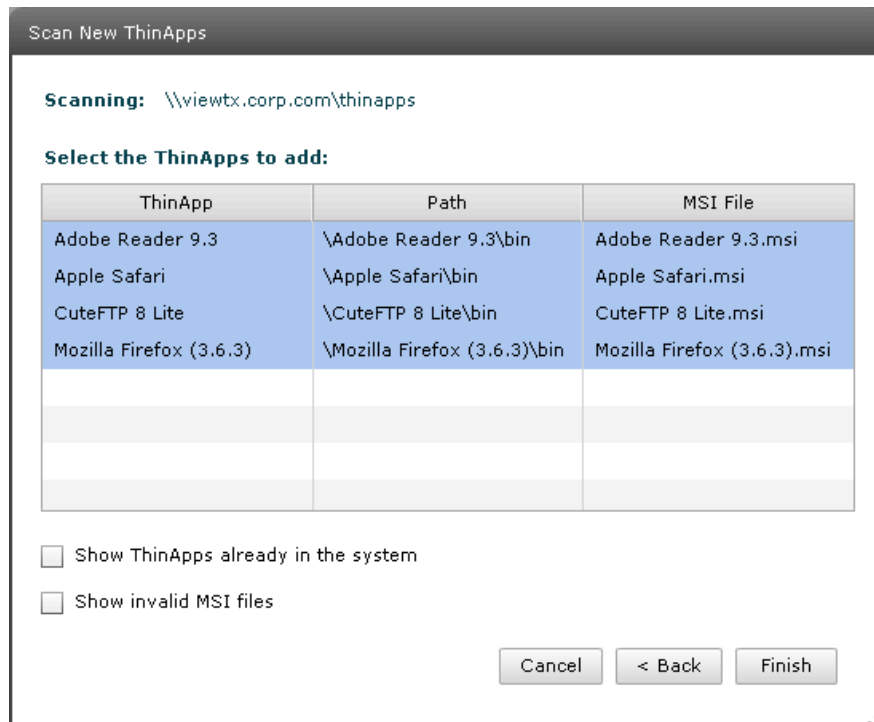
3. In the Scan New ThinApps... dialog box, from the **“Application repository”** dropdown list, select the share location configured a moment ago, and click the **Scan** button



Note:

As you can see, I didn't stop with Adobe Reader 9.3. For a bit of realism, I packaged up some other applications as well, and uploaded them to my repository. This will help later when I come to create what are called Application Groups.

4. In the next dialog box, **select the discovered ThinApp(s)** and click the **Finish** button to import them into the View environment



Note:

The "Show ThinApps already in the system" option displays ThinApps where this process has already completed. By default, this scan process ignores generic .MSI files that may have nothing to do with the ThinApps – it's possible to show these .MSI files by also selecting the "Show invalid MSI files" option

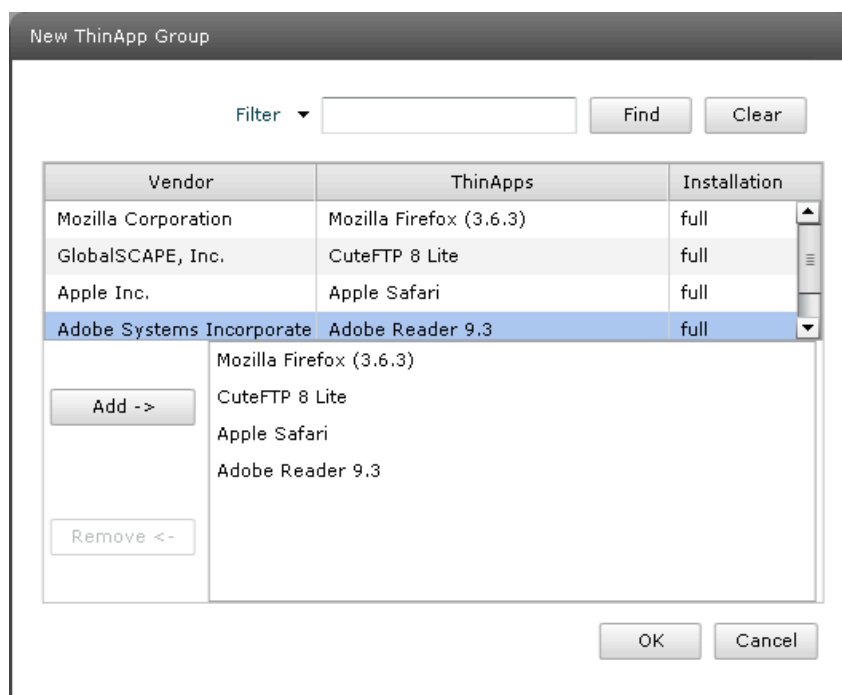
Entitling a ThinApp to a Desktop Pool via an Application Group

There are in fact many ways to entitle a ThinApp so users get the applications they need. If you have many ThinApps, it's possible to create groups of ThinApps and then assign them to pools of desktops. It's possible to assign a ThinApp to:

- **Desktop(s)** – this is useful if you have a dedicated pool, and one user's desktop needs a particular application which they would not normally receive via their membership of a group
- **Pools** – this is useful for building standard desktops replete with standard applications
- **An Application Group** (which contains multiple ThinApps) – this is the most efficient method of entitling many applications to a desktop or pool

Whichever method you use, you will have the option of running the ThinApp locally (which VMware refer to as a full install), or streaming it from the repository file share configured earlier. The full installation is only supported for the Dedicated pool type.

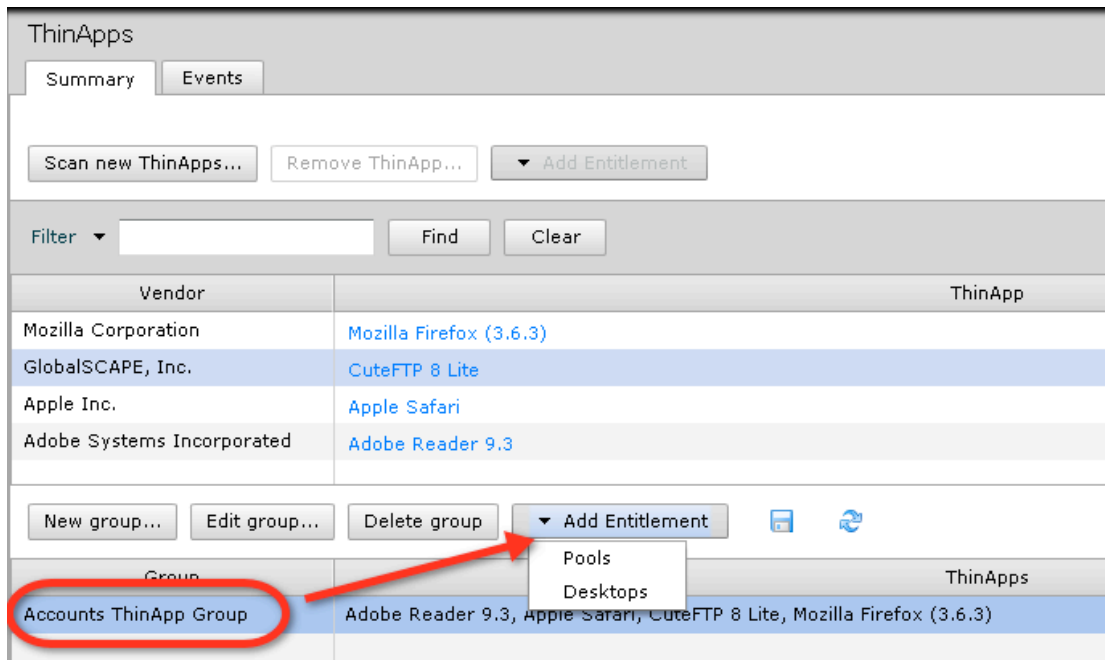
1. In the **ThinApps** node, below the Scan new ThinApps... button select the **New Group... button**
2. **Type in a new group name** such as "Accounts ThinApp Group" and then click the **Add** button
3. In the list **select a ThinApp** and click the **Add>> button**



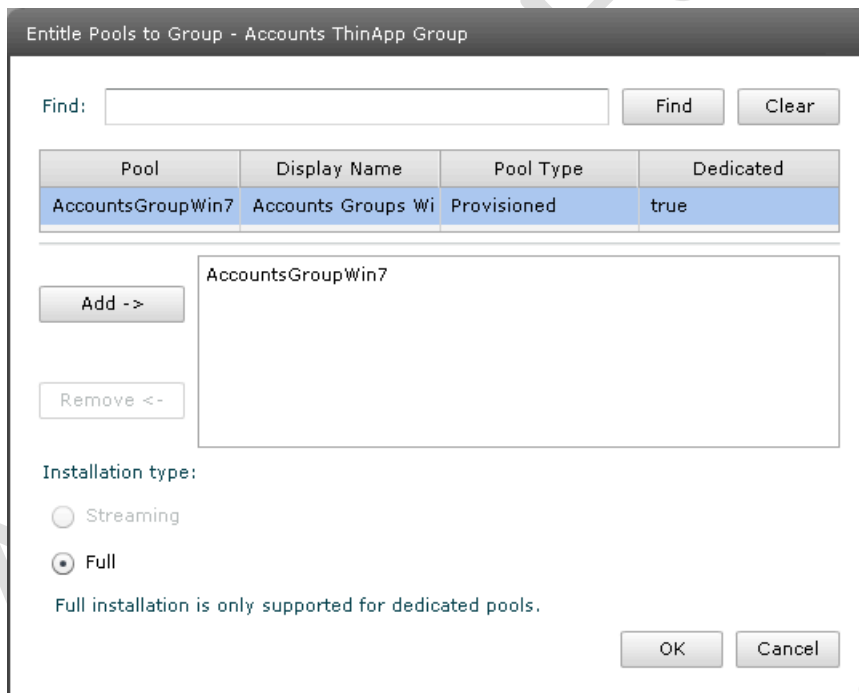
Note:

Sadly this dialog box does not support multiple selections in the shape of shift+click or ctrl+click

4. Now we have our ThinApp Application Group, we can entitle the group of applications to the pool. **Select the Application Group**, click the **Add Entitlements** button, and select **Pools** from the list



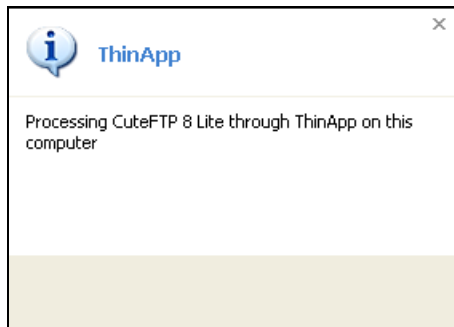
5. In the **Entitle Pools to Group** dialog box, click the **Find** button – and select the Pool you wish to **Add** to the group – and then **select the Installation type** based on your preferences and then click **OK**



Note:

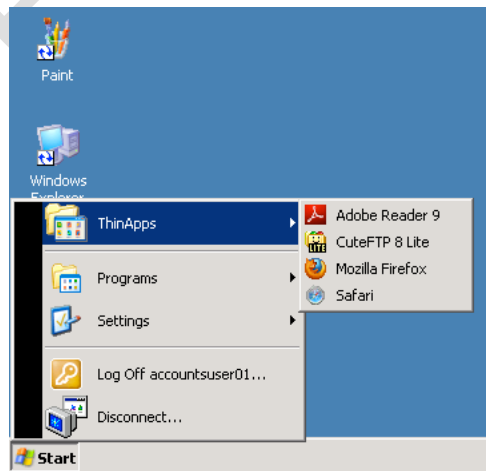
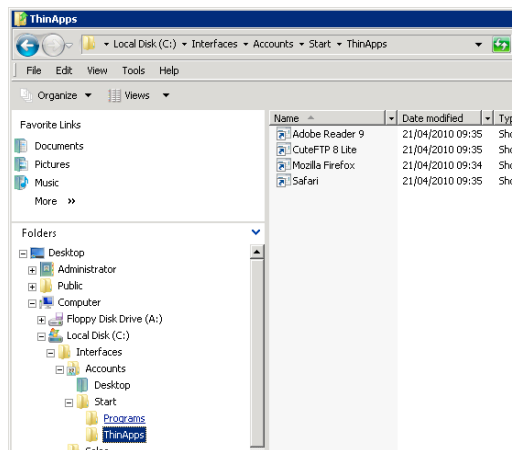
If you are using the Full format, end users see this popup message (shown in the screen grab below) near the tray location in Windows as each application is installed using the MSI created in the ThinApp build process. Shortcuts are created on the Start Menu with the same look and feel as if the standard installer had been run, and the ThinApp

applications are copied into the C:\Program Files location, each with the label "(VMware ThinApp)" in their directory name.



Warning:

By default, this ThinApp install process creates shortcuts on the user's desktop. However, if you impose rigorous folder redirection policies as discussed in Chapter 14: "Microsoft and VMware Policies", this will fail. Instead, you will have to create these shortcuts yourself. I found I could log in as a local administrator to test a virtual desktop, and then copy these shortcuts to a shared folder redirection location.



Rebuilding a ThinApp with Custom Package.ini Settings

There are many custom options available to ThinApp that can be leveraged by editing the package.ini file. Personally, I find it a bit odd that ThinApp's advanced options are held in an .ini file, which feels somewhat Windows 3.x to me! I'm hoping that in future versions, ThinApp will come with a management application that holds all your ThinApps in a library, from which these advanced settings can be found and applied with a graphical front end.

If you make edits to this file after the ThinApp has been built, you will need to rebuild the ThinApp using the build.cmd utility, and then re-upload and import the ThinApp into your ThinApp Repository. So it's perhaps worth reviewing these advanced options before embarking on a large full-scale project to ThinApp every application you can. This guide is not intended to be an exhaustive explanation and review of every package.ini setting. What I have tried to do below is document, explain and demonstrate the package.ini settings that I feel are the most important. Invariably they fall into four categories – settings that improve performance, stability or functionality and settings that stop you needing to capture the installation of the application every time you need to make a change. You should also know that there is an attributes.ini file that can be used for further settings. Sometimes VMware recommend changes to this file rather than the package.ini file for more granular control.

Package.ini Setting	Value	Setting
DirectoryIsolationMode RegistryIsolationMode	WriteCopy Merged	Controls the isolation mode used in the Setup Capture for the file system and registry. A more aggressive Full Isolation mode is available within attributes.ini
FileTypes	File extensions in .doc.docx format	Allows you to modify file extensions. If you want to run Word 2003 and Word 2007 you could modify the FileTypes to make Word 2003 open .doc files, and Word 2007 open .docx files.
AccessDeniedMsg PermittedGroups	String Group Name	Allows you to modify both the access

	separated by comma	denied message and the list of permitted groups from the Groups section of the Setup Capture wizard. Permitted Groups is normally remarked out of the file if you have not set any restrictions
UACRequestedPrivilegesLevel	asinvoker, requireAdministrator highestAvailable	Used to control how the Microsoft User Account Control (UAC) feature is managed, if enabled within Windows Vista or Windows 7. You can preset the option to stop UAC messages appearing
UACRequestedPrivilegesUIAccess	True/False	Stops privileged access to operating system if set to "false". UAC is not included in Setup Captures taken from Windows XP
RemoveSandboxOnExit	1 or 0	Controls whether the sandbox is deleted when the last part of the ThinApp closes. This value is remarked by default in package.ini file. Using 1 enables the removal of the sandbox. Set this option to make it impossible for the user to change settings within the ThinApp

Remember, if you change any of these options you will need to run the build.cmd file to recompile the ThinApp.

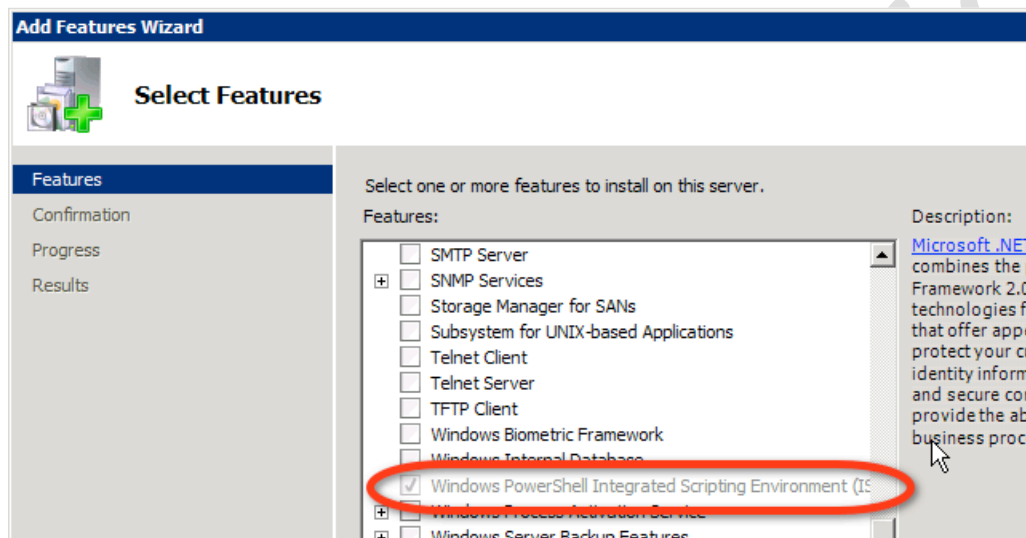
Other ThinApp Utilities

There are plenty of other important ancillary utilities bundled with ThinApp and these will be useful if you decide to become a long-term user of the product. These include:

Utility	Description
relink	A new .exe introduced in ThinApp 4.5 for legacy ThinApp. It allows the administrator to update older ThinApps to work with the new ThinApp runtime
thinlogcapture	Used to troubleshooting ThinApps
thinreg	Allows you control File (or mime) type association
applink	Allows you to link ThinApps links together. So for example you could make Internet Explorer load the Java Runtime Environment 1.3 under some circumstances, and the Java Runtime Environment 6.0 under others. This stops you from having to create an ThinApp for each and every blend of Java runtime.
AppsSync	Used to update a ThinApp that can be done manually or via the sbmerge utility. AppsSync check a location on the network for an update or a new version of the ThinApp.

Chapter 23: Managing VMware View with View PowerCLI

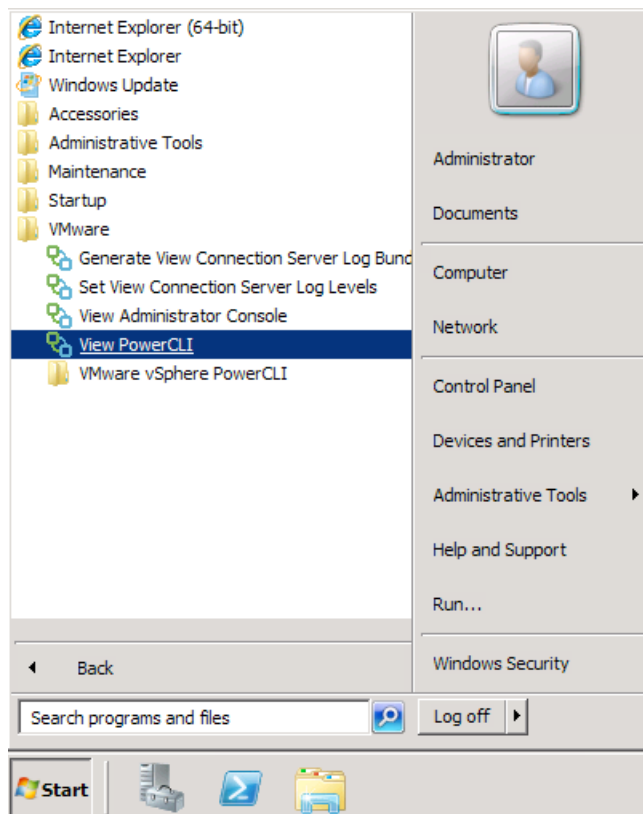
New to VMware View is PowerShell and PowerCLI support. VMware's adoption of Microsoft's PowerShell has ripped through the VMware Community since its introduction in Vi3. It's really great that VMware have chosen to adopt and embrace this technology, and PowerShell/CLI usage continues to grow – its become the defacto standard for any CLI based activity as new cmdlets are added to the pool on a yearly basis. Remember if you want to use this you will need to first install (Windows 7) or enable (Windows 2008 R2) Microsoft PowerShell on your management system:



Then install the vSphere PowerCLI 4.1 extensions. At the time of writing the cmdlets for View are in the form of a snap-in that has been loaded into the PowerCLI environment. These are currently held in:

```
C:\Program Files\VMware\VMware View\Server\extras\PowerShell
```

The snap-ins are installed by merely running the .PS1 file called add-snapin.ps1. The running of the PS1 file adds shortcuts to your start menu so when a View PowerCLI session is started the appropriate snap-ins are loaded into the environment.



What follows here is some examples of the View PowerCLI cmdlets. I'm indebted to VMware's "VMware View Integration Guide" which covers the PowerCLI. You might be interested to know the guide also covers customizing LDAP data in View, and its new integration with Microsoft SCOM.

Managing vCenter to View Connections

If you have an environment that is already configured, you can use various cmdlets to manage the relationship between vCenter and View.

List vCenters

The cmdlets "Get-ViewVC" can be used to retrieve information about the current vCenter connection with:

Get-ViewVC -serverName vc4nyc.corp.com

```
PS C:\> Get-ViewVC -serverName vc4nyc.corp.com

vc                : 0
vc_id             : 41d25ffb-4dc4-46fc-9715-b8fdf4f4108f
description       : Connection to the New York vCenter
serverName        : vc4nyc.corp.com
serverUrl         : https://vc4nyc.corp.com:443/sdk
port              : 443
username          : corp\administrator
composerUcConfigId : b65f40ce-89ef-4d6f-8577-6b6593af71d6
composerUrl       : https://vc4nyc.corp.com:18443
adConfig          : [corp\administrator]corp.com;
composerPort      : 18443
composerUsername  : corp\administrator
createRampFactor  : 8
deleteRampFactor  : 5
```

The "createRampFactor" and "deleteRampFactor" values represent the current settings for the "Max concurrent provisioning operations" and the "Max concurrent power operations" respectively.

If you have multiple vCenter servers listed in View, you can use the * asterisks as wildcard to list all vCenters configured for View.

Get-ViewVC -serverName *.corp.com

Remove vCenter

It is possible to remove a vCenter listing from the View server with the cmdlets:

Get-ViewVC -serverName vc4nyc.corp.com | Remove-ViewVC

However, the cmdlets will return an error and fail to complete if there is any desktop pool that utilizes the vCenter connection you are trying to remove. Additionally, any Transfer Server would also have to be placed in maintenance mode and removed. If you remember transfer servers are virtual machines, and are automatically discovered by the vCenter and View servers relationship.

```
PS C:\> Get-ViewVC -serverName vc4nyc.corp.com | Remove-ViewVC
Remove-ViewVC : PowershellService:RemoveViewUC FAILED, error=Unable to remove Virtual Center entry <41d25ffb-4dc4-46fc-9715
88faf4f4108f>: UC <0> is still used by <1> pools
At line:1 char:55
+ Get-ViewVC -serverName vc4nyc.corp.com | Remove-ViewVC <<<<
+ CategoryInfo          : InvalidResult: (vmware.view.pow...ts.RemoveViewUC:RemoveViewUC) [Remove-ViewUC], Exception
+ FullyQualifiedErrorId : PowershellService:RemoveViewUC FAILED,vmware.view.powershell.cmdlets.RemoveViewUC
```

So to remove a vCenter reference you may have to remove pools it offers as well and its references to Transfer Servers

Add a vCenter to View

In a large environment you may have a number of vCenter servers to add into View. This can be achieved more efficiently using the Add-ViewVC cmdlets like so:

```
Add-ViewVC -serverName vc4nyc.corp.com -username corp\administrator  
-password vmware -description "Connection to New York vCenter" -  
createRampFactor 5 -deleteRampFactor 5 -useComposer $true
```

This would add in the vc4nyc.corp.com vCenter and using the option `-useComposer` also enable the View Composer Linked Clones component, using the same credentials as the vCenter.

Creating Desktop Pools

Using the Add-AutomaticPool and Add-AutomaticLinkedClonePool cmdlets you can create virtual desktop pools and linked cloned virtual desktop pools respectively. As you might imagine with all the settings in View the number of possible sub parameters is quite dizzying. This can be problem when it comes documentation like this guide – because the strings become very long and difficult to read. So what you will see is me put a long command as series of lines. To create a desktop pool you need to provide at least 6 parameters:

- `-pool_id` Internal name of the pool
- `-displayName` As it is shown to end user
- `-vmFolderPath` Path to the folder to hold desktop
- `-resourcePoolPath` Path to the Resource pool
- `-templatePath` Path to the Template
- `-customizationSpecName` Guest Customization used

One easy way to learn the parameters is by querying an existing pool with:

```
get-pool -pool_id "SalesGroupWin7"
```

This will give you an output like so:

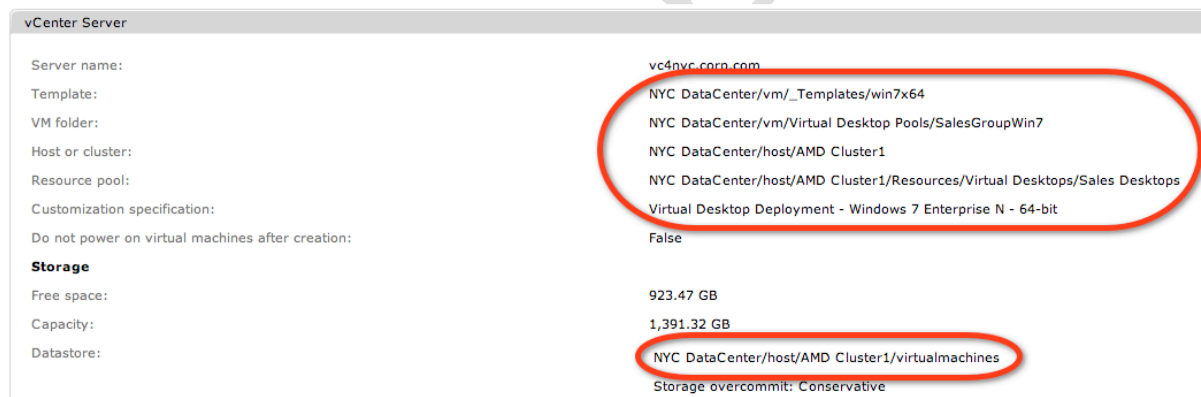
```
pool : 1  
pool_id : SalesGroupWin7  
description :  
displayName : Sales Group Windows 7 Desktop  
enabled : true  
folderId : /  
deliveryModel : Provisioned  
multiSessionAllowed : false  
userResetAllowed : false  
assignOnFirstLogon : true  
desktopSource : VC  
powerPolicy : RemainOn  
vc_id : efad478d-d82f-434f-9bf3-65defceb263b  
vcServerName : vc4nyc.corp.com  
provisionEnabled : true
```

```

provisionSuspendOnError : true
postProvisionState      : READY
startClone               : true
calculatedValues        : false
deletePolicy             : Default
headroomCount            : 25
maximumCount             : 50
minimumCount             : 10
datastorePaths         : /NYC DataCenter/host/AMD Cluster1/virtualmachines
datastoreDisplayPaths    : /NYC DataCenter/host/AMD Cluster1/virtualmachines
customizationSpec     : Virtual Desktop Deployment - Windows 7 Enterprise N - 64-bit
resourcePoolPath      : /NYC DataCenter/host/AMD Cluster1/Resources/Virtual Desktops/Sales Desktops
resourcePoolDisplayPath  : /NYC DataCenter/host/AMD Cluster1/Resources/Virtual Desktops/Sales Desktops
templatePath          : /NYC DataCenter/vm/_Templates/win7x64
templateDisplayPath      : /NYC DataCenter/vm/_Templates/win7x64
vmFolderPath         : /NYC DataCenter/vm/Virtual Desktop Pools/SalesGroupWin7
vmFolderDisplayPath      : /NYC DataCenter/vm/Virtual Desktop Pools/SalesGroupWin7
namePrefix               : salesdesktop
persistence              : Persistent
autoLogoffTime           : Never
poolType                 : Persistent
markedForDelete          : 0
protocol                  : PCOIP
allowProtocolOverride     : true
flashQualityLevel        : NO_CONTROL
flashThrottlingLevel     : DISABLED

```

You can also see these paths to learn the conventions on existing desktop pool under the Settings tab:



Whilst the get-pool cmdlets is helpful for learning more about the parameters. You can get tripped up with these if you are not careful. For example Get-Pool -protocol RDP will list all the pools configured with Microsoft RDP as a default. Now you would thinking it would be -protocol PCOIP to change it. WRONG! Actually, the flag is -defaultProtocol PCOIP. Elsewhere in the list of attributes there is the option to set allowProtocolOverride \$false. This works perfectly fine. So the attribute names on list – well sometimes they work and sometimes they don't. Nice!

Creating Pools

One of my first examples of pools – was a manual pool – where an existing single VM is given to specific user or even a group of users. This used to be a

referred to as personal desktop in previous releases but was deprecated as a feature and a concept in View 4.5.

Creating Manual Pools (Personal Desktop)

It possible to create manual "pools" from existing virtual desktops that you have created. Earlier in this book I should how you could still affectively create a "personal desktop" by using this option. To do the same with the ViewCLI, you use the Add-ManualPool cmdlets, together with Get-DesktopVM to find the existing VM with vCenter.

```
Get-ViewVC -serverName vc4nyc.corp.com | Get-DesktopVM -name mikel | Add-ManualPool -pool_id mgl_win7desktop -displayName "Mike's Windows 7 Desktop" -isUserResetAllowed $true
```

The `-isUserResetAllowed $true` value controls whether the user can reboot their virtual desktop using the View Client toolbar, as such its an optional component.

Creating a Dedicated Pools

To create a dedicated pool you use the Add-AutomaticPool cmdlets like so:

```
PS C:\> Get-ViewVC -serverName vc4nyc.corp.com | Add-AutomaticPool -pool_id SalesGroupWin7 -displayName "Sales Windows 7 Desktop" -namePrefix "salesdesktop" -vmFolderPath "NYC DataCenter/vm/Virtual Desktop Pools" -resourcePoolPath "NYC DataCenter/host/AMD Cluster1/Resources/Virtual Desktops/Sales Desktops" -templatePath "NYC DataCenter/vm/_Templates/win7x64" -dataStorePaths "NYC DataCenter/host/AMD Cluster1/virtualmachines" -customizationSpecName "Virtual Desktop Deployment - Windows 7 Enterprise N - 64-bit" -maximumCount 10 -headroomCount 5 -minimumCount 2
```

```
Get-ViewVC -serverName vc4nyc.corp.com | Add-AutomaticPool -pool_id SalesGroupWin7 -displayName "Sales Windows 7 Desktop" -namePrefix "salesdesktop" -vmFolderPath "NYC DataCenter/vm/Virtual Desktop Pools" -resourcePoolPath "NYC DataCenter/host/AMD Cluster1/Resources/Virtual Desktops/Sales Desktops" -templatePath "NYC DataCenter/vm/_Templates/win7x64" -dataStorePaths "NYC DataCenter/host/AMD Cluster1/virtualmachines" -customizationSpecName "Virtual Desktop Deployment - Windows 7 Enterprise N - 64-bit" -maximumCount 10 -headroomCount 5 -minimumCount 2
```

Hopefully, most of the above make sense. I've asked for pool with an internal ID of SalesGroupWin7 and friendly name of Sales Windows 7 Desktop, and when they are sysprep'd they will be given a NetBIOS name of salesdesktop1,2,3 and so on. The rest of the syntax (`-vmFolderPath`, `-resourcePoolPath`, `-templatePath`, `-dataStorePaths` and `-customizationSpecName`) are just path statements to the relevant objects and location in vCenter need for a virtual desktop pool to be created. The last three parameters control the sizing of the desktop pool with a maximum of least 10 virtual desktops and no more. The default is this would be

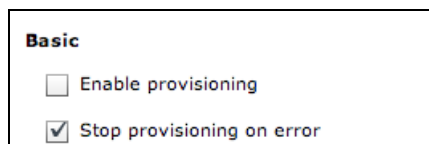
a dedicated pool and provisioning would begin as soon as entering the command.

Important:

Hopefully, you can see there's a limitation here. The cmdlets for View currently don't allow me to use the whole PowerCLI cmdlets. So I could not replace the line `-resourcePoolPath "NYC DataCenter/host/AMD Cluster1/Resources/Virtual Desktops/Sales Desktops"` with `get-resourcepool "Sales Desktops"`

TIP:

If you experimenting with the ViewCLI and creating pools, you may not every attempt you try kick off a full blown provisioning process especially if the systems storage backend is limited in capacity or IOPS. You can switch of automatic provisioning by using the `-isProvisioningEnabled $false` parameter. This is the same removing the checkbox when you run through the GUI Wizard.



The screenshot shows a 'Basic' configuration window with two checkboxes. The first checkbox, 'Enable provisioning', is unchecked. The second checkbox, 'Stop provisioning on error', is checked.

Creating a Floating Desktop Pools (with Automatic Deletes)

If I wanted a "floating" pool that deleted the virtual desktop when the use logout – I would add the `-persistence` and `-delete` policy flags to a similar command like so:

```
Get-ViewVC -serverName vc4nyc.corp.com | Add-AutomaticPool -pool_id Student -displayName "Student Desktop" -namePrefix "student"
```

```
-vmFolderPath "NYC DataCenter/vm/Virtual Desktop Pools"
```

```
-resourcePoolPath "NYC DataCenter/host/AMD Cluster1/Resources/Virtual Desktops/Student Desktops"
```

```
-templatePath "NYC DataCenter/vm/_Templates/win7x64"
```

```
-dataStorePaths "NYC DataCenter/host/AMD Cluster1/virtualmachines"
```

```
-customizationSpecName "Virtual Desktop Deployment - Windows 7 Enterprise N - 64-bit"
```

```
-maximumCount 10 -headroomCount 5 -minimumCount 2
```

```
- persistence NonPersistent – deletePolicy DeleteOnUse
```

Creating Linked Cloned Pools

I've got something here. But it errors.

```
Get-ViewVC -serverName vc4nyc.corp.com | Add-AutomaticPool -pool_id
AcctsGroupWin7 -displayName "Accounts Windows 7 Desktop" -namePrefix
"acctsdesktop" -vmFolderPath "NYC DataCenter/vm/Virtual Desktop Pools" -
resourcePoolPath "NYC DataCenter/host/AMD Cluster1/Resources/Virtual
Desktops/Accounts Desktops" -parentVMPath "NYC DataCenter/vm/Parent
VMs/winxpSP3-parentVM" -parentSnapshotPath
/AutoPoolSnapshots/parent1_snapshot -datastoreSpecs
[Aggressive,os,data]/NYC DataCenter/host/AMD Cluster1/virtualmachines -
dataDiskLetter "D" -dataDiskSize 100
```

the parentVMpath errors and says it doesn't exist as a parameter... BUT it does appear in the get-pool output! It's clear something else, and the guide sample have listed too. Guide is wrong?

parentSnapshotPath is actually -parentVMSnapshotPath in the get-pool cmdlets. Can't verify if the PDF is wrong because I can't get past the first error!

Updating Pool Settings

All the off "add-" style cmdlets which are used to add pools of various types each come with the own "Update-" style cmdlets which are used to modify pool or pools after they have been defined such as the Update-AutomaticPool, Update-AutomaticLinkedCLonePool and Update-ManualPool. Let say you want to change default away from PCoIP Protocol, and to set Microsoft RDP as the standard – and at the same time disable the users ability choose the protocol on a Automatic Pool. The command would like this:

```
Update-AutomaticPool -pool_id SalesGroupWin7 -displayName "Sales
Windows 7 Desktop" -dataStorePaths "NYC DataCenter/host/AMD
Cluster1/virtualmachines" -allowProtocolOverride $false -defaultProtocol
RDP
```

Deleting Pools

It also possible to delete pools using the ViewCLI. It's relatively simple process the main question is whether you merely want unlist the pool from View, or whether you actually want to logoff existing users, and delete the pool and all the VMs as well.

```
Remove-Pool -pool_id SalesGroupWin7 -DeleteFromDisk $true -
TerminateSession $true
```

Managing User Assignments

Add & Remove User and Group Assignments

Now we have a good handle on creating virtual desktops of the various types, its time consider allocating the user assignments that would actually the desktop to be accessible. In terms of discovering more about your users and groups in AD

the ViewCLI is pretty limited. For example it only query AD for users, and their group membership – it doesn't allow for querying groups, to check membership list. I guess this isn't the end of the world, if you want really powerful AD cmdlets that's what the Microsoft PowerShell is for. Nonetheless, if you did want to know more about a specific user via the ViewCLI you could use the following:

Get-User -name mikel -domain corp -includeGroup \$true

```
user           : 0
displayName    : corp.com\mikel
distinguishedName : CN=mikel,CN=Users,DC=corp,DC=com
Firstname     : mikel
Surname      :
sid           : S-1-5-21-348834269-3077800960-1586127433-1200
cn            : mikel
```

To add the MikeL user to his personal desktop you can use:

Get-User -name mikel -domain corp | Add-PoolEntitlement -pool_id mgl_win7desktop

Note:

At the time of writing – corp\mikel, corp/mikel, mikel@corp.com currently all create an error. The official documentation that I'm working from indicates corp\mikel should work but it doesn't. However as you can see from above – name <username> -domain <domainname> does work.

To assign a group of users to pool, it's the same syntax:

Get-User -name "Sales Group" -domain corp | Add-PoolEntitlement -pool_id SalesGroupWin7

If you wish to remove all the entitlements to a specific pool you would use:

Get-PoolEntitlement -pool_id SalesGroupWin7 | Remove-PoolEntitlement

Viewing User & Group Assignments

The Get-PoolEntitlement can be used to print a report of the current entitlements on a pool.

Get-PoolEntitlement -pool_id SalesGroupWin7

Of course if you wanted a complete report of all the pools and their current assignments you could simply use:

Get-PoolEntitlement -pool_id *

```

PS C:\> Get-PoolEntitlement -pool_id *

entitlement      : 0
displayName      : corp.com\Carmel Edwards
distinguishedName : CN=Carmel Edwards,CN=Users,DC=corp,DC=com
Firstname       : Carmel Edwards
Surname         :
sid             : S-1-5-21-348834269-3077800960-1586127433-1188
cn             : Carmel Edwards
pool_id         : ckme_win7desktop

entitlement      : 1
displayName      : corp.com\mikel
distinguishedName : CN=mikel,CN=Users,DC=corp,DC=com
Firstname       : mikel
Surname         :
sid             : S-1-5-21-348834269-3077800960-1586127433-1200
cn             : mikel
pool_id         : mgl_win7desktop

entitlement      : 2
displayName      : corp.com\Sales Group
distinguishedName : CN=Sales Group,OU=Sales,OU=View Users,DC=corp,DC=com
Firstname       :
Surname         :
sid             : S-1-5-21-348834269-3077800960-1586127433-1119
cn             : Sales Group
pool_id         : SalesGroupWin7

entitlement      : 3
displayName      : corp.com\Students
distinguishedName : CN=Students,OU=Students,OU=View Users,DC=corp,DC=com
Firstname       :
Surname         :
sid             : S-1-5-21-348834269-3077800960-1586127433-1216
cn             : Students
pool_id         : Student

```

Managing User Sessions

You can get list of currently connected users by using the

Get-RemoteSession -username *

```

session      : 0
Username     : corp.com\mikel
pool_id     : mgl_win7desktop
startTime    : Wed Aug 29 12:18:25 BST 42604
session_id   : CORP\mikel(cn=s-1-5-21-348834269-3077800960-1586127433-1200,cn=foreignsecurityprincipals,dc=vdi,dc=vmware,dc=int)/10cn=8ae34ed3-5cba-4ce1-bccf-c98cd46f2222,ou=servers,dc=vdi,dc=vmware,dc=int.cn=mgl_win7desktop,ou=server_group,dc=vdi,dc=vmware,dc=int:PCOIP:0
DNSName     : MIKEL.corp.com
duration     : Clock Skewed
state        : CONNECTED
protocol     : PCOIP

```

Notice how the info shows a "clock skewed". The time on the virtual desktop was 12:18, but it was actually 13:19 when I took the screen grab.

This is the End of the Book -

Conclusions

Personally, I still think View has some way to go before it evolves into the killer application VMware wishes it to be. Its weakness lies in the multiple dependencies required to make operations like Automated Pools work. I guess you could say that systems that need Setting A to function, before Setting B works, which allows Task C to function, are nothing new. In part, our responsibility is to put those dependencies together reliably, and fix them when they break under the weight of unexpected changes. But the sheer scale of those dependencies makes supporting a VDI environment a significant challenge. I'm firmly of the opinion that the more dependencies you have, the greater the probability of those dependencies failing, and the harder it becomes to identify them and resolve them. When I make this statement, I have in mind the hostd service that runs as part of the ESX host. It's the core management service that works with the VPX agent to allow vCenter to function. It's not totally unheard of to see this service fail, and for the ESX host to be marked as "Not Responding" and then later "Not Connected". If this occurs midway through the creation of a new pool, or as a new virtual machine is created, it can often upset the delicate relationships between ESX, vCenter and View. Similarly, if the vCenter service stalls and become unavailable, then the relationship between user, View and vCenter also begins to crumble. You could make the same claim about any of the advanced management products VMware currently sells such as Site Recovery Manager or Lab Manager. With that said, VMware do have an enviable reputation in the industry for products that work reliably and well, and it's my sincere wish that rapid product development doesn't undermine this hard-won reputation.

Virtualization is a rapidly-evolving and mutating subject, and while VMware may well have started out with the focus on server consolidation with ESX, you might remember their first commercial product back in 1998 was a desktop application called VMware Workstation. So VMware have been there on the desktop from the very beginning. It is, however, fair to say that the innovation of VDI was one that came originally from VMware's customer base and some would say that the company was a bit slow to react to this – leaving their offering to be an "initiative" at first, and then acquiring what became VDM to be later renamed as View. However, despite these somewhat sketchy beginnings, the View product is certainly rapidly maturing, and with the inclusion of application virtualization and printing solutions, we're coming closer and closer to the Holy Grail for many of us – a single solution from a single vendor to really rival the client computing deliverer of them all, namely the mighty Citrix.

Authors Edition