

vmware® PRESS



# VMware® Horizon Suite

Building End User Services

Paul O'Doherty  
Stephane Asselin



# **VMware Horizon Suite**

Building End-User Services

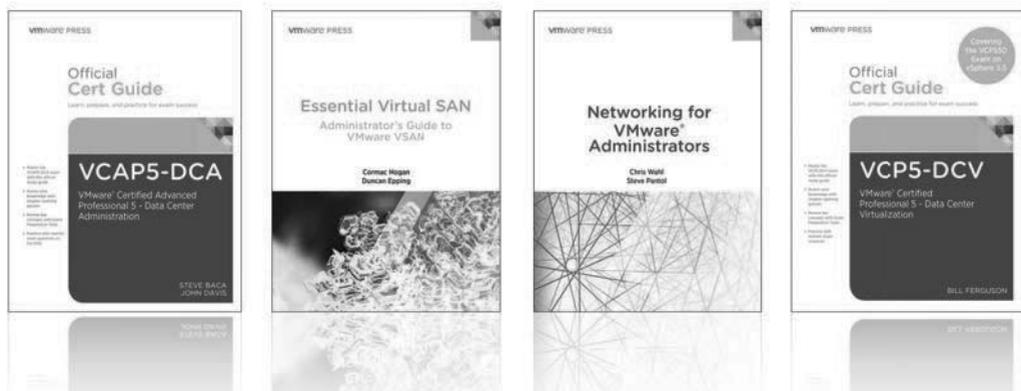
VMware Press is the official publisher of VMware books and training materials, which provide guidance on the critical topics facing today's technology professionals and students. Enterprises, as well as small- and medium-sized organizations, adopt virtualization as a more agile way of scaling IT to meet business needs. VMware Press provides proven, technically accurate information that will help them meet their goals for customizing, building, and maintaining their virtual environment.

With books, certification and study guides, video training, and learning tools produced by world-class architects and IT experts, VMware Press helps IT professionals master a diverse range of topics on virtualization and cloud computing. It is the official source of reference materials for preparing for the VMware Certified Professional Examination.

VMware Press is also pleased to have localization partners that can publish its products into more than 42 languages, including Chinese (Simplified), Chinese (Traditional), French, German, Greek, Hindi, Japanese, Korean, Polish, Russian, and Spanish.

For more information about VMware Press, please visit [vmwarepress.com](http://vmwarepress.com).

# vmware® PRESS



[vmwarepress.com](http://vmwarepress.com)

Complete list of products • User Group Info • Articles • Newsletters

**VMware® Press** is a publishing alliance between Pearson and VMware, and is the official publisher of VMware books and training materials that provide guidance for the critical topics facing today's technology professionals and students.

With books, eBooks, certification study guides, video training, and learning tools produced by world-class architects and IT experts, VMware Press helps IT professionals master a diverse range of topics on virtualization and cloud computing, and is the official source of reference materials for preparing for the VMware certification exams.



Make sure to connect with us!  
[vmwarepress.com](http://vmwarepress.com)

vmware®

PEARSON  
IT CERTIFICATION

Safari®  
Books Online

*This page intentionally left blank*

# VMware Horizon Suite

## Building End-User Services

Stephane Asselin  
Paul O'Doherty

**vmware**® PRESS

Upper Saddle River, NJ • Boston • Indianapolis • San Francisco  
New York • Toronto • Montreal • London • Munich • Paris • Madrid  
Capetown • Sydney • Tokyo • Singapore • Mexico City

## VMware Horizon Suite

Copyright © 2014 VMware, Inc.

Published by Pearson Education, Inc.

Publishing as VMware Press

All rights reserved. Printed in the United States of America. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise.

ISBN-10: 0-13-347908-0

ISBN-13: 978-0-13-347908-9

Library of Congress Control Number: 2014907775

Printed in the United States of America

First Printing: June 2014

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. The publisher cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

VMware terms are trademarks or registered trademarks of VMware in the United States, other countries, or both.

### Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The authors, VMware Press, VMware, and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

The opinions expressed in this book belong to the author and are not necessarily those of VMware.

### Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at [corpsales@pearsoned.com](mailto:corpsales@pearsoned.com) or (800) 382-3419.

For government sales inquiries, please contact [governmentsales@pearsoned.com](mailto:governmentsales@pearsoned.com).

For questions about sales outside the U.S., please contact [international@pearsoned.com](mailto:international@pearsoned.com).

#### ASSOCIATE PUBLISHER

David Dusthimer

#### ACQUISITION EDITOR

Joan Murray

#### VMWARE PRESS

#### PROGRAM MANAGER

David Nelson

#### DEVELOPMENT EDITOR

Ellie Bru

#### MANAGING EDITOR

Sandra Schroeder

#### SENIOR PROJECT EDITOR

Tonya Simpson

#### COPY EDITOR

Keith Cline

#### PROOFREADER

Paula Lowell

#### INDEXER

Lisa Stumpf

#### EDITORIAL ASSISTANT

Vanessa Evans

#### COVER DESIGNER

Chuti Prasertsith

#### COMPOSITOR

Trina Wurst

## Dedication

*Stephane and Paul worked many long hours to bring together their thoughts, ideas, and experience to collaborate on this project. They would like to dedicate this book to the readers who have provided feedback, support, and insight to their work, thus enabling them to develop and deliver great content.*

*This page intentionally left blank*

# Contents

Introduction ix

## Chapter 1 The New End-User Model 1

The Evolution of the End User 1

An End-User Service Catalog 2

How Do View, Mirage, and Horizon Workspace Deliver a Service Catalog? 3

Considerations for Deploying View, Mirage, and Workspace 4

An Introduction to VMware View, Mirage, and Workspace 18

VMware View 18

VMware Mirage 21

VMware Workspace 24

Summary 25

## Chapter 2 VMware View Architecture 27

Introduction 27

Approaching the Design and Architecture 27

Phase I: Requirements Gathering and Assessment 28

Phase II: Analysis 29

Phase III: Calculate 30

Phase IV: Design 32

VMware View Server Architecture 33

VMware View Connection Server 34

VMware View Replica Server 34

VMware View Security Server 35

Local Mode VMs 38

VMware View Transfer Server 39

Summary 51

## Chapter 3 VMware Workspace Architecture 53

Introduction 53

Approaching the Design and Architecture 53

Planning Considerations 54

IP Pools 55

Network Services 55

NTP 57

Authentication 58

Certificates 60

SMTP 62

External Storage 62

PostgreSQL 65

- Postgres Availability 67
- Postgres Clusters 71
- Summary 74

**Chapter 4 VMware View Implementation 75**

- VMware View Deployment and Design Considerations 76
- Installing VMware View 80
- Configuring the View Connection Server 85
  - Adding vCenter Server 89
  - Configuring View Replica Server 92
  - The Event Database 93
  - Security Servers 95
  - Firewall Rules 96
  - Adding the Security Servers 97
- Installing the View Agent 99
  - View Agent Custom Setup Options 100
  - Installing the View Client 101
  - Working with Certificates in View 103
  - Creating Certificate Templates 105
- Summary 111

**Chapter 5 VMware Workspace Implementation 113**

- VMware Workspace Deployment and Design Considerations 113
- Workspace Implementation: Initial Setup 115
  - Workspace vApp Appliances 115
  - Workspace Configurator VA 116
  - Workspace Service VA 116
  - Workspace Connector 116
  - Workspace Data VA 116
  - Workspace Gateway VA 116
- Deploying the Workspace vApp 118
  - Workspace Initial Configuration 120
  - Workspace Setup Wizard 122
  - Security Exception 123
- Navigating the Administrative Console 135
  - Enable Workspace Data Module 135
  - User Entitlement 138
  - Configuring CoS in Data 140
  - Enable Integration with View 142
  - Launch a View Pool 144
- Web Applications: SaaS 145

---

Modifying Workspace Data Module Storage	148
Add Additional VMDKs for Storage	149
Upgrading a Workspace Environment	152
Enabling Workspace with NFS	152
Installing the Workspace Agent on Client Endpoints	153
Workspace Windows/OS X/iPad/Android Client Deployment	153
Using SSL Certificates in Workspace	156
Applying an SSL Certificate from a Trusted Third-Party CA	157
Applying an SSL Certificate from an Internal or Nontrusted External Certificate Authority	158
Summary	158

## **Chapter 6 Integrating VMware View and Workspace 161**

VMware View and Workspace Integration Considerations	163
VMware Workspace and View Integration	165
Troubleshooting Certificate Errors	174
Add a SAML 2.0 Authenticator	176
Manage Authenticators	177
Select an Existing SAML 2.0 Authenticator	177
Dashboard	177
Scaling View and Workspace Deployment	179
Summary	183

## **Chapter 7 View Operations and Management 185**

VMware View Operations	185
Using View Access Groups	185
Types of Desktop Pools	187
Automated Desktop Pools	188
Manual Desktop Pools	188
Microsoft RDS Desktop Pool	189
Creating Desktop Pools	189
Power Settings	197
Pool Settings	200
View Composer	206
vCenter Settings	209
Provisioning Settings	211
Sysprep or QuickPrep?	212
Entitlement	213
Replicas	214
Refresh	214
Recompose	215
Rebalance	216

Managing Persistent Disks	216
Backing Up View	218
Replacing Certificates	221
Composer and Certificates	225
Summary	226

## **Chapter 8 VMware Workspace Operations 227**

Operation of VMware Workspace	227
Dashboard	230
Users & Groups	230
Entitlement	232
Remove Users	233
Catalog & Modules	233
ThinApp Integration	234
Policies	236
SAML Overview	237
Auditing and Tracking	239
Workspace Clients	240
Horizon Files	242
Enable Horizon Files	242
Add Additional Data VAs	245
System Diagnostics	246
Summary	247

## **Chapter 9 VMware Horizon Mirage 249**

VMware Horizon Mirage Deployment and Design Considerations	249
Horizon Mirage Planning	251
Horizon Mirage Components	251
Prerequisites	253
Storage Considerations	256
External Dependencies	256
Mirage Architecture	256
Deploying Horizon Mirage Management Server	257
Horizon Mirage Server	264
Mirage Day-to-Day Administration	265
Horizon Mirage Endpoint Restoration	268
Horizon Mirage Base Layer	269
Deploying Mirage Base Layer	272
Horizon Mirage Layer Updates	273
Horizon Mirage Endpoint Migration	274

---

Horizon Mirage File Portal	277
Horizon Mirage Web Management	279
Horizon Mirage Driver Library	280
Horizon Mirage Collections	283
Horizon Mirage Application Layers	285
Horizon Mirage Reports	287
Horizon Mirage Logs	288
Summary	289

## **Chapter 10 Multimedia 291**

How Do You Deliver a Rich End-User Experience?	292
vSGA, Virtual Shared Graphics Acceleration	295
Configuring ESXi for vSGA	296
VMware View with vSGA	298
vDGA, Virtual Direct Graphics Acceleration	300
Enhancements in PCoIP	300
Building a Performance Test Environment	302
Installing and Configuring WANem	305
Installing and Configuring Wireshark	309
Tuning PCoIP	312
Tuning Parameters	313
Further Analysis	318
PCoIP Bandwidth Utilization	320
PCoIP Connection Quality	320
PCoIP Packet Counts	320
PCoIP Connection Latency	321
Encoding Graphs	321
The Impact of Load	323
Setting Up VMware ViewPlanner	325
Setting Up the Client Desktop	327
Summary	328

## **Chapter 11 Integrating Lync and VMware View 329**

Microsoft Lync and VMware View	329
Microsoft Lync 2013	331
Creating a Lync Environment	332
Preparing for Lync 2013	332
Lync 2013	335
Windows 2012 and .NET Framework 3.5	335
Installing Lync Server	339

- Build and Publish a Lync Topology 343
- Set Up Users and Test Lync 352
- View Desktops 355
- View Clients 357
- Verifying the Plug-In 358
- Summary 360

**Chapter 12 Performance and Monitoring of VMware Horizon 361**

- Performance Monitoring Solutions 362
  - Establishing a Performance Baseline 363
  - Xangati VDI Dashboard 364
  - Liquidware Labs Stratusphere UX 369
  - VMware vCenter Operations Manager 377
- vApp Overview 380
  - vCOps for View Adapter 380
- Summary 394

**Appendix A A Design Questionnaire Worksheet 397**

**Appendix B VMware View Network Ports 403**

**Index 405**

# Introduction

Writing this book has been a challenge because of the speed of change in the VMware end-user computing software products. When we first talked about the idea of writing about Horizon Suite, Mirage had just been acquired, Workspace was a 1.0 product, and the current release of View was 5.1. It is hard to believe that the evolution of the product line has happened so quickly in a little over a year. With the release of Horizon Suite 6, the need for a book that covers VMware View, Mirage, and Workspace has never been greater, so the effort was worth it.

Much greater than our challenge is the challenge for you, the reader, who is facing a world in which desktop management has become the management of stateless, mobile, streamed desktop or mobility tablet and smartphone workspace management. One might wonder whether in this age of readily available content, along with a plethora of how-to videos, a book dedicated to understanding these technologies has value.

We asked ourselves the same question, and when we reflected, we considered all the times that we really learned something. In reflecting, we realized that we learned the most when we got information that was relevant to what we were doing and was easy to understand and that stepped us through what we really needed to know and allowed us to understand 80% of what was important while leaving the 20% for us to look up. It is with this attitude that we approached our topics to save you some time and ease the learning process.

In approaching each topic, we have considered architecture, deployment, and operations, which represent the key understanding that you need to deploy each product within the Horizon Suite comfortably. We have also considered the important integration points between the products, such as delivering View or ThinApp through Workspace. Based on feedback, we have also looked at some critical areas of interest to our readers such as VMware View and Microsoft Lync integration and PC over IP (PCoIP) offloading technologies.

VMware has done much innovation at the infrastructure level that delivers key competitive advantages. Topics such as virtual software-area networking (SAN) and other performance accelerators are considered in addition to vSphere features such as View Storage Accelerator. Although we have covered much, some topics will have to wait until the next release, such as vCenter Automation Center for Desktops. As always, your feedback and support is key in determining what topics make it into the next release.

## Motivation for Writing This Book

As fast as *VMware View: Building a Successful Desktop* was completed, the market evolved from virtual desktop infrastructure to end-user computing. The difference is that

end-user computing takes into account all end-user services and not just desktop requirements. Addressing all end-user computing requirements cannot be done with a single product and requires a suite of products. Horizon is that answer. There was, however, no comprehensive guide to the suite, so we have pulled together expertise, experience, and resources to develop *VMware Horizon Suite: Building End-User Services*.

It is our hope that after reading this book you will be equipped with a more thorough understanding of how to deploy the components of Horizon Suite. We also hope that in reviewing each product you will understand how to match up the solution with the requirement. Each component of Horizon is targeted toward a user requirement; a better understanding of the features and capabilities ensures that they are deployed to meet the right use case. For example, VMware Mirage is designed to address the complexities in managing a distributed desktop environment, whereas Workspace is designed for user mobility and device independence. In bringing together this information under a single publication, we hope to simplify the learning process and shorten your timeframe. Stephan and I polled our subscribers and learned that there was strong interest in certain areas. We have addressed those explicitly, such as in our chapters reviewing View and Lync integration as well as multimedia options. By stepping you through the architectural and design considerations for View, Workspace, and Mirage, we also hope we can save you some time by avoiding common missteps or pitfalls by sharing our own experience with these products.

## Who Should Read This Book

This book is targeted at IT professionals who are involved in delivery of end-user services from an enterprise, managed service, or provider perspective. Those individuals who might already be comfortable with VMware View should read this book to understand the other products of Horizon Suite, such as Mirage or Workspace.

## How to Use This Book

If you are looking for knowledge on a particular product (View, Workspace or Mirage), you can read just the relevant chapters. We have approached the topics starting with the familiar View, and then the closely related Workspace, and then Mirage to help you develop an understanding of Horizon Suite. This book is split into 12 chapters, as follows:

- **Chapter 1, “The New End-User Model”:** The chapter covers the evolution of the end user and an introduction to Horizon Suite.
- **Chapter 2, “VMware View Architecture”:** This chapter covers the architecture of VMware View 6.
- **Chapter 3, “VMware Workspace Architecture”:** This chapter covers the architecture of VMware Workspace 1.8.

- **Chapter 4, “VMware View Implementation”:** This chapter covers the installation of VMware View 6.
- **Chapter 5, “VMware Workspace Implementation”:** This chapter covers the installation of VMware Workspace 1.8.
- **Chapter 6, “Integrating VMware View and Workspace”:** This chapter covers the integration of VMware View and Workspace.
- **Chapter 7, “View Operations and Management”:** This chapter covers the most common VMware View operations.
- **Chapter 8, “VMware Workspace Operations”:** This chapter covers the most common VMware Workspace operations.
- **Chapter 9, “VMware Horizon Mirage”:** This chapter covers VMware Mirage architecture and installation.
- **Chapter 10, “Multimedia”:** This chapter covers how to deliver multimedia within a View desktop environment.
- **Chapter 11, “Integrating Lync and VMware View”:** This chapter covers the integration of Microsoft Lync and VMware View.
- **Chapter 12, “Performance and Monitoring of VMware Horizon”:** This chapter covers performance monitoring of VMware View.
- **Appendix A, “A Design Questionnaire Worksheet”:** This is a comprehensive design checklist for end-user computing.
- **Appendix B, “VMware View Network Ports”:** Network diagrams showing the configuration for VMware View for an internal deployment and one that has components in the DMZ and clients connecting from the Internet.

## Bonus e-Chapter

Technology is ever changing, at a pace where it’s not easy to keep up with all the changes. This couldn’t be truer at VMware. Just take a look at the releases of VMware View within the past 12 months: three minor releases and one major release, which was just recently announced publicly. VMware View 6 is a game-changer. It has multiple new functionalities and major improvements in the end-user experience and the delivery of high-end graphics. VMware added a major component that delivers full integration of Microsoft Windows Remote Desktop Services Hosts (RDSH) in this release, which at the time of this writing was not yet public.

For this reason, we decided to dedicate an electronic chapter on application virtualization. In this chapter, we cover various aspects of AppVirt, including how to deliver hosted applications using View 6. This feature delivers fully integrated applications and server-based desktops running on Microsoft RDSH. In addition, it will also provide Windows applications seamless window access from Windows or OS X clients. View with hosted applications will give full-screen access to Windows apps from iOS and Android devices to enable mobility in this critical era of cloud computing. The simplicity of this solution is that it leverages existing technology using standard Horizon clients (Windows, OS X, iOS, and Android) with PCoIP.

We firmly believe that even though we were not able to provide this chapter within the book at the time of release, it is important enough to provide electronically. With the purchase of *VMware Horizon Suite: Building End-User Services*, you receive access to the electronic chapter “Application Virtualization: How to Configure and Integrate Application Virtualization and VMware Hosted Applications,” available for download at [www.informit.com/store/vmware-horizon-suite-building-end-user-services-9780133479089](http://www.informit.com/store/vmware-horizon-suite-building-end-user-services-9780133479089).

## About the Authors

**Stephane Asselin**, with his 22 years of experience in IT, is an architect in the End-User Computing business unit at VMware. In his recent role, he had national responsibility for Canada for EUC planning, designing, and implementing virtual infrastructure solutions and all processes involved. At VMware, Stephane has worked on EUC presales activities, internal IP, and he has worked as a technical specialist lead on beta programs. He has also done work as a subject matter expert for Horizon Workspace, View, Mirage, vCenter Operations Manager, and ThinApp projects. Previously, he was with Computer Associates as a senior systems engineer, where he worked on enterprise monitoring presales activities and as a technical specialist. As a senior consultant at Microsoft, he was responsible for the plan, design, and implementation of Microsoft solutions within major provincial and federal government, financial, education, and telcos.

In his current role in the EUC business unit at VMware, he's one of the resources developing enablement materials for all products of the Horizon Suite and technical documentation for training. Knowledge transfer to customers is a key element of his current role. Stephane has co-produced whitepapers such as "VMware Horizon Mirage Branch Office Reference Architecture" and "Horizon Workspace Reference Architecture." In addition, he runs the popular website [myeuc.net](http://myeuc.net).

**Paul O'Doherty** works for the CTO office of OnX enterprise solutions as a cloud solutions and EUC specialist, specializing in the architecture and delivery of cloud-based infrastructure and end-user services. Paul has written several books, including *VMware View 5: Building a Successful Virtual Desktop*, released by VMware Press. Prior to that, Paul spent 10 years as the managing principal consultant at Gibraltar Solutions architecting and delivering end-user computer and virtualization environments in Fortune 500 companies involving VMware, VMware View, Citrix XenApp, and XenDesktop technologies. Paul has a broad range of infrastructure experience and has achieved numerous industry certifications, such as VCP, CCEA, MCITP, and RCSP, and is recognized as a VMware vExpert. In addition, Paul maintains a popular blog at <http://virtualguru.org> and has contributed to sites such as <http://virtualization.info> and is reoccurring speaker at VMUG sessions and other technical conferences.

*This page intentionally left blank*

# Acknowledgments

This is my third project where I have had the opportunity to publish, but it is the first where I'm co-author with a good friend. In the past, I have contributed chapters, but sharing the full writing responsibility has been a whole different ball game.

When Paul and I spoke, I knew that this was the right project for us to bring our experience together to create a good reference for others. This, of course, could not have been possible without the contributions and review of our own tech editors, Justin Venezia and Mike Barnett. Technical review is a critical piece in developing a project like this. In addition to the direct support of our technical editors, I want to thank a number of people for their support and guidance, including Simon Long, a colleague and avid blogger ([www.simonlong.co.uk](http://www.simonlong.co.uk)), Michael Burnett at Nutanix, and Todd Methven, an HP end-user client expert who has contributed to our lab and enabled us to test all the ideas and concepts we had. In addition, I would not have been able to dedicate the time without the support and understanding of my manager at VMware, Andrew Johnson.

I also want to thank my supporting team for providing the opportunity and effort to get this book done: Joan Murray, Ellie Bru, as well as my friend and co-author Paul O'Doherty.

My biggest support group is my family, who continue to support all of daddy's crazy projects. I would like to thank my wife, Marie-Josée, for her incredible patience and understanding, and finally, my three, not "so little anymore" kids: Vincent, Raphaëlle, and Guillaume.

—Stephane Asselin

After writing my first publication, *VMware View: Building a Successful Desktop*, I was elated by the response and support I received from the people who invested in it. I was equally excited about the changes in the VMware product line that transformed a virtual desktop product into an entire end-user computing suite. Trying to cover the entire Horizon Suite would not have been possible if I had not been able to engage my good friend Stephane as co-author. I was also relieved when my original editing team, Joan Murray and Ellie Bru, offered their continued support. (Why they do not run in the opposite direction whenever I come up with a new idea still puzzles me.) I also want to thank Tonya Simpson and Seth Kerney, who worked hard to put this book together. In addition to this great team, we were lucky to work with two knowledgeable and experienced technical editors, Justin Venezia and Mike Barnett. My thanks goes out to them for keeping us both focused and honest. Writing a book can be challenging, but I found the experience of writing with this group a real pleasure, which is a measure of their professionalism.

My greatest appreciation goes to my wife, Heather, and family, who even after the time asked on the first book were willing to provide unwavering support on the second. My two wonderful girls, Briar and Hannah, never complained about the time spent writing and kept me motivated with their enthusiasm and encouragement for this project.

I hope that our efforts translate to a greater level of understanding of Horizon Suite for those of you reading this book. I would also like that if in reading this we save you a little time or help in your success so that you can pursue the things you are passionate about.

—Paul O’Doherty

# Technical Reviewers

**Justin Venezia** is a consulting architect with VMware's End-User Computing Professional Services Engineering group. In this role, he actively participates in real-world delivery of EUC solutions to VMware customers, he supports VMware's EUC PSO organization with technical content development and enablement, and is involved in EUC engagement delivery. Prior to his role at VMware, Justin was a field architect with Citrix Consulting Services. He has also worked as an architect and IT manager in the healthcare and banking/financial verticals.

**Mike Barnett** is a systems engineer at VMware specializing in end-user computing. He has worked in IT for 11 years and has been working with VMware technology since 2008. Mike has presented at local VMware user groups as well as VMworld in 2011. He worked in the VMware Global Support Services organization supporting end-user products before moving into the field.

# We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write us directly to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

*Please note that we cannot help you with technical problems related to the topic of this book.*

When you write, please be sure to include this book's title and author as well as your name, email address, and phone number. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: [VMwarePress@vmware.com](mailto:VMwarePress@vmware.com)

Mail: VMware Press  
ATTN: Reader Feedback  
800 East 96th Street  
Indianapolis, IN 46240 USA

## Reader Services

Visit our website at [www.informit.com/title/9780133479089](http://www.informit.com/title/9780133479089) and register this book for convenient access to any updates, downloads, or errata that might be available for this book.

*This page intentionally left blank*

# View Operations and Management

## VMware View Operations

This chapter covers the operation of VMware View versus installation or architecture considerations. Perhaps the primary activity that you tend to repeat often is the creation and management of desktop pools, which are covered in this chapter. A few other functions also fall into the general category of management and operations, such as backing up the environment, patching, and replacing the certificates (all of which this chapter also covers).

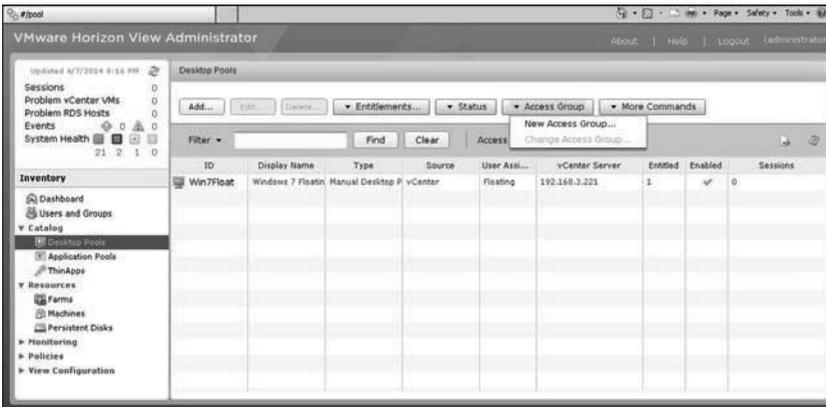
## Using View Access Groups

Before you start creating pools, take advantage of the ability to create access groups to organize your environment and to enable delegation of roles and responsibilities.

Let's consider the example of task-based workers and assume that they will use Windows Remote Desktop Services (RDS) pools. We are generalizing here, but you would use categories based on your analysis of your environment. Desktop pools are usually categorized by the function of the user, because the function tends to relate to a specific application workload, or by location if you are deploying a multisite architecture. In our example, you can create an access group called Task-Based Users and use it to further segregate the RDS Server pools within the VMware View Administrator console. You can then use the access group structure to delegate roles and responsibilities. Because it is likely that the team that manages your RDS Servers is not the same team that manages your desktops, this is a good use case for creating access groups. If you work in a fairly small organization, I still recommend using access groups, but just restricting their

number. This way, you can delegate easily in the future. In this example, we use the category of Task-Based Users. To create the access group structure, follow these steps:

1. Log in to the VMware View Administrator console.
2. Browse to Inventory and Pools.
3. On the right pane, select **Access Group**, **New Access Group** from the drop-down, as shown in Figure 7.1.



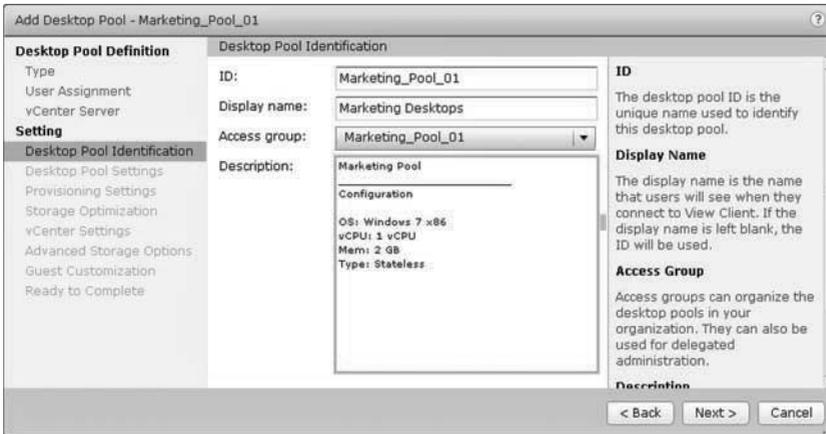
**Figure 7.1** Creating access groups

4. Create the access groups that you need to organize your VMware View environment. It is ideal if you take the category details that you have created and paste them into the Description field, as shown in Figure 7.2.



**Figure 7.2** Providing full descriptions

- After you create your pool, under Pool Identification, you now see the access group you created to help categorize your environment properly, as shown in Figure 7.3. This feature also enables you to delegate roles and responsibilities for the access group.



**Figure 7.3** Access groups logically segregate your environment.

## Types of Desktop Pools

Within VMware View, there are several types of desktop pools. Pools are used to describe clusters of desktop types that are assigned to users or groups of users. They are also used as objects in the View Management Console for the same purpose—to define desktop types, associate users, and entitle virtual applications. One type of desktop we have not covered is physical. It is possible to proxy physical desktops by installing the VMware Agent on the desktop and adding it to a pool for assignment. In addition, with View 5.1 and above, you can use View Persona on physical desktops. The process is the same in terms of installing the agent, but the creation of the pool varies slightly. We examine this topic further within this chapter.

Although the integration of physical desktops is no longer common due to the improvements in multimedia support in virtual desktops, it can still be used to transition from a PC blade environment to VMware View. For example, you can proxy PC blade users through the VMware View environment while you migrate from physical desktops to virtual ones and use View Persona to migrate the user settings.

## Automated Desktop Pools

Automatic desktop pools are desktops that are provisioned and customized by VMware View automatically. They can be deployed either persistently or floating. When we talk about *persistence* or *floating* in this case, we are talking about the relationship between the user and the assigned desktop. If you choose persistent, the desktop is assigned to a specific user. You can select to do this automatically so that whatever desktop the user logs in to first becomes the assigned desktop. In addition, you can explicitly assign a desktop by defining a relationship between a desktop and user login as part of the deployment options, or you can manually assign desktops after they have been created through the View Administration console. Persistent pools can be used when the application load is tailored to an individual user or if there is a requirement to store some local data.

Nonpersistent, or floating, pools are assigned for the duration of the session. After a user logs off, the View desktop is available for other users. A floating desktop can be used when you have a large number of users but they do not sign on at the same time (for example, nursing stations in a hospital, management terminals on a manufacturing floor, or kiosk displays).

You can also set properties of the pools to allow for a dynamic and reactive creation of virtual desktops as they are assigned. For example, you can specify a minimum number of virtual desktops to be created when the pool first comes online. Desktops are created until the minimum number is reached. This capability ensures that an adequate number of desktops exist to service users.

You also can adjust the maximum setting for the number of virtual desktops that can exist in a pool. You can use this setting to make sure you do not overtask the supporting physical resources of the virtual desktop environment, such as the volume or logical unit number (LUN) on which the desktops are deployed.

Another setting that you can configure in a pool is the available number. The available number ensures that a constant number of virtual desktops exists to deal with demand. As the available number goes down, new virtual desktops are deployed to ensure the available number is maintained.

Within automated desktop pools, you can deploy full desktops or View Composer desktops. View Composer desktops are made up of linked clones. We discuss Composer later in this chapter.

## Manual Desktop Pools

Manual desktop pools are created from existing machines or physical desktops. Machines may be managed by vCenter or unmanaged, as in the case of a physical device. If the users are allowed and the desktops are VMs managed by vCenter, manual desktop pools can also

be used for offline virtual desktops. As with automated desktop pools, these manual pools can be persistent or floating. The source of either persistent or floating manual pools can be vCenter virtual machines (VMs) or physical machines.

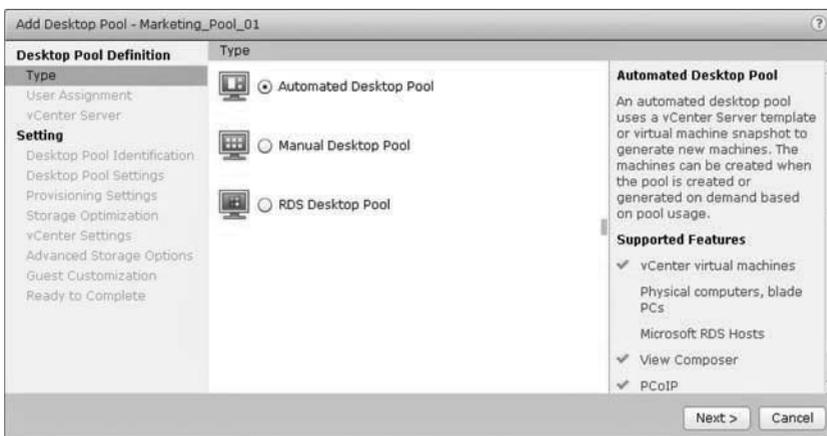
## Microsoft RDS Desktop Pool

RDS sessions can be managed by VMware View using the Microsoft RDS desktop type of pool. As explained in the preceding chapter, with recent releases of Windows, you can add many desktop attributes, such as themes, to give users the feeling they are using a dedicated and customizable desktop. With the release of View 6, native PCoIP support is available for RDS hosts.

## Creating Desktop Pools

You can create a desktop pool within the VMware View Administrator console under Inventory and Pools. From the right pane, click **Add**.

You have three types of pools to choose from: automated, manual, or RDS. In the example in Figure 7.4, we selected **Automated Desktop Pool**. In the bottom-right corner, you see a list of supported features. This list varies, especially in the case of a Terminal Services pool.



**Figure 7.4** Types of pools

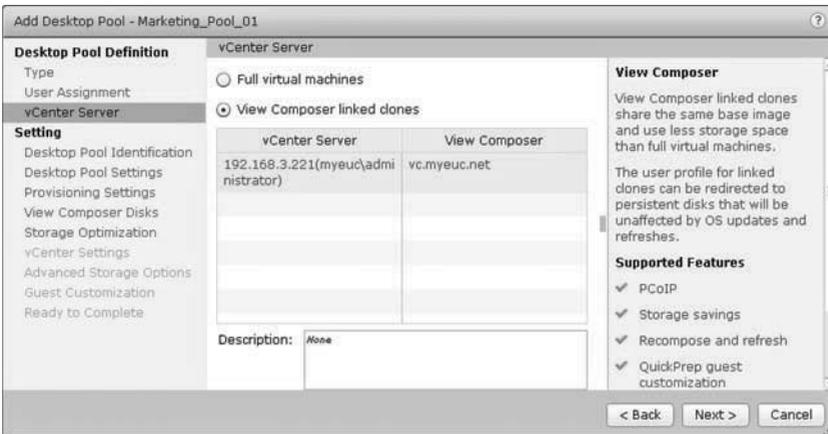
Within the type, desktops can be dedicated or floating. The setting really describes whether the relationship between the user and virtual desktop persists when the user logs off. Again, in the bottom right of this screen, you see how the features change depending

on what options are selected as you build out the pool. In the example shown in Figure 7.5, we selected **Floating**. After the type is selected, click **Next**.



**Figure 7.5** Dedicated or floating pool?

You can create full virtual machines or linked clones using View Composer. If you select View Composer, one of the features is storage savings, as shown in Figure 7.6. Choose either Full Virtual Machines or View Composer Linked Clones and click **Next**.



**Figure 7.6** View Composer linked clones

Provide an ID (no spaces allowed), display name, view access group, and description; be complete, as shown in Figure 7.7. Configure the pool identification and click **Next**.

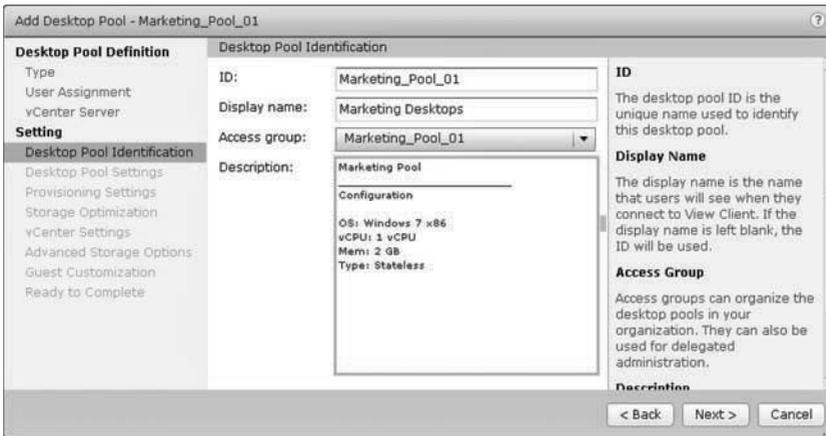


Figure 7.7 Pool identification

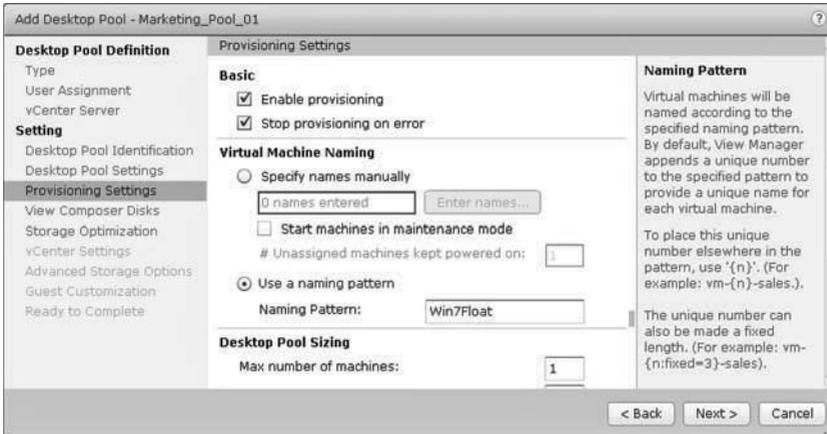
You can select numerous settings to control the pool, from power to display to Adobe Flash acceleration, as you can see in Figure 7.8. We review these settings after this example. Select **Desktop Pool Settings** and click **Next**.



Figure 7.8 Pool settings

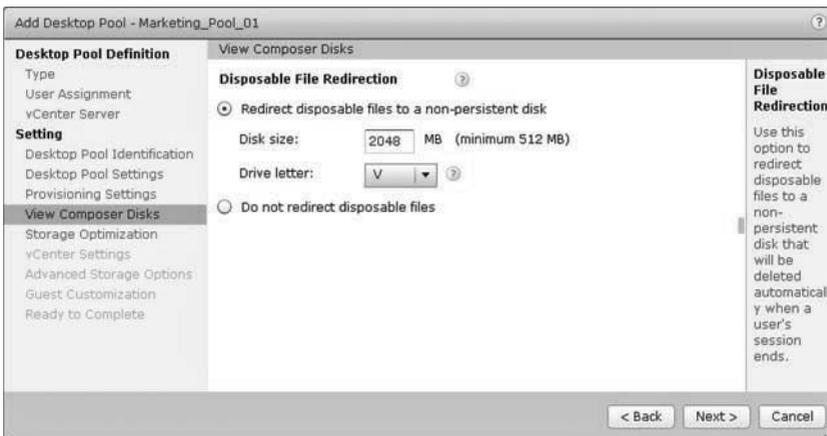
You can adjust the provisioning of the View desktops under the Provisioning Settings. For example, you can stop the provisioning when an error occurs or allow it to continue by deselecting the option because the default is to stop, as shown in Figure 7.9. You can define a standard naming pattern to keep the names of the View desktops standard and consistent. You also can set a maximum number of desktops allowed in the pool or a number of spare desktops. Setting a value for spare desktops forces desktops to be

deployed in the event that all View desktops in the pool are in use. Plus, you can provision desktops as requested or demanded, which allows you to set a minimum number of available desktops to ensure users are not waiting on View Composer to finish provisioning. Alternatively, you can provision them all upfront. Select **Provisioning Settings** and click **Next**.



**Figure 7.9** Provisioning settings

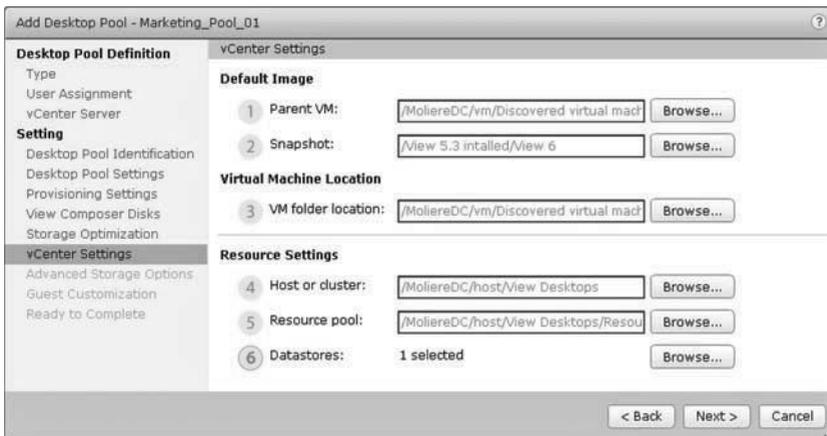
If you select View Composer Disks, you have an opportunity to tailor both the disposable file and the user data disk or persistent disk, as shown in Figure 7.10. The “Pool Settings” section later in this chapter covers these settings.



**Figure 7.10** View Composer settings

Under the Storage Optimization section, we don't have Virtual SAN or Fast FS Clones (VAAI) configured. Leave the options unchecked, and click **Next**.

Under vCenter Settings (see Figure 7.11), you select the default image and the VM folder in vCenter under which you would like the VMs created, the host or cluster, resource pool, and datastore. View has added some additional options under the Datastore settings, which we discuss in the next section. Select a datastore here and click **Next**.



**Figure 7.11** vCenter settings

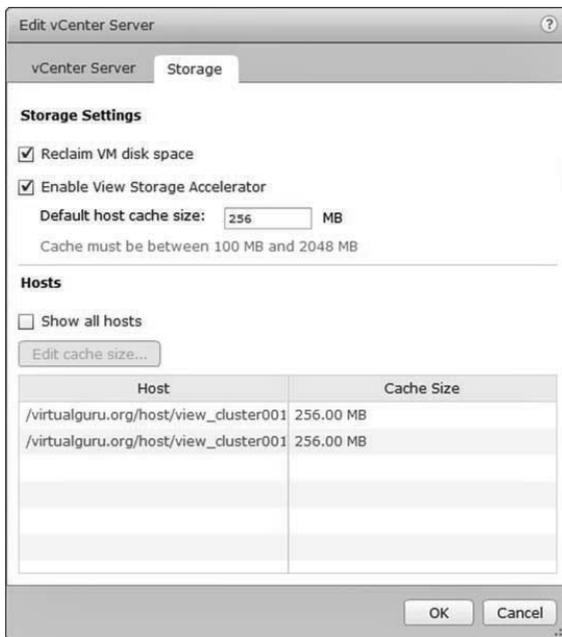
In VMware View 5.3 and above, you can also take advantage of storage features supported in vSphere 5. One of these enhancements is a Content-Based Read Cache (CBRC) or Host-Based Cache, which is referred to as View Storage Accelerator (VSA) in the View Administrator console. This cache is local to the vSphere ESXi host and stores frequently used blocks of VM disk data. CBRC improves performance by offloading some of the I/O read requests to the local ESXi host versus sending them to the storage system or storage-area network (SAN). Using VSA, you can significantly reduce your peak read requests or input/output operations per second (IOPS) in your VMware View environment.

When VSA is enabled a disk digest file is created for each virtual machine disk (VMDK). You can enable VSA for both OS and user disks; however, VMware recommends that you enable it for the OS only.

The disk digest file creates hash values for all the blocks in the VMDK when the pool is created. When a user desktop reads a block, the hash value is checked to determine the block address. If it is in memory, it is returned to the user; otherwise, it is read from disk and placed into memory. The acceleration is done on reads only, so writes are always read from disk and used to update stale data in memory.

You must enable support of VSA through the View Administrator console by enabling it under the properties of your vCenter Server and enabling it under the properties of the desktop pool, as shown in Figure 7.12. To enable this support under the properties of the vCenter Server, follow these steps:

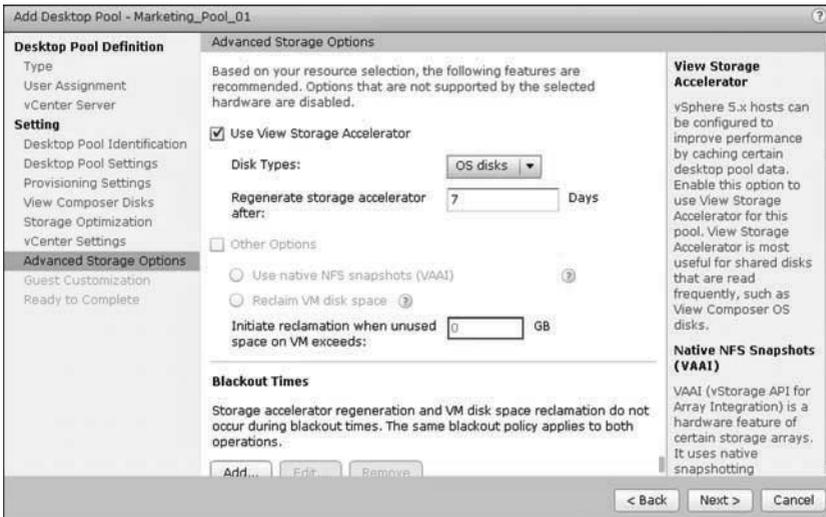
1. Open the View Administrator console and expand Server Configuration.
2. Select your vCenter Server and display the Storage tab.
3. Under Storage, select **Enable View Storage Accelerator**.



**Figure 7.12** Enabling the VSA

When you enable it, you can specify how much memory is used across all hosts or on a per-host basis. The default is 1024 MB, but this can be changed from as little as 100 MB to 2048 MB. If you have different memory configurations on your hosts, configuring per host makes the most sense.

After enabling the VSA under the vCenter properties, you can selectively enable it under the pool settings, as shown in Figure 7.13. It provides the biggest benefit for shared disks that are read frequently, such as View Composer OS disks.



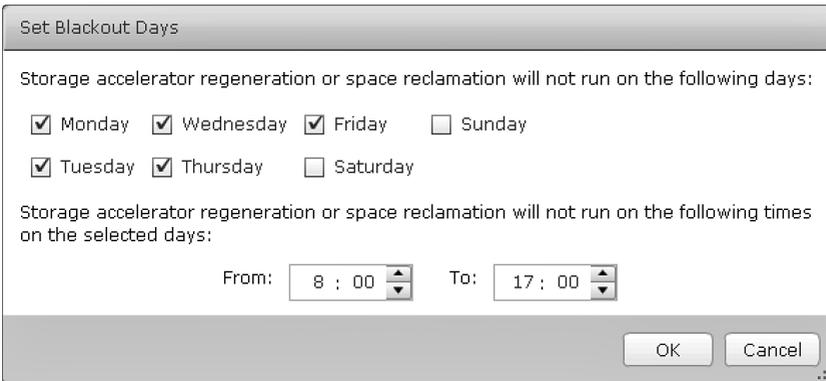
**Figure 7.13** Advanced storage settings options

In addition, you can edit the advanced storage settings options after the deployment of a desktop pool by following these steps:

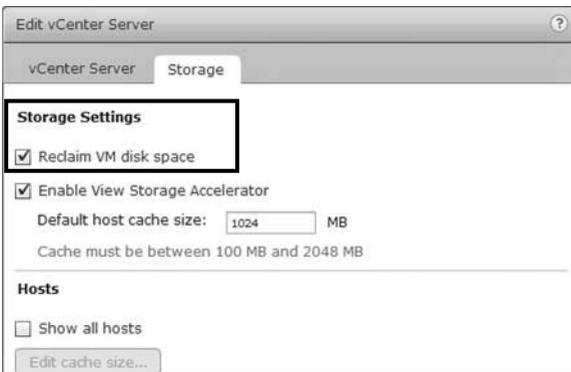
1. Open the View Administrator console and expand **Inventory**.
2. Select the pool from the right pane and click the **Edit** button.
3. Display the Pool Settings tab and Advanced Storage Options, which will display the window that enables you to select VSA, as shown in the figure.

Because it is cache, it must be regenerated on a regular basis. This activity can take up resources on the vSphere host, so you can enforce a “blackout” time period during which regeneration cannot occur, as shown in Figure 7.14.

In addition to the VSA, you can also turn on the reclaim disk space option under the advanced storage options, as shown in Figure 7.15. The reclaim option impacts only the OS disk in linked clones, but it enables ESXi to reclaim disk space without having to initiate a VMware View Refresh operation. You simply enable it and specify a threshold for how big the OS disk is allowed to grow before a reclaim event occurs; the default value is 1 GB. The blackout times you configure for the VSA also apply to reclaim operations. Reclaim is supported on vSphere 5.1 and later, although a patch is required. In addition, the VMs in the pool must be running on virtual hardware version 9 or later.

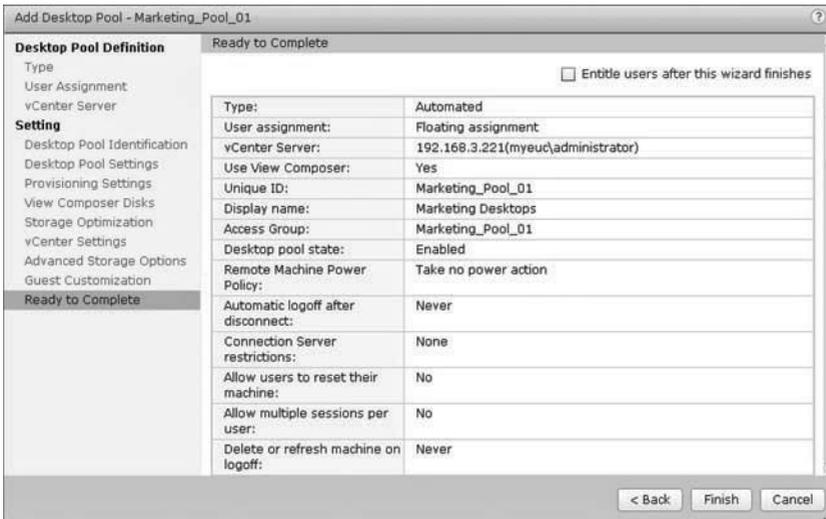


**Figure 7.14** Blackout time period



**Figure 7.15** Reclaiming disk space

Each View desktop needs some form of customization to ensure that it deploys properly and is unique on the network. To customize the View desktop, you can use QuickPrep or Sysprep. See the section on pool settings so that you understand the differences between each. After the guest customizations, you can review your settings and click **Finish** to start the deployment of View desktops, as shown in Figure 7.16.



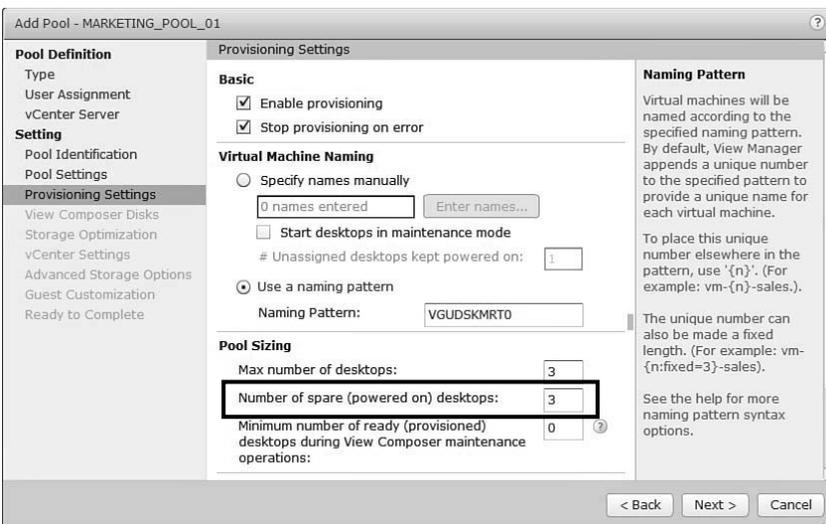
**Figure 7.16** Click Finish to begin deploying desktops.

## Power Settings

You can make a number of customizations to each pool that allow tighter control over the behavior of a VM, such as what happens when the user logs off. For example, it is possible to power off VMs when not in use to free up resources so that they are available for use by other virtual desktops in the environment. Some settings should be used with other settings. For example, powering off the VM makes sense provided that when you provisioned the pool, you set a value under Pool Sizing for the Number of Spare (Powered On) desktops, as shown in Figure 7.17, to ensure that users are not waiting for virtual desktops to boot. The other options within the pool are as follows:

- **Take No Power Action:** VMware View does not adjust the power option if the user powers down the VM.
- **Always Powered On:** VMware View does not power down the machine, and if it is powered down, the VM is automatically restarted.
- **Suspend When Not in Use:** When a user logs off, the virtual desktop is suspended. This option is also applied to floating desktops when the number of virtual desktops exceeds the setting in the available desktops counter.

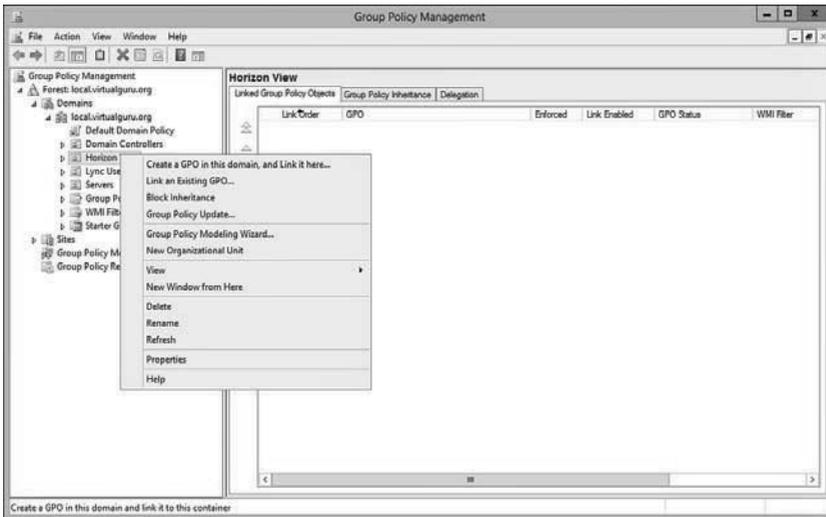
- Power Off When Not in Use:** If a virtual desktop is not in use, it is powered off. For example, if you deploy 10 desktops and 9 are not in use or logged off, View will power them off. I recommend that you combine this option with an available desktop number so that you avoid a situation in which you have users waiting for a VM to boot when connecting. Having a large number of VMs start at the same time can cause significant I/O to the storage system and is generally referred to as a boot storm. By using proper care in setting and tuning the power state options, you can avoid this situation in normal operations.



**Figure 7.17** Number of spare (powered on) desktops

It is also recommended that because you are specifically defining what happens when a user logs off that you disable the user's ability to change the power state of the VM. You can do this through the Group Policy Object associated with the organizational units (OUs) in which the virtual desktops are deployed. Simply run the Group Policy Management tool and browse to the OU in which your View desktops are deployed. You should already have a Group Policy Object defined, but if you do not, create one by using the following procedure:

1. Select the OU (Horizon in Figure 7.18), right-click, select **Create a GPO in This Domain, and Link It Here**.



**Figure 7.18** Creating a GPO

2. Provide a name for the Group Policy Object and click **OK**.
3. Select the Group Policy Object (in this example, it is named VMware Group Policy Object), right-click, and select **Edit**.
4. Browse to User Configuration, Administrative Templates: Policy Definitions and select the folder **Start Menu and Taskbar**.
5. Select the **Change Start Menu Start Button Policy** and enable it, and then change the action to remove the shutdown option. You can select Shutdown, Sleep, Logoff, Lock, Restart, Switch User, or Hibernate.
6. Click **Enabled**, as shown in Figure 7.19, and then click **OK**.

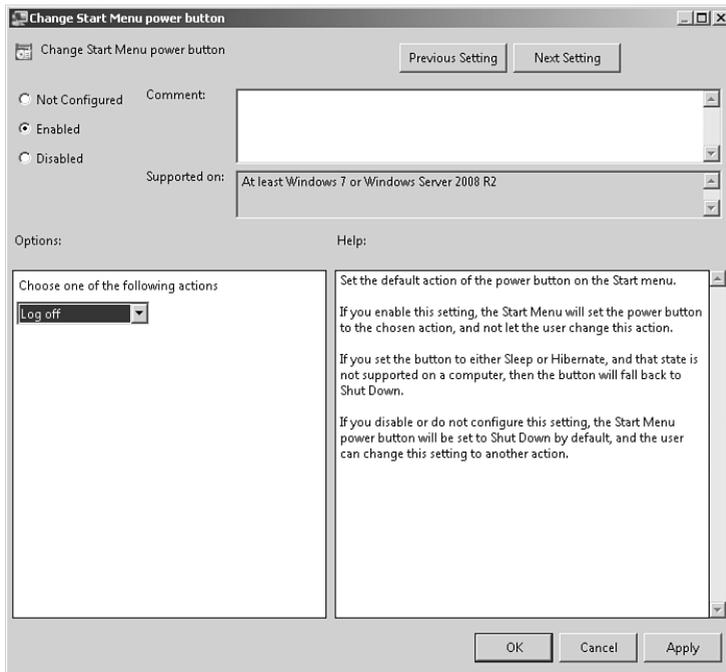


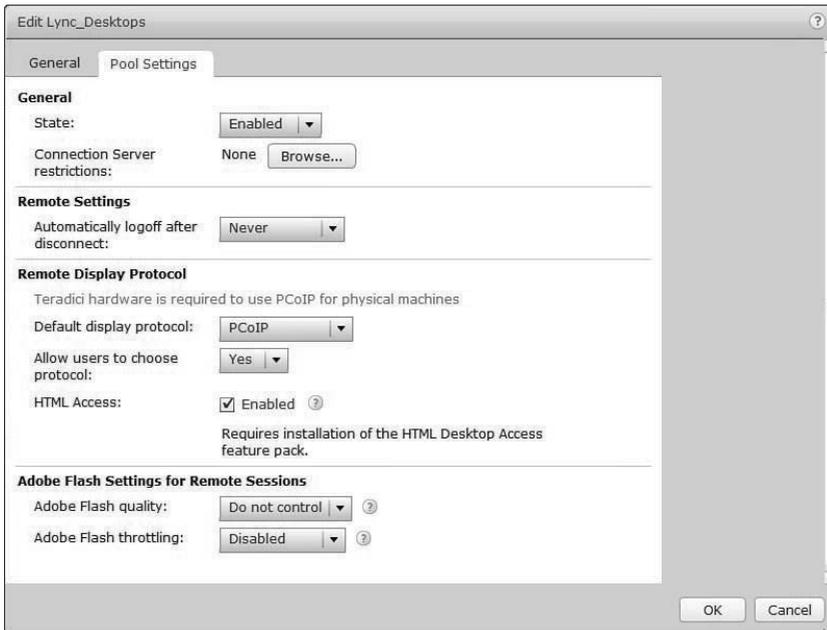
Figure 7.19 Enabling the policy

## Pool Settings

It is important to understand all the settings when configuring a pool and where they would likely apply. Not all settings are available for each type of desktop. For example, for Windows RDS pools, many of the settings are not available because they are not supported. We step through each setting possible and provide a short description, and then give you some idea when they might apply. Because we have covered the types of pools, let's review the settings under the Pool Settings configuration page.

Pool settings are broken down into General, Remote Settings, Remote Display Protocol, and Adobe Flash Settings for Remote Sessions, as shown in Figure 7.20.

The first setting, which is the state of the pool, determines whether the pool is active or inactive. To activate a pool, set the state to **Enabled**. You can disable the pool if you need to perform maintenance, such as the refreshing of images.



**Figure 7.20** Pool settings

The next general setting is the capability to restrict the pool to only certain Connection Servers. The general use case is to separate Connection Servers that provide desktops to remote users from Connection Servers providing desktops to users internally. This setting also proves handy if you are a hosting provider and need to separate desktops by company, for example. To see the tags, you must first set them using this procedure:

1. In View Administrator, select **View Configuration, Servers**.
2. In View Connection Servers, select the **View Connection Server** instance and click **Edit**.
3. In the Tag text box shown in Figure 7.21, enter a tag. Separate multiple tags.
4. Click **OK** to save your changes.

The next group of options is in the Remote Settings pane, and the first is the power policy. You have the option of not adjusting what happens when the user logs off, always ensuring desktops are on, suspending them, or powering them off. These options are available from the drop-down menu, as shown in Figure 7.22.

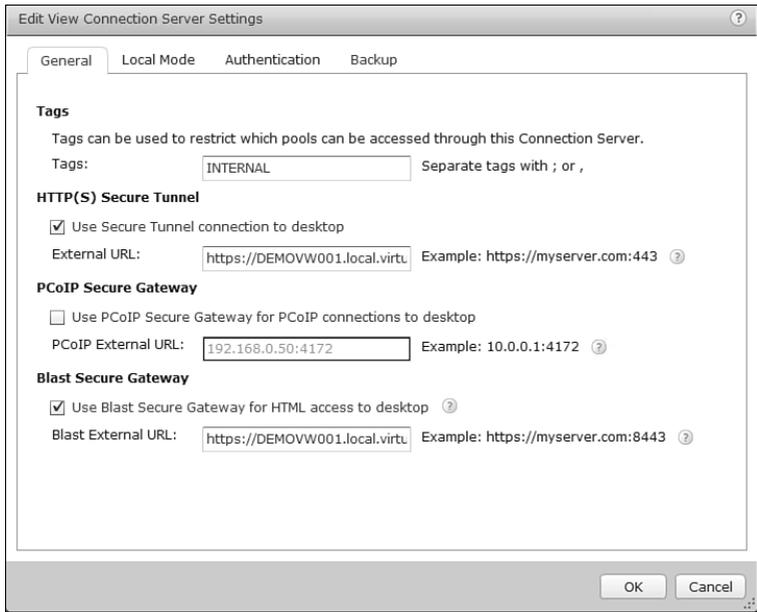


Figure 7.21 Connection Server restrictions

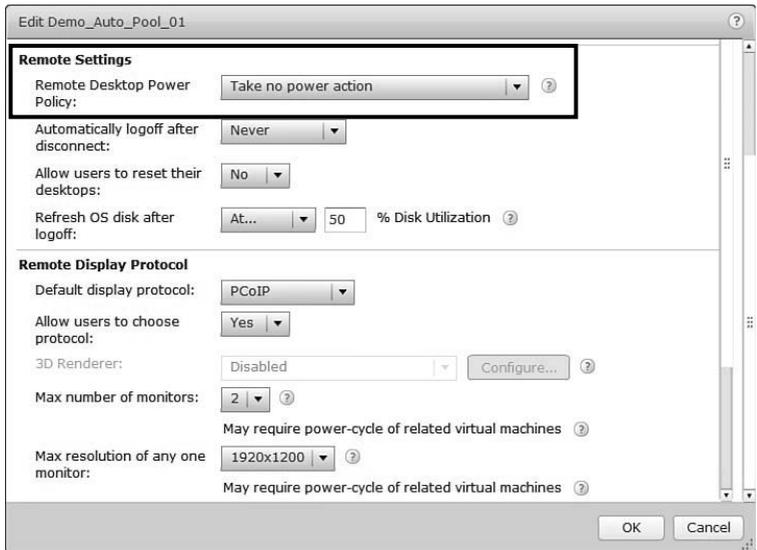
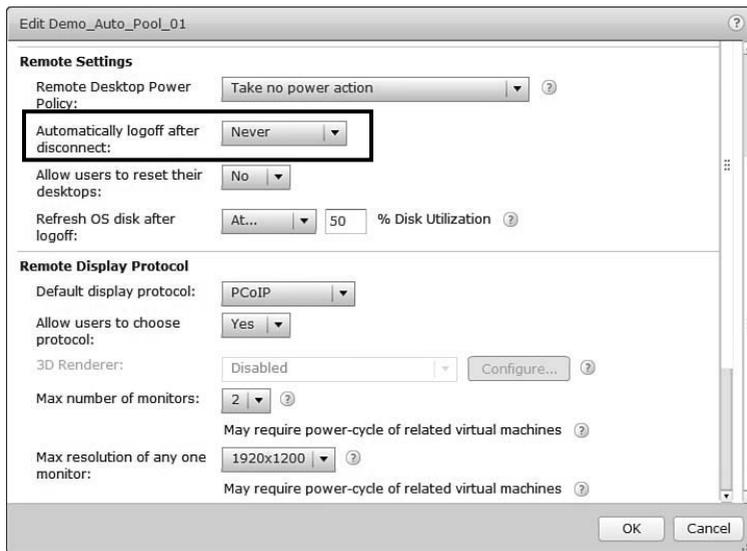


Figure 7.22 Remote desktop power policy

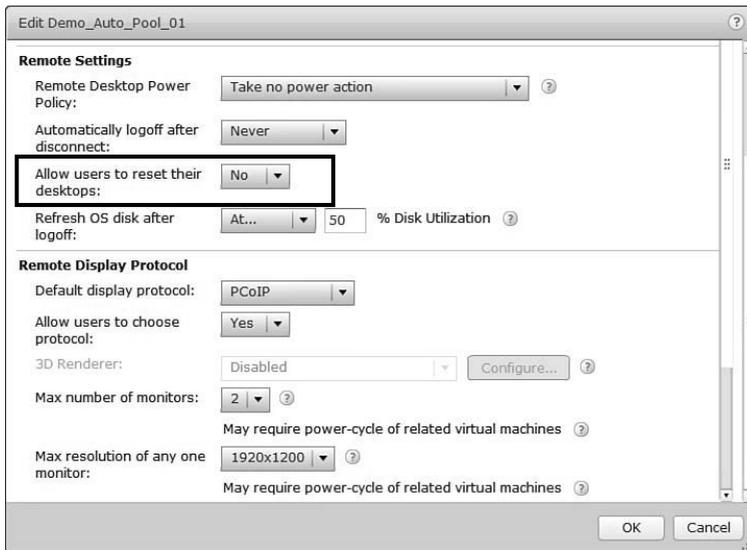
The next setting controls how long the desktop waits before logging off a disconnected user, as shown in Figure 7.23. The options are Immediately, Never, or After a Set Number of Minutes. Immediate is appropriate in a floating desktop pool in which it does not matter which desktop users log in to. If a pool provides remote access to users, you should allow for a certain number of minutes to compensate for some intermittent connectivity. If the users run batch processes that need to run for an extended period of time, Never might be the more appropriate selection.



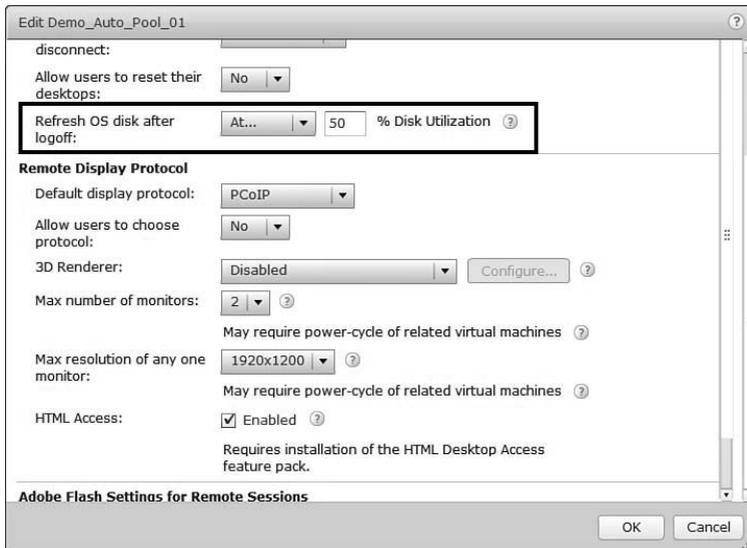
**Figure 7.23** The Automatically Log Off After Disconnect option

The next available option (see Figure 7.24) determines whether an option to do a hard reset of the VM is available from the user interface (UI) to the user. This does not affect the user's ability to do an in-guest reboot within Windows.

The last item in the Remote Settings section is the Refresh OS Disk After Logoff, which allows you to complete a refresh operation selectively on a per-desktop basis versus initiating a refresh on the entire pool. This setting applies only to persistent linked clones. If the user association of the pool is set to floating, this option is not available. To configure it, you simply specify a percentage of the total size of the OS disk you would like to trigger the refresh. This only applies to Composer-based VMs and by default is set to Never. In this example, we set it to trigger when the OS disk is 50% utilized, as shown in Figure 7.25.



**Figure 7.24** The Allow Users to Reset Their Desktops option



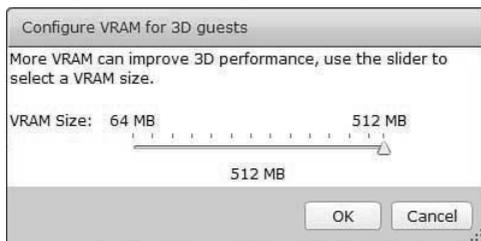
**Figure 7.25** Refreshing the desktop after logoff

The next category of pool settings adjusts the display. In View 5, you can force either PCoIP, RDP, or allow users to select which one they would like. For most users, you

should generally control the display protocol. If you do not segregate desktops specifically for remote access, you may allow users to choose, but it requires some education so that the users understand when to use which protocol.

In addition, you can turn on Windows 7 3D Rendering provided you have forced the PCoIP as the display protocol and you are using Windows 7 desktops, of course. Enabling this option restricts the number of monitors to two and the resolution maximum to  $1920 \times 1200$  pixels. Enabling it also provides support for Windows Aero within the desktop. Enabling 3D Rendering and allowing a higher maximum resolution increases the number of pixels required to deliver the View desktop. This, in turn, has an impact on the overall network utilization of the PCoIP session. Take care that you thoroughly test these settings to ensure that a balance exists between the quality of the user experience and the overall network utilization.

Enabling this option allows you to adjust the vRAM setting within View, as shown in Figure 7.26, which adjusts the vRAM setting in the properties of the VM.



**Figure 7.26** Adjusting vRAM settings

PCoIP supports a maximum of four monitors. You can select a maximum number between one and four for the desktop pool, as shown in Figure 7.26. If you force RDP, you do not have the option of adjusting the number of monitors or the resolution settings. The Max Monitors and Max Resolutions are designed to allow tuning of PCoIP. You can limit the resolution of display to one of the following:

$1680 \times 1050$

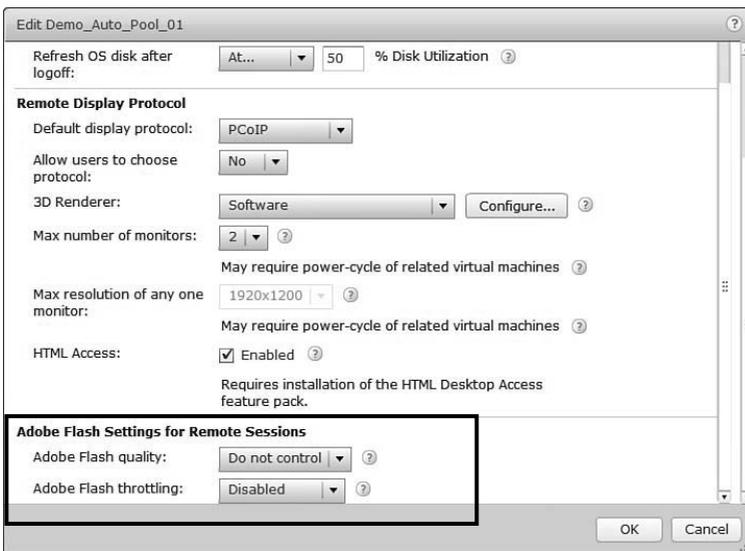
$1920 \times 1200$

$2560 \times 1600$

Lowering the resolution reduces the number of pixel changes required, reducing the bandwidth compared to higher-resolution settings as well as lowering the amount of video RAM consumed by the VM. You might want to restrict the max resolution and the number of monitors to control general bandwidth utilization.

The last setting in the Remote Display Protocol section allows you to enable access to the View desktop over HTML using HTML 5. What is great about HTML access is that it is clientless access through your HTML 5–compliant web browser. Why wouldn't you enable this for every pool and avoid client-side software installations? VMware still recommends a native PCoIP client for a feature-rich end-user experience versus HTML access. It was initially released as an option pack for VMware View 5.2.

In the next section, Adobe Flash Settings for Remote Sessions, you are controlling Adobe Flash frame rates and bandwidth to manage traffic while still providing reasonable Flash video quality, as shown in Figure 7.27. Across the LAN the defaults may be acceptable, but for remote-access and WAN situations, you should adjust and test these settings.



**Figure 7.27** Adobe Flash settings

## View Composer

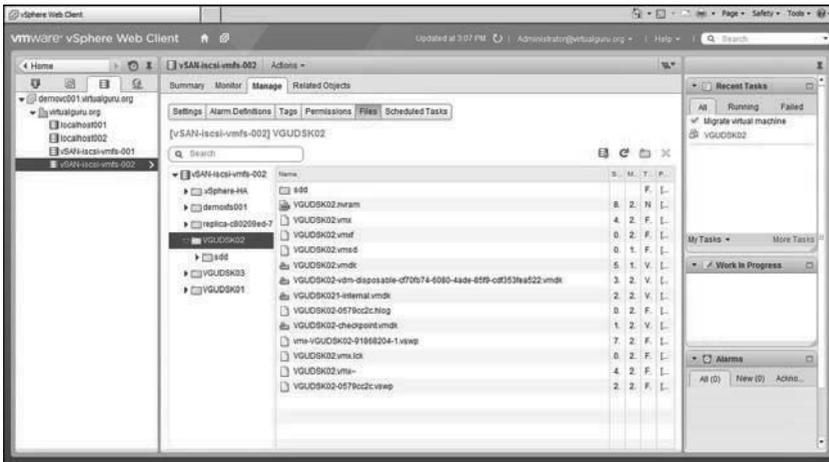
In this section, we look at what types of VMDKs make up a View Composer–created VM. With Composer, you can separate user settings onto a second drive to allow them to persist. This capability is important because VMs created by Composer need the OS disk to be refreshed, rebalanced, and recomposed as part of normal operations. By not separating user data from the OS VMDK, you run the risk of user data loss when these activities are initiated.

Redirecting user data changes the default location of the user profile to a persistent disk. In addition, you can create a disposable disk or VMDK that becomes the default location of Windows temporary files. Persistent and disposable drives are thinly provisioned, so they consume space only as they are written to.

The VM sees these View Composer drives as additional local drives within the operating system. If you look at the persistent disk, you see the Users folder containing the profiles and a personality folder if you have integrated Persona. In addition, My Documents is redirected to the persistent disk so that the redirection is transparent to the users. If you look at the disposable disk, you see the Windows Temp folder. Both the persistent disk and Persona Management can be used together or independently. Using a persistent disk to provide localization of the profile speeds up login, but it may add an additional degree of complexity. Using a persistent disk to complement Persona Management creates a local persistent cache for the profile while also ensuring it is stored centrally on a file share. When a user requires a Persona profile, the majority of the data is locally available on the persistent disk. Only the differences between the unsynchronized data need to be downloaded from the central file share. If you are going to use them together, you need to ensure that the Remove Local Persona at Log Off policy is not enabled so that the Persona profile is not removed from the persistent disk. The other option is to forgo a persistent disk and just use View Persona to back up user data to a central repository.

Logically, the separation of VMDKs makes sense. The combination of the OS and internal VMDKs and snapshots enables you to refresh the operating system, the persistent disk allows you to keep user configuration activities so that they are not lost, and the nonpersistent disk flushes temporary files on reboot. What, then, is the internal disk for? The internal disk separates the unique machine information in a separate VMDK so that it can be managed properly. This disk is created when the machine is Sysprepped or Quick-Prepped. In addition, the disk stores the machine trust account that is used to authenticate a client machine to a domain controller. It is more generally referred to as the *computer account*. A computer account password is changed every 30 days by default (it is the same for all Windows versions from 2000 on up) and is set by default in the local policy of the operating system.

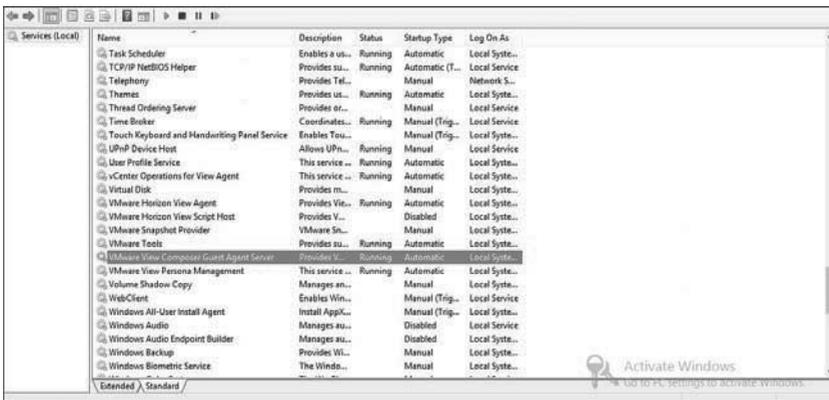
If you actually browse the directory store of the VM's folder, you see the VMDKs shown in Figure 7.28.



**Figure 7.28** View Composer VMDKs

In this case, we have VGUDSK02.vmdk, which is the VM’s virtual hard drive. We also have VGUDSK02-checkpoint.vmdk, which is the delta file. In addition we have a VMDK file that starts with VGUDSK02-vdm-disposable, which is where the nonpersistent data such as Windows temp files are stored. These files are deleted if the View Connection Server powers off the VM, but not if the user shuts down the desktop within Windows. We also have a VGUDSK02-internal.vmdk that stores the unique properties of the computer such as the computer account password to ensure connectivity to the domain is maintained when the OS disk is refreshed. Because the VGUDSK02-internal.vmdk persists, the relationship between the computer and domain is maintained.

Within a View Composer-created VM, an additional service called the VMware View Composer Guest Agent Server runs, as shown in Figure 7.29.



**Figure 7.29** VMware View Composer Guest Agent Server

One of the things this service does is monitor changes to the computer account and ensure that any changes are updated to the internal VMDK. This ensures that if you run a recompose, for example, the computer account and its unique identity persist and are not corrupted in the Active Directory.

## vCenter Settings

You have the option of specifying where on your storage system you want to store your replicas and OS disks. When creating a Composer pool under Storage Optimizations, you can specifically direct the OS disk and replicas to certain datastores; you can separate the location of the Replica and the Composer datastore as shown in Figure 7.30. The default location is to store the Replica and OS disk together on the same datastore.



**Figure 7.30** Storage optimizations

If you click **Select Separate Datastores for Replica and OS Disks**, on the following vCenter Settings page, under datastores using the Browse button, you can specify on which datastores you would like the Replica and OS disks. Because you have fine control on where certain components of View Composer are located, you can take advantage of all the innovations in solid-state drive (SSD) storage. New companies and technologies are allowing you to even more effectively manage I/O. Examples of these companies are Nexenta, PureStorage, and Fusion-I/O. You also can combine both local and shared datastores for this purpose. If you have included localized SSDs in your ESXi hosts, you can also deploy a Replica and Composer linked clones here.

VMware View also attempts to calculate the size required for the VMDKs created on the datastore selected; you can override the sizing calculation by changing the storage overcommit.

Storage overcommit adjusts how much capacity VMware View reserves for the dynamic growth of the files. It can be set to Conservative, Moderate, or Aggressive. Setting it to Aggressive, for example, increases the amount of overcapacity View factors into the deployment of VMs. Some storage systems do inline deduplication with very little impact to performance. If you have this underlying capability, you can get aggressive, but you should also be aware that depending on how your storage subsystem is designed, you could also be consolidating a larger number of I/Os.

- **None:** Storage is not overcommitted.
- **Conservative:** Four times the size of the datastore. This is the default level.
- **Moderate:** Seven times the size of the datastore.
- **Aggressive:** Fifteen times the size of the datastore.

At the bottom of this screen, you see the sizing estimated provided by VMware View. It is important to understand just how View sets the sizing so that you can understand how much is allocated by default. You can find additional information from VMware at [www.vmware.com/files/pdf/view\\_storage\\_considerations.pdf](http://www.vmware.com/files/pdf/view_storage_considerations.pdf).

- **Selected Free Space (GB):** This column shows how much free space is available in the selected datastores. This is just a sum of the real free space with no calculation applied.
- **Min Recommended (GB):** Based on the max number of desktops, View Administrator calculates the minimum you should have available on your storage and allows
  - Space for two replicas
  - Two times the memory of VM times the number of desktops
  - 20% of the size for persistent desktops times the number of desktops
- **50% Utilization (GB):** The calculation incorporates 50% OS disk growth compared to the parent VM disk for each desktop and allows
  - Space for two replicas
  - 50% of replica disk times the number of desktops
  - Memory of VM times the number of desktops
  - 50% of the size for the persistent desktops times the number of desktops

- **Max Recommended (GB):** This calculation determines that each desktop consumes the maximum disk space and allows
  - Space for two replicas
  - 100% of replica disk times the number of desktops
  - Memory of VM times the number of desktops
  - 100% of the size for persistent desktops times the number of desktops

## Provisioning Settings

You can adjust how the VMs are provisioned using the provisioning settings. You are able to adjust the naming convention and provision all at once or provision on demand, for example. Why would you provision on demand? If you have a group of users who require access to computers periodically throughout the day but are not sitting in front of a computer, as a primary function, provisioning on demand ensures virtual desktops are available on request but conserves resources until needed. Let's look at these settings a little more closely.

The first part of the provisioning settings allow you to enable and stop provisioning on error (see Figure 7.31). Enabling the Stop on Provisioning option is a good idea while you are testing all the functionality of an environment.



**Figure 7.31** Provisioning settings

The second part of the provisioning settings allows you to specify a general naming pattern or get very specific and specify VM names manually, as shown in Figure 7.32. If you select a manual naming convention, you can start a desktop in maintenance mode,

which denies a login until the desktop is taken out of maintenance mode. You can also associate specific users and start desktops in maintenance mode to allow additional applications to be loaded before users log in.

Enter Desktop Names

Enter names that will be used to create new virtual machines.

Each line must contain a unique desktop name. Optionally, for dedicated pools, a user name can be specified also. User names will be ignored for floating pools.

```
vdesktop1, virtualguru\jsmith
vdesktop2, virtualguru\jdoe
vdesktop3, virtualguru\msmall
```

Examples:

Desktop-001

Desktop-002-jdoe,abccorp.com\jdoe

Next > Cancel

**Figure 7.32** VM naming

If this is a dedicated desktop pool, you can enter a list of names and associated users so that you can selectively control which user is assigned to which desktop, as shown in Figure 7.33. If this is a floating pool, user IDs are ignored. When you click **Next**, a lookup is performed in the Active Directory to ensure the users have associated accounts.

Enter Desktop Names

3 names entered 0 entries with error

Line	Desktop name	User name	Status
1	vdesktop1	virtualguru\jsmith	
2	vdesktop2	virtualguru\jdoe	
3	vdesktop3	virtualguru\msmall	

< Back Finish Cancel

**Figure 7.33** Associating users to desktops

## Sysprep or QuickPrep?

With Composer, you can use QuickPrep or select a customization file within virtual center, which provides a full Sysprep to the VM. Sysprep, supplied by Microsoft, is

designed to change the attributes of the computer to ensure the computer is unique within the environment. This includes the security ID (SID) of the computer. Each computer should have its own local unique SID number that gets updated when the computer joins a domain. The SID is a unique number that is used to identify the system to Windows. Sysprep goes through all files and registry keys on the computer and replaces the current local SID number of the computer with a new local SID. When you use VMware clones, it is possible for two computers to have the same SID. This is why it is necessary to apply a Sysprep to a VM to ensure that it has a unique SID.

Sysprep runs through all the files on the computer and replaces any SID references on the computer with new SIDs and therefore can take longer than QuickPrep. QuickPrep, provided by VMware, is used with View Composer-created VMs (in other words, linked clones). It changes the computer account and adds it to the Active Directory, taking much less time than Sysprep.

Due to the large provisioning time difference between using Sysprep and QuickPrep, you should use QuickPrep unless the applications that you are installing require a unique local SID. For example, some antivirus software requires a locally unique SID on each desktop to run properly.

## Entitlement

After creating your desktop pools, you need to assign them to users. Within VMware View, this process is called *entitlement*. Entitlements associate a desktop pool with a selected group of users using Active Directory groups. The procedure for entitling users is as follows:

1. Log in to the VMware View Administrator console.
2. Browse to Inventory and Pools.
3. Select a pool of desktops from the right pane.
4. Select **Entitlements**.
5. You have the option of searching by user or group. Simply deselect the **User or Group** check box and click **Add**. Generally, you should associate pools of desktops to Active Directory groups and not individual users.
6. Enter a name or description and select **Find** to search for the AD group or user.
7. Select the group and click **OK** and **OK** again to entitle the desktops.

## Replicas

A *replica* is a read-only copy of the parent VM and contains a snapshot file of the original configuration. View Composer uses the replica to create the linked clone View desktops. The replica is used to right-size the VM by moving from the parent VM format to a thin-provisioned VM. From VMware View 4.5 and on, you can store replicas in separate datastores.

This enables you to store the replica on high performance disk on the SAN or local SSDs. It is from the replica that the linked clone tree is built. Keep in mind, though, that if you use a local disk, the linked clone tree also resides on the local disk.

The use of local SSDs should be reserved for stateless View desktops in a nonpersistent environment. The point of using a local SSD is to take advantage of the extremely high I/O capabilities of the technology.

When you use View Composer, desktops are created from a replica, a linked clone is created for each VM, and a snapshot is taken to create a checkpoint to enable a refresh or rollback operation.

Now that you have a basic understanding of the makeup of the Composer VMs, you can look a little more in depth at the operational management. In View Composer, you can do several activities to manage the desktops.

## Refresh

As the VM grows, the size and storage requirements of the linked clones increase. To reclaim this space and reduce the size of the virtual desktops, you can initiate a *refresh*. A refresh essentially reverts the machine to the snapshot that was created when the VM was deployed.

The OS disk is reduced in size as the machine is reverted to its initial creation size, reclaiming the space. Because the VM's machine-specific information is stored in the internal VMDK, this change can happen without having to re-create the computer account in the Active Directory because the trust relationship between the View desktop and the Active Directory is maintained.

You can control how the refresh is initiated. For example you can determine how long it is delayed and adjust the notification provided to users. Let's go through the steps to apply a refresh to the desktop pool:

1. Within the VMware View Administrator console, browse to Inventory and then Pools.
2. Double-click the pool you want to refresh on the right.
3. Display the Inventory tab to refresh individual desktops or the Settings tab to do the entire pool.

You can select individual desktops from the Inventory tab if you like. From the Inventory tab, under the View Composer drop-down menu, you can select operational tasks such as Refresh, Recompose, Rebalance, or Publish.

You can reschedule the day and time in which the activity takes place (the default is current day and current time) and force or wait for users to log off. You cannot change the grace period for logoff here, but you can see it and update it in the global settings if it needs to be adjusted.

## Recompose

A *recompose* is designed to replace the OS disk of the VM, but it has limitations. You cannot recompose to a different operating system. For example, if your linked clones are using a Windows 7 OS, you cannot recompose to a Windows XP OS. Before you can recompose, you must either change the existing parent VM or create a new one to introduce the linked clones. After the parent has been updated or created, View goes through a similar process to the creation of a new pool. A replica is created first, and then the linked clones are built from the replica. A recompose operation generally follows your image refresh or rebuild cycles, which typically happen every 6 months to a year.

Because a new OS disk is used, a new vdm-initial-checkpoint snapshot is created for use in future refresh operations. The persistent disk with all the user configurations is not replaced as a part of the recompose, allowing the OS to change but preserving the users' settings. Because it is a new OS, the sysprep Or QuickPrep process is rerun, and a new internal disk is created. A recompose can use a lot of resources in the virtual desktop environment, so it is generally recommended that you initiate a recompose after work hours. The process is similar to a refresh, except that you select Recompose from the View Composer drop-down. The exact process to initiate a recompose is as follows:

1. In View Administrator, browse to Inventory and then Pools.
2. Select the pool to recompose by double-clicking the pool ID in the left column.
3. Choose whether to recompose the whole pool or selected desktops.
4. On the selected pool's page, display the Settings tab and select **View Composer and Recompose**. To recompose specific desktops, select individual desktops from the pool by displaying the Inventory tab. Select the desktops to recompose and select **View Composer and Recompose**.
5. Click **Finish**.

## Rebalance

A *rebalance* of View desktops redistributes linked clones among available datastores based on the amount of free space available (see [http://kb.vmware.com/selfservice/microsites/search.do?language=en\\_US&cmd=displayKC&externalId=1021506](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1021506)). This is the only way to move linked clone trees between datastores. The redistribution takes place only if there is an unequal amount of space across datastores. When you rebalance a pool of desktops, the first thing View does is put the VM in maintenance mode so that no one can log in. View then determines what to move based on the amount of space in the datacenters. View separates the OS and persistent disks from the Composer desktop. It then removes the OS and persistent disks and creates a new replica and tree in the datastore. If a replica does not exist in the datastore, it is created first, unless a specific datastore has been identified for replica storage. View deletes the OS disk and creates a new OS linked to the replica. Because this is a new OS disk, Sysprep or QuickPrep is run and a new machine is created. When this process is complete, a new initial-vdm-checkpoint snapshot is created, and the VM's status is updated from provisioned to available. Be aware that the activity you are starting may involve copying a number of full VMs to many datastores plus snapshots and delta files to create the replicas and View desktops. The impact of this process can be very heavy in a large environment, so it should be performed within a maintenance window. The persistent disks are moved from the original target virtual desktop to the new one, so the user configuration information is maintained through the process:

1. In View Administrator, browse to Inventory and then Pools.
2. Select the pool to rebalance by double-clicking the pool ID in the left column.
3. Choose whether to rebalance the whole pool or selected desktops.
4. On the selected pool's page, display the Settings tab and select **View Composer and Rebalance**. To rebalance selected desktops, display the Inventory tab. To rebalance specific desktops, select the desktops to rebalance and select **View Composer and Rebalance**.
5. To rebalance specific desktops, select the desktops to rebalance and select **View Composer and Rebalance**.
6. Click **Finish**.

## Managing Persistent Disks

It is possible to manage persistent disks on an individual basis. From an operations perspective, you might need to do this if you want to preserve settings from a virtual

desktop that has had a problem to be able to copy them to a new one you have re-created. You need to detach and reattach the persistent disk to preserve the settings.

If you have integrated Persona Management, the user configurations and profile are available centrally from the file repository, so there is less need to reattach persistent disks. This capability can come in handy, however, from time to time. For example, if a user is having issues with a persistent desktop, the help desk can ask that user to log off and reassign the user to another desktop to which you have reattached the user's persistent disk. Because View Persona ensures the user's settings transfer to the new View desktop, there is minimal impact to the user. While the user is working, troubleshooting can be performed on the problematic virtual desktop.

All persistent disks are organized into a single view under the Inventory and Persistent Disks section in the VMware View Administrator console. If you look in the right pane, you see all your persistent disks and what state they are in (attached or detached). You also see the desktop, pool, datastore, and the current capacity of the persistent disk.

You can select any disk from the Attached tab and detach its persistent disk. When you do, the associated VM is deleted and removed from inventory. When you detach, you are prompted to keep the disk on the current datastore or move it to another. If you move it to another datastore, you are asked to select a VM folder that the persistent disk should be moved to. From the Detached tab, you can view the detached persistent disks, refresh the inventory, and create new VMs to be reattached to the persistent disks. This capability is a substantial improvement over older releases of View, which required scripts to be run to reassociate user data disks.

The operational procedures to detach and attach persistent disks are as follows:

1. In View Administrator, click **Inventory** and **Persistent Disks**.
2. Select the persistent disk to detach.
3. Click **Detach**.
4. Choose where to store the persistent disk.
5. Use the current datastore. Store the persistent disk on the datastore where it is currently located.
6. Move to the following datastore. Select a new datastore on which to store the persistent disk. Click **Browse**.
7. Click the down arrow and select a new datastore from the Choose a Datastore menu.
8. The View Composer persistent disk is saved on the datastore. The associated linked clone desktop is deleted and removed from inventory.

Provided the desktop you want to reattach it to is the same OS, you can reattach it as follows:

1. In View Administrator, click **Inventory** and **Persistent Disks**.
2. Display the Detached tab.
3. Select the persistent disk.
4. Click **Attach**.
5. Select a linked clone desktop on which to attach the persistent disk.
6. Select **Attach as a Secondary Disk**.
7. Click **Finish**.

#### **IMPORTANT**

Double-check the permissions on the persistent disk to ensure that System and Administrators have full access. You should also ensure that the local user group has Read & Execute, List Folder Contents and Read, and the special permission Create Folder and Write Data.

After the desktop is joined to the domain, the domain users group is added to the local users group, ensuring the user has the appropriate access to download or create a profile. From the same Detached tab, you can select a detached disk and re-create a desktop OS by selecting the persistent disk and clicking the Recreate Desktop button.

## **Backing Up View**

The practice of redirecting user data to file servers versus backing up user content on their desktops is the same on virtual as it is on physical desktops. Rather than backing up each virtual desktop, you will employ user, group, and profile management to centralize the content on a file server and back up from that point. This exception to backing up View desktops is when you have stateful desktops or desktops in which user configurations or data is stored within the virtual desktop. Although it is still simpler to employ folder redirection and Persona Management to centralize user data for backup even with stateful, it is possible that the View desktops configuration and toolset is unique to the requirements of a single user (for example, developer desktops in which the developer installs and customizes the configuration for their specific need). In this case, the stateful desktop should be backed up.

Whether to back up a desktop is largely determined by the nature of its use and whether it is a full clone or linked clone. There is little value in backing up a linked clone, but it may make sense on a full clone. For example, if the full clone desktop is highly customized when it is initially deployed by the developer, but changes very little after that, once a week might be overkill.

The opposite of a stateful desktop is, of course, a stateless desktop. A stateless desktop does not contain any unique user configuration or data and therefore does not require backup.

There are, however, a few components of the View architecture that you should take steps to protect by having backup policies. This section examines which components of the View architecture are critical and therefore warrant backup. The components that you should consider backing up include the following:

- View Connection Server
  - Including AD-LDS datastore
- View Composer
  - Including database
- View Transfer Server and offline desktop file repository
- The central repository of ThinApp packages
- User Persona file repository
- vCenter database

VMware recommends that with respect to the AD-LDS and vCenter and Composer databases that you back them up in the following order:

1. View Connection Server AD-LDS
2. View Composer database
3. Back up vCenter database

You can use traditional backup tools for backing up the OS, file repositories, and databases, but there is a specific process for backing up the AD-LDS datastore and a sequence recommended by VMware. In addition, by default, each Connection and Composer Server automatically backs up the AD-LDS database locally every day at midnight to a text file that is kept for 7 days. To back up the AD-LDS database manually, you need to ensure that there are no operational desktop pool processes in progress such as a refresh, recompose, creation, or deletion of View desktop instances. For desktop pools that are autoprovisioning VMs based on min and max settings, for example, it is important to turn off the provisioning during the backup. To back up the AD-LDS database, complete the following steps:

1. Log in to the VMware View Administrator console by browsing to the URL `https://[FQDN of View Server]\admin`.
2. Expand the Inventory menu and select **Pools**.
3. Select each automated pool and right-click and select **Disable Provisioning**.
4. After you have verified that all operational activity has been temporarily disabled, you can run the AD-LDS database export utility. You can find this utility on the VMware View Server within `C:\Program Files\VMware\VMware View\Server\tools\bin`; it is called `vdmexport.exe`.

The tool exports the content in LDAP Data Interchange Format (LDIF), which is a text-based format for exchanging LDAP information. To run the tool, just execute the utility and redirect the content to a file with an `.ldf` extension. For example:

```
vdmexport.exe>Viewconfig.ldf
```

Although you learned how to here, doing this process manually is not very practical (and it is fully automated by View). You can, however, automate many of the processes within View. VMware provides VMware View PowerCLI cmdlets. When you install the View Connection Server, a View PowerCLI console is also installed. When you first run the View PowerCLI, though, you will receive errors because PowerShell's default settings restrict unsigned or untrusted scripts. To enable the scripts, open Windows PowerShell and follow this process:

1. To verify the current policy, type **Get-ExecutionPolicy**. You should see that the default setting is restricted.
2. To update the current policy, type **Set-ExecutionPolicy Unrestricted**.
3. When prompted, type **Y** to confirm that you want to update the policy.
4. To verify that the policy is now unrestricted, type **Get-ExecutionPolicy** one more time and you should see that it is now unrestricted.

You can now close the Windows PowerShell console and open the View PowerCLI console.

It is possible to disable provisioning using PowerCLI commands. To explain how, we provide an example, but this is not intended to be an extensive review of VMware View PowerCLI. For detailed information on the VMware View PowerCLI, refer to VMware's online documentation. In this example, we update an automated pool that has been created using View Composer. To update an automated Composer desktop pool, you will use the `Update-AutomaticLinkedClonePool` cmdlet. Because it is likely that you will have a variety of pool types, you want to ensure that you disable provisioning on the appropriate type and specific pool. You can specify a specific pool by providing the pool's unique ID, which is the name of

the pool within View (and not the display named presented to the users). In this example, we are disabling provisioning on an automated linked clone pool called `CALL_CENTER`:

```
Update-AutomaticLinkedClonePool -pool_id CALL_CENTER -isProvisioningEnabled $false
```

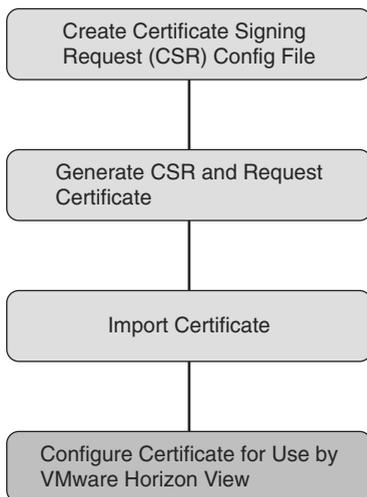
You can reenable provisioning by changing the value to `$true`, as shown in the following example:

```
Update-AutomaticLinkedClonePool -pool_id CALL_CENTER -isProvisioningEnabled $true
```

## Replacing Certificates

When you first install View, it uses self-signed certificates. VMware does not recommend that you use these in production. In a highly secure environment, updating certificates may be required on a regular basis as the certificates expire. This section covers how to replace certificates on the VMware View Server as well as the Composer and Security Server. A Transfer Server does not really use certificates, so replacing them would be of no net benefit.

At a high level, the process that you will follow is to create a Certificate Signing Request (CSR) config file that is used to generate the CSR to request a certificate. Once you receive the signed certificate you will import it and then configure View to use it. This process is outlined in Figure 7.34.



**Figure 7.34** Updating certificates

The first part of the process starts with creating a configuration file from which to generate the CSR, as shown in the example request.inf file. The Subject line contains the distinguished name and location of the View Server.

In addition, you can adjust the key length to increase the security of the certificate:

```
----- request.inf -----
[Version]
Signature="$Windows NT$"
[NewRequest]
Subject = "CN=demovw001.virtualguru.org, OU=IT, O=virtualguru,L=Newmarket,
S=Ontario, C=CA"
; Replace View_Server_FQDN with the FQDN of the View server.
; Replace the remaining Subject attributes.
KeySpec = 1
KeyLength = 2048
; KeyLength is usually chosen from 2048, 3072, or 4096. A KeyLength
; of 1024 is also supported, but it is not recommended.
Exportable = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication
-----
```

Create this file, adjust the appropriate values, and save it within a directory on the View Server (for example, c:\cert\request.inf).

After you have the input file, you can use the Microsoft Certificate Request Utility certreq.exe to generate the CSR using the following command syntax from within the directory (in our example, c:\cert):

```
certreq -new request.inf [output file]
```

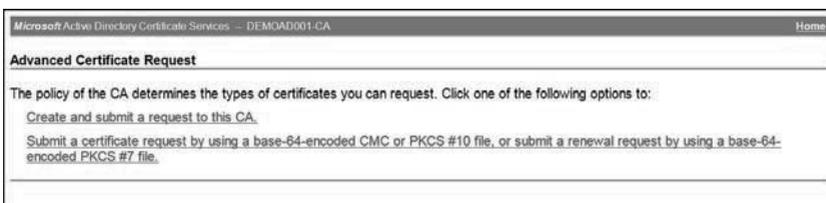
The utility will generate a CSR within the output file you specified. It is this file that you will submit to the third-party certificate authority (CA) to receive the certificate file. If you maintain your own Windows CA, you can create your own certificate internally. To continue our example, we will use a Microsoft CA.

From the Microsoft CA's website, select **Request a Certificate**, as shown in Figure 7.35.



**Figure 7.35** Requesting a certificate

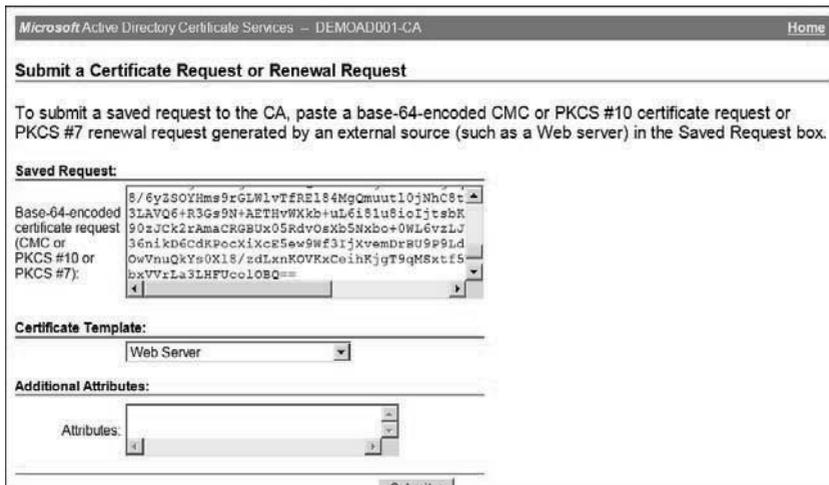
On the Advanced Certificate Request web page, submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file, as shown in Figure 7.36.



**Figure 7.36** Advanced certificate request

On the Request a Certificate web page, click the **Or, Submit an Advanced Certificate Request** link.

On the Submit a Certificate Request or Renewal Request web page, paste the contents of your CSR into the Saved Request window and select the drop-down under the Certificate Template heading and ensure that the Certificate Template being used is Web Server, as shown in Figure 7.37, and click **Submit**.



**Figure 7.37** Submitting a certificate request

On the Certificate Issued page, leave the default **Der Encoded**, and click the **Download Certificate** link. Ensure that you save the certificate on the View Server (in our example, back in the c:\cert directory).

To import the certificate to the View Server, you can use the certreq.exe utility by using the following command:

```
certreq.exe -accept [certificate name]
```

The utility imports the certificate, but View does not start using until you rename it. To rename it, follow these steps on the View Server. If you have multiple View Servers, you will need to run the process on each server:

1. Run an Management Console (MMC) by typing **MMC** in the Search Program and Files box from the Start menu of the View Server.
2. From the MMC console, select **File, Add/Remove Snap-In**.
3. Select **Certificates** from the Available Snap-Ins options and click **Add**.
4. When prompted for which account will be managed by the snap-in, select **Computer Account**, and then click **Finish**.
5. When prompted to select the computer, accept the default **Local Computer**, and then click **Finish** and **OK**.

6. From the MMC, expand **Certificates** and **Personal** and **Certificates**.
7. Right-click the original certificate and select **Properties** and rename to the friendly name **vdmold**.
8. Right-click the new certificate and select **Properties** and add a friendly name called **vdm** and restart the Connection Server.
9. After the reboot, log in to the Connection Server and ensure that under the Dashboard the System Health for the Connection or Security Server shows green, as shown in Figure 7.38.



**Figure 7.38** Verifying the certificate is accepted

## Composer and Certificates

The processes of replacing the certificate on the Composer Server is similar except that you do not need to change the common name but you do have to run the SviConfig utility to bind the updated certificate to the port that Composer uses. The syntax for the utility is as follows:

```
sviconfig -operation=ReplaceCertificate -delete=[false/true]
```

The false or true statement determines whether as part of the process the existing certificate is deleted. False prevents the deletion, and true deletes the certificate when the binding is updated.

## Summary

This chapter examined the operational steps in creating, configuring, and managing VMware pools. You looked at what it takes to perform backups of key View components and also replace and update the certificates. Although the steps here are important, they are no substitute for having a good operational process. This involves ensuring that you have predetermined operational windows, for example, so that you can do pool refreshes or rebalances and not impact end-user activity in the environment.

VMware View provides a set of tools that add a lot of capabilities, but it is up to you to integrate them in a way that minimizes disruptions. As with any hosted environment, disruptions to service are amplified in a large VMware View environment. A well-managed change management process for effecting change in your View environment goes a long way to ensuring that users have confidence in the solution and that it remains stable and provides good performance.

# Index

## Symbols

---

- 3D graphics, 294
- 3D graphics cards, 293

## A

---

- access groups, VMware View, 185-187
- Active Desktops Statistics, 391
- Active Directory
  - Horizon Mirage, 256
  - Workspace vApp, 124
- Active Directory computers, Create Computer Objects permission, 168
- Active Directory Lightweight Directory Service (AD LDS), 8
- AD LDS (Active Directory Lightweight Directory Service), 8, 19, 34
  - databases, backing up, 219
- adapter tuning, vCenter Operations for View, 386
- adding
  - data VAs, Administrator web page (Workspace), 245-246
  - SAML 2.0 Authenticator, 176-177
  - Security Servers, 97-99
  - VAs (virtual appliances) in Workspace, 63
  - VMDKs for storage, Workspace Data module, 149-151
- administration, Horizon Mirage, 265-268
  - application layers, 285-287
  - base layers, 269-272
  - collections, 283-284
  - deploying base layers, 272-273
  - driver libraries, 280-283
  - endpoint migration, 274-277
  - endpoint restoration, 268-269
  - file portal, 277-279
  - Horizon Mirage Web Management, 279-280
  - logs, 288
  - reports, 287-288
  - updating base layers, 273-274

- Administrator console, Workspace, 135
  - configuring CoS (Class of Service), 140-142
  - Data module, 135-137
  - integrating with VMware View, 142-144
  - launching View pools, 144-145
  - user entitlement, 138-140
- Administrator web page, Workspace, 229
  - adding data VAs, 245-246
  - auditing and tracking, 239-240
  - catalogs, 229, 233
  - Dashboard tab, 229-230
  - entitlement, 232-233
  - Horizon Files, 242-245
  - Mobile Profiles, 230
  - modules, 234
  - policies, 237
  - Policies tab, 230
  - removing users, 233
  - SAML, 237-239
  - system diagnostics, 246
  - ThinApp integration, 234-236
  - Users & Groups tab, 229-232
  - Workspace clients, 240-241
- Admission Control Policy, 66
- Adobe Flash settings, 206
- AirWatch, 17
- alerts
  - vCenter Operations for View, 391-393
  - VDI, 388
- analysis, design and architecture, 29-30
- Analytics VM, 380
- Android, Workspace Client, 153-156
- application layers, Horizon Mirage, 285-287
- application-level reports, Horizon Mirage, 288

- applications, legacy applications, 163
- architecture
  - Horizon Mirage, 256
  - VMware
    - local mode VMs, 38
    - View Connection Server, 34
    - View Replica Server, 34
    - View Security Server, 35-37
    - View Transfer Server, 39-40
  - VMware View, 50
    - analysis, 29-30
    - calculating, 30-32
    - design, 32
    - requirements gathering and assessment, 28
  - Workspace, 53
    - authentication, 58
    - certificates, 60-62
    - external storage, 62-65
    - IP pools, 55
    - network services, 55-56
    - NTP (Network Time Protocol), 57
    - planning, 54
    - Postgres availability, 67-71
    - Postgres clusters, 71-74
    - PostgreSQL, 65-66
    - SMTP (Simple Mail Transfer Protocol), 62
- audio, bandwidth (PCoIP), 317
- audio quality, PCoIP, 316
- auditing Administrator web page, Workspace, 239-240
- authentication
  - design and architecture, Workspace, 58
  - SAML authentication, 174
- automated desktop pools, 188

**B**

backing up  
 AD LDS databases, 219  
 virtual desktops, 218-221

ballooning, 65

bandwidth, 49, 303  
 audio, PCoIP, 317

bandwidth utilization, PCoIP, 320

Base DN (distinguished name), Active Directory, 126

base layer dry-run reports, Horizon Mirage, 287

base layers, Horizon Mirage, 269-272  
 deploying, 272-273  
 updating, 273-274

baselines, performance baselines, 363-364

bind DN, Active Directory, 126

branch reflectors, Horizon Mirage, 16, 23, 252

broker agents, vCops, 383-384  
 configuring, 384-386

BTL (build-to-lossless), 50

Build-to-Lossless feature, 313

**C**

calculating design and architecture, 30-32

catalogs, Administrator web page (Workspace), 229, 233  
 end-user service catalogs, 2-3

CBRC (Content-Based Read Cache), 193

centralization process, 268

centralized virtual desktop (CVD), 1, 252

certificate errors, troubleshooting, 174-176

certificate notification, Workspace Client, 155

certificate templates, creating in VMware View, 105-111

Certificate Wizard, 350

certificates  
 Composer Server, 225  
 design and architecture, Workspace, 60-62  
 private, 61  
 renaming View Servers, 224  
 requesting, 223  
 self-signed, 61  
 SSL, Workspace, 156-158  
 VMware View, 103-105  
 creating certificate templates, 105-111  
 replacing, 221-225

change, perception of, 291

check-in process, VMware View, 41

checklist for installing VMware View, 79-80

check-out process, VMware View, 40

CIFS (Common Internet File System), 256

client desktop, 327

client software, installing Liquidware Labs Stratusphere UX, 374

clients, View clients (Microsoft Lync 2013), 357

clusters, Postgres clusters (Workspace), 71-74

collection intervals, vCenter Operations for View, 386

collections, Horizon Mirage, 283-284

Common Internet File System (CIFS), 256

components, Horizon Mirage, 251-253

Composer Server, certificates, 225

compression, 301

computer accounts, 207

configuration  
 View Composer, 206-207  
 View Connection Server, 85-88

configurator VA, 25, 114, 152

- configurator virtual appliance, certificates, 61
- configurator virtual appliance information, 121
- configuring
  - ESXi for sVGA, 296-297
  - View Replica Server, 92
  - VMware View Servers, 107
  - WANem, 305-308
  - Wireshark, 309-312
  - Workspace vApp, 120-122
- Connection Latency, PCoIP, 321
- Connection Server
  - installing, 82
  - load balancing, 34
  - View, 85-88
- Connection Server pods, 8
- connector VA, 25, 114
- Content-Based Read Cache (CBRC), 193
- CoS (Class of Service), Workspace Administrator console, 140-142
- Create Computer Objects permission, 168
- CVD (centralized virtual desktop), 1, 252
- CVD Integrity report, Horizon Mirage, 288
- CVD policy, Horizon Mirage, 263

## D

---

- DaaS (desktop-as-a-service), 4
- Dashboard tab, Administrator web page (Workspace), 229-230
- dashboards
  - Manage Authenticators, 177-179
  - vCenter Operations for View, 387-391
  - View Adapter Status dashboard, 391
  - View Desktop Sessions dashboard, 390
  - View Main dashboard, 387
  - View Pools dashboard, 389
  - View Top Desktop VMs dashboard, 389
  - View Top Sessions, 388
  - View Users dashboard, 388
- data collection, 368, 386
- data compression, 50
- data module, 134
  - Workspace Administrator console, 135-137
- Data module storage (Workspace), modifying, 148
  - adding VMDKs, 149-151
- data VAs, 25, 114-116
  - Administrator web page, Workspace, 245-246
- database permissions, Horizon Mirage, 255
- database software, Horizon Mirage, 255
- databases
  - AD LDS, backing up, 219
  - Event Database, 93-94
- datastores, linked clones, 216
- DDV (Distributed Desktop Virtualization), 14
- Delegation of Authentication to VMware, 175
- demilitarized zone. *See* DMZ
- deploying
  - base layers, Horizon Mirage, 272-273
  - Horizon Mirage Management Server, 257-263
  - Horizon View, considerations for, 76-77
  - VMware View, 4-12
    - considerations for, 76-78
  - Workspace vApp, 118-120
    - initial configuration, 120-122
    - security exception, 123-133
    - Workspace Setup Wizard, 122
- deployment
  - OVF deployment, 365
  - VMware View and Workspace, scaling, 179-182

- Workspace, 113-115
- Workspace Pod, 182
- design and architecture
  - Horizon View, considerations for, 77
  - VMware View, considerations for, 76-78
  - Workspace, 53, 113-115
    - authentication, 58
    - certificates, 60-62
    - external storage, 62-65
    - IP pools, 55
    - network services, 55-56
    - NTP (Network Time Protocol), 57
    - planning, 54
    - Postgres availability, 67-71
    - Postgres clusters, 71-74
    - PostgreSQL, 65-66
    - SMTP (Simple Mail Transfer Protocol), 62
- desktop, client desktop, 327
- desktop-as-a-service (DaaS), 4
- desktop pools, 185-187
  - automated, 188
  - creating, 189-196
  - manual, 188
  - refresh, 214
  - VMware View, 43
- desktops
  - replicas, 208
  - View desktops, Microsoft Lync 2013, 355-356
- DHCP (Dynamic Host Control Protocol), 119
- disk digest files, 193
- disk space
  - Liquidware Labs Stratusphere, 371
  - reclaiming, 196
- disks, View Composer, 207

- Distributed Desktop Virtualization (DDV), 14
- Distributed Resource Services (DRS), 6
- DMZ (demilitarized zone), 19, 35, 119
- DNS (Domain Name System), 115, 368
- domains
  - multidomain environments, View integration, 171
  - VMware View, 169
- driver libraries, Horizon Mirage, 280-283
- DRS (Distributed Resource Services), 6
- dynamic collections, Horizon mirage, 284
- Dynamic Host Protocol (DHCP), 119

## E

- endpoint migration, Horizon Mirage, 274-277
- endpoint restoration, Horizon Mirage, 268-269
- endpoints, rebooting, 266
- end-user computing (EUC), 2
- end-user license agreement (EULA), 372
- end-user service catalogs, 2-3
- enterprise pools, 339
- entitlement, 2
  - Administrator web page, Workspace, 232-233
  - VMware View, 213
    - refresh, 214-215
    - replicas, 214
- entitlements
  - VMware, rebalance, 216
  - VMware View, recompose, 215
- environment software, Horizon Mirage, 254
- environmental hardware, Horizon Mirage, 253
- environments, scaling in view, 7

**ESXi**, 294

- configuring for sVGA, 296-297

- EUC (end-user computing), 2

- EULA (end-user license agreement), 372

- Event Database, 93-94

- external dependencies, Horizon Mirage, 256

- external file-sharing workflow, 138

- external storage, design and architecture (Workspace), 62-65

**F**

- file portals, Horizon Mirage, 253, 277-279

- firewall rules, VMware View, 96-97

- floating desktops, 47

- floating pools, 188

- folders, VMware View, 187

- FPS (frames per second), 315

- FQDN (Fully Qualified Domain Name), 89, 167

- frames per second (FPS), 315

- Fully Qualified Domain Name (FQDN), 89, 167

**G**

- gateway VA, 25, 114-117

- GPU (graphics processing unit), 6

- Graphics, video support, 6

- graphics processing unit (GPU), 6

- graphs, PCoIP, 321-323

- grep cpuinfo, 68

- grep meminfo, 69

- Group Policy Management tool, 198

- Group Policy Objects, creating, 198-199

**H**

- HA (high authority), 65-66

- hairpinning, VoIP, 330

- HCL (hardware compatibility list), 17

- HHDs (host hard drives), 13

- Hirstius, Chuck, 303

- Horizon Files, Administrator web page (Workspace), 242-245

- Horizon Mirage, 249

  - Active Directory, 256

  - administration, 265-268

    - application layers, 285-287

    - base layers, 269-272

    - collections, 283-284

    - deploying base layers, 272-273

    - driver libraries, 280-283

    - endpoint migration, 274-277

    - endpoint restoration, 268-269

    - file portal, 277-279

    - Horizon Mirage Web Management, 279-280

    - logs, 288

    - reports, 287-288

    - updating base layers, 273-274

  - CVD, 252

  - CVD policy, 263

  - database permissions, 255

  - database software, 255

  - deployment and design considerations, 249-250

    - architecture, 256

    - components, 251-253

    - external dependencies, 256

    - Horizon Mirage Servers, 264

    - Mirage Management Server, 257-263

    - planning, 251

- prerequisites, 253-255
- storage considerations, 256
- environment software, 254
- environmental hardware, 253
- ports, 255
- reference CVD, 271
- reference machine, 255, 270
- SQL Server, 256
- Horizon Mirage branch reflectors, 252
- Horizon Mirage Client, 254
- Horizon Mirage file portal, 253
- Horizon Mirage Management Console, 251-254
- Horizon Mirage Management Server, 251, 254
  - deploying, 257-263
- Horizon Mirage reference machine, 252
- Horizon Mirage Server, 251, 254, 264
- Horizon Mirage Web Management, 251, 254, 279-280
- Horizon Mobile Management, 25
- Horizon Mobile Manager, 24
- Horizon View
  - certificates, creating certificate templates, 108
  - deployment and design considerations, 77
  - Event Database, 93
- host hard drives (HHDs), 13
- hypervisor swapping, 65

---

## I

- IANA (Internet Assigned Numbers Authority), 48
- identity provider (IDP), 237
- IDP (identity provider), 237
- input/output operations per second (IOPS), 11

## installing

- Connection Server, 82
- Microsoft Lync 2013, 339-343
- Microsoft VDI plug-in, 357
- Mirage Client, 265
- Security Servers, 98
- View Client, 101-103
- VMware View, 80-85
  - checklist, 79-80
  - Connection Server, 82
  - Windows Server, 84
- VMware View Agent, 99
  - View Agent custom setup options, 100-101
- VMware View Composer on vCenter, 87
- WANem, 305-308
- Wireshark, 309-312

## integrating

- ThinApp, Administrator web page (Workspace), 234-236
- VMware View and Workspace, 165-173
  - considerations for, 163-164
  - troubleshooting certificate errors, 174-176

- Internet Assigned Numbers Authority (IANA), 48

- IOPS (input/output operations per second), 11, 193

- IP addresses, Workspace vApp, 119

- IP pools

- design and architecture, Workspace, 55
- Workspace Gateway, 117

- iPad, Workspace Client, 153-156

---

## J

- Java server restart, Workspace vApp, 132
- Jitter, 303

**K**

Knoppix ISO, 306  
KPI (key performance indicator), 370

**L**

La Cita Collegiale, 295  
latency, 303  
launching View pools from Workspace, 144-145  
LDIF (LDAP Data Interchange Format), 220  
legacy applications, 163  
legacy PC gap, 163  
libraries, driver libraries (Horizon Mirage), 280-283  
linked clones, 214

- creating, 208
- datastores, 216
- decreasing size of, 214-215

Liquidware Labs Stratusphere UX, 362, 369-374

- client software installation, 374
- disk space, 371
- hubs, 371
- metrics, 375-376
- time synchronization, 372

load, PCoIP, 323-324  
load balancing, Connection Server, 34  
local mode VMs, 38  
logical unit numbers (LUNs), 364  
logs, Horizon Mirage, 288  
lossless compression, 301  
lossless data compression, 50  
lossy compression, 301  
lossy data compression, 50

LUNs (logical unit numbers), 364  
Lync Server 2013 Deployment Wizard, 339  
Lync Server Topology Builder, 343-352  
Lync topology, publishing and building, 343-352

**M**

MAM (Mobile Access Management), 25  
Manage Authenticators, 177

- dashboard, 177-179
- SAML 2.0 Authenticator, 177

Management Console, Horizon Mirage, 254  
manual desktop pools, 188  
MDM (mobile device management), 25, 229  
media redirection, Microsoft Lync 2013, 355  
memory compression, 65  
metrics

- Stratusphere UX, 375-376
- vCenter Operations for View, 393-394

Microsoft Lync 2013, 329, 331-332

- installing, 339-343
- Lync Server Topology Builder, 343-352
- media redirection, 355
- .NET Framework 3.5, 335-339
- preparing for, 332-334
- testing, 352-355
- users, setting up, 352-355
- verifying you have all prerequisites, 335
- View clients, 357
- View desktops, 355-356
- Windows 2012, 335-339

Microsoft Management Console (MMC), certificate templates, 105  
Microsoft VDI plug-in, installing, 357  
migrating endpoints, Horizon Mirage, 274-277

- Mirage, 1, 4, 14-17
    - branch reflectors, 16, 23
    - overview, 21-23
  - Mirage Client
    - installing, 265
    - Pending Devices, 267
    - upgrading, 267
  - Mirage Server, 22
  - MMC (Microsoft Management Console), certificate templates, 105
  - MMR (multimedia redirection), 330
  - Mobile Access Management (MAM), 25
  - mobile apps, 134
  - Mobile Device Management (MDM), 25, 229
  - mobile management, 134
  - Mobile Profiles, Administrator web page (Mobile Profiles), 230
  - Mobile Virtual Platform (MVP), 17
  - modifying workspace Data module storage, 148
    - adding VMDKs, 149-151
  - modules
    - Administrator web page, Workspace, 234
    - security exceptions, Workspace vApp, 134
  - monitoring View Adapter performance, 386
  - multidomain environments, View integration, 171
  - multimedia
    - delivering a rich end-user experience, 292-294
    - PCoIP, 300-302
      - bandwidth utilization, 320
      - Connection Latency, 321
      - Connection Quality, 320
      - encoding graphs, 321-323
      - load, 323-324
      - packet counts, 320
      - third-party tools, 318-319
      - tuning, 312-313
      - tuning, parameters, 313-318
    - performance test environment, 302-305
    - sVGA, configuring ESXi for, 296-297
    - vDGA (virtual direct graphics acceleration), 300
    - VMware View with vSGA, 298-300
    - vSGA (virtual shared graphics acceleration), 295-296
    - WANem, installing and configuring, 305-308
    - Wireshark, installing and configuring, 309-312
  - multimedia redirection (MMR), 330
  - multitenant, 58
  - MVP (Mobile Virtual Platform), 17
- 
- ## N
- 
- NAS (network-attached storage), 63, 256
  - .NET Framework 3.5, Microsoft Lync 2013, 335-339
  - Network Filesystem Storage (NFS), 63
  - network mapping, Workspace vApp, 119
  - network services, design and architecture (Workspace), 55-56
  - Network Time Protocol. *See* NTP
  - NFS (Network Filesystem Storage), 63
    - Workspace, 152-153
  - Non-trusted external certificate authority, SSL certificates, 158
  - NTP (Network Time Protocol), 120, 368
    - design and architecture, Workspace, 57
  - NVIDIA, 295-296

**O**

OEM (original equipment manufacturer), 300  
 OS disks, VMs (virtual machines), 215  
 OS X, Workspace Client, 153-156  
 OVA deployment, 118  
 OVF deployment, 365

**P**

packages, ThinApp, 226  
 packet counts, PCoIP, 320  
 packet delay variation (PDV), 303  
 packet loss, 303  
 parameters, tuning (PCoIP), 313-318  
 Password authentication, 238  
 PBX (private branch exchange), 330  
 PC over IP (PCoIP), 48  
 PCoIP, 292, 300-302
 

- bandwidth utilization, 320
- Connection Latency, 321
- Connection Quality, 320
- encoding graphs, 321-323
- firewall rules, 97
- load, 323-324
- packet counts, 320
- parameters, tuning, 313-318
- QoS, 50
- templates, 312
- third-party tools, 318-319
- tuning, 312-313
- VMware View, 48-50

 PCoIP Connection Quality graph, 320  
 PCoIP Encoder, 322  
 PCoIP Encoder Stats, 322  
 PCoIP Log Viewer, 303, 318-319  
 PCoIP Packet Counts, 320

PCoIP (PC over IP), 48-50  
 PCoIP Server services, 319  
 PDV (packet delay variation), 303  
 Pending Devices, Mirage Client, 267  
 perception of change, 291  
 performance, monitoring (View Adapter), 386  
 performance baselines, 363-364  
 performance monitoring solutions, 362
 

- Liquidware Labs Stratusphere UX, 362, 369-374
  - client software installation, 374
  - disk space, 371
  - hubs, 371
  - metrics, 375-376
  - time synchronization, 372
- performance baselines, 363-364
- vCenter Operations Management (vCOps), 362
- vCOps, 377-379
  - Xangati VDI dashboard, 362-369

 performance test environment, 302-305  
 permissions
 

- databases, Horizon Mirage, 255
- persistent disks, 218

 persistent disks, managing, 216-218  
 Persona Management, VMware View, 47  
 planning
 

- design and architecture, Workspace, 54
- Horizon Mirage deployment and design, 251
- for VMware View, considerations, 77

 plug-ins
 

- Microsoft VDI, installing, 357
- verifying, 358-359

 PoC (proof of concept), 28  
 pods, Connection Server pods, 8  
 policies, Administrator web page (Workspace), 237

Policies tab, Administrator web page (Workspace), 230

Pool Settings, VMware View, 200-205

pools, 43

- desktop, 187-189
  - creating, 189-196
  - desktop pools, 185
  - refresh, 214
- enterprise pools, 339
- floating pools, 188
- IP pools, Workspace, 55
- RDS desktop pools, 189
- settings, 197-198
- standard pools, 339
- View pools, synchronizing, 171

port requirements, Security Server, 37

ports, Horizon Mirage, 255

Postgres availability, design and architecture (Workspace), 67-71

Postgres clusters, design and architecture (Workspace), 71-74

PostgreSQL, design and architecture (Workspace), 65-66

postgresql.conf, 69

power options, VMware View, 197-200

preparing for Microsoft Lync 2013, 332-334

prerequisites

- Horizon Mirage, 253-255
- for Microsoft Lync 2013, 335

private branch exchange (PBX), 330

private certificates, 61

Program Executable (PE)-level report, Horizon Mirage, 288

proof of concept (PoC), 28

provisioning settings, VMware View, 211-212

public file sharing, 137

publishing Lync Topology, 343-352

## Q

---

QoS (Quality of Service), PCoIP, 50

Quality Table, 322

QuickPrep, 212

## R

---

RAID penalties, View, 11

RDS desktop pools, 189

RDSH (Remote Desktop Session Host), 229

rebalancing, 216

rebooting endpoints, 266

reclaim disk space option, 195

reclaiming

- disk space, 196
- storage, View, 13

recompose, VMware View, 215

reference CVD, Horizon Mirage, 271

reference machines, Horizon Mirage, 252-255, 270

refresh

- View Composer, 214-215
- VMware View, 214-215

relays, setting up on Workspace or Exchange, 62

Remote Desktop Session Host (RDSH), 229

Remote Graphics Software (RGS), 300

removing users, Administrator web page (Workspace), 233

renaming certificates, View Servers, 224

replacing certificates, VMware View, 221-225

Replica Server, 34

replicas

- View Composer, 208
- VMware View, 214

replication, VMware View, 41

## reports

- Horizon Mirage, 287-288
- UX inspector reports, 377
- requesting certificates, 223
- restoring endpoints, Horizon Mirage, 268-269
- RGS (Remote Graphics Software), 300
- rich end-user experiences, delivering, 292-294
- Roles and Features Wizard, 336
- rollback, VMware View, 42
- RTC objects, 346

**S**

- SaaS, Workspace, 145-148
- SAML (Security Assertion Markup Language), 134
  - Administrator web page, Workspace, 237-239
- SAML 2.0 Authenticator, 177
  - adding, 176-177
- SAML authentication, 174
- SAN (storage-area network), 13, 193, 364
- scaling
  - environments, View, 7
  - VMware View and Workspace deployment, 179-182
- Security Assertion Markup Language. *See* SAML
- security exception, Workspace vApp, 123-133
- Security Server port requirements, 37
- Security Servers
  - adding, 97-99
  - installing, 98
  - VMware View, 95
- self-signed certificates, example, 61

## servers

- Horizon Mirage Management Servers, 251, 264
  - deploying, 257-263
- local mode VMs, 38
- Mirage Server, 22
- Security Servers, 98-99
  - adding, 97
  - installing, 98
  - VMware View, 95
- vCenter servers, 8, 89-91
- View Connection Servers, 8, 19, 34, 85-88
- View Replica Server, 34
  - configuring, 92
- View Security Server, 19, 35-37
- View Transfer Server, 20, 39-40
- VMware
  - check-in process, 41
  - check-out process, 40
  - desktop pools, 43
  - PCoIP, 48-50
  - Persona Management, 47
  - replication, 41
  - rollback, 42
  - View Composer, 44-46
- VMware View Servers, 33
  - configuring, 107
- Windows Server, services, 84
- service catalogs, 2-3
  - Mirage, 4
  - VMware View, 3
  - Workspace, 4
- service VA, 25, 114-116
- services, Windows Server, 84
- Session Initiation Protocol (SIP), 334
- shuffling virtual desktop environments, 330
- Simple Mail Transfer Protocol (SMTP), 62

Simple Network Management Protocol (SNMP), 391

single-instance store (SiS), 252

SIP (Session Initiation Protocol), 334

SiS (single-instance store), 252

SMTP (Simple Mail Transfer Protocol), Workspace, 62

SNMP (Simple Network Management Protocol), 391

Soft 3D, 6

software rendering, 292-294

solid-state drives (SSDs), 11

SQL Server, Horizon Mirage, 256

SSDs (solid-state drives), 11

SSL certificates, Workspace, 156-158

SSL offload, 56

standard pools, 339

stateful desktops, 31-32

- backing up View, 218

stateless desktops, 13, 219

storage

- external storage, Workspace, 62-65
- reclaiming, 13
- vCenter settings, 210

storage-area network (SAN), 13, 193, 364

storage considerations, Horizon Mirage, 256

storage report, Horizon Mirage, 287

storage sizing, View, 11

storage vendors, VMware view, 11

Stratusphere Sizing Guide, 371

SUSE, verifying hardware changes, 68

SVGA (Super Video Graphics Array), 6

- configuring ESXi for, 296-297

swap to host cache, 65

switches, 305

synchronization, Workspace vApp, 129

synchronizing View pools, 171

SysPrep, 212

system diagnostics, Administrator web page (Workspace), 246

System Diagnostics page, Workspace, 246

System Info link, Dashboard tab, 230

## T

tail drop, 50

tarball format, 304

templates

- certificate templates, creating
  - Horizon View, 105
  - VMware View, 106-111
- PCoIP, 312

Teradici, 48

Teradici APEX 2800 Server Offload Card, 294

testing Microsoft Lync 2013, 352-355

ThinApp, Administrator web page (Workspace), 234-236

ThinApp packages, 134, 226

third-party CA, SSL certificates, 157

third-party tools, PCoIP, 318-319

time synchronization, Liquidware Labs Stratusphere UX, 372

tools, Group Policy Management tool, 198

TPS (transparent page sharing), 65

tracking Administrator web page, Workspace, 239-240

Trango, 17

transaction logs, Horizon Mirage, 288

Transfer Server, 39-40

transparent page sharing (TPS), 65

troubleshooting certificate errors, 174-176

tuning

- adapters, vCenter Operations for View, 386
- PCoIP, 312-313
  - parameters, 313-318

**U**

UDP (User Datagram Protocol), 48, 301

UI VM, 380

updating base layers, Horizon Mirage,  
273-274

upgrading

Mirage Client, 267

Workspace, 152

UPN (user principal name), 169

use-case scenarios, considerations when  
deploying VMware View, 76

user attributes mapping, Workspace  
vApp, 127

User Datagram Protocol (UDP), 48, 301

user entitlement, Workspace Administrator  
console, 138-140

user principal name (UPN), 169

user segmentation, architecture and  
design, 29

users

removing from Administrator web page  
(Workspace), 233

rich end-user experiences, delivering,  
292-294

setting up in Microsoft Lync 2013,  
352-355

Users & Groups tab, Administrator web  
page (Workspace), 229-232

USMT (User State Migration Tool), 263

UX inspector reports, 377

**V**

V4V adapter, 382

vApp, 116, 380

vCenter Operations for View

adapter tuning, 386

alerting, 391-393

dashboards, 387-391

metrics, 393-394

vCOps for View Adapter, 380-383

vCOps for View Broker Agent, 383-384  
configuring, 384-386

vApp appliances, Workspace, 115

VAs (virtual appliances), Workspace, 24-25,  
53-54

adding, 63

vCenter, installing (View Composer), 87

vCenter Operations, 364

vCenter Operations for View, 378

adapter tuning, 386

alerting, 391-393

dashboards, 387-391

metrics, 393-394

vCenter Operations Management.

*See* vCOps

vCenter Operations Manager

Advanced, 378

vCenter Operations Manager

Enterprise, 378

vCenter Operations Manager for View, 378

vCenter Operations Manager VMs, 378

vCenter Operations Server, 379

vCenter Servers, 8

adding, 89-91

vCenter settings, VMware View, 209-211

vCOps (vCenter Operations Management),  
362, 377-379

performance baselines, 364

vApp, 380

configuring vCOps Manager for View  
Broker Agent, 384-386

installing vCOps for View Broker  
Agent, 383-384

- vCenter Operation for View, adapter tuning, 386
- vCenter Operation for View, alerting, 391-393
- vCenter Operation for View, dashboards, 387-391
- vCenter Operation for View, metrics, 393-394
- vCOPS for View Adapter, 380-383
  - workflow, 379
- vCOPS for View Adapter, 380-383
- vCOPS for View Broker Agent, 383-384
  - configuring, 384-386
- vDGA (virtual direct graphics acceleration), 6, 300
- VDI (virtual desktop infrastructure), 2, 28, 76, 330
- VDI alerts, 388
- VDI Environment Indicators, 387
- VDI Health Tree, 388
- VDI Tier Health, 388
- VDM (Virtual Desktop Manager), 300
- verifying
  - plug-ins, 358-359
    - SUSE recognizes hardware changes, 68
- VIB (vSphere installation bundle), 297
- video support, 6
- view
  - scaling environments, 7
  - storage, reclaiming, 13
- View Adapter, 378
  - monitoring performance, 386
- View Adapter Status dashboard, 391
- View Agent custom setup options, 100-101
- View Blast, 7
- View blocks, 8
- View Client
  - installing, 101-103
    - Microsoft Lync 2013, 357
- View Composer, 13, 21
  - configuring, 206
  - disks, 207
  - refresh, 214-215
  - replicas, 208
  - VMware View, 44-46
- View Connection Server, 19, 34
  - configuring, 85-88
- View Connection servers, 8
- View desktops, 8-9, 12
  - Microsoft Lync 2013, 355-356
- View Desktop Sessions dashboard, 390
- view events collection, vCenter Operations for View, 386
- View Main dashboard, 387
- View Planner, 302, 323-327
- View Pool Statistics, 390
- View pools, 134
  - launching from Workspace, 144-145
  - synchronizing, 171
- View Pools dashboard, 389
- View PowerCLI, 220
- View Replica Server, 34
  - configuring, 92
- View Security Server, 19, 35-37
- View Servers, renaming certificates, 224
- View Top Desktop VMs dashboard, 389
- View Top Sessions dashboard, 388
- View Transfer Server, 20, 39-40
- View Users dashboard, 388
- virtual appliances. *See* VAs
- virtual desktop environments, shuffling, 330
- virtual desktop infrastructure (VDI), 2, 28, 76, 330

Virtual Desktop Manager (VDM), 300

virtual desktops, 12

- backing up, 218-221

- rebalancing, 216

- reducing size, 214-215

- replicas, 208

virtual direct graphics acceleration (vDGA), 6, 300

virtual machine. *See* VMs

Virtual SAN, 13-14

virtual Shared Graphics Acceleration (vSGA), 6, 295

virtual storage acceleration (VSA), 12

VM disks (VMDKs), 148

VM monitoring, 66

VMDKs (virtual hard drives), 62, 148, 193

- adding for storage, Workspace Data module, 149-151

VMotion, 6

VMs (virtual machines), 1

- Analytics VM, 380

- OS disks, 215

- UI VM, 380

VMware

- certificates, replacing, 221-225

- entitlements, rebalance, 216

VMware Horizon View Connection Server, 84

VMware Horizon View Framework Component, 84

VMware Horizon View Message Bus Component, 84

VMware Horizon View PCoIP Secure Gateway, 84

VMware Horizon View Script Host, 85

VMware Horizon View Security Gateway Component, 85

VMware Horizon View Web Component, 85

VMware Mirage. *See* Horizon Mirage

VMware View, 1

- access groups, 185-187

- architecture, 50

- backing up, 218-221

- certificates, 103-105

  - creating certificate templates, 105-111

- Composer, 206-208, 214-215

- deploying, 4-12

- deployment and design considerations, 76-78

- design and architecture

  - analysis, 29-30

  - calculating, 30-32

  - design, 32

  - requirements gathering and assessment, 28

- desktop pools, 187-189

  - creating, 189-196

- domains, 169

- entitlement, 213

  - refresh, 214-215

  - replicas, 214

- entitlements, recompose, 215

- Event Database, 93-94

- firewall rules, 96-97

- folders, 187

- installing, 80-85

  - checklist, 79-80

  - Connection Server, 82

  - Windows Server, 84

- integrating with Workspace, 142-144, 165-173

  - considerations for, 163-164

  - troubleshooting certificate errors, 174-176

- overview, 18-21

- persistent disks, 216-218

- Pool Settings, 200-205

- power options, 197-200
  - provisioning settings, 211-212
  - QuickPrep, 212
  - RAID penalties, 11
  - scaling deployment, 179-182
  - Security Servers, 95
    - adding, 97-99
  - servers, 33
    - check-in process, 41
    - check-out process, 40
    - desktop pools, 43
    - local mode VMs, 38
    - PCoIP, 48-50
    - Persona Management, 47
    - replication, 41
    - rollback, 42
    - View Composer, 44-46
    - View Connection Server, 34
    - View Replica Server, 34
    - View Security Server, 35-37
    - View Transfer Server, 39-40
  - service catalogs, 3
  - stateless desktops, 13
  - storage sizing, 11
  - storage vendors, 11
  - SysPrep, 212
  - vCenter settings, 209-211
  - vCOPs, 377
  - with vSGA, 298-300
  - VMware View Agent, installing, 99
    - View Agent custom setup options, 100-101
  - VMware View Blast Secure Gateway, 84
  - VMware View Composer, installing on vCenter, 87
  - VMware View Composer Guest Agent Server, 208
  - VMware View Planner, 325-327
  - VMware View Servers, configuring, 107
  - VMware Workspace. *See* Workspace
  - VMware Workspace FQDN, 60
  - VMwareVDMDS, 85
  - VoIP, 329-330
    - hairpinning, 330
  - vPostgres virtual appliance, 67-68
  - VSA (virtual storage acceleration), 12
  - vSGA (virtual shared graphics acceleration), 6, 293-296
    - VMware View, 298-300
  - vSphere Flash Read Cache, 13
  - vSphere HA, 65-66
  - vSphere installation bundle (VIB), 297
  - vSwitch, 304
- 
- ## W
- WAL (Write Ahead Log), 67
  - WAN (wide area networks), 49
  - WANem, 302-304
    - installing and configuring, 305-308
  - Wanova, 1
  - Web Applications, Workspace, 145-148
  - Web apps, 134
  - Web Management console, Horizon Mirage, 279
  - Weighted Random Early Detection (WRED), 51
  - Windows, Workspace Client, 153-156
  - Windows 2012, Microsoft Lync 2013, 335-339
  - Windows AERO, 293
  - Windows Server, services, 84
  - Wireshark, 303
    - installing and configuring, 309-312

## wizards

- Certificate Wizard, 350
- Lync Server 2013 Deployment Wizard, 339
- Roles and Features Wizard, 336
- Workspace Client Wizard, 155
- Workspace Setup Wizard, 122

## Workflow, vCOps, 379

## Workplace, 18

## Workspace, 17

- Administrator console, 135
  - configuring CoS (Class of Service), 140-142
  - Data module, 135-137
  - integrating with VMware View, 142-144
  - launching View pools, 144-145
  - user entitlement, 138-140
- Administrator web page, 229
  - adding data VAs, 245-246
  - auditing and tracking, 239-240
  - catalogs, 229, 233
  - Dashboard tab, 229-230
  - entitlement, 232-233
  - Horizon Files, 242-245
  - Mobile Profiles, 230
  - modules, 234
  - policies, 237
  - Policies tab, 230
  - removing users, 233
  - SAML, 237-239
  - system diagnostics, 246
  - ThinApp integration, 234-236
  - Users & Groups tab, 229-232
  - Workspace clients, 240-241

deployment and design considerations, 113-115

## design and architecture, 53

- authentication, 58
- certificates, 60-62
- external storage, 62-65
- IP pools, 55
- network services, 55-56
- NTP (Network Time Protocol), 57
- planning, 54
- Postgres availability, 67-71
- Postgres clusters, 71-74
- PostgreSQL, 65-66
- SMTP (Simple Mail Transfer Protocol), 62

## implementation

- vApp appliances, 115
- Workspace Configurator VA, 116
- Workspace Connector, 116
- Workspace Data, 116
- Workspace Gateway, 116-117
- Workspace Service VA, 116

## integrating with VMware View, 165-173

- considerations for, 163-164
- troubleshooting certificate errors, 174-176

## modifying Data module storage, 148

- adding VMDKs, 149-151

## NFS, 152-153

## overview, 24-25

## scaling deployment, 179-182

## service catalogs, 4

## SSL certificates, 156-158

## upgrading, 152

## VAs (virtual appliances), 25, 53-54

## Web Applications, 145-148

## Workspace Client

Administrator web page, Workspace, 240-241

Windows/OS X/iPad/Android deployment, 153-156

- Workspace Client certificate notification, 155
- Workspace Client Wizard, 155
- Workspace configurator, 114
- Workspace Configurator VA, 116
- Workspace Connector, 114-116
- Workspace Data, 114-116
- Workspace Gateway, 114-117
- Workspace Manager, 114
- Workspace Pod, deployment, 182
- Workspace Service VA, 116
- Workspace Setup Wizard, 122
- Workspace vApp, 116
  - deploying, 118-120
    - initial configuration, 120-122
    - security exception, 123-133
    - Workspace Setup Wizard, 122
- WRED (Weighted Random Early Detection), 51
- Write Ahead Log (WAL), 67

## **X-Y-Z**

---

- Xangati Flow Summarizer (XFS), 369
- Xangati GUI login, 366
- Xangati VDI dashboard, 362-369
- XenApp, 134
- X-Forwarded-For, Workspace gateway, 132
- XFS (Xangati Flow Summarizer), 369