vmware PRESS

Official Cert Guide

Learn, prepare, and practice for exam success

- Master the VCP5-DT exam with this official study guide
- Assess your knowledge with chapter-opening quizzes
- Review key concepts with Exam Preparation Tasks
- Practice with realistic exam questions on the CD-ROM

VCP5-DT

VMware® Certified Professional - Desktop

PEARSON

LINUS BOURQUE

VCP5-DT
Official Cert Guide

Official Cert Guide
The Official VCP5 Certification Guide
VMware Certified Professional on vSphere 5
BILL FERGUSON
PEARSON
Automating vSphere with VMware vCenter Orchestrator
TECHNOLOGY HANDS-ON
Cody Bunch
Administering VMware Site Recovery Manager 5.0
TECHNOLOGY HANDS-ON
Mike Laverick
Storage Implementation in vSphere 5.0
TECHNOLOGY DEEP DIVE
Mostafa Khalil

This page intentionally left blank

VCP5-DT
Official Cert Guide

Linus Bourque

vmware® PRESS

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

VCP5-DT Official Cert Guide

Published by Pearson plc

Publishing as VMware Press

Library of Congress Control Number: 2013909352

ISBN-13: 978-0-7897-5027-3

ISBN-10: 0-7897-5027-9

Printed in the United States of America

First Printing: August 2013

Text printed in the United States at Courier, Westford, MA.

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 DVD or programs accompanying it.

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

Corporate and Government Sales

VMware Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact

U.S. Corporate and Government Sales
(800) 382-3419
corpsales@pearsontechgroup.com

For sales outside the United States, please contact:
International Sales
international@pearsoned.com

VMWARE PRESS PROGRAM MANAGERS
Erik Ullanderson
Anand Sundaram

ASSOCIATE PUBLISHER
David Dusthimer

ACQUISITIONS EDITOR
Joan Murray

DEVELOPMENT EDITOR
Ellie Bru

MANAGING EDITOR
Sandra Schroeder

SENIOR PROJECT EDITOR
Tonya Simpson

COPY EDITOR
Keith Cline

INDEXER
Tim Wright

PROOFREADER
Debbie Williams

COORDINATOR
Vanessa Evans

BOOK DESIGNER
Gary Adair

COMPOSITION
Bumpy Design

Contents at a Glance

Table of Contents

This page intentionally left blank

About the Author

So, as with any book, there is always this blurb by the author where you learn how great he or she is (or they are). If you have ever attended one of my classes, you know that I am rather personable and love nothing more than sharing everything I can on VMware products. My biggest challenge has always been the "where to start." I suppose it is best to start at the beginning. Let's see. A long, long, long time ago there was this huge big bang.

Oh. Wait. That might be a bit too far back, eh?

So I am Canadian (I bet you can tell by my accent, eh?) and live in the sunny land known as Los Angeles. This year (2013) I will celebrate 8 great years with VMware. I started my career with VMware when a good friend and former Seneca College (Toronto) colleague Scott Laforet said, "Dude! You gotta come and get a job with Andrew and me at this little start-up! It rocks!"

I was skeptical about leaving my life of leisure as a professor at Seneca College. I mean, here I was enjoying a hard week of about 12 to 16 hours, lecturing on the "evils" of "acquiring" access into network systems and how to build PHP games. But it was time for a change and I figured, why not? Couldn't be worse than what I was doing, eh?

So I packed up my two cats and we moved to Burlington, Ontario. I joined the VMware Global Support Services group. At first I was hesitant about doing "telephone support," as I envisioned my day consisting of "Yes, did you turn it on and off again? Did you do it three times?" If anything, it was not that. VMware customers showed me a side of IT support that challenged every little brain cell that eagerly loved puzzles.

But, I missed teaching. There's a joy that comes from seeing people succeed and go beyond what they can imagine when you show them so much more than they expected. So, I decided to get into teaching but for VMware Global Education. Like most instructors, you start with the basics. In this case, it was the Virtual Infrastructure 3.x Install, Configure, Manage class. After doing that for a short bit, I got asked whether I would do the new class: VDM 2.0. For a while, I was the only one teaching it in all of the Americas (for VMware's direct delivery group). VDM evolved into View 3.0 and then 4.0 and then... well, we're up to 5.2 as of now.

During the 4.5 days, I got invited to participate in creating exams for VMware's Certification group. From deciding who the exam targets to even some of the questions (don't ask me for questions; I don't even remember what the answers are to the questions I created, let alone what they are!), I've been part of every one of our desktop certification exams and have been part of the betas for them all.

These days, my life is so much more than just teaching. I still do that, but I also certify who becomes an instructor in the Americas, remain as lead instructor for our End User Computing (EUC) instructor-led classes (as John Dodge says, “I’m the View guy!”), help with creation of classes and labs for the classes, and so much more. I often teach View classes at our education boot camps before PEX (Partner Exchange) and VMworld (USA only). This is my first book, and I already know what I want to do for a second edition (if I get to do it).

When I’m not livin’ la vida loca in the virtual world, I stomp around in Warcraft as a Tauren hunter. Or sit out in the warm evening of Los Angeles, a cigar and whiskey in hand, enjoying the night with my girlfriend and our two pugs, Lily and Lawfawda. (If you ever do an online class with me and hear barking or snoring, that’s them!) And between all that, I read voraciously all sorts of technical material, philosophy, steampunk, science fiction, and whatever else I find interesting. (So, if you have anything to suggest, send it my way!)

I’ll end with a thought from Albert Einstein: “Learn from yesterday, live for today, hope for tomorrow. The important thing is not to stop questioning.”

Dedication

I would like to dedicate this to the following: my everything, Kristen Williams,
who listens to my ramblings and rants and loves me as I am.

And to my colleagues who are always there when I ask for help,
no matter how small or large the task or idea.

Acknowledgments

I never wrote a book until this one. I learned *a lot*! There is so much that goes into producing a book; you'd be amazed! I have to start off by giving huge kudos to Joan Murray and Ellie Bru for keeping at me when I forgot or missed a deadline. I'm sure I drove both of you nuts with missed deadlines and not fully understanding the process.

Thank you to Owen Thomas who helped out with some chapters when the deadline came faster than my brain cells could process. Thanks also to Stephane Asselin, Simon Long, Justin Venezia, and Pranesh Raghavender Rao.

Thanks to my colleagues (Damian Wraa, Brian Watrous, Phil Cohen, John Krueger, Andrew Ellwood) who offered great support and listened to me while I went on about the challenges of writer's block. And a special thanks to Randy Becraft, who suggested this to me in the first place.

Last but not least, thank you to VMware for letting me do this. Very few companies are as supportive of its employees as VMware is. And very few companies make amazing products like we do.

About the Reviewers

Agustín Malanco (VCP 3,4,5, VCAP4/5-DCA, VCAP4/5-DCD, VCP4/5-DT, VCP-Cloud) has been working with VMware's technologies for 6 years, and has worked in various fields, including consulting, support, and training. As a VMware Certified Instructor (VCI4), he taught courses in Latin America. Currently, he works for VMware as a Partner Systems Engineer covering Mexico. Some of his primary responsibilities are enabling partners and distributors from a technical perspective and giving presales support for the whole partner ecosystem. Agustín is a contributor at the official VMware Latam Blog (http://blogs.vmware.com/latam) and he also has his own blog (http://blog.hispavirt.com). He has been recognized as vExpert 2011 and 2012 for his contributions to the community.

Envor Enrico Pillay is currently a part-time consultant and international traveler working as a VMware Certified Instructor (VCI) for a leading IT training provider in Africa, Torque IT. He is certified in many technologies: VMware, Microsoft, and CompTIA, to name a few. He shares his passion for the VMware technology through the VMware authorized classes he delivers, inspiring individuals from all walks of life across Africa. As a virtualization solutions architect, he has provided and assisted in numerous designs and implementations for customers in Africa. He recently received a prestigious award, the EMEA VCI of the Quarter Award for Q1 2013.

Owen Thomas is a senior technical instructor for Global Knowledge, teaching VMware classes and writing white papers for View and vSphere since 2008. Classes include the Install Configure, Manage classes, FastTracks, as well as Design and Troubleshooting. In addition to teaching most of the available VMware classes, his customer-site consulting has included audits, installs, designs, assessments, documenting current environments, and providing road maps for future growth with vSphere and View. Prior to teaching VMware courses, Owen was an analyst in a large enterprise-level network operations center (NOC) in Louisville, Kentucky, where he was first exposed to VMware.

This page intentionally left blank

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

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

Reader Services

Visit our website and register this book at www.informit.com/title/9780789750273 for convenient access to any updates, downloads, or errata that might be available for this book.

This page intentionally left blank

Introduction

It's hard to believe how enterprise computing has changed as a whole, but particularly when it comes to virtualization. The idea of taking the four common resources (CPU, memory, disk, and network) and abstracting them into effective processes is not as new as we might think. (The initial starting point can be traced as far back as in 1965, when IBM had memory that was split for the IBM 360/65.) However, it has been advancing at a much more rapid pace in the past decade.

Our traditional datacenters often consisted of lots of physical boxes of varying sizes. Administrators would order new server boxes from a major vendor, install Windows or Linux or some other *Nix on the box, and configure a single application or service to run on it. Once we set these up, we then had to maintain, upgrade, and manage the hardware and software. Updating software was a relatively straightforward aspect of the job, but hardware changes often presented challenges. Even with all the planning and practice, something could still go wrong.

I remember when I first got into IT as a network/system administrator. We were just starting to fit servers into the closet, but we were rapidly discovering that a lack of space, power, cooling, and security was something that we needed to address to ensure a well-running environment. So, we began to assign whole rooms and, sometimes, whole warehouses to be datacenters. They had to have massive cooling infrastructures, complex cabling, and backup power options. And for larger environments, this can be challenging.

If we had to deal with a hardware failure, we had to go to that specific server and get the part from the vendor (hoping for sooner rather than later). We had to plan for some kind of physical failover for each critical server, potentially doubling or tripling cooling costs, power consumption, UPS, and administrative hours to try to minimize our outage risk. Perhaps we would get a new manager who preferred vendor A over vendor B, even though vendor B had been our main vendor for years. Moving over critical systems is not as easy as one might think, and it requires a fair amount of planning, processes, and a lot of luck.

The worst challenge, however, was the orphaned application: that one piece of software that the company needed but whose only source was a vendor that went out of business 10 years earlier. Let's make this even more fun: The original software floppy disks cannot be found, and the application runs only on Windows NT 4 with Service Pack 6 (and not Service Pack 6a). The server it runs on is kept together with glue and duct tape and the occasional wish upon a falling star. All attempts to move it to a new server have failed spectacularly, and the department that depends on it refuses to use a new application that could do the same and more. We've all run into this, even in today's market. These various scenarios have led me to often remark that I will never be out of work in IT (because these challenges ensure a perpetual need for someone to be around to address them). But, the reality of keeping this application running and stable highlights the critical need to migrate it to a more flexible and reliable environment.

And while traditional datacenters were evolving and expanding, a newer technology was emerging in the background: hardware abstraction virtualization (or just virtualization). For me, my first exposure to virtualization occurred more than 15 years ago when I first installed VirtualPC on my Quadra 650. VirtualPC, which was still owned by Connectix, allowed me to run a Windows 95/98 system on my Mac, but to do so, it had to do both the hardware abstraction and the CPU translation. This resulted in some less-than-stellar performance behavior. At this time, virtualization was viewed as something strictly used at the desktop. Over the past 15 or so years, virtualization has dramatically changed both itself and the datacenter.

What Is Virtualization?

Modern virtualization is almost exclusively an abstraction of the four main resource groups: CPU, memory, network, and storage. I sometimes call these the *four food groups of virtualization*. We see this done primarily on the x86 platform in one of two ways: hypervisor (Type 1) or hosted (Type 2). We will start with hosted virtualization (for example, VMware Server, Workstation or Fusion, Parallels). This puts the abstraction layer into an application-like environment. This means that calls to hardware will have to go through the host's operating system (for example, Windows, Linux, OS X) before reaching the hardware and then returning to the virtual machine. For systems like desktops and laptops, this means running operating systems without having to give up the local system. It also means that whatever the local operating system sees as hardware can be presented to the virtual machine. The challenge, in this scenario, is that both the operating system and the virtual machine, the abstracted virtual hardware environment, fight for the limited local resources on the system on which they are installed, usually a laptop or desktop environment for a single user.

This kind of virtualization works great for single users who want to try a different operating system without having to do a new install or multibooting the system, developers who do cross-platform development, and security geeks who want to test or try things that cannot be done on the base operating system. But when we have many more systems to virtualize, this can prove challenging, as mentioned previously.

In comparison, we find that hypervisors, like VMware ESXi (sometimes referred to as bare-metal hypervisors), are better at sharing resources between the virtual machines and the hardware. These hypervisors can ensure that a virtual machine's Guest OS gets access to all the physical resources and then divvy that up between the virtual machines based on their requests, contention, and other factors.

The hypervisor itself is the operating system for the hardware and acts as the go-between for the virtual machine and the hardware, ensuring equitable resource allocation where possible. Normally, an operating system will take full control over a piece of hardware and "own it." This will not work in a virtual environment, where I may have up to 500 virtual machines residing on a single hypervisor host and acting as individual systems. As I often say in class, virtual machines are like 2-year-olds. Everything, for a virtual machine, is "*mine*!" The hypervisor does its best to ensure that the virtual machines share appropriately and do not misbehave.

I will admit it: I'm biased toward ESX/ESXi as hypervisors (and not just because I work for VMware and have been primarily using ESX since it was version 2.5.x). I've always believed in using the tools that best fit and meet the needs of what I need to do. I write this on a MacBook Pro using Office 2011 for Mac (although I could have done it on one of my Fusion Windows 7 virtual machines or my View desktop). There is a reason why the majority of companies use VMware: It works. Over the years, ESX/ESXi has evolved from where the ESX/ESXi server was the most critical piece to recover immediately from an outage (it still is, but it is not as disastrous as it might have once been) to where it does not matter as much as getting the virtual machine running and we do not care where it runs.

vSphere 5

So, this is where vSphere 5 comes in. Introduced in 2011, vSphere 5 was the first version of VMware's hypervisor Type 1 to not offer a service console in it and returned to a single version, this time as just ESXi. (ESX was officially dropped in vSphere 5 as part of the removal of the service console.) Previously, this had been used as a mechanism to manage and bootstrap the hypervisor. Getting rid of this ensured a smaller footprint, fewer security vectors, and a more stable platform. vSphere is the suite name of the VMware enterprise virtualization and cloud computing environment. It includes the two main pieces of ESXi and vCenter as well as Update Manager, Orchestrator, and more. Figure I-1 shows a logical representation of the suite at the time of this writing. New features are added each year, but the core concepts remain the same.

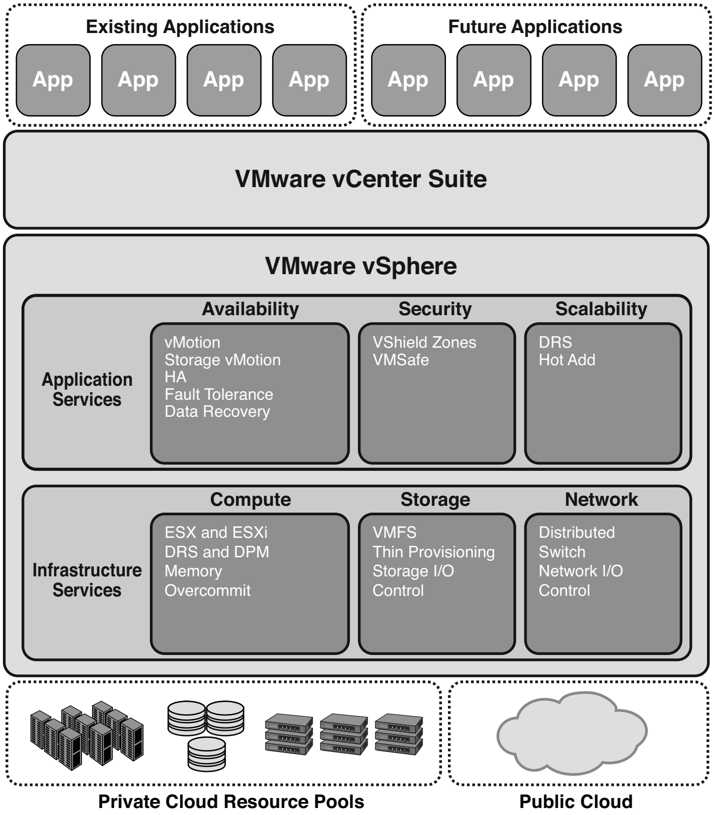


Figure I-1 vSphere 5 virtualization.

More and more, virtualization is more than just the hypervisor. It has instead become how we manage the environment effectively and ensure that the critical virtual machines continue actively running. When you manage multiple ESXi servers, however, individual administration can be too challenging. That is where something like vCenter helps. It brings the management of those servers under the control of a single system. vCenter adds additional features that we would not have available in a single system. As Figure I-1 shows, vSphere is more than just the hypervisor. At the base, we have the actual server hardware, which often represents the CPU and memory resources available to the virtual machines. For vSphere, it is important to ensure that the hardware has been certified on the hardware compatibility list (to avoid common problems that occur when hardware has not been tested to work with vSphere).

In addition to the server, we have storage and network. Storage types come in many flavors, but we tend to see Fibre Channel (also known as FC), iSCSI, NFS, and local storage. On top of FC, iSCSI, and local storage, we can place a VMFS (Virtual Machine File System) and leverage it for many of the features found in vSphere. For the network, we can leverage both standard virtual switches and distributed virtual switches (available only with Enterprise Plus licensing). With these, we can leverage various predictive load balancing, VLANs, basic network security, and bandwidth throttling.

But it really is vCenter that ties everything together. vCenter is the glue that manages a good virtual environment. With it, we can take advantage of features like Distributive Resource Scheduler (DRS), High Availability (HA), Storage DRS (SDRS), vMotion, Template Provisioning, Thin Provisioning, Storage I/O Control (SIOC), Distributive Power Management (DPM), and so on. I could continue with a long list of features, but I think you get the idea. vCenter alleviates some of the tasks that are considered repetitious and does them for us so that we do not have to worry. A feature like DRS helps my environment to balance both CPU and memory utilization better across servers.

And as organizations began to virtualize their servers and to realize significant benefits from doing so, we began to see desktops appear as virtual machines. Administrators and users alike wanted to make it easier to deploy and use desktops. Companies wanted to expand but not deal with new computer costs or the cost of upgrading whole systems (many of which provide many more resources than are truly needed for end users); they also did not want to have to find space for these users (and so on). The reality is that the cost of individuals and providing them with the tools that they need can sometimes outweigh the immediate need to have that person.

We have, as an industry, excelled at server virtualization. When most of IT says *virtualization*, they think of server virtualization (and especially on VMware vSphere). But we now have to look beyond the land of servers.

What Is VDI and View?

So this is where virtualizing the desktop comes in. Virtual desktop infrastructure (VDI) is not a new concept. At the very beginning of server virtualization, administrators began to look for ways to virtualize terminal servers. And when they did, the first virtual desktop environment was started. It was cumbersome, to say the least, but it did alleviate the need for actual desktops in individual cubes. All that was needed was a thin client that could connect, via Remote Desktop Protocol (RDP) or another remote access protocol, back to the terminal server. It was effective enough for small configurations, but what about the environments that wanted to virtualize 300 users? Or 3,000? Or 10,000? This kind of piecemeal setup would, very quickly, become a challenge to manage. And it would require a separate team from those that manage the physical environment.

Many corporations worried *only* about their servers and virtualized those. Meanwhile, employee desktops were changing—or rather, how they accessed those desktops was changing. We are moving from a traditional grey box access from one's cubical to having a variety of devices (such as smartphones or tablets) to access a desktop, which is primarily a Windows flavored desktop (such as Windows XP, Vista, 7 or 8). To make management somewhat easier, we allowed users to look after their system and trusted them to install only what was needed. This meant that organizations allowed some user flexibility, but it also resulted in a kind of a bonding between end users and their desktop. In fact, it became rather a possessive thing.

Back then, if you were to ask a user to give up his desktop, the wrath of some computer deity would come down on your head. A few too many organizations forgot to remind employees that the computer they were using (whether a desktop or laptop) was, in fact, a tool provided to them by the company. Returning that ownership to the organization would mean better control, better security, and a stronger ability to centralize and standardize the desktop image in general. Bringing the desktop into the datacenter would allow this because it would mean that IT would once again control it.

Some organizations started the process of virtualizing their desktops. Often, this form of virtualization, known as VDI or virtual desktop infrastructure, was an ad hoc process. A Windows or Linux system would be created, a remote protocol enabled or installed, and the employee given access. The user would either use an existing full system (laptop or desktop) or a thin client.

But unless organizations were willing to build football field size datacenters just for the desktops (and all the costly support and redundant equipment), the only effective way to achieve this was with virtualization. Back around 2007, VMware purchased a little Swiss company called Dunes. They had a nifty little product called Virtual Desktop Manager. For all intents and purposes, VDM was more of an orchestration kind of tool. It told vCenter what to build, and vCenter went and did. And it was more. It became the central location to manage the desktops. Instead of reinventing how virtual machines were created, we just took what we had and automated the process to make it easier to configure.

And it was easy to set up.

VDM was the first step, but it did need to evolve. A new name and a new protocol did that. From VDM, View emerged as the next generation of VDI. Along with it, we saw the introduction of VMware's linked-clone concept, a mechanism to save on storage space. Further evolutions beyond the initial View 3 introduced a new protocol designed for the end user, regardless of the kind of end user it was. It could have been Georgie, the call center representative who takes your monthly widget order; Sally, the mobile sales representative who pounds the pavement looking for new leads around the Northeast; Angie, the IT administrator who is a Windows-ninja at fixing blue screens; or it could be Kelly, who does the actual CAD design of the widgets and what next year's model will look like. The protocol PC-over-IP (PCoIP) was designed for all these users and those in-between.

The protocol itself was developed by Teradici, who partnered with VMware to make it one of the main features of View. One of the main features of the protocol is that it was designed to be efficient, adaptive, and secure (right out of the box). To have a protocol designed for the modern desktop computing environment is significant because it ensures that we do not need to tack on additional items to achieve a regulatory-compliant environment. As each version of View has come about, we've seen VDI switch from an ad hoc collection of virtual machines that were designated as desktops to complex desktop environments configured with ease and simplicity (and no, that's not contradictory).

Today, you can quickly put up a View environment, usually with little effort. The bigger challenge is the desktop operating system optimization and how the virtual machines play together in memory and storage. But we'll get into that. Understanding where we have come from helps us address some of the challenges that still exist, primarily one of the biggest assumptions that constantly challenges VDI instances: the idea that we can treat desktop virtual machines exactly like we treat server virtual machines.

Virtual desktops behave differently than servers with regard to how resources are used. Although both use the "four food groups," desktops tend to be consistently the same across the board in activities and often do huge bursts (think of Monday morning logins, antivirus updates, and the like). In addition, content changes much more on desktops than it does on servers. The desktop landscape is also being changed by the likes of tablets, smartphones, iPads, zero clients, and more. Figure I-2 provides a logical representation of all the possible features of View. There are other features and pieces not shown, but this figure does highlight how a virtual desktop environment might look for some environments.

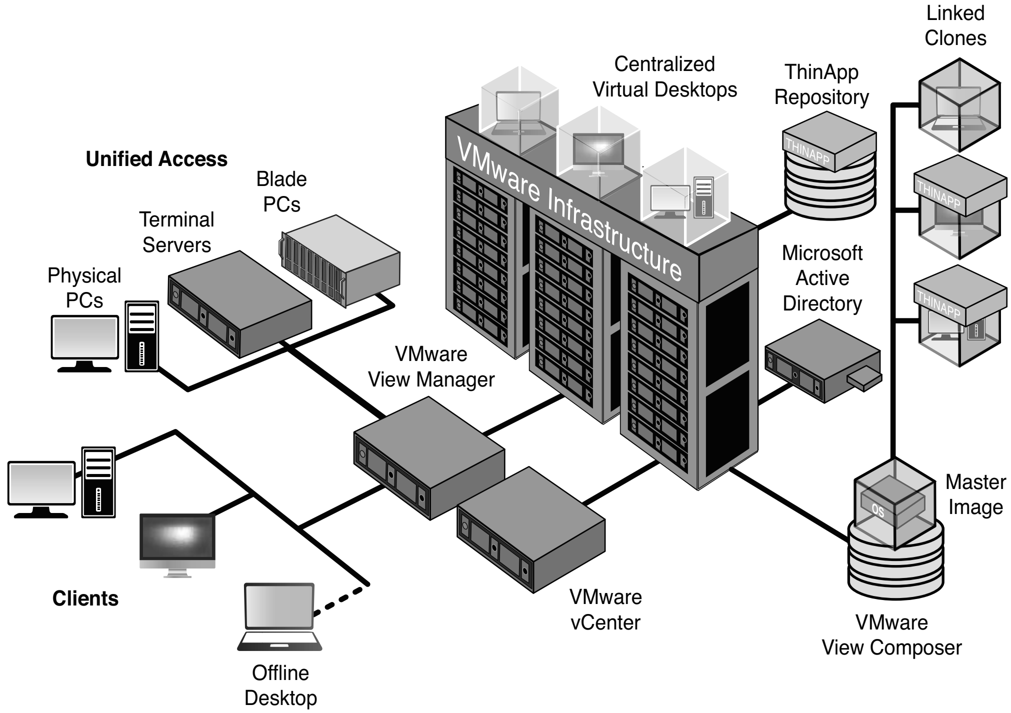


Figure I-2 VMware View components.

So, what makes up View (besides what Figure I-2 shows us)? Well, the central piece of View is the Connection Server. This acts as both the management piece and the point of contact for end users. A single Connection Server, however, cannot manage and handle all the users that would connect to it. Like any system, there are a finite number of resources. Although virtualization does make better use of those resources, there is always a limit to what is there. So, we'll install replica servers to help expand the View instance and allow for a better balance of resource utilization and availability for users. It is through the View Connection Servers that users are able to connect to their desktops that run on vSphere. In addition, the Connection Server allows us to create automated pools, manual pools, or even terminal service pools of desktops if we want. For those pools, we can use the traditional template provisioned virtual machines, but this can eat up a lot of storage space for the environment. So, to help with this, we can leverage the Composer piece that makes linked clones, which can use as little as 90% less space compared to fully provisioned virtual machines. To further help shrink down the size of the virtual desktop, we can leverage a technology like ThinApp to take applications from residing as part of the base image and move them to remote storage for streaming.

When most people think of VDI, they think of the head office or the telecommuter. However, there is a special kind of user whom we need to consider: the remote road warrior user. Normally, our remote users are given a laptop and expected to back up important data once in a while. Because these systems are basically the responsibility of the user, who may or may not make it back into the office occasionally, any number of things can happen to the system over the course of the life of the laptop on the road. Or, worse, it could be stolen or compromised. The desktop support team can monitor systems that are local, but those on the road tend to be a little harder to do.

We often hear in the news about the laptop that got left at the airport or the system that got compromised. These kinds of events result in huge dollar losses. But even when we look beyond that and think of the kinds of people who do business with us (contractors and partners and so on) who might need access to sensitive data or unique applications, we often see that providing a centrally controlled system would be ideal. We do not, however, need to think that broadly. What about the university that has students who do study/work sessions abroad and has research it needs to protect? Maybe the students are part of a special South Pole team that has limited or no network access. Or perhaps they are journalists in the middle of a conflict writing the next Pulitzer Prize-winning article.

In any scenario where you cannot access the environment normally, View provides for a unique kind of desktop: local mode desktop (what used to be referred to as *offline* desktops). If I have a Windows system with the View Client with Local Mode installed on it, I can download a whole virtual machine to my system. Once downloaded and running on the local hardware, any changes I do can be synchronized back to the View environment and the copy that resides, protected, on the ESXi host. If the laptop gets stolen, the virtual machine virtual disk is encrypted. Even if the laptop gets infected with every malware, Trojan, and other nasty thing you can find, the virtual machine remains protected. And, if that local virtual machine shouldn't be used any more, as an administrator I can revoke someone's access easily and when it happens, the virtual machine can delete itself on the remote system once it knows it's not needed any more.

But all that aside, what I find really nice about View is that I do not need to create a separate user environment for this. I can use my existing Active Directory environment and leverage existing Group Policy Objects (GPOs) and add View-specific GPOs to help manage the environment. It is easy to incorporate into the environment. And just as easy to set up. For one customer, I set up a simple proof of concept (POC) in less than 4 hours. The longest piece was tweaking Windows 7 so that it behaved better in a virtual environment.

As you go through this book, you will learn how to configure and set it up based on what the exam blueprint covers. However, I would be remiss if I failed to address a final thought: design. As announced in 2011, we are working on a VCAP5-DT exam. This exam will deal with design issues. No View environment should just be slapped up with the hope that it will work. Unlike other virtual environments, desktops seem particularly sensitive to two specific resources: storage (specifically input/output per second [IOPS] activity) and memory usage.

Before setting up any production environment, ensure that you are aware of what each desktop will actually use for each of these. This does not mean that you ignore the CPU and network; you still need to consider those, too. In my experience, the majority of performance issues with View relate to poor planning, specifically with storage. Although it is easy to create 1,000 linked-clone virtual machines on my storage, that same storage may not be able to handle all of them being created, powered on, refreshed, antivirus scanned, and so on all at the same time on the same storage. What might have been 5 IOPS per virtual machine for behavior may be 100 times greater when doing activities such as power ons, refreshes, rebalances, and so forth.

Because it is so easy to install and configure View, it becomes easy to ignore what needs to be done to ensure optimal performance of the virtual desktops. As the proverb says, “He who fails to plan, plans to fail.” This is particularly apt for View. So with that said, let’s get un-lulled and install the various parts of View in Chapter 1, “What Makes Up View?”

Who Should Read This Book

The VCP certification was listed on http://www.techrepublic.com/ as one of the top five in-demand certifications to have in 2013. If you are currently working with VMware vSphere virtual datacenters, it could be a valuable certification for you. If you are considering your options in the IT world, you will not go wrong if you learn about virtualization now. In either case, this book will help you obtain the knowledge and the skills necessary to certify as a VCP.

Goals and Methods

My number one goal of this book is simple: to help you pass the VCP5-DT certification exam and obtain the status of VMware Certified Professional 5 – Desktop (VCP5-DT).

To aid you in gaining the knowledge and understanding of key topics, I use the following methods:

- **Opening topics list:** This list defines the topics to be covered in the chapter. Each chapter is a part of the exam blueprint and the chapters and topics are written in blueprint order.
- **"Do I Know This Already?" quizzes:** At the beginning of each chapter is a quiz. The quizzes, and answers/explanations (found in Appendix A), are meant to gauge your knowledge of the subjects. If the answers to the questions do not come readily to you, be sure to read the entire chapter.
- **Key topics:** The key topics indicate important figures, tables, and lists of information that you should know for the exam. They are interspersed throughout the chapter and are listed in table format at the end of the chapter.
- **Review questions:** All chapters conclude with a set of review questions to help you assess whether you have learned the key material in the chapter.
- **Exam-type questions:** Exam questions are included with the printed and digital editions of this book. They are written to be as close to the type of questions that appear on the VCP5-DT exam.

How to Use This Book

Although you could read this book cover to cover, I designed it to be flexible enough to allow you to easily move between chapters and sections of chapters to work on the areas that you feel are the most important for you. If you intend to read all the chapters, the order in the book is an excellent sequence to follow.

The core chapters, Chapters 1 through 9, cover the following topics:

- **Chapter 1, "What Makes Up View?":** This chapter focuses on installing, upgrading, and securing all of the key components in your vSphere. I discuss ESXi hosts, vCenter, datastores, and network components.
- **Chapter 2, "Configuring the View Environment":** This chapter focuses on storage of virtual datacenters and virtual machines. I discuss configuring and managing all forms of storage, including Fibre Channel, iSCSI, and network-attached storage.
- **Chapter 3, "Printing in the View Environment":** This chapter focuses on creating, configuring, and managing virtual machines and vApps. I cover many other topics, including cloning, troubleshooting, and exporting virtual machines and vApps.

- **Chapter 4, "The Protocols":** This chapter focuses on keeping your vSphere running smoothly and recovering quickly from any failure. I cover many topics, including services that improve overall utilization and recoverability.
- **Chapter 5, "Interacting with Active Directory":** This chapter focuses on understanding the key components of your vSphere and how they work together. You learn how to spot a problem and make the necessary corrections. I cover troubleshooting your ESXi hosts, network, storage, and key services.
- **Chapter 6, "Optimizing the Operating System":** This chapter focuses on the "core four" resources in any computer system: CPU, memory, disk, and network. I cover guidelines for monitoring each of the core four. By knowing how to monitor your resources and knowing what you should expect to see, you will be able to spot any metrics that seem to be "out of place" and take the necessary action.
- **Chapter 7, "Kiosk Mode":** This chapter describes the steps required to set up VMware View Clients to behave as kiosk machines.
- **Chapter 8, "Local-Mode":** This chapter illustrates the purposes of local mode and how to configure the VMware View environment to permit this option.
- **Chapter 9, "Troubleshooting":** This chapter discusses the processes involved to assist administrators when problems arise in their View environment.

NOTE I highly recommend that you schedule the test now and then study. Go to Pearson/Virtual University Enterprises (http://vue.com) on the Web and find a testing center close to you. The cost of the exam at the time of this writing is $225. If you put your money down and set the date, you will focus more and study better.

Certification Exam and This Preparation Guide

When I originally started this book, it was more freeflow than I had intended. We then switched to trying to map as many of the chapters to the VCP510-DT Exam Blueprint as we could. Future editions of the book likely will exactly map each chapter to each objective. The idea of mapping the chapters to the objectives makes it easier for you to identify your strengths and weaknesses for understanding the topics. Table I-1 lists the VCP510-DT Exam Blueprint objectives and the chapter of this book that covers them.

Table I-1 VCP5 Exam Topics and Chapter References

Exam Section/Objective	Chapter Where Covered
Section 1: Install View Server Components	
Objective 1.1: Install View Composer	Chapter 1
Objective 1.2: Install View Standard and Replica Connection Server(s)	Chapter 1
Objective 1.3: Install View Transfer Server	Chapter 1
Objective 1.4: Install View Security Server(s)	Chapter 1
Objective 1.5: Prepare Active Directory for Installation	Chapter 1
Section 2: Configure the View environment	
Objective 2.1: Configure View Composer	Chapter 2
Objective 2.2: Configure VMware View Events Database	Chapter 2
Objective 2.3: Configure View Standard and Replica Connection Server(s)	Chapter 2
Objective 2.4: Configure View Security Server(s)	Chapter 2
Objective 2.5: Configure View Transfer Servers	Chapter 2
Objective 2.6: Configure advanced display protocol settings (PCoIP/RDP)	Chapter 4
Objective 2.9: Configure remote and/or location-based printing for View Desktops	Chapter 3
Objective 2.10: Configure the environment for Local Mode	Chapter 8
Objective 2.11: Configure the environment for Kiosk Mode	Chapter 7
Section 3: Create and configure pools	
Objective 3.4: Configure Local Mode use	Chapter 8
Objective 3.5: Build desktop sources	Chapter 6
Section 4: Implementation Troubleshooting	
Objective 4.1: Troubleshoot Composer installation on vCenter Server	Chapter 9
Objective 4.2: Troubleshoot events database	Chapter 9
Objective 4.3: Troubleshoot guest OS customization	Chapter 9
Objective 4.4: Troubleshoot accounts and permissions	Chapter 9
Objective 4.5: Troubleshoot connectivity between View Components	Chapter 9
Objective 4.6: Troubleshoot PCoIP configuration	Chapter 9
Objective 4.7: Troubleshoot View Servers (Connection, Security, Transfer)	Chapter 9
Objective 4.8: Troubleshoot View Persona Management	Chapter 9

Exam Section/Objective	Chapter Where Covered
Section 5: Component features and functions	
Objective 5.1: Describe and differentiate between component functions and feature level (i.e., not only what they do but how they work)	All chapters

Book Content Updates

Because VMware occasionally updates exam topics without notice, VMware Press might post additional preparatory content on the web page associated with this book at http://www.pearsonitcertification.com/title/9780789750273. It is a good idea to check the website a couple of weeks before taking your exam, to review any updated content that might be posted online. We also recommend that you periodically check back to this page on the Pearson IT Certification website to view any errata or supporting book files that may be available.

Pearson IT Certification Practice Test Engine and Questions on the DVD

The DVD in the back of this book includes the Pearson IT Certification Practice Test engine—software that displays and grades a set of exam-realistic multiple-choice questions. Using the Pearson IT Certification Practice Test engine, you can either study by going through the questions in Study Mode or take a simulated exam that mimics real exam conditions.

The installation process requires access to the Internet and two major steps: installing the software, and then activating the exam. The DVD in the back of this book has a recent copy of the Pearson IT Certification Practice Test engine. The practice exam—the database of exam questions—is not on the DVD.

NOTE The cardboard DVD case in the back of this book includes the DVD and a piece of paper. The paper lists the activation code for the practice exam associated with this book. Do not lose the activation code. On the opposite side of the paper from the activation code is a unique one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Install the Software from the DVD

The Pearson IT Certification Practice Test is a Windows-only desktop application. You can run it on a Mac using a Windows virtual machine, but it was built specifically for the PC platform. The minimum system requirements are as follows:

- Windows XP (SP3), Windows Vista (SP2), Windows 7, or Windows 8
- Microsoft .NET Framework 4.0 Client
- Microsoft SQL Server Compact 4.0
- Pentium class 1GHz processor (or equivalent)
- 512MB RAM
- 650MB disc space plus 50MB for each downloaded practice exam

The software installation process is pretty routine as compared with other software installation processes. If you have already installed the Pearson IT Certification Practice Test software from another Pearson product, there is no need for you to reinstall the software. Just launch the software on your desktop and proceed to activate the practice exam from this book by using the activation code included in the DVD sleeve.

The following steps outline the installation process:

Step 1. Insert the DVD into your PC.

Step 2. The software that automatically runs is the Pearson software to access and use all DVD-based features, including the exam engine and the DVD-only appendixes. From the main menu, click the **Install the Exam Engine** option.

Step 3. Respond to window prompts as with any typical software installation process.

The installation process gives you the option to activate your exam with the activation code supplied on the paper in the DVD sleeve. This process requires that you establish a Pearson website login. You need this login to activate the exam, so please do register when prompted. If you already have a Pearson website login, there is no need to register again. Just use your existing login.

Activate and Download the Practice Exam

After installing the exam engine, you should then activate the exam associated with this book (if you did not do so during the installation process) as follows:

Step 1. Start the Pearson IT Certification Practice Test software from the Windows Start menu or from your desktop shortcut icon.

Step 2. To activate and download the exam associated with this book, from the My Products or Tools tab, click the Activate button.

Step 3. At the next screen, enter the activation key from the paper inside the cardboard DVD holder in the back of the book. Once entered, click the Activate button.

Step 4. The activation process downloads the practice exam. Click **Next**, and then click **Finish**.

When the activation process completes, the My Products tab should list your new exam. If you do not see the exam, make sure you have opened the My Products tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam and click the **Open Exam** button.

To update a particular exam you have already activated and downloaded, open the Tools tab and click the **Update Products** button. Updating your exams will ensure you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson Cert Practice Test exam engine software, open the Tools tab and click the **Update Application** button. This will ensure you are running the latest version of the software engine.

Activating Other Exams

The exam software installation process, and the registration process, only has to happen once. Then, for each new exam, only a few steps are required. For instance, if you buy another new Pearson IT Certification Cert Guide or VMware Press Official Cert Guide, extract the activation code from the DVD sleeve in the back of that book; you do not even need the DVD at this point. From there, all you have to do is start the exam engine (if not still up and running), and perform steps 2 through 4 from the previous list.

Premium Edition

In addition to the free practice exam, you can purchase two additional exams with expanded functionality directly from Pearson IT Certification. The Premium Edition eBook and Practice Test for this title contains an additional two full practice exams and an eBook (in both PDF and ePub format). In addition, the Premium Edition title also has remediation for each question to the specific part of the eBook that relates to that question.

If you have purchased the print version of this title, you can purchase the Premium Edition at a deep discount. A coupon code in the DVD sleeve contains a one-time-use code and instructions for where you can purchase the Premium Edition.

To view the Premium Edition product page, go to http://www.pearsonitcertification.com/title/9780133445671.

This chapter covers the following subjects:

- Optimizing the Operating System
- Configuring Virtual Hardware
- Installing the Agent
- Creating Customization Specifications

(This chapter covers Objective 3.5 of the Blueprint.)

CHAPTER 6

Optimizing the Operating System

Up to now, we have reviewed the steps necessary to install and configure View, and to provide an optimal delivery experience for users connecting to virtual desktops. However, for the best possible end-user experience, the virtual desktop itself must also be optimized. The first step in this optimization process is fine tuning the operating system (OS) to function well in a View environment. Windows operating systems were not initially designed for a virtual platform. Although they have been adapted in recent years to function in this type of environment, changes should still be made to ensure that they perform well. For example, in a virtualized environment, all components of a desktop exist as files. Therefore, optimizing storage resources when virtualizing a desktop is a critical step in ensuring proper performance. Some of these optimization steps are simple tricks that can result in an impressive performance improvement, not only for virtual environments but for physical environments as well. This chapter takes a look at these optimization methods.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter or simply jump to the "Exam Preparation Tasks" section for review. If you are in doubt, read the entire chapter. Table 6-1 outlines the major headings in this chapter and the corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions."

Table 6-1 Headings and Questions

Foundation Topics Section	Questions Covered in This Section
Optimizing the Operating System	1–2
Configuring Virtual Hardware	3
Installing the Agent	5
Creating Customization Specifications	4, 6–10

1. What two guides can you use to optimize virtual desktops in a View environment?
   a. *VMware View XP Deployment Guide*
   b. *VMware View XP Optimization Guide*
   c. *VMware View Optimization Guide for Windows* 7
   d. *VMware View Optimization Guide for Windows XP*

2. Which setting immediately improves performance on a Windows virtual desktop?
   a. My Computer > Properties > Advanced Tab > Performance Options
   b. My Computer > Advanced Settings > Performance Options
   c. My Computer > Properties > Performance > Performance Options
   d. My Computer > Properties > Performance Options

3. What virtual hardware can you remove from a virtual desktop to optimize performance?
   a. vCPU
   b. vRAM
   c. Floppy drive
   d. Disk drive

4. What must be installed on the virtual desktop image to ensure the latest drivers and other performance improving features are present?
   a. View drivers
   b. VMware drivers
   c. VMware Tools
   d. View Agent

5. What feature must be installed on the master image to allow a desktop to be used for linked clones?
   a. View linked-clone agent
   b. View Composer Agent
   c. VMware linked-clone agent
   d. VMware Composer Agent

6. What should the BitLocker Drive Encryption Service be set to?
   - a. Default
   - b. Started
   - c. Manual
   - d. Disabled

7. Which service should be enabled on the master image but disabled for linked clones to help improve disk performance?
   - a. Desktop Window Manager Session Manager
   - b. VMware Composer Agent Service
   - c. Disk Defragmenter Service
   - d. Disk Defragmenter Session Manager

8. Which service should not be used to back up a virtual desktop?
   - a. Centralized File Backup
   - b. Backup with MS Software Copy Provider
   - c. Windows Backup
   - d. Centralized Profile Backup

9. A View implementation requires Superfetch and has been optimized to handle the increased I/O workload. When configuring Superfetch, what is the default setting?
   - a. Cache boot files only
   - b. Cache documents only
   - c. Cache applications only
   - d. Cache everything

10. What PowerShell script enables you to stop Windows services?
    - a. `powershell set-service <service name> -startuptype "disabled"`
    - b. `powershell setservice <service name> -startuptype "disabled"`
    - c. `powershell setservice <service name> -servicetype "disabled"`
    - d. `powershell set-service <service name> -servicetype "disabled"`

Foundation Topics

Virtual Hardware and Installation of the Operating System

Microsoft has been producing operating systems for a while now. I still remember my first DOS system and the first time I started using Windows with version 3.1. I've poked and prodded pretty much all of Microsoft's operating systems with the exception of Microsoft Me and Microsoft BOB. All of the Microsoft operating systems, with the exception of Windows 8, were pretty much designed for standalone hardware. This is particularly true for the desktop operating systems (XP, Vista, and 7). Windows 8, released as of the time of this writing, has been designed more for a tablet or touchscreen laptop. At this time, View does not support Windows 8. Although most environments deploy View during their next operating system refresh (usually from XP to Windows 7), quite a few are deployed with Windows XP, usually because of application dependency or end-user comfort.

VMware created two guides to help with optimization of both XP and Windows 7 operating systems in a View environment: the *VMware View Windows XP Deployment Guide* and the *VMware View Optimization Guide for Windows* 7. They are excellent references to keep handy. Remember to check the VMware website, because these guides are regularly updated as VMware finds new optimizations that can benefit organizations as they migrate Windows 7 to a virtual environment.

Key Topic

If I were to simplify the process of building and optimizing a virtual desktop, it would look something like the following:

1. Create a virtual machine as a template for your virtual desktops. Optimize the virtual hardware for the desktop during this step.
2. Install the latest version of VMware Tools.
3. Select a time-synchronization method where the virtual machine either synchronizes to the ESXi host or to the Active Directory time source.
4. Join the Active Directory domain.
5. If using VMware time synchronization in step 3, disable Windows time.
6. Install appropriate applications, and tune them for optimal performance.
7. Enable remote connections.
8. Install the View Agent.
9. Patch Windows desktops as needed. Note, this may require a reinstallation of VMware Tools and the View Agent.

Certain steps can be performed regardless of the OS used. By using local GPOs that prevent the use of themes, solid backgrounds, simple screensavers, and other similar settings like adjusting the Performance Options (right-click **My Computer >** click **Properties > Advanced** tab), you can realize a fair amount of performance improvement. Part of this process may require training your end users on how best to use their virtual desktops compared to what they might have been used to. Some organizations allow users a bit too much freedom with regard to the management of their desktops. The move to a virtual environment can be the perfect time to reassess end-user requirements and implement appropriate changes. As I often mention in class, one benefit of a virtual desktop infrastructure (VDI) deployment is that the organization regains ownership over the desktop as a tool provided to their end users and not something to use as their personal laptop.

Computers as personal devices have been around for decades, but it's only in the past 20 years or so that we've seen such an explosion of multipurpose need. Today, many organizations are leveraging bring-your-own-device (BYOD) or employee-owned IT (EOIT) policies. These policies enable employees to have a computer system that meets their specific needs and lets them personalize it without putting organizational data at risk. There would likely still need to be an organizational policy on what's allowed on the desktop versus what's not allowed, but this kind of configuration allows users flexibility while minimizing risk.

The main thing to keep in mind when it comes to virtual desktops is that services and processes that work well in a physical environment might not work well in a virtual environment. The emphasis placed on storage in a virtual environment may require changes to those services and processes. For example, in Windows 7, an indexing service runs continuously in the background. This adds roughly three to five input/output operations per second (IOPS) of read behavior on a disk. By itself, on a physical system, this is a negligible amount of IOPS. But when you have multiple systems all running regular indexing at the same time, utilizing storage from the same shared storage device, the collective amount of IOPS can result in a significant impact to storage performance. Disabling this service on the master image for a linked clone desktop pool reduces the possibility of unexpected resource contention for end users. The goal is to always ensure the same or better experience for end users than they had before virtualizing their desktops.

Configure Virtual Hardware

The first step in virtual desktop optimization is to optimize the hardware configuration. The best way to do this is when first creating the master image. Do not use a physical-to-virtual (P2V) conversion method to create the master image. Creating an image from a P2V results in a virtual desktop image that includes physical drivers and other components that might not behave well when virtualized. VMware recommends creating a new virtual machine and performing a fresh OS installation. Using the Microsoft Deployment Toolkit (MDT) is one way to ensure that the initial install meets the necessary requirements and allows for the creation of a unique ISO image that is specific to the environment. This ISO image can then be used as part of a zero-touch installation that requires no user interaction. By removing that interaction, you significantly reduce the chance of mistakes occurring. In addition, the MDT can install various applications as part of the base image install. These applications can include VMware Tools and the VMware View Agent. As mentioned earlier, the more interaction that is removed from the install process the better. In this case, by including VMware Tools and the VMware View Agent as part of the install, you ensure that they will automatically be part of the base image.

Many administrators simply accept the default virtual hardware when creating a new virtual machine. To ensure optimal performance, adjusting that hardware is worthwhile. This is often referred to as *right sizing* the environment and ensures that CPU, memory, disk, and network resources are sized exactly to what is needed by the environment. Removing any hardware that is not needed (such as a CD-ROM or floppy drive) can help keep the virtual machine optimized. Modifying the BIOS of the virtual machine can provide some benefit. For example, you can modify the BIOS to disable serial ports and parallel ports not in use on the virtual machine.

A part of this optimization process is sizing virtual CPU and virtual memory resources. As part of the initial planning of any VDI environment, an analysis of how the current environment is being used, including how the four “food groups” of CPU, memory, disk, and network are used, can help determine how many vCPUs are needed, how much memory is required, the proper sizing of the disks, and how much bandwidth is needed by the virtual desktops. For Windows 7, you can leverage the VMXNET3 virtual network adapter to help ensure better performance for virtual machine network activities.

After the virtual hardware is configured, a fresh install of the operating system should be performed, along with any required patches (as per organizational policy) and service packs. In addition to doing a fresh install, consideration should be given to minimizing the number of applications included with the master image. The fewer applications that exist on the image, the better it will perform and the better the end-user experience will be with it. This has the nice side effect of reducing application conflicts and reducing the number of support calls in relation to those conflicts. Ideally, applications should be virtualized using ThinApp and then streamed, either as a mapped drive to the desktop or through other methods. This will also result in a smaller image, which will allow for the faster deployment of images, whether fully provisioned or linked-clone provisioned.

After you have a basic clean image, you can clone this to create other "master" images for each of your use cases. Many organizations make the mistake of creating a single image with multiple levels of snapshots on it to represent different use cases. Having multiple images can result in a little more administration, but it allows for proper image management for each use case and not just from an operating system or application standpoint. An individual master image for each use case means that individual virtual hardware configuration can also be performed.

As mentioned in the steps listed previously, you must choose how to synchronize the guest operating system to a time source. This is a critical step, particularly with regard to Active Directory. As an experiment, I once tested what would happen when a virtual machine was not synchronized. Over an 18-hour period, the virtual machine drifted by 23 minutes! That is a significant time drift that can cause problems for things like Active Directory, and even some applications. As part of VMware Tools, the ESXi host can be selected as a time source. Alternatively, you can use a centralized time source, ideally the one that Active Directory uses. The rule I follow is that whatever you choose should be consistent across the board for all desktops, the Connection Servers, and Active Directory. For updates on how time changes with each ESXi version, check http://kb.vmware.com/kb/1318.

If you need to stop Windows time (W32Time), you can adjust it by modifying the following Registry entry type to **NoSync**:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\
Parameters
```

The last steps to perform are to install VMware Tools and the VMware View Agent. VMware Tools is needed to ensure that the latest drivers and other features specific to a virtual environment are in place. The VMware View Agent ensures that connectivity and management between the desktop and the Connection Server and between the desktop and the client are maintained. Keep in mind that as you install base applications and additional drivers you might need to reinstall VMware Tools again to ensure that the right drivers stay in place.

To install the View Agent, start by double-clicking the installer executable. This file is named VMware-viewagent-*xxxxxx*.exe, where the *xxxxxx* represents the build version. Remember to always read the release notes with each version to see whether a reinstallation of VMware Tools is required before or after upgrading the View Agent. Once the installer starts, complete the steps laid out in the following sections.

Installing the Agent

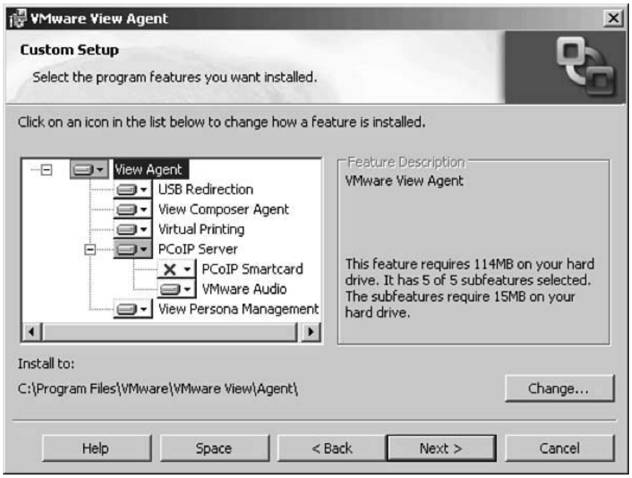
To install the Agent, follow these steps:

Key Topic

Step 1. On the first two screens (the Introduction and the End User Patent Agreement screens), click **Next**.

Step 2. Read the VMware end user license agreement. Then choose **I accept the terms in the license agreement** and click the **Next** button.

Step 3. Choose which options you want to use with the agent. See Table 6-2 for more details on the options shown in Figure 6-1.



VMware View Agent

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- View Agent
  - USB Redirection
  - View Composer Agent
  - Virtual Printing
  - PCoIP Server
    - ☒ PCoIP Smartcard
    - VMware Audio
  - View Persona Management

Feature Description

VMware View Agent

This feature requires 114MB on your hard drive. It has 5 of 5 subfeatures selected. The subfeatures require 15MB on your hard drive.

Install to:

C:\Program Files\VMware\VMware View\Agent\

Figure 6-1 View Agent install options.

Step 4. Select the location where the View Agent will be installed if different from the default location of C:\Program Files\VMware\VMware View\Agent\, and then click **Next**.

Step 5. If Remote Desktop was not already made available, you will seen a screen asking if you want to enable Remote Desktop. Select the choice that is appropriate for the use case of the desktop and click **Next**.

Step 6. Read the summary page and ensure that all the choices are correct. Click **Next** and wait for the installer to finish.

If the installer includes USB Redirection, this forces the Windows OS to reboot to add a virtual USB device to the system.

Table 6-2 VMware View Agent Custom Installation Options

Key Topic

Option	What Does It Do?
USB Redirection	Allows for USB devices connected to the client to be passed through (if allowed by GPO and View Connection Server policy) to the virtual desktop to be used by the desktop.
View Composer Agent	Allows for the creation of special virtual machines as part of the composer process. This is required for master images that will be used to build linked-clone pools.
Virtual Printing	Allows users with the full Windows client to print to their local printer rather than to a network printer.
PCoIP Server	Allows users to connect to the desktop through the View Connection Server by using the PCoIP protocol. Note that by installing this piece on Windows Vista and Windows 7, guest operation will disable the sleep mode service. On Windows XP systems, this disables standby mode. This helps prevent desktops from going into a state that could make them unusable or appear otherwise hung.
PCoIP Smartcard	Allows users to authenticate with smart cards while using PCoIP. If the environment uses smart cards, this setting must be enabled to use them with the PCoIP protocol.
View Persona Management	Allows for profile synchronization from the virtual desktop to the repository to ensure that the user's profile is maintained.

Now that a master image has been created and virtual hardware has been configured, we can begin to optimize the OS.

Creating Customization Specifications

Before getting into the details of OS customization, it is worthwhile to review some of the options needed for Sysprep customized pools. In essence, the customization specification is key to the Sysprep process. Having it ready and tested before doing a pool deployment, whether template-provisioned virtual desktops or linked clones using Sysprep, can make the difference between a successful deployment and a frustrating one. The process to create a customization specification is straightforward:

1. Go to the Customization Specifications Manager found on the vSphere Client Home page.
2. Click the **New** button.
3. Choose the appropriate OS from the Target Virtual Machine OS. In this case, it is **Windows** because Linux is not a supported OS for View.

4. In the Customization Specification Information dialog box, enter a name. You can enter a description as well (helpful when multiple customization specifications exist). Click **Next**.
5. Enter the virtual machine owner's name and organization. This will likely be a generic owner name and the actual organization name. Click **Next**.
6. Specify that the computer name will be derived from the virtual machine name. This option *must* be selected for desktops that will be used with Sysprep. Select **Use the virtual machine's name** and click **Next**.
7. Specify a volume license and click **Next**.
8. Configure the local administrator and click **Next**.
9. Select the time zone and click **Next**.
10. (Optional) If there are scripts or commands that have to be run when the user first logs in, add them to the Run Once page. Click **Next**.
11. Network settings should always be set to **Typical settings** because Dynamic Host Configuration Protocol (DHCP) is currently the only supported addressing method for automated pools. Click **Next**.
12. Add appropriate domain information. The computer should be removed from the domain before you attempt to join the template to the same (or a different) domain. If the computer has not been removed, it is very likely that attempting to join the template to the domain will fail. Click **Next**.
13. Select **Generate new security ID (SID)** and click **Next**.
14. Click **Finish** to save all the settings.

This ensures that any new desktop created will have a consistent look and feel to it. Also, using a customization specification reduces the possibility of user errors interspersed in various desktops as part of their creation.

Most environments will deploy a VDI environment as part of an operating system refresh when moving from Windows XP to Windows 7. To that end, the focus in this chapter is on Windows 7 as the OS that will be optimized. Although the *Optimization Guide* does have two .bat scripts to turn services off, it is important to understand why it is necessary to turn off certain services and why some may be left on.

One of the big challenges with administering desktops is the reliance on the end user to keep the system up to date and to not perform activities that are harmful to the desktop and the network it is part of. In an attempt to reduce vectors of attacks and find ways to optimize performance, Microsoft moved a variety of tasks into service processes that could be automated. This ensures that activities like defragmentation of the disk occur on a regular schedule. As mentioned earlier, these processes were initially designed for physical systems and might not perform well for virtual machines with shared storage. Understanding what each service is, what it does, and whether to allow it to continue to run is a critical part of virtual desktop optimization.

Before looking at each service, note this one important thing: Even if a service is set to Manual, you might want to disable it to avoid the possibility that it might get restarted. You can adjust these services using a post installation script or by building the settings into the ISO image that is created.

The first service to look at is the *BitLocker Drive Encryption Service*. This service was introduced to encrypt whole volumes as an extra layer of protection against compromise, particularly if a laptop (or even just a disk) is stolen. The challenge with this service is that the constant encryption behavior performed by the service increases activity on the disk. This adds additional load for full-provisioned virtual machines that exist on a shared storage array. For linked clones, this method of encryption is unnecessary and would seriously impact performance for the shared C: drive of the replica. The setting for the service defaults to Manual, but you should definitely set it to Disable. Even if the image might be used with local mode, you should avoid the use of this feature. Local mode has its own encryption method, so using this feature would be unnecessary and would only impact performance. Put simply, this feature should not be used in a VDI environment.

The *Block Level Backup Engine Service* was created to allow workstations to perform a block-level backup rather than backing up individual files. This ensures that decentralized environments are backed up and data is protected. Because a VDI implementation relocates all data into the datacenter and allows for centralized backup to occur, this service is not needed. Again, this service defaults to Manual, but you should set it to Disable as a best practice.

Desktop Window Manager Session Manager, besides being a mouthful to say, is a service that may or may not be disabled for an environment. This service renders the desktop Aero environment if used. If the environment requires Aero, this service must be enabled. If Aero will not be used, set the value to Disable. By default, the service is enabled and set to start and run at boot.

One feature that has been part of Windows for a long time is disk defragmentation. Users often forget to do a disk defrag regularly, and as a result, disk performance slows down as fragmentation increases. Making this available as an automated scheduled service addressed this problem. However, having the defragmentation feature running on virtual disks causes unnecessary I/O, particularly for linked clones. The *Disk Defragmenter Service* should be run only on the master image. This will ensure that it is part of the replica, and then whenever a linked clone is refreshed, the disk will be optimized to begin with. By default, the service is set to Manual, but you should definitely set it to Disable for all virtual desktop types.

Sometimes, trying to determine what is causing problems on a desktop can prove challenging. The *Diagnostic Policy Service* was added to help identify problematic issues and to help end users troubleshoot them. For environments where end users need to perform troubleshooting, and for environments with various hardware and software footprints, this service can prove helpful. However, in a View environment, the master image remains unchanged and the hardware settings remain unchanged, so you have no need for this service.

Both the Home Group Listener service and Home Group Provider service were introduced to help make home networking and shared printer setup easier for the home environment. Within Active Directory environments, these services are unnecessary and should have their default setting of Manual changed to Disable for all systems, physical or virtual. Another networking service, the IP Helper service, should also be looked at. If your environment leverages IPv6, it is worthwhile to keep this service; otherwise, you should change its setting from the default of Automatic to Disable.

A number of services are not needed after a desktop is virtualized. These services may offer something for physical hardware, but they become unnecessary because we are leveraging virtual hardware. Leaving the following services running or potentially available could result in excess resource utilization or spikes in disk I/O by the guest OS:

- Microsoft iSCSI Service
- Tablet PC Input Service
- WLAN AutoConfig
- WWAN AutoConfig
- SSDP Discovery

If the desktop I was configuring were physical, I would have to consider whether these services might be needed. For example, the WLAN AutoConfig service is for wireless access, definitely an unnecessary service in a virtual environment because the virtual desktops reside in the datacenter. The Simple Service Discovery Protocol (SSDP) service was designed to help home and small business environments with network IP assignment without needing a full server to provide for things like DHCP and other similar services. Disabling SSDP also means that Universal Plug-and-Play (UPnP) service, the actual service that makes it easier to connect devices to PCs, will have to be disabled (because it is dependent on SSDP).

You still have to consider the use of some services, however, regardless of whether you want to use them because other services or functions might be dependent on the service in question. The Microsoft Software Shadow Copy Provider service, which is used by the Virtual Shadow Service (VSS) for backups, is one such example. If you back up the user data from a central location because of profile configuration, individual desktops do not necessarily need to be backed up and you might consider disabling this service. But if you are using View Persona Management, this service *must* be running because Persona Management utilizes the VSS to maintain the regular in-session backup of the profile between the user session and the repository. In fact, if you are using View Persona Management, even though this service is required, you should not use a VSS-based backup application. This can potentially cause corruption of files, which generally is not a good thing.

The Microsoft Software Shadow Copy Provider service, used as a mechanism for backup, should not be confused with Windows Backup. The Windows Backup service allows for the backup of individual workstations. But in a virtualized environment the desktops are located within the datacenter, and backups are performed either with the Microsoft Software Shadow Copy Provider service or with the backup mechanism that takes care of the centralized files, and personas are kept as per organizational policy.

Because the environment will be hosted within the datacenter and any remote sessions will come through either a View Security Server or a point-to-point VPN, the Secure Socket Tunneling Protocol Service is unnecessary. This service is meant for virtual private network (VPN) connections from the desktop to a VPN broker. Because the desktop has no need to do this, this is definitely a service that should be set to Disable.

The Security Center service might seem an odd service to turn off, but it is appropriate to set this service to Disable for virtual desktops because the features it provides are better provided outside of the guest OS in larger organizations. The Security Center service monitors whether security features like host-based firewall, antivirus, malware detection, and other security programs are running. Because these services often add additional I/O when using traditional versions of them (rather than versions optimized for virtual desktops), it is best not to use them. Products such as vShield Endpoint Protection and other similar vApps, where the protective service runs outside of the virtual machine, are better for overall disk I/O.

One thing that Microsoft attempted to do for Windows Vista (and tried to improve in Windows 7) was to be proactive about starting and loading applications to help speed up performance through the introduction of a service called Superfetch. It uses an algorithm based on commonly used applications to determine what applications would benefit from being cached in memory. Because memory for a virtual machine can be done at a disk level (vswp) as well as within the guest operating system (pagefile.sys), Superfetch use might cause problems for a virtual desktop.

This is one service that should be thoroughly tested to verify whether disabling it will adversely affect specific applications. For most virtual desktop environments, it is safe to disable this service. However, there are always unique cases where specific applications behave differently. One option is to "partially" leverage the Superfetch service by limiting it to just applications. You can also adjust the shadow storage size. The following steps describe how to adjust Superfetch settings. This should be done in the master image/template so that it is pre-optimized when clones are deployed:

Step 1. Click the **Start** button and type **regedit** in the Search box.

Step 2. Press **Enter**.

Step 3. Navigate to the following key location:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\MemoryManagement\PrefetchParameters

Step 4. Double-click the **Enable Superfetch** key. By default the value will be 3. Change this value to one that is appropriate:

0 = Disable Superfetch

1 = Cache applications only

2 = Cache boot files only

3 = Cache everything (default)

Step 5. Choose the value and click **OK**.

Step 6. Select **File** from the top menu and click **Exit**.

Step 7. Click the **Start** button and type **C:\Windows\Prefetch** in the Search box.

A Windows Explorer window showing the contents of this location should open.

Step 8. Delete all the files in this location.

Step 9. Restart the Windows OS. The first reboot might take longer because Superfetch will need to repopulate the C:\Windows\Prefetch location with the appropriate files, depending on which option was chosen.

The decision as to whether to run Superfetch also depends on the kind of virtual machine being used and the disk density of the storage device. Those decisions are generally made during the design phase and are thus beyond the scope of this exam. As a best practice, an administrator should consult the appropriate personnel about the design before making these configuration changes.

Another service that can be disabled is the Themes service. Themes were first introduced with Windows 98 and the Plus! add-on. The idea was to enable end users to customize the desktop look and feel to whatever they wanted. Users could have dancing hamsters, leaves falling, or magical snowy backgrounds. All these animations increase the overall utilization of both CPU and memory resources, which can present a challenge for virtual desktops. VMware recommends disabling this service to reduce resource utilization and improve performance. However, it is a required service for Windows Aero and must be enabled if Windows Aero will be used. If a decision has been made to use Windows Aero, the environment should be tested to ensure that the functionality can be supported without undue performance impact. It might be that not every desktop will need Aero, or perhaps you can offer Aero as an optional desktop choice for some users. The default setting is for it to automatically start. If possible, though, you should set this to Disable.

During the Internet boom of the late 1990s and early 2000s, Windows was one of the more prolific operating systems and was the main target for worm, virus, and other malware creators. Most of these developers depended on users not being savvy with regard to the protection of their systems, and for the most part they were correct. Although Microsoft was not in the antivirus or antimalware business, it did recognize the need for these services. In 2004, it acquired GIANT AntiSpyware (originally developed by GIANT Company Software, Inc.). The idea was to include a combo antivirus/antimalware program as part of the OS so that users would not have to determine which third-party application they should trust. In 2006, Windows Defender was officially released as part of Windows Vista. The initial version of this application was limited to antimalware capabilities. Subsequent versions added an antivirus component, and today both Windows 7 and Windows 8 provide full coverage by default.

The inclusion of the antimalware portion was critical as users ventured more and more out to the Internet and spyware was becoming more and more prevalent. For home users and small offices, this is a nice piece of software to help secure desktops. However, in organizations, it is not sufficient because the user can turn off the protection. In addition, the program regularly scans the hard drive for any potential unwelcomed “visitors.” For a virtual enterprise environment, using something like vShield Endpoint or a similar product, where the scan occurs in active processes through the hypervisor, results in less disk I/O impact compared to traditional system protection software. If Defender is going to be used in an enterprise environment, no change needs to be made. If an enterprise application will be employed, you should change this service from the default of Automatic to Disable.

Another service with similar conditions is the Windows Firewall service. This service began with Windows XP as the Internet Connection Firewall service (ICS), which was a basic firewall application. By default, the service was disabled, largely because of concerns about compatibility with existing programs. However, this mindset changed after the Blaster and Sasser worms began to ravage the Internet. With Windows XP Service Pack 2, the service was renamed and significantly improved. One of the main improvements was that the service was enabled by default. With each release, Microsoft has added significant improvements to this service. If this will be the only firewall for your virtual desktops, leave the service running. It is best to ensure that the settings for the service are controlled by Group Policy Objects (GPOs) and that appropriate settings for access are configured. If an organizational firewall will be in place, whether physical or software based, this service should be disabled.

It might seem odd to disable the Windows Error Reporting service, but the logic behind doing so is twofold. This service (originally known as Dr. Watson) was designed as a way for application developers to get error reports sent to them, over the Internet, when errors occurred. This would help lead to better programs and fewer issues. Although this is a good idea for the average home user, for organizations it is better for the IT team to be aware of any issues and address them as part of their support mandate. For an ideal virtual desktop environment, any support application would be virtualized and in a central location where logs would be collected. In addition, because of the nature of virtualization, the number of errors that occur due to conflict with other programs (the more common scenario) will lessen significantly. This brings us back to the clean image concept. Assuming a clean image was used, the need for this service is minimal, and the performance impact from using the service makes it disadvantageous. This service defaults to Manual, but you should set it to Disable.

The Windows Media Center was designed as a way for Windows to control various media devices and to provide access to various devices like TV tuners or FM access. The Windows Media Center Receiver service and the Windows Media Center Scheduler service are not needed for desktops because there is no access to a device like a tuner on the ESXi host. Both services default to Manual, but you should set them to Disable.

The states of the last three services that we look at here depend on use cases and fall into the “it depends” category. The utility of the Windows Search service, the Windows Update service, and the Offline Files service depend largely on how and if they are needed and used. The Windows Search service enables users to find files or folders on the desktop. If very little virtual desktop searching is necessary, you should disable this service. In environments where searching is necessary, it is wise to reduce the density of desktops found within the datastore to help reduce conflicting I/O behavior from the resulting searches against other desktops with similar activity.

The Windows Update service, another service introduced with Windows 98, was originally designed to give users access to additional themes, games, driver updates, and other features not found with the base operating system. Over time, however, this service came to be used for patch management, the most notable being the Y2K fixes. The ability to keep the system up to date in the face of challenges and threats from the Internet has been critical to keeping Windows systems running. However, for virtual environments (particularly linked clones), this service might not be needed. The base image and any patching should come from a central location after sufficient testing of the patch has been performed. (To this day, I still have nightmares over NT4 and Service Pack 6.) Linked clones should never have the Windows Update service running because a refresh would cause any updates to no longer exist. It is better to have the update applied to the base image and a recompose done to ensure that the whole pool has the updated features as part of the desktops. The default setting for the Windows Update service is Automatic, so this should be changed to Disable unless needed (say, for a local mode desktop or fully provisioned virtual machines).

The last service, the Offline Files service, was created to enable users to access files even when the network is down. Because the virtual environment is based on the network, this service is not really needed. Again, the exception would be for local mode desktops. The default for this service is Manual, but you should change it to Disable.

You can disable all of these services manually via the graphical user interface (GUI), or you can disable them through command-line options or even a PowerShell script. To do this via a script, use the following syntax:

```
Powershell Set-Service <Service Name> –startuptype "disabled"
```

The *VMware View Optimization Guide for Windows* 7 comes with two batch-shell scripts, one for environments leveraging Persona Management and one for use without Persona Management. These scripts will disable all the services reviewed in this section. Because the scripts are text based, you can modify them as needed to ensure that master images are configured according to use case requirements.

A last thought with regard to these services is this: Disabling these services makes complete sense for virtual desktops that reside in the datacenter. If local mode will be used, any desktops that run locally can actually benefit from leaving these services running. While disabling the services can provide some performance optimizations, the use cases should be carefully considered before any changes are made.

Additionally, the services may still need to be used for any physical desktops that will exist in the environment. This highlights the importance of having a separate organizational unit (OU) for the virtual desktops apart from that of any physical desktops. Conversely, it might be important to block the effects of GPOs used for the physical desktops from being applied on the virtual desktops because those GPOs may have an adverse effect.

To help with the variety of GPOs that could be used within an environment, leverage loopback policy processing. This will tie the use of GPOs to the computer OU the user is in and ensure that the appropriate GPOs are applied, particularly when users move between different desktop OUs.

Although the majority of the optimization benefits come from disabling services, some benefits derive from GPOs being leveraged or through manual adjustments to the master computer image. The assumption may be that everything should be removed or disabled, but certain settings are required, such as enabling RDP access. If these settings are not configured as part of the base image and the user needs RDP to access the desktop, this would present an obvious challenge for accessing the environment. In this section, we take a look at adjustments that should be made using the GPO Editor. To get to the editor, follow these steps:

Step 1. Click the **Start** button.

Step 2. In the Search box, type **MMC**. This opens a blank Microsoft Management Console (MMC).

Step 3. Select **File** from the menu.

Step 4. Choose **Add or Remove Snap-ins**.

Step 5. From the Available Snap-ins list, find **Group Policy Object Editor**.

Step 6. Click the **Add** button.

Step 7. For the Group Policy Object, choose either **Local Computer** (beneficial for computer specific policies like Themes) or the appropriate domain.

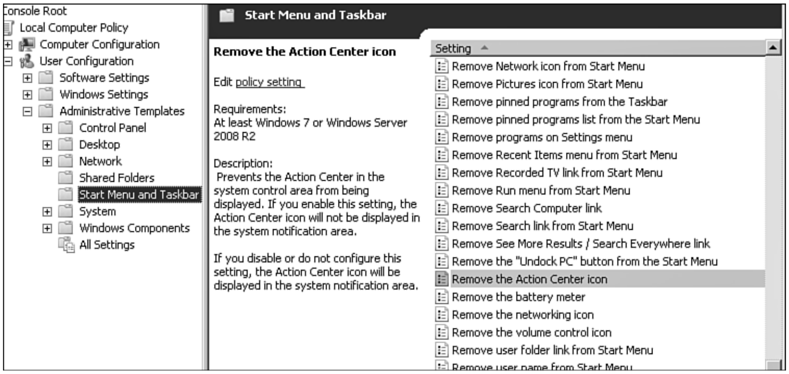
Step 8. Click **Finish** and verify that the snap-in shows in the Selected Snap-ins window.

Step 9. Click **OK**.

Over the years, Microsoft has tried to get end users to realize the importance of addressing security issues and updates. Of equal importance was identifying when a Windows system did not have enough protection in place when the user was online. As Microsoft introduced more security features as part of the Windows OS, it became important to let users know when those security services (such as Windows Firewall or Windows Defender) or replacement services weren't running so that the user would be aware of the issue, and thus protect the OS. To that end, Microsoft added a mechanism to alert users when a vulnerability was present.

Originally known as the Windows Security Center, the Windows Action Center lets users know when those services are not enabled or available and it provides diagnostic advice on how to address maintenance issues (for example, patch updates). Given that the services might have been disabled as part of the optimization process, this could result in warnings that would be unnecessary in a virtual desktop environment and resources being used by the Action Center. By default, this service cannot be turned off completely. However, through a GPO setting, you can disable and remove the Action Center by changing the value of the Remove the Action Center Icon to Enabled in the Administrative Templates under User Configuration, as shown in Figure 6-2. This needs to be done for VDI environments because the security comes through mechanisms in the datacenter rather than through the Guest OS.

Key Topic



Remove the Action Center icon

Edit policy setting

Requirements:
At least Windows 7 or Windows Server 2008 R2

Description:
Prevents the Action Center in the system control area from being displayed. If you enable this setting, the Action Center icon will not be displayed in the system notification area.

If you disable or do not configure this setting, the Action Center icon will be displayed in the system notification area.

- Remove Network icon from Start Menu
- Remove Pictures icon from Start Menu
- Remove pinned programs from the Taskbar
- Remove pinned programs list from the Start Menu
- Remove programs on Settings menu
- Remove Recent Items menu from Start Menu
- Remove Recorded TV link from Start Menu
- Remove Run menu from Start Menu
- Remove Search Computer link
- Remove Search link from Start Menu
- Remove See More Results / Search Everywhere link
- Remove the "Undock PC" button from the Start Menu
- Remove the Action Center icon
- Remove the battery meter
- Remove the networking icon
- Remove the volume control icon
- Remove user folder link from Start Menu
- Remove user name from Start Menu

Figure 6-2 GPO of Action Center

Most applications leave a trail of their activities within the event log. This helps users troubleshoot when application issues arise. The default size of the logs is 1024KB (or 1MB). Depending on the number and complexities of applications on the desktop, the values for these logs might need to be adjusted. You can adjust the various log sizes, in chunks of 64KB, by going to the Event Log Service in the Administrative Templates under Computer Configuration. This particular setting would benefit from being specific to the image rather than applied from the domain.

The same is true for GPO configuration if the Windows Firewall is going to be used. If the Firewall service is disabled, there is no need for a GPO configuration. If the firewall is used, it will be necessary to adjust the settings for items such as Define Port Exceptions, Allow Logging, Allow Remote Desktop Exception, and other features would be necessary for a virtual desktop. The choices made will depend on the use case of the desktop. As part of the test of the master image, adjust each setting one at a time until you reach your required security level.

Internet Explorer is the browser that many users choose for their web experience. If this browser is used in your environment, you must be aware of two settings, one under Computer Configuration and one under User Configuration, that must be adjusted to ensure a better end-user experience. The first, Internet Explorer Settings (cache), is found under User Configuration. By default, Internet Explorer has a cache of 50MB. To improve performance and behavior, you can configure the setting for temporary Internet files to delete upon browser closure. This helps reduce the amount of space used by the browser on the desktops and ensures that data is not carried over from session to session, particularly for fully provisioned virtual machines that are in a floating pool. You can find this setting at **Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Advanced Page**.

The second setting, Internet Explorer Settings (using the First Run Wizard), enables you to configure the default behavior of Internet Explorer when it is first launched. By default, Internet Explorer starts by going to the Welcome to IE page. However, this can be changed to a home page appropriate for your users. If you configure this setting in a GPO, you can prevent users from changing the default home page to another that could be detrimental to the performance of the virtual desktop. Because this setting is applied to the computer configuration, this can be done as part of the master image to ensure that it carries over to all users. You can find this setting in the Administrative Templates at **Windows Components > Internet Explorer**.

Each use case can have a different default home page if necessary because the home page option is configured under User Configuration and can be applied to different OUs. The default home page option is found in the Important URLs GPO under Internet Explorer Maintenance in the Windows Settings section. You can configure other URLs here, too, such as the Search bar URL and Online support page URL. You can configure each setting as appropriate for the organization.

When files are deleted on a Windows system they end up in the Recycle Bin. The files are not deleted until you choose Empty Recycle Bin, and even then the files are not actually deleted and can be recovered using the Restore option. Beginning with Windows Vista, the ability to recover recycled files became possible for each drive. The capability to allow or disallow the recovery can either be adjusted via GPO or configured in the Registry. In a virtual environment, enabling this setting using a GPO allows you to apply it based on each use case found within the environment rather than as a *carte blanche* setting. You can find this setting under **User Configuration > Administrative Templates > Windows Components > Windows Explorer**.

Although PCoIP is the default protocol for a View implementation, some end-user clients must use RDP. To ensure that those users can connect using RDP, and to enable the use of network-level authentication, you must enable the settings found in Administrative Templates under Computer Configuration. In the **Windows Components > Remote Desktop Services > Remote Desktop Session Host**, you can enable the Connections and the Security options.

In the information age, keeping up to date on information can be a challenge. One often used technique is to utilize Rich Site Summary (RSS) feeds. With RSS, websites can publish brief synapses of information to a browser link or other location so that interested individuals are made aware of changes or to aggregate website updates from a variety of sites. To help keep these feeds up to date on a Windows system, Windows 7 typically runs this service in the background. Not surprisingly, this can have an adverse performance effect. Some users (for example, power users or local mode users) might require this feature, so disabling it for them would not be beneficial. If a use case requires the feature to be disabled, you can do so in the Windows Components of the Administrative Templates under User Configuration.

Screensavers were first implemented as a way to save cathode ray tube (CRT) monitors from "ghost" burn-in of the desktop. Over the years, as newer technology was introduced, the need to use screensavers for that purpose lessened, and screensavers began to be used more commonly for security and/or entertainment purposes. The challenge with screensavers is that the more complex they are (for example, screensavers that show a lot of images or have many moving parts) the greater the possibility of a performance hit. In virtual environments, screensavers not only cause performance issues, but in some cases they have been known to cause the desktop to hang. So, the general rule is to not enable screensavers.

For environments that need screensavers (for example, in environments where users forget to lock their desktops), it is worthwhile to configure a GPO for users. As part of the configuration, you can configure specific features of the screensaver so that it works in a manner that benefits both the user and the organization. These features include configuring a requirement for a password to be used to unlock the screensaver, setting a timeout period of inactivity before launching the screensaver, and choosing a specific screensaver. Because these settings are tied to the user configuration under the Control Panel in the Administrative Templates, they will follow the user regardless of the desktop he uses (if that is the desired result).

As the Windows operating system became more and more mainstream, drivers, applications, updates, hardware changes, and more were added to the environment in so many different permutations that the resultant side effects could not be predicted. As a result, these variations could potentially leave a desktop unstable and unusable, frustrating users because of the time needed to perform a full reinstall or an in-place upgrade. These frustrations don't even account for the possibility of data loss. Because of this issue, Microsoft introduced System Restore, which allows the OS to be restored to a previous state that was functional (sometimes referred to as last known good state). This feature first appeared in Microsoft Me and has evolved over the years. For environments that have a wide variety of hardware/software combinations, this feature has saved more than a few users from having to do a full reinstallation due to the installation of faulty hardware or software.

Because virtual hardware never changes for virtual environments, and because the base Guest OS is configured based on the virtual hardware configuration, the need to return to a last known good state is lessened significantly. As a result, System Restore becomes an unnecessary feature, especially for desktops like those found in a linked-clone pool. So, it is beneficial to configure the Computer Configuration GPO to turn off System Restore. You can find this under the Administrative Templates in the System section.

The use of desktop wallpaper represents another challenge for desktops in a similar vein as screensavers do. The challenge with wallpapers is that they consist of complex images that can cause performance degradation. To alleviate performance concerns, you should configure the desktop to use either a solid-color background or no background. To configure the desktop not to use a background image (and use the default color associated with the desktop profile) using a GPO, go to the GPO Editor under User Configuration in the Desktop section of the Administrative Templates and set the value for Desktop Wallpaper equal to a blank space. The other option is to set the value to a nonexistent file. This will prevent user changes to the desktop background.

Although some might think that the Windows Sideshow service is related to a screensaver concept, it actually relates to how information is displayed on secondary display devices, including mobile phones, tablets, and so on. Because the desktop is located in the datacenter, this is not possible. So, disabling this feature via GPO is important because this will reduce the number of services active on the base image. You can find this particular GPO under Computer Configuration in the Administrative Templates within the subgroup of Windows Components. Just enable the **Turn Off Windows Sideshow** option.

Summary

This chapter covered a significant amount of information related to optimizing the virtual desktop by optimizing the underlying operating system. The operating system features enabled or disabled should not be chosen based only on the performance benefit but also based on the use case for the desktop. This will ensure that the configuration satisfies the use case while also providing the best possible performance. Without properly optimizing the virtual desktop, there is a good chance that the end user experience will suffer regardless of the chosen protocol.

In the next chapter, we look at a unique desktop configuration known as kiosk mode.

Exam Preparation Tasks

Review All Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. Table 6-3 lists a reference of these key topics and the page numbers on which each is found.

Table 6-3 Key Topics

Key Topic

Key Topic Element	Description	Page
List	How to create a build and optimize a virtual desktop	136
Step list	How to install the View Agent	140
Table 6-2	VMware View Agent Custom Installation Options	141
Figure 6-2	Image showing the GPO for Action Center	151

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

EOIT/BYOD, IOPS, P2V, MDT, ThinApp, master image

Review Questions

You can find the answers to these review questions in Appendix A.

1. An end user has difficulty logging in to his View desktop. Upon investigation, the administrator discovers that time synchronization is not configured. Which step should the administrator perform to correct the issue?

   a. Let Active Directory reset the virtual machine time.

   b. Set the virtual desktop to sync time with the ESXi host.

   c. Set the virtual desktop to sync time with another virtual desktop.

   d. Let Active Directory reset the virtual machine token time.

2. A CEO decides to let employees purchase their own laptops or tablets for use as a work device. Which of the following acronyms describes this policy?
   - a. EOIT
   - b. COIT
   - c. BYOB
   - d. PCOD

3. It is important to "right size" a virtual machine. What does this term refer to?
   - a. Allocating maximum memory and CPU resources
   - b. Using P2V to create the virtual desktop
   - c. Sizing a virtual machine for all four "food group" types: CPU, memory, disk, and network
   - d. Sizing a virtual machine for all four "food group" types: pizza, soda, ice cream, and chips

4. VMware recommends creating a master image from scratch. What method is strongly discouraged from being used to create a master image?
   - a. Template-created image
   - b. Clone-created image
   - c. P2V-created image
   - d. MDT-created image

5. What option is not a valid choice when installing the View Agent using custom installation options?
   - a. View Composer Agent
   - b. Virtual Printing
   - c. RDP Smartcard
   - d. View Persona Management

6. What service is needed if Aero is to be used in a Windows 7 virtual desktop?
   - a. Desktop Window Manager Session Manager
   - b. Aero Desktop Window Manager
   - c. Desktop Windows Session Manager
   - d. Aero Window Manager Session Manager

7. Which service should be disabled because the virtual hardware in a master image will not be altered?
   a. Diagnostic Policy Service
   b. Master Hardware Service
   c. Hardware Diagnostic Service
   d. Diagnostic Hardware Service

8. If you use a VSS backup service, what service should not be used?
   a. Roaming profiles
   b. Persona Management
   c. Profiles service
   d. Persona service

9. What is the main reason for disabling the Windows Defender service?
   a. Causes too much I/O during scans
   b. Not available in Windows 8
   c. Causes too much swapping
   d. Only works with Internet Explorer

10. What common Windows element should be disabled or locked via GPO to help improve a performance impact and to prevent the virtual desktop from locking up?
   a. Accessibility
   b. Screensaver
   c. Screen resolution
   d. RSS feeds

This page intentionally left blank

Index