Making Everything Easier!™

Red Hat Special Edition

Virtualization

FOR DUMMIES®

Learn:

- **How you can use virtualization to control project costs and do more with less**
- **The answers to some common questions about virtualization**
- **How security issues play out with virtualization**

Brought to you by

redhat.

Richard Blum

About Red Hat

Red Hat is the world's leading provider of open source solutions, offering choice to customers building open source IT infrastructures.

Its unique business model provides open source subscriptions for its high-quality, affordable technology. Its operating system platform, Red Hat Enterprise Linux, and virtualization solution, Red Hat Enterprise Virtualization, together with applications, management, service-oriented architecture (SOA) solutions, included in the JBoss Enterprise Middleware portfolio, and cloud solutions, deliver industry-leading value. The company is based in Raleigh, NC and has 66 offices around the world.

Virtualization FOR DUMMIES®

RED HAT SPECIAL EDITION

by Richard Blum

Wiley Publishing, Inc.

Virtualization For Dummies®, Red Hat Special Edition

Published by
Wiley Publishing, Inc.
111 River Street
Hoboken, NJ 07030-5774
www.wiley.com

Published by Wiley Publishing, Inc., Indianapolis, Indiana

ISBN: 978-1-118-08817-3

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Project Editor: Jennifer Bingham
Editorial Manager: Rev Mengle
Business Development Representative: Melody Layne
Custom Publishing Project Specialist: Michael Sullivan
Project Coordinator: Kristie Rees
Layout and Graphics: Claudia Bell, Carl Byers
Proofreader: Debbye Butler

Introduction

Welcome to the fascinating world of virtualization. In this book, I introduce you to the benefits of using virtual servers and desktops in your data center. My goal is to initiate you into the rapidly growing ranks of virtualization users, allowing you to quickly save time and money in your IT projects. This book focuses on the Red Hat Enterprise Virtualization products, but also gives you a general overview of the topic.

About This Book

My objective is to keep the amount of technobabble to a minimum and stick with plain English as much as possible. Trying to grasp the concepts behind server virtualization can be tricky, so I include a few examples plus some detailed explanations to help give you the most information about a virtual server environment without turning this into a PhD thesis.

Think of this book as a friendly guide to tackling the terminology and concepts behind virtualization. Although virtualization can get complicated, the basics are fairly straightforward after you get a handle on them.

Although it may seem, at first glance, that working with virtualization requires advanced computer science training, it's not true! This book focuses on Red Hat Enterprise Virtualization, which makes implementing server and desktop virtualization in any computer environment much easier than you think!

This book was written for, with information supplied by, Red Hat.

Icons Used in This Book

Within each chapter, I use icons to highlight particularly important or useful information. You find the following icons in this book.

The Tip icon flags useful information that makes living with your virtual server system even less complicated than you feared that it might be.

This icon flags information that you may want to write down somewhere so that you don't forget it. Or maybe just tie a piece of string around your finger to remind you.

This icon flags information that lets you know that you need to be careful.

Chapter 1

Virtualization 101

In This Chapter

- Defining virtualization
- Introducing server virtualization
- Explaining the hypervisor

Welcome to the world of virtualization. Although the phrase *virtual machine* may remind you of the *air guitar* you played as a child, there really is something behind virtualization. In this chapter, you find out just what virtualization is, and get an introduction to server virtualization and the hypervisor.

Defining Virtualization

Just a few years ago, the typical server in your data center had just (barely) enough processing power, memory, and disk space to run one application (like a database, a mail server, or a web server) and that's it. Each application you wanted to run got its own physical server. And soon your data center was full of separate servers chugging away, serving applications to your customers and employees.

Fast forward a few years. The number of applications in a typical data center has exploded — now you have a whole bunch of racks containing a whole bunch of servers, each box running one application. In the meantime, servers have become more powerful, with more processing cores, more memory, and more disk space than ever before. That's a lot of resources in a single server, but they're trapped, available only to one application.

Virtualization is a technology that lets one big physical server pretend to be a whole bunch of little PC machines, each with its own processor, memory, disk, and network devices.

Explaining Server Virtualization

When most organizations get started with virtualization, they start with the servers in their data center. *Server virtualization* is when you virtualize the servers that are providing the applications that run important programs like accounting, web servers, CRM, and others to your users and your customers.

Consolidating servers

When you can run more than one application per server, you can fit more applications into less space. Say you have 100 applications and you don't want to run 100 servers. You can actually run those 100 applications on 10 physical servers. This is called *server consolidation.* Each of these *virtual servers* thinks it is running on its own physical server; instead it's actually sharing one physical server and its system resources (CPU, memory, and so on) with many other virtual servers. Each virtual server has its own dedicated and independent environment and thinks it is running independently. The physical server can therefore run different versions of Linux on the different virtual servers. You can even mix and match Linux and Windows environments.

You also get the benefit of *hardware abstraction.* With virtualization, each of your virtual servers thinks it is installed on exactly the same hardware, no matter what the physical hardware really is. Therefore, if you have to move a virtual server from one physical host server to another, you don't have to worry that the host servers are from different manufacturers, or have different network cards or a different motherboard. As far as the virtual server is aware, it's still running on the same hardware it was running on before.

Virtualization also gives you higher resource utilization. With physical servers, you often had to buy a server big enough to handle the *peak load* (which means that you had to

accommodate for the period of greatest usage that would ever happen), even if 99 percent of the time, the server was being underutilized. In virtualization, you can size for the average load. If one virtual server needs a lot more resources, it can borrow them from other host servers that are underutilized. You can actually use more of the resources you've already paid for.

With virtual servers, your deployment time also decreases substantially. If you need a new server to host a new application, you don't have to buy a new server, wait for it to arrive, install it, and then install the operating system and application. You just click a button and create a new virtual server. And you can create a *virtual server template,* a complete copy of a commonly used server and its applications that you can deploy over and over.

Virtual infrastructure

Virtualization is a great technology when used on a single physical server, but it really begins to pay off when you run virtualization on multiple servers. Products like Red Hat Enterprise Virtualization for Servers allow you to run many physical servers with many virtual machines on them, and manage the whole infrastructure centrally.

What if you deploy a virtual server on one physical host but need to move it somewhere else? With virtualization, you can easily move any guest virtual machine to any host physical server. Thus, if one application starts taking over too many resources on one server, you can easily live migrate it to a less active host server, without having to go through the process of building a new server. *Live migration* allows you to move a running virtual machine from one physical server to another with no downtime. Users don't see any disruption. Technology like system scheduler can use live migration throughout the day to move your virtual machines around dynamically to balance load or to conserve power, based on policies you configure. For example, if one of your virtual servers suddenly needs a lot of power and it's impacting the other virtual machines, the system scheduler can live migrate that virtual machine to another physical server that's not so busy.

All these things can be done from a command line, but it's easier to manage from a graphical user interface. Red Hat Enterprise Virtualization Manager is the Red Hat management interface.

What about up-time?

With the high demands of 24/7 operation, availability is a crucial factor for any application. Sometimes physical servers fail unexpectedly, and sometimes you need to do maintenance. Having an application fail at any time of the day or night can be catastrophic for your customers or your business.

So what happens when one of your virtualization host servers goes down? All the virtual machines on that host go down too. You can make your mission-critical virtual machines *highly available,* so they will automatically restart on a running physical server. For planned outages, like a firmware upgrade, you can use maintenance manager to live migrate all the virtual machines safely to another physical server. Then you can perform maintenance, reboot, and return the virtual machines automatically.

What about security?

With server virtualization, you can have many virtual servers running on a single physical server. How can you guarantee the security of your systems in such a mixed environment? How can you guarantee that users on your "Website" virtual machine can't access data on your "Finance" virtual machine?

The short answer is that all virtual machines are completely separate, running in their own virtual world on the host server. There's no chance that any application files running on one virtual server can find their way onto another virtual server. (I go into this in more detail in Chapter 2.)

What about virtual desktops?

Talking about virtual desktops could take a whole chapter. In fact, it does. See Chapter 4 for the ins and outs of desktop virtualization.

Getting to Know the Hypervisor

So what makes virtualization tick? The hypervisor. The *hypervisor* is a special piece of software that acts like a traffic cop to direct traffic from the multiple virtual machines running on a single physical server. When a virtual machine needs to access memory or the CPU, the hypervisor schedules each virtual machine's request so that they don't conflict.

Much of the time, virtual machines are sending simple instructions, like requests to access memory or perform a calculation. These instructions can be passed to the hardware directly, with the hypervisor scheduling the requests. When the hypervisor can pass instructions directly to the hardware without modification, it's nearly as fast as when the operating system is running on bare metal.

Sometimes, however, the virtual machines need access to physical hardware, like the network card. There are also certain operations only the operating system is allowed to make, and PC-based servers were designed to handle only one real operating system. The hypervisor can't pass these instructions directly to the hardware — it would crash the server. You could modify every operating system you run to make it virtualization aware, but that would make virtualization very difficult to implement. So the hypervisor provides two solutions:

- **Hardware emulation** is when the hypervisor pretends to be the CPU or a piece of hardware, like a virtual network card, and makes each virtual machine think it has its own hardware. The virtual machine thinks it has full control and sends an instruction. The hypervisor intercepts the instruction, runs it in emulation, and then returns the expected result back to the virtual machine. With good emulation, you give each virtual machine the illusion that it has its own dedicated hardware. The disadvantage of emulation is that it happens in software, so it can be very, very slow. The more the virtualization system has to emulate, the slower the virtual machine is, compared to bare metal.
- **Hardware-assisted virtualization** takes advantage of technologies built into the latest Intel and AMD chipsets. Called VT-x and AMD-V, respectively, these technologies do the hard work the hypervisor used to have to do with

> emulation and they do it in hardware, where it's much faster. The virtual machines get the advantage of emulation but with the speed of direct hardware access. Here, the hypervisor still intercepts the command from the virtual machine, but instead of emulating, it passes the command to the special hardware-assisted virtualization technology.

Most modern hypervisors take advantage of both emulation and hardware-assisted virtualization. Older hypervisor technologies have enough emulation code that they can run, albeit slower, on servers without VT-x or AMD-V. The Red Hat Enterprise Virtualization hypervisor leverages hardware-assisted virtualization extensively, so it doesn't have to offer a large amount of redundant emulation code. But it does require that these extensions be present and enabled in the BIOS.

Chapter 2

Looking at Virtualization and Security

In This Chapter

- Looking at SELinux
- Using security in layers
- Playing in the sandbox

The hot topic in just about any IT circle these days is security. It's no surprise that the virtualization world has given security a high priority in implementing virtualization solutions. In this chapter, I discuss how Red Hat Enterprise Virtualization implements security, and how you can use that security in your IT environment.

Battening Down the Hatches

The most vulnerable part in any virtualization environment is the host virtual server. The host virtual server is the gatekeeper to all the guest virtual machines, often controlling what hardware they have access to. If the host virtual server becomes compromised, the virtual machines will soon follow. Whether the host virtual server is a thin hypervisor program or a full operating system, the capability to ensure that it remains virus-free and uncompromised is crucial.

Red Hat Enterprise Virtualization leverages the Linux operating system. The Linux operating system is an open source solution that employs the latest technologies in security protection. One of these technologies is *Security Enhanced Linux,* or SELinux. The SELinux feature provides additional security to the standard Linux operating system. It was designed specifically by the U.S.

Government's National Security Agency (NSA) to harden Linux implementations that require high levels of security.

This section takes a look at the SELinux environment used in Red Hat Enterprise Virtualization environments, and shows just why it's considered the best security solution available in the Linux world.

Mandatory security

The core of SELinux is a method called *Mandatory Access Control* (MAC). In a MAC security setup, the Linux kernel assigns and enforces the security settings for all items on the operating system. This includes all files, folders, and even running processes on the system. No element of security control is left to the discretion of the individual users.

Setting rules

The key to MAC security is a set of *policy rules* — set by the system administrator, and enforced by the Linux kernel. The policy rules dictate what security objects may be accessed by other security objects, and what security objects have privileges to perform tasks on the system. No individual user or application can circumvent the policy rules defined by the system administrator.

In SELinux, every file, process, and user is an object that is controlled by a MAC security policy rule. The administrator of the host operating system sets the MAC policy rules from a graphical interface.

Standard Linux security

In a standard Linux installation, individual users on the system handle their own security. Any user can grant privileges on his or her files and folders to any other user on the system. This method of security is called *Discretionary Access Control (DAC)*.

Although DAC security provides a robust climate for sharing files and folders, it's not the most secure environment. Not knowing what files and folders individual users are sharing can be a security nightmare for system administrators.

Laying It on Thick

One key element to security is *layering*. By layering security, you can provide multiple security features to each object. Providing more than one approach to security is a fundamental feature of any quality security system.

With virtualization, security layering is built in. The SELinux environment controls the underlying host virtual server, and each individual guest virtual machine provides its own security from intrusion, using its own standard security features.

So if you're running a Microsoft Windows operating system as a guest on Red Hat Enterprise Virtualization, you can still run the standard Windows security software you normally run on a server. These security products provide protection to the individual guest virtual servers above the protection provided by the SELinux security environment on the host virtual server.

If you run different guest operating systems on your host virtual server, each one can still run its own security software, as shown in Figure 2-1.

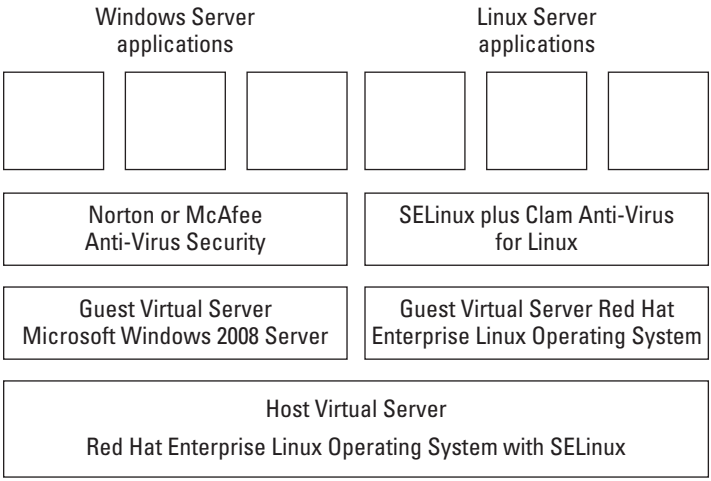

Figure 2-1: Running separate security solutions for each guest virtual server.

Each guest operating system is secure, not only using its own security infrastructure, but also benefiting from the host operating system's security.

Restricting Play

A key security component in Red Hat Enterprise Virtualization is protecting individual guest operating systems running on the host server. The virtualization environment should provide the same protection that would be available had the guest virtual machines been on separate physical servers. In the virtualization environment, there are three main goals for guest server security:

- Prevent unauthorized communication between guest virtual servers
- Prevent a guest virtual server from accessing resources not assigned to it
- Prevent any guest virtual server from taking over the host operating system

These rules are crucial to the complete security environment in the virtual server. Red Hat Enterprise Virtualization restricts the guest virtual machines to ensure each guest has access to only the hardware resources you define. The host hypervisor system is completely shielded from the guest virtual servers. Guests that attempt to oversubscribe hardware are thwarted by the hypervisor, ensuring that no runaway process or any guest operating system can take down the entire host virtual server environment.

Chapter 3

Examining the Advantages of Virtualization

In This Chapter

- Keeping your projects on budget
- Using less energy
- Doing more with less

In these tough economic times, business decisions aren't made in a vacuum. Plenty of outside considerations have an impact on the implementation of any technical solution. Nowhere is this truer than in the data center. This chapter explores the business benefits of implementing virtualization.

Controlling Project Costs

The bottom line for any technical project is the financial bottom line. This section discusses the economic benefits of implementing a virtualization solution, and shows how you can justify a virtualization project to the bean counters.

Offsetting physical server costs

In a standard environment, deploying new server applications or adding desktops usually means having to purchase and install new physical hardware. Although funds for purchasing software and paying programmers may be in the budget, the money used to purchase new hardware often requires capital funds, and in many environments, the ability to acquire capital funds can make or break a project.

However, using virtualization to implement new projects means you don't have to buy new hardware for each project (see Chapter 1). Instead, you can make a single upfront purchase of the physical server hardware, and then just purchase the necessary guest virtual machine operating systems and software to add new projects to the existing physical hosts as they come up. Without having to go through a capital budget fire drill for each project, you may even be able to streamline the time it takes to implement projects!

Eliminating redundant costs

With any high-profile application, backup and contingency capabilities are a must. With standard server solutions, having to dedicate a backup server for a project often means having to purchase redundant equipment, further adding to the cost of the project.

With a virtualization solution, you don't have to pay for redundant equipment for each project. Guest virtual machines can easily be moved to other physical hosts, and even configured to monitor a primary virtual machine and take over if the primary fails.

The Red Hat Enterprise Virtualization solution provides this capability with the Red Hat Enterprise Virtualization Manager. This management server allows you to easily create load balancing and failover environments for all your applications, using a minimum number of physical hosts.

For example, two physical servers can provide a simple load balancing and failover environment for three guest virtual machines. Thus, instead of having to purchase six total physical servers to provide complete redundancy, you only need two physical servers. The Red Hat Enterprise Virtualization Manager can monitor the three individual guest virtual machines, and enable the failover guest virtual machines when necessary. Further, if one guest virtual machine is under heavy load, the other two under lower load can be live migrated to a less busy physical server, allowing the heavily loaded server to receive the maximum amount of compute resources available.

This feature greatly reduces the cost of having failover equipment available for each application.

Going Green

The drive to save energy and protect the environment is taking over the business world. Trying to reduce energy consumption and electronic waste can be a full-time job, especially when it comes to computer environments.

Nowhere is energy consumption more prevalent than in the computer room. Implementing virtualization can help you run a more energy-efficient and environmentally friendly data center. Some of the environmental benefits of virtualization are:

- **Electrical cost:** A physical server requires the same amount of electricity whether the CPU is running at a low load or at high load. Working with unused CPU capacity on a physical server can reduce the number of physical servers you need in your data center, and thus reduce your electrical consumption.
- **Cooling cost:** Having fewer servers spewing heat puts less load on your cooling system, and may even allow you to decrease the capacity of your cooling system.
- **Hardware waste:** Eventually, your shiny new server will need to be replaced to keep up with new operating system requirements. With fewer physical servers, there's less hardware to replace when it comes time for upgrades.

Not only does this help the environment, but these cost savings also add up, and over years, they may more than make up for the cost of virtualization.

Doing More with Less

With shrinking budgets, many organizations are required to reduce resources. For data centers, that often equates to both less space for data centers and fewer support workers to manage the computing environment. Virtualization can assist you in your efforts to continue your operations even in times of reduced resources.

Using less space

As organizations consolidate, you often have to use less space to perform the same functions. With the reduced physical server count provided by server virtualization, you can think about using smaller, more energy-efficient data closets, supporting a couple of racks of servers and associated hardware. You could also consolidate many departmental data centers into a centralized data center. The departments can still maintain control, but the physical space is centralized, allowing optimization of expensive data center space, power, and cooling.

Maximizing staff

Shrinking budgets often go hand-in-hand with smaller personnel budgets. Because of shrinking staff sizes, system administrators need to support more servers and desktops, and the capability to have more work performed automatically becomes a necessity. Virtualization comes to the rescue again.

The automated load balancing and failover features available in the Red Hat Enterprise Virtualization Manager require less systems administration work. In a standard server environment, moving an application from a failed server means building and installing a separate server, then physically copying the application files over — often an all-day (or night) job. With virtual machines, a single technician can live migrate a guest virtual server to another host virtual server without service interruption — with just a click of the mouse button!

The same applies to starting up new application servers. In the past, starting up a new application required a systems administrator to slave over a new server installation before the application could be up and running. Now all you need to do is build a new guest virtual machine in the existing physical host.

Chapter 4

Understanding Desktop Virtualization

In This Chapter

- Explaining desktop virtualization
- Looking at the benefits of desktop virtualization
- Knowing when to use desktop virtualization

Welcome to your (mostly painless) introduction to desktop virtualization, commonly called VDI (short for virtual desktop infrastructure). Although this technology is built on the same foundation as server virtualization, virtualizing the desktop requires a very different approach in order to give users an experience as close as possible to using an actual PC. In this chapter, you learn what desktop virtualization is and why it is important to your organization.

Because every business is different, be sure to fully understand your unique user requirements when considering a virtual desktop solution. Whether you have basic requirements, such as providing multiple monitors to users, or perhaps more challenging requirements, like VoIP soft phone usage in a call center, be certain to find a solution that meets your needs, doesn't break your budget, and remains flexible enough to scale as your business grows.

Desktop Virtualization Basics

After server virtualization took the data center by storm, IT professionals everywhere began to ask, "Can we apply those same benefits to our desktop infrastructure?" Fortunately, the answer was "Yes!" and desktop virtualization was born.

The concept is relatively simple. Instead of running your desktop environment on the physical desktop or laptop PC that your staff uses, your IT department instead creates a virtual machine of the same desktop operating system and applications and runs that virtual machine on reliable server-grade hardware in the controlled data center. Users remotely access each virtual machine over a network from a client device of their choosing — either a repurposed PC or a *thin client,* which is basically a dumbed-down computer whose sole purpose is to access remote computers.

The experience of accessing a remote desktop can be as simple as navigating a web browser to the user portal, clicking on the desktop you want, and entering your username and password. And in most cases when a thin client is used, much of that simple process can be automated, requiring users to simply enter a username and password.

Most virtual desktop solutions provide a unique management utility to manage both the virtual machines and the virtualization platform itself, called the hypervisor. The hypervisor is installed directly on the servers in the data center and "hosts" all the virtual machines. You can learn more about the hypervisor in Chapter 1.

Benefits of Desktop Virtualization

With desktop virtualization, you benefit from separating your users' desktop environments from physical desktop or laptop PCs. Your desktop virtual machines become dynamically adaptable — your users can access their desktop from nearly anywhere (a thin client, a web browser at an airport kiosk, on the road, and so on) and your IT department can move that virtual machine around in the data center as needed to balance the workload, to perform maintenance, or even reallocate computing resources to accommodate a *power user* (a user that might require higher than normal computing resources).

Because the client device no longer runs the operating system (it's now in the data center), the client device can be a much cheaper device with significantly less computing power. And

because less is needed from the client device, it can generally be used for a much longer period of time than a typical PC. Your existing, repurposed PCs can keep accessing virtual desktops long after they'd be too slow to run Windows 5000, and your thin clients are much less expensive, more secure, and longer lived than any PC. In fact, most thin clients outlive a typical desktop PC by three to four times its average lifespan.

You no longer have to buy new machines whenever the next version of Windows is released or when your user needs a more powerful computer. IT admins can instantly deploy new versions of Windows or Linux to all users with one click, and you can give your power users more power whenever you need to.

Because your desktops are now virtual machines running in the data center, businesses have more flexibility with the client device. They no longer need to standardize on a single laptop or device, allowing workers to utilize a device of their own choosing, even their own personal laptops. Desktop virtualization also significantly reduces the need for IT staff to run around the office or around the world to support your desktop users. If a user has a problem with her desktop, requires new applications to be installed, or maybe even needs Windows 5000, administrators can take care of it right from the data center, through a centralized, single point of management for the entire virtual desktop infrastructure.

With any virtual desktop solution, the virtual desktop should look, sound, and feel just like a regular PC. Users want high quality video, sound, and a cursor that never skips a beat. This is where many virtual desktop solutions fall short. However, with Red Hat Enterprise Virtualization for Desktops, users get a true PC experience when using their virtual desktop. It uses a protocol called *SPICE* (short for Simple Protocol for Independent Computing Environments), which provides out-of-the-box support for bi-directional audio and video, VoIP and video conferencing, fullscreen HD quality video, native frame-rate playback, and full USB data redirection for pretty much any USB device. These features ensure users feel like they're using the latest model of a regular PC.

Using Virtualized Desktops

Sure this all sounds great, but at this point you may be wondering how you'd really use desktop virtualization in your organization.

One of the most common uses for desktop virtualization is to provide desktops to a group of users who all have exactly the same OS and application requirements, like basic office workers or call center staff members. With desktop virtualization, IT admins can set up *pools* of identically configured desktop virtual machines copied from a master template. If you need to give everyone a software update, you can make the change to the template once and all the users get the update.

Also, if someone accidentally downloads a virus, admins can easily revert users back to the master template in minutes instead of rebuilding desktop machines for days.

Desktop virtualization can also help you secure your confidential data. Because all the desktop virtual machines are safe within your data center, administrators can maintain much better control over who actually accesses the data by configuring authentication and authorization policies. Additionally, because data isn't stored locally on a user's computer, such as a laptop, should it be lost or stolen, you've only lost the hardware, not the data. Also, storing all your desktop environments in the data center makes backup and recovery for desktops a much simpler and more cost-effective task. In the event of stolen equipment or even a disaster recovery scenario, all desktops can be easily included into your current data center backup and recovery plans, maintaining your business operations and mitigating any risk of unplanned downtime.

For the security-minded organization, Red Hat Enterprise Virtualization for Desktops provides an optional feature to securely encapsulate the data connection between the client device and the host server, using SSL (Secure Sockets Layer). Turning this feature on ensures security of your confidential data.

Chapter 5

Top Ten (Okay, Seven) Questions about Virtualization

In This Chapter

- Recapping the basics
- Digging deeper into virtualization

This chapter tackles some of the common questions system administrators have about virtualization:

- **If the host platform dies, doesn't that kill all the virtual machines?** Yes, which is why virtual machine load balancing and failover in virtualized environments are crucial. With the optional failover features properly configured, it's easy to set up a backup host server to support multiple guest virtual machines. Using this formula, you can save in redundancy costs, because multiple guest virtual machines only need one redundant host server for failover support.
- **What is the cost savings of virtualization?** The bottom line of server and desktop virtualization is doing the same job with fewer physical machines. If you just have one application running on one server, server virtualization won't save you anything. If, however, you have many applications running on a number of servers, server virtualization may allow you to reduce your data center footprint significantly. Of course, this same principle applies to your desktop infrastructure. This will allow you to save in floor space, electricity, cooling requirements, and IT staff and resources.

- **What guest operating systems can be used?** The Red Hat Enterprise Virtualization hypervisor currently supports Red Hat Enterprise Linux versions 4 through 6 (32 and 64 bit), and Microsoft Windows 2003 and 2008 Server, as well as Microsoft Windows XP and Windows 7 (32 and 64 bit) desktop operating systems.
- **How does load balancing work?** The Red Hat Enterprise Virtualization Manager allows easy migration of guest virtual machines between independent host servers. When one host server becomes overloaded, you can migrate any guest virtual machine to another host server that's less impacted. The entire guest operating system environment migrates as a single operation — there's no need to reinstall applications or data.
- **How does failover work?** Similar to the load balancing feature, the Red Hat Enterprise Virtualization Manager allows you to configure failover policies between host servers. If a guest virtual machine becomes unresponsive, it can automatically be killed and restarted on the same or a different host server. If the host server itself becomes unresponsive, that host is removed from the Red Hat Enterprise Virtualization host infrastructure and its guests are automatically restarted on another host server without the need of operator intervention. Now picture this happening at a data center level — an entire data center that can failover instantly to a different location.
- **Can multiple servers be managed?** With the Red Hat Enterprise Virtualization Manager, it's a snap to quickly monitor and manage multiple virtual servers and desktops, all from a single web interface. The Red Hat Enterprise Virtualization Manager provides instant access to both the individual guest virtual machines and the host server configurations. A single systems administrator can easily manage multiple host servers and hundreds of virtual machines (or more), all from a remote location if necessary.
- **What type of customer support does Red Hat offer?** Red Hat offers the choice of Standard support or Premium support with any purchase of Red Hat Enterprise Virtualization. Standard support provides e-mail and telephone support for an unlimited number of cases during business hours. Premium support provides the same benefit and adds 24/7 support for Severity 1 and 2 issues.

A useful guide to what virtualization is and how it works

Welcome to *Virtualization For Dummies,* Red Hat Special Edition. This friendly book introduces you to the benefits of virtualization technology and offers insight into using it to save time and money. This book focuses on Red Hat Enterprise Virtualization, a virtualization platform for both servers and desktops.

- ***Understand virtualization basics and its benefits* — *before you can apply it to your business, you have to know exactly what it is***
- ***Industry-leading security* — *it's a hot topic and you want to know all the ins and outs***
- ***How virtualization works* — *use it to control project costs, go green, and do more with less***
- ***Desktop virtualization solutions* — *virtualizing the desktop can be a great way to use the technology***

Open the book and find:

- **Some different applications for virtualization**
- **How to make sure your virtualized infrastructure is more secure**
- **The top questions people ask about virtualization — and the answers**
- **How VDI can improve data access and save you money**
- **Information on what the hypervisor does**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

For Dummies®
A Branded Imprint of
WILEY

978-1-118-08817-3
Not for resale