IT HANDBOOK

Security Best Practices

Learn new tricks when running server
virtualization to ensure better levels of security
while delivering timely IT services to meet
your business needs.

BY DANIELLE RUEST AND NELSON RUEST

► **BEST SECURITY PRACTICES
FOR VIRTUALIZATION**

► **VIRTUALIZATION
AND COMPLIANCE**

► **SECURING VMWARE
INFRASTRUCTURES**

► **SECURING MICROSOFT
HYPER-V**

SECOND
EDITION
2011

Best Security Practices for Virtualization

WHETHER YOU'RE WORKING with virtual or physical machines, you should always keep security as a foremost concern. Many IT professionals have had to learn new practices when they began implementing server virtualization infrastructures. Then they had to learn new skills to manage virtual service offerings and update old skills when learning to manage their physical infrastructures in new ways.

This division of resources into both resource pools has forced IT pros to change the way they do things. Nowhere has this been more evident than in the security aspects of virtual infrastructures.

The best way to update existing skills and learn new ones is to follow best practices that address four key areas of virtual implementations. They are:

- General security for virtual infrastructures
- Compliance for virtual infrastructures
- Security for VMware infrastructures
- Security for Microsoft Hyper-V infrastructures

Moving to virtualization should not imply losing or relaxing your security and compliance measures. This is why following best practices will help ensure that your virtual environments are just as secure or—better yet—even more secure than your former physical infrastructures were.

The first thing you'll notice when you run a virtual infrastructure is that the structure of your data center is completely different. Because one of the main objectives of a virtual infrastructure is to take physical workloads and transform them into virtual workloads, you quickly learn that all of the machines that offered traditional services to your end users are now VMs.

This transformation into VMs is the only change you can make for this level of service offering. The directory and other services your end users rely on are

now completely virtualized, but they still require the same management practices you used to provide when this infrastructure was physical. What is different is the way you treat and work with physical machines.

Because the physical machines are now designed to provide resources—storage, networking, CPU and memory—to VMs, the role of physical machines no longer requires interaction with end users. Similarly, the nature of the machines that previously offered services to end users and that continue to offer these services has been transformed into a VM—nothing more, in reality, than a set of files in a folder somewhere.

These two changes require an update to your security practices. Although you'll want to continue existing security practices for the end-user service offerings, which are now provided by VMs, you'll also want to ensure that new components such as the resource pool are fully secured.

Follow these updated security guidelines:

→ **Segregate hardware.** Because hardware no longer needs to interact with end users, you should completely segregate it from end-user access. This means creating and providing access credentials to technical staff only—administrators, technicians and management. The best way to do this is to create a utility directory.

A utility directory provides several benefits. First, a directory is essential because it centralizes all access rights—you don't want to have to manage access rights on a per-machine basis.

Second, a utility directory's sole purpose is to allow access for technical staff to the components that provide hardware resources to the VMs you run and, therefore, reduce its potential attack surface. If end users do not have accounts in this directory, there is no way for them to access any of its components.

→ **Manage fault-tolerant components.** You also need to learn how to manage the fault-tolerant components of your resource pool. Because each physical server manages several VMs, you have to implement failover clusters—or groups of

physical servers that can protect each other from potential failures and take over the workloads of other servers during maintenance windows.

Securing server clusters is different than securing single standalone machines. Learn your virtualization manufacturer's recommended guidelines for implementing secure clusters.

→ **Manage supporting components.** Another important aspect of resource pool security is the management of its supporting components. Although hardware components—storage fabric, networking components, servers and cabling—are essential to a resource pool, you'll also generate a few virtual or physical machines whose role will be to provide support services to resource pool machines.

For example, you'll have at least two machines that will run the utility directory service. These machines can be VMs, but make sure they are auto-started VMs in the event of a complete resource pool shutdown. Auto-starting these VMs will ensure you can get back into your resource pool once it is back up.

The number of services your resource pool will require usually depends on the size of your network and the number of users you support.

You'll also need other machines that will run a variety of services such as the virtual infrastructure management service, databases to store virtual infrastructure information, servers to provide update services to both physical and virtual machines as well as backup services, email and monitoring services, antivirus engine management services and optional services such as network access protection.

The number of services your resource pool will require usually depends on the size of your network and the number of users you support. Smaller organizations generally run fewer services while large organizations deploy full-powered resource pools. Each service you implement in the resource pool must be fully secured at all times.

→ **Provide strict control to all VM files.** You'll also want to provide strict control to all of the files that make up your VMs. Remember that a VM is self-contained. Anyone who leaves with a full VM can easily take all the time they need to break into it once it is away from your premises.

Therefore, you should make sure no one can leave with one of your VMs. The best way to do this is to secure the files with proper access rights and to audit all VM file access. Remember to monitor the audit logs closely.

→ **Run minimal installations on all host servers.** This is especially important if you run a hypervisor such as Microsoft Hyper-V, which runs on an otherwise general-purpose operating system. Make sure the underlying OS on your host servers is hardened; it will go a long way toward reducing attacks on your environment.

→ **Segregate network traffic.** All resource pool management traffic should be completely segregated from general public traffic generated by end users. Resource pool traffic contains highly privileged information such as administrative account names and passwords for host machines and VMs. Therefore, it should be protected at all times. Rely on your virtualization engine's capabilities to create networks for each traffic type so that they cannot interact.

→ **Update all VMs and host servers when required.** Many organizations have multiple copies of the same VM or multiple VMs that are not running at all times. Make sure your update system can also update offline VMs when you apply updates to your environment.

These practices form the groundwork you'll need to protect your new infrastructures. ∎

Virtualization and Compliance

COMPLIANCE IS ALSO a critical aspect of network infrastructures. And, just as virtual infrastructures affect the way you apply security measures, they affect the way you manage and maintain compliance to the regulations that govern your organization.

Compliance and security have several aspects in common, but where compliance tends to focus much more on data management, security tends to affect every single aspect of your infrastructure and administration practices. Both require excellent documentation—something that is often the bane of IT professionals. However, there are automated ways to produce this documentation.

When you move to a virtual infrastructure, apply the following best practices if you want to maintain compliance now that many of your machines are also in the form of data or in the form of files contained within folders.

Keep on top of the following tasks to ensure compliance:

Auditing VMs for access and backing them up regularly will help protect the data they contain.

→ **Identify which information is controlled by the regulations that affect your organization.** Different regulations focus on different types of information. Therefore, the best way to maintain compliance is to identify the requirements of a regulation and pay special attention to the VMs that contain this information.

→ **Put in place appropriate mechanisms to ensure the protection of this data.** Because VMs now provide your service offerings, make sure the critical VMs that contain data required to meet compliance requirements are secured at all times. Auditing VMs for access and backing them up regularly will help protect the data they contain.

→ **Document all system components and structures and keep all documentation up to date.** Now that your service offerings are in VMs, you'll need to update all of your infrastructure documentation and clearly identify the locations of the VMs that contain critical information. One good way to do this is to create a visual map of your virtual infrastructure.

→ **Track all the changes of the system components and structures.** Do this by implementing a monitoring system that tracks your physical infrastructure and your virtual environment. This is especially tricky with virtual infrastructures because of the mobility of VMs within physical hosts. Create VM groupings that will ensure that VMs stay within a specific and small cluster of physical servers so they're easier to track.

→ **Implement a standard change management approach for all IT operations.** Change is the very nature of IT. It can be even worse with virtual infrastructures because of both the mobility of VMs and the ease of VM creation. Track all changes and implement a strict VM creation process that requires both validation and authorization before it can proceed.

→ **Implement virtual machine documentation tools.** VM configurations are often modified as business needs change. Using an automated VM configuration documentation tool helps track those changes as they occur.

→ **Include your security practices in your compliance documentation.** There is never too much documentation when it comes to compliance. Therefore, if you include documentation on your new virtual infrastructure security practices, you'll kill two birds with one stone.

Rely on these measures to help maintain compliance even in a virtual environment. ∎

Securing VMware Infrastructures

VMWARE STANDS OUT in the virtualization industry because its hypervisor runs on a proprietary operating system whose sole purpose is to support the operation of VMs. For that reason, its attack surface is reduced compared to other manufacturers' products.

For example, Citrix Systems builds its XenServer hypervisor on top of open source versions of Linux. Microsoft builds its on top of Windows Server. Although both manufacturers have done a lot of work to provide secure and hardened operating systems in support of their hypervisors, their work is more difficult than VMware's because of the general nature of the underlying operating systems in their products.

In addition, VMware has built custom APIs into its hypervisor, allowing both itself and its partner ecosystem to build additional security functionality in support of its virtualization platform. And, finally, VMware has a small footprint hypervisor—ESXi—which it designed to provide virtualization functionality while removing any extraneous features from host servers. That said, you still need to make sure that you secure your VMware implementation.

Use the following best practices to do so:

VMware stands out in the virtualization industry because its hypervisor runs on a proprietary operating system whose sole purpose is to support the operation of VMs.

➜ **Apply hardening practices to your entire virtual infrastructure.** VMware publishes a vSphere Hardening Guide that provides guidelines to do this. There is also a VMware Infrastructure 3 Hardening Guide if you're running an older version of the product.

→ **Harden your configuration database.** VMware relies on a central configuration database to store information about the entire virtual infrastructure. If the database becomes poisoned, it can possibly compromise your entire virtualization environment. Make sure you use the proper hardening practices to tighten the security of your configuration database engine.

→ **Rely on VMware's vShield Zones to create isolated logical networks in your virtual environments.** Using vShield Zones allows you to completely segregate network traffic from different machine groups as well as from each other. This allows you to further increase the density of your host server configurations and lets you run more VMs on each host, which lets you run VMs of different sensitivity on the same host group.

For example, using vShield Zones, you can configure separate networks for VMs belonging to a perimeter network and machines belonging to your intranet. VShield Zones can span the entire resource pool to create distinct levels of trust and confidentiality between VMs (see **FIGURE 1**, page 10). These zones support both security practices and compliance methodologies. Zones are controlled through a policy-based engine, letting you easily modify the structure of a zone with a few clicks.

If the database becomes poisoned, it can possibly compromise your entire virtualization environment. Make sure you use the proper hardening practices to tighten the security of your configuration database engine.

→ **Rely on VMware's APIs to continually monitor host-to-VM communications.** One of the problems you face when running VMs is the possibility of content "escaping" from the machine and affecting host operations. By implementing an intrusion detection/intrusion prevention system (IDS/IPS), you ensure that

communications between hosts and VMs are not only segregated but also monitored at all times.

If your configuration runs fewer than 100 VMs, you can use a free version of Third Brigade for VMware to implement IDS/IPS protection for your VMs. If you run more than 100 VMs, you can acquire a commercial version of Third Brigade.

➜ **Ensure all your hosts and VMs are protected at all times.** You can rely on the VMsafe API to implement protection mechanisms for your VM. VMsafe supports the integration of antivirus, encryption, firewall, IDS/IPS and even system integrity engines. Many of these utilities are available for free, and many are in the form of virtual appliances—preconfigured VMs that include a custom ap-

FIGURE 1: Use vShield Zones to configure different trust levels for virtual machine groups.
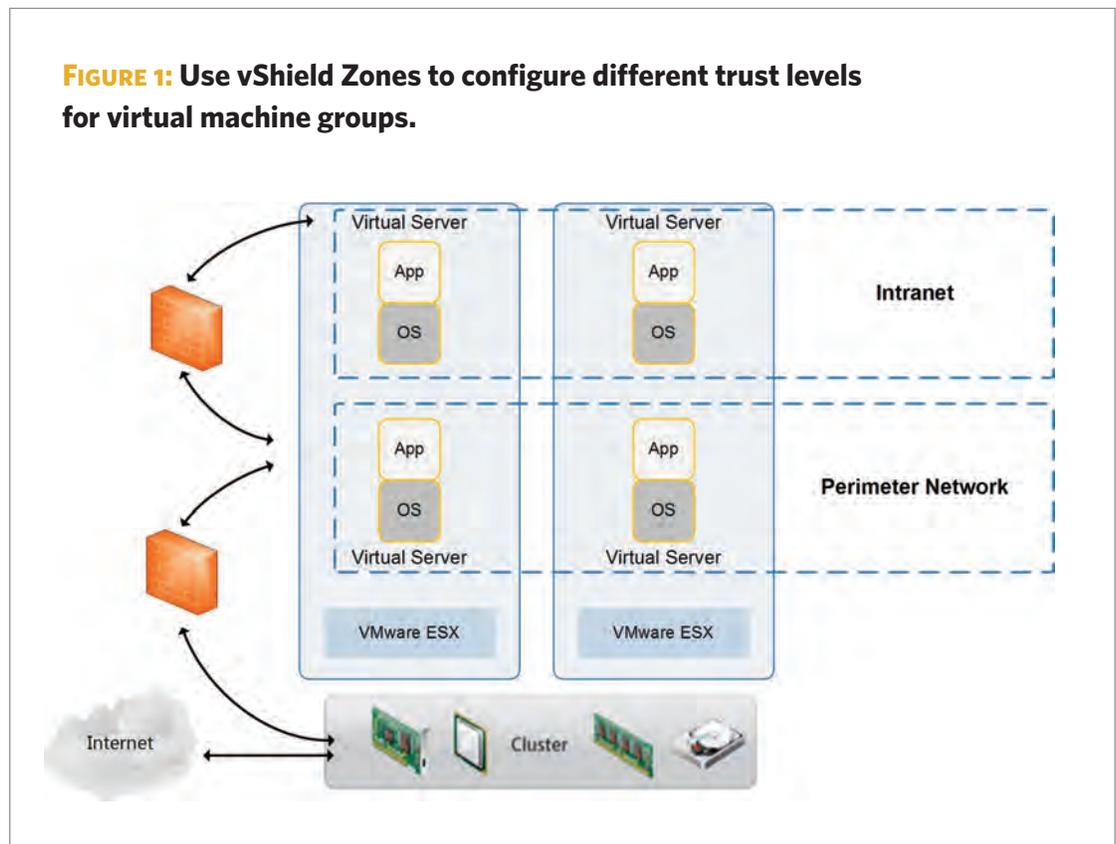
plication that is ready to run as soon as you integrate it into your infrastructure.

Virtual appliances significantly reduce the time to implementation of a utility. So there is no reason why you can't have a complete protection system up and running quickly.
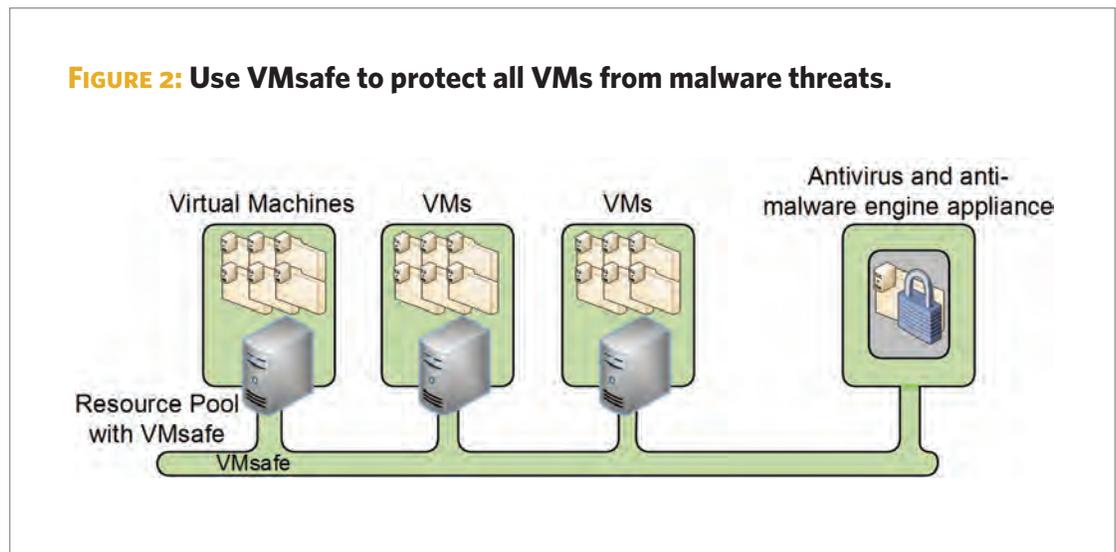
➔ **Ensure all your hosts and VMs are protected against malware attacks.** Once again, you can rely on the VMsafe API to integrate a complete malware protection mechanism into your infrastructure. The advantage of VMsafe is that you do not need to install antivirus engines on each VM because VMsafe provides the scanning engine with a view into the VMs on any host directly from within the VMsafe engine itself (see **Figure 2**). Any VM you place on a host will be automatically protected as soon as it is up and running.

Virtual appliances significantly reduce the time to implementation of a utility. So there is no reason why you can't have a complete protection system up and running quickly.

Figure 2: Use VMsafe to protect all VMs from malware threats.

➔ **Implement a complete software update strategy.** Once again, VMware provides a custom Update Manager that allows you to deploy software updates into any VM that is running on host machines (see Figure 3). Update Manager is a critical component of any VMware infrastructure security strategy.

These strategies will ensure that your VMs and your host servers are protected. But they are not the only strategies to implement. Rely on the VMware Security Center to discover more about securing VMware implementations and to ensure that your virtual infrastructures are compliant at all times. ∎

FIGURE 3: Use Update Manager to provide software updates to all systems.
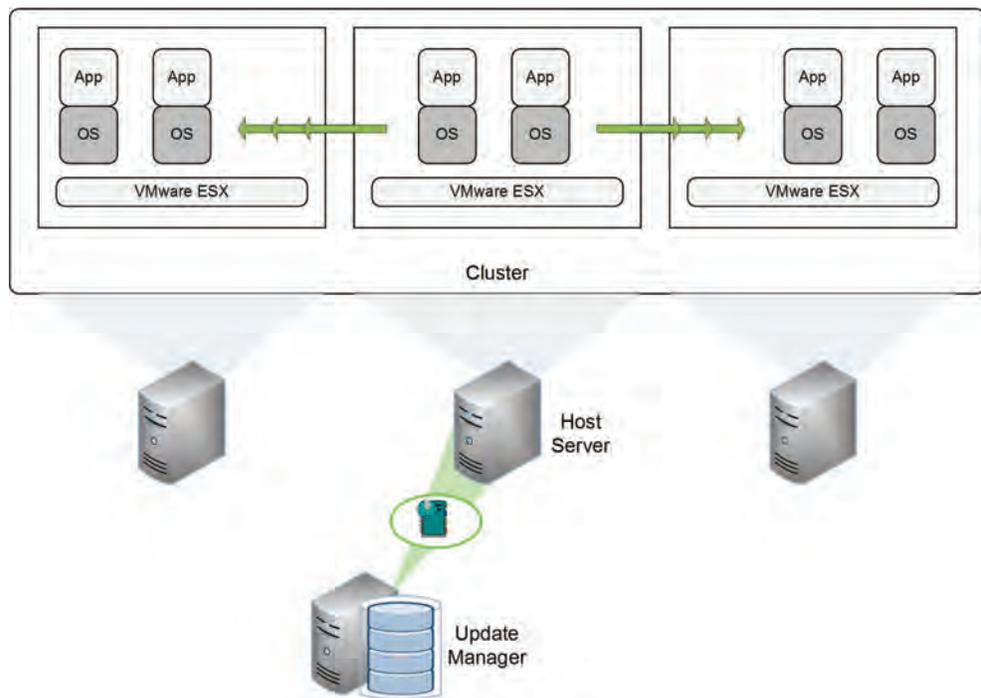
Securing Microsoft Hyper-V

EVEN THOUGH MICROSOFT is a latecomer to the field of enterprise virtualization, it has a strong product in the form of Windows Server 2008 Hyper-V, especially in the more recent R2 version. Organizations running Hyper-V may be concerned that this hypervisor runs on a general-purpose OS. That's why it's essential to configure and deploy only secure configurations of this OS when deploying it to host servers.

The best place to start is to look to Microsoft's general Security Guide for Windows Server 2008. Next, look to specific security and compliance practices for Hyper-V. A good source of information is the freely downloadable Chapter 8: Securing Hosts and Virtual Machines from *MCTS Self-Paced Training Kit (Exam 70-652): Configuring Windows Server Virtualization with Hyper-V* or the Microsoft Hyper-V Security Guide.

Whichever guidance you choose, keep in mind that you need to secure both the host servers and the VMs that run on top of them. Use these guidelines:

Organizations running Hyper-V may be concerned that this hypervisor runs on a general-purpose OS.

→ **Apply hardening practices to your entire resource pool.** First, make sure you run only Server Core installations on your host machines and then harden those configurations. The advantage of Server Core configurations is that they do not run extraneous services and are, therefore, easier to harden.

→ **Deploy a centralized host server management engine.** Rely on System Center Virtual Machine Manager (SCVMM) to do this (see **FIGURE 4**, page 14). SCVMM provides a central location for the management of standalone hosts and failover host clusters and simplifies the delegation of authority process, which ensures that only authorized technical staff will have access to your infrastructure.

➜ **Rely on Windows Server features to secure additional aspects of your infra-structure.** The advantage you gain when you run Hyper-V is that Windows Server is a server operating system with a long history of security and compliance. This OS includes a host of features that can provide additional security to your resource pool.

Tools such as Software Restriction Policies ensure only authorized software will run on host servers. The Windows Firewall reduces host server access, and Active Directory Domain Services supports the utility directory you need for a resource pool. Device Control allows only authorized devices to be connected to host servers, protects the VMs they run and much more.

FIGURE 4: Use SCVMM to centralize host server management.
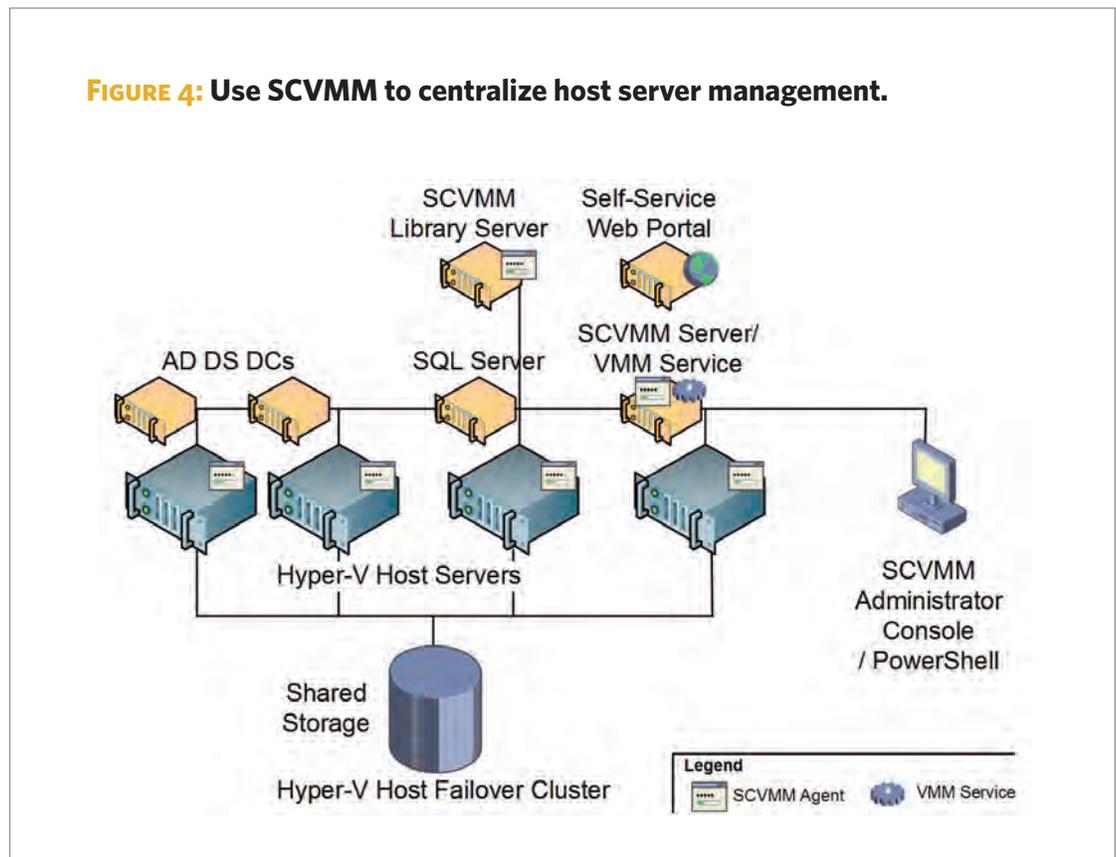
➜ **Create segregated networks on your host servers to protect VM traffic.** Rely on Hyper-V virtual network switch to create appropriate virtual networks for the VMs that run on the host (see **Figure 5**). Perform this configuration on each host server in a cluster to ensure the same virtual networks are available to each VM in a group.

➜ **Segregate host servers from VMs.** Hyper-V provides natural segregation between the host or parent partition and child partitions. But legacy VMs will not take full advantage of this segregation. That's why you should run enlightened guest operating systems or operating systems that are aware of being virtualized within your VMs. Enlightened guests will support a more secure operation on Hyper-V hosts.

Figure 5: Use Hyper-V's virtual network switch to control VM traffic.
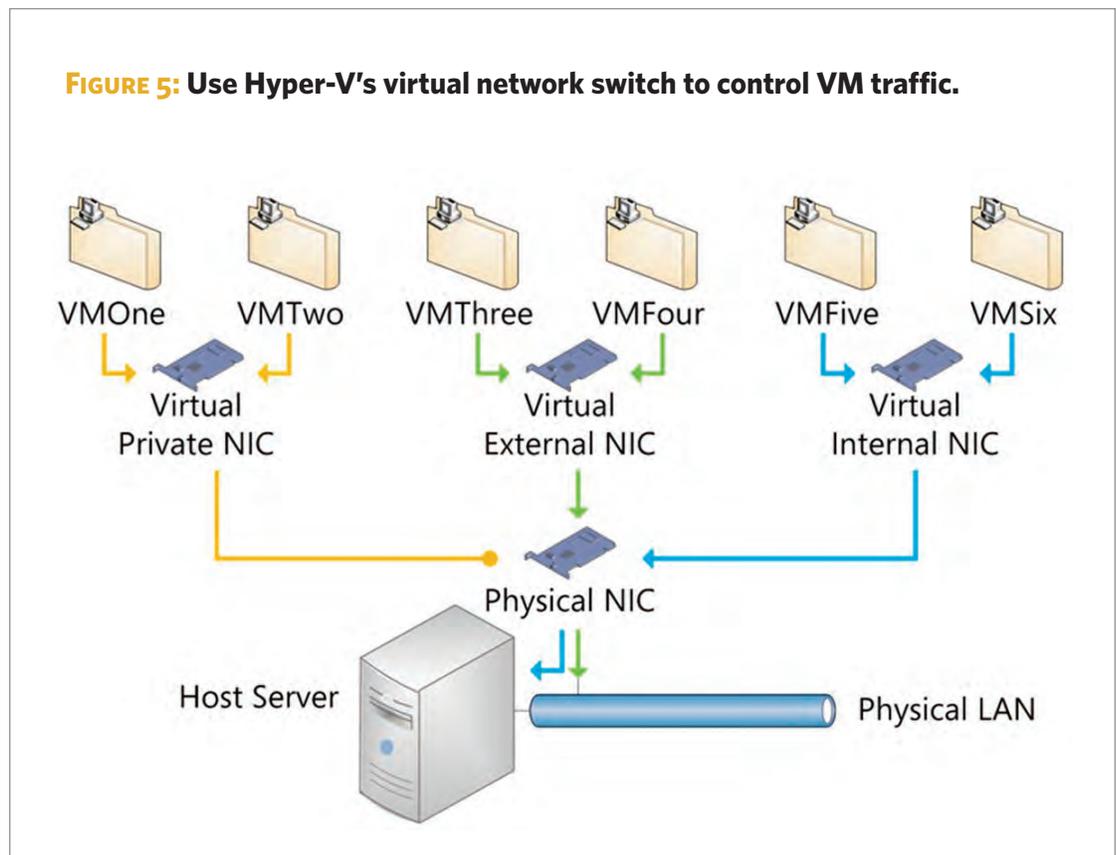
→ Do not run applications on the parent partition. Windows Server is a general OS, and because of this, it can run a number of additional roles and applications besides Hyper-V. Keep these roles to a minimum to ensure your hosts are as secure as possible. In fact, you should run only the Hyper-V role on a host server.

→ Run a complete software update environment. One of the least known dangers of VM environments is the possibility of running older VMs that are not up to

Virtualization Security Checklist

WHICHEVER VIRTUAL infrastructure you run, keep the following in mind to make sure you run server virtualization environments that are both compliant and secure:

- Protect the entire resource pool, not just host servers.
- Continue existing protection mechanisms for your service offerings that are now virtualized.
- Use new administrative and technical roles in the data center to run the resource pool.
- Add new ways to support security processes in both the resource pool and the VSO contexts.
- Always segregate the resource pool from the VSOs. Be disciplined— don't be lax in this practice.
- Remain vigilant at all times.

Remember: Security is not a one-time task. It is an ongoing activity that you must invest in at all times. If you follow these best practices, you'll soon discover that even though you have to learn new tricks when running server virtualization, you can probably ensure better levels of security than ever before while delivering timely IT services to meet your organizational and business needs.

date, which would create a potential security hole within your infrastructures. Parked VMs or VMs that are in suspended or off modes are often overlooked during the update process. Rely on the Microsoft Offline Virtual Machine Servicing Tool to update all of your production VMs all the time (see **FIGURE 6**).

Rely on these recommendations to form the foundation of your Microsoft Hyper-V security strategy. But don't stop there. And don't forget that VMs are assets too, and that you need to continue existing security strategies to make sure the services they provide to end users are also secure at all times. ∎
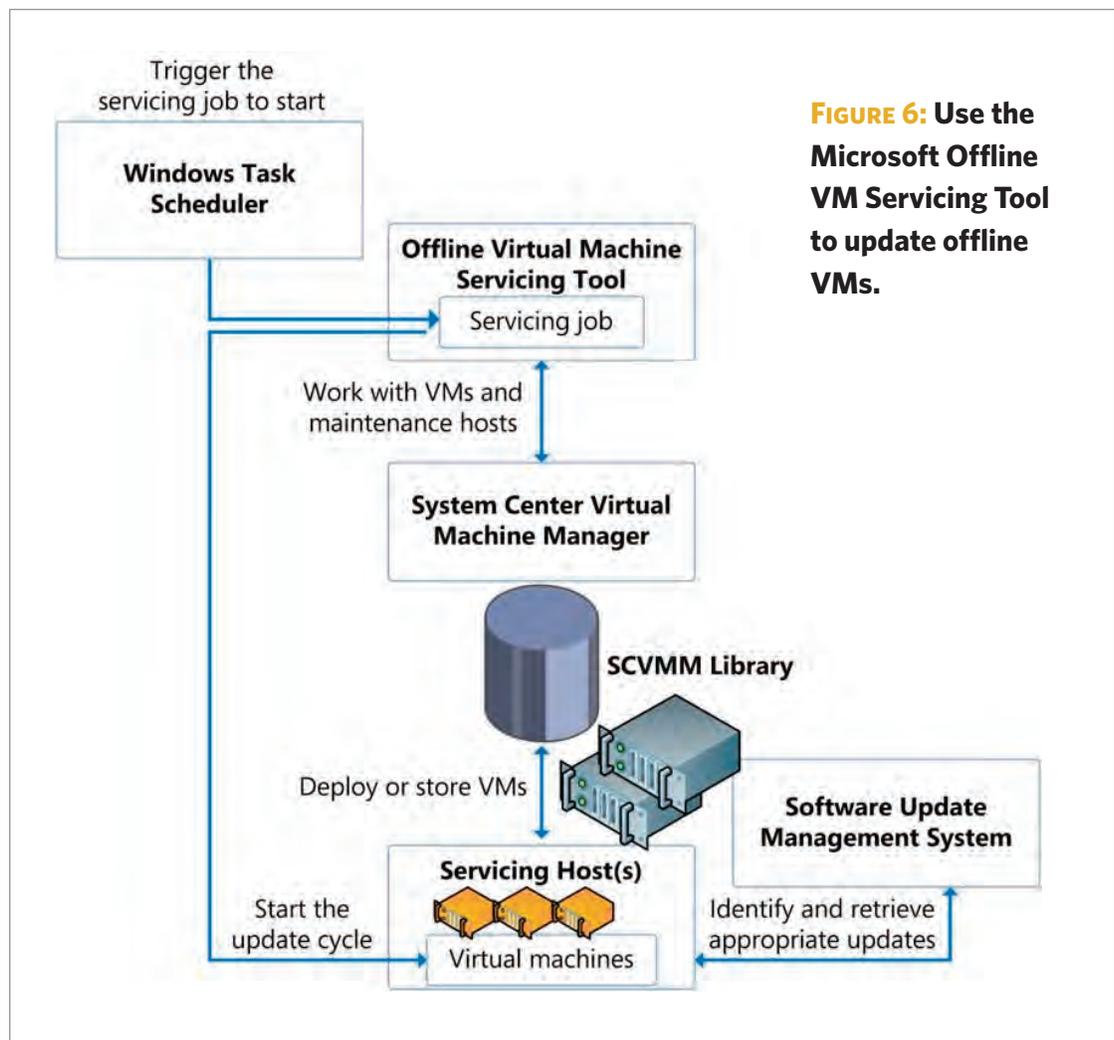
FIGURE 6: Use the Microsoft Offline VM Servicing Tool to update offline VMs.

Danielle Ruest and **Nelson Ruest** *are IT experts focused on continuous service availability and infrastructure optimization. They are authors of multiple books, including* Virtualization: A Beginner's Guide *for McGraw-Hill Osborne, as well as the* MCTS Self-Paced Training Kit (Exam 70-652): Configuring Windows Server Virtualization with Hyper-V *from Microsoft Press. Contact the Ruests at infos@reso-net.com.*

SearchServerVirtualization.com

EXECUTIVE EDITOR
Jo Maitland

SENIOR SITE EDITOR
Colin Steele

SENIOR MANAGING EDITORS
Michelle Boisvert
Lauren Horwitz

MANAGING EDITOR
Christine Casatelli

ASSOCIATE MANAGING EDITORS
Jeannette Beltran
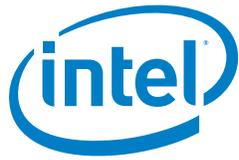**Eugene Demaitre**
Martha Moore

DIRECTOR OF ONLINE DESIGN
Linda Koury

EDITORIAL DIRECTOR
Cathleen Gagne

PUBLISHER
Marc Laplante

TechTarget
275 Grove Street
Newton, MA 02466
www.techtarget.com

- **Resource Protection in Virtualized Infrastructures**

- **Desktop Virtualization Planning Guide**

About Intel:
For more than three decades, Intel Corporation has developed technology enabling the computer and Internet revolution that has changed the world. Founded in 1968 to build semiconductor memory products, Intel introduced the world's first microprocessor in 1971. Today, Intel supplies the computing and communications industries with chips, boards, systems, and software building blocks that are the "ingredients" of computers, servers and networking and communications products. These products are used by industry members to create advanced computing and communications systems. Intel's mission is to be the preeminent building block supplier to the Internet economy.