CHAPTER 6

HOW VIRTUAL INFRASTRUCTURES CHANGE SECURITY

Securing a virtual infrastructure doesn’t need to be more difficult than protecting a physical network. The key is to remain vigilant.

↘ SECURITY ISSUES: UNDERSTAND THE RISKS

↘ CASE STUDY

↘ NEW APPROACHES TO VIRTUALIZATION SECURITY

↘ SECURE THE RESOURCE POOL

↘ PREVENT OVER-ADMINISTRATION

How virtual infrastructures change security

SECURITY CONCERNS IN the data center are pervasive and constant. Occasionally, a new element is introduced, forcing administrators to take a fresh look at their security strategies. Virtual infrastructures do just that by transforming the very structure of the modern data center.

Server virtualization provides a powerful operational model and offers many benefits. When you run a virtual infrastructure, physical servers become resources that can be pooled together. Additionally, service offerings—those that end users interact with—are converted into virtual machines (VMs). The dichotomy of resource pools versus virtual service offerings (VSOs) alters the way administrators look at data center security.

Protecting virtual infrastructures doesn't have to be more difficult than protecting traditional physical networks. When securing any data center—traditional or virtualized—the key is to remain vigilant.

SECURITY ISSUES: UNDERSTAND THE RISKS

Beyond the transformation of the data center, virtual infrastructures create their own security issues. New threats crop up and new ways to deal with them are required. But how will virtualization affect your current security practices? Experts at the Center for Internet Security, a nonprofit organization that creates benchmarks for operating systems, network devices and other applications, tried to answer this question by creating the virtual machine security benchmark report, which identifies several potential virtualization securi-

↘ SECURITY ISSUES: UNDERSTAND THE RISKS

↘ CASE STUDY

↘ NEW APPROACHES TO VIRTUALIZATION SECURITY

↘ SECURE THE RESOURCE POOL

↘ PREVENT OVER-ADMINISTRATION

ty threats. Still, as more organizations move to virtual infrastructures, other threats appear.

If you're concerned about security in your virtual infrastructure, consider the following facets when preparing to protect it. In most cases, each issue relies on existing tools and practices, but both tools and practices must be updated to meet and eradicate threats to your virtual infrastructure.

■ One of the main reasons organizations use server virtualization is to perform physical machine consolidation—converting physical machines into VMs. When consolidating machines, be careful when placing systems with different security contexts on the same host. You should also use caution when hosting multiple operating systems within VMs on the same host.

□ Machines with different security contexts can compromise secure systems if they're not configured correctly. Make sure that the virtual network adapters connecting VMs of each given security context are tied to specific physical network adapters in the host server. Don't tie machines with different security contexts to a single physical adapter because that can cause secure data communications to leak to unsecure networks.

□ Machines with different operating systems may support different levels of patches and updates—one machine may not be protected from a particular vulnerability while others are protected. The vulnerable machine could compromise other machines.

Machines with different OSes may support different levels of patches—one machine may not be protected from a vulnerability while others are.

■ When you run VMs on a host, it's possible to share the clipboard between VMs and the host. Shared clipboards not only support data transfers, but they also enable malicious programs to "piggyback" with data on the clipboard and infect other VMs or the host itself. This usually occurs when you use a software hypervisor that runs as a program on top of an existing OS. Some software hypervisors are VMware Workstation, Sun xVM VirtualBox, Microsoft Virtual Server and Microsoft Virtual PC.

Running a hardware hypervisor—one that runs directly on top of the hardware—can mitigate this. Hardware hypervisors include Microsoft

↘ SECURITY ISSUES: UNDERSTAND THE RISKS

↘ CASE STUDY

↘ NEW APPROACHES TO VIRTUALIZATION SECURITY

↘ SECURE THE RESOURCE POOL

↘ PREVENT OVER-ADMINISTRATION

Hyper-V, VMware vSphere, Virtual Iron or Citrix XenServer.

- Some host servers log keystrokes and screen activities from within the VMs they run. You can control this behavior, called host virtual machine logging, through the virtual infrastructure management interface. If you choose to log VM activity, then make sure that host log files are thoroughly secured at all times.

- Programs within VMs can "escape" and affect the host, so you must ensure that VMs include proper firewalls and malicious software-protection programs, such as antivirus and anti-malware programs. Make sure, too, that all signatures and patches are up to date.

- Monitoring can be an issue. Hosts can monitor VMs; VMs can monitor other VMs; VMs can also monitor host servers. In all cases, monitoring logs and databases must always be secured. You must also control access to all monitoring data and management interfaces.

- VMs can cause a denial of service on the host. All VMs running on a given host share host resources. One VM can go out of control and grab all available resources on the host, denying service to other VMs. Avoid this issue by implementing proper resource throttling on all VMs.

- Protect VMs—especially highly secured VMs—from uncontrolled external modifications. The ideal way to do this and avoid modifications is to ensure that files making up VMs are digitally signed.

> Communications with the hypervisor should be protected at all times because they contain vital information.

- Communications with the hypervisor should be protected at all times because they contain vital information such as privileged account names and passwords. Most virtual infrastructures support the use of the Secure Sockets Layer (SSL) in all management communications with hypervisors, but the feature is not always installed by default. Make sure you implement it to protect yourself from potential management communications issues.

- Virtual machines are nothing but a set of files in a folder, but those files can contain quite a bit of sensitive information. Make sure all of the files that make up a VM are contained within the same folder. Some hypervisors do not store VM files such as

(Continued on page 6)

↘ SECURITY ISSUES: UNDERSTAND THE RISKS

↘ CASE STUDY

↘ NEW APPROACHES TO VIRTUALIZATION SECURITY

↘ SECURE THE RESOURCE POOL

↘ PREVENT OVER-ADMINISTRATION

BALANCE SECURITY AND FUNCTIONALITY

CASE STUDY

AS HEALTHCARE INDUSTRY software vendor Quantros Inc. dove deeper into virtualization, its IT team had to find new ways to tighten virtual security. With a range of hosted Software-as-a-Service applications for hospitals and medical offices, as well as internal applications, the company worried about security holes.

"One challenge was trying to segregate each application," said Bryan Rood, IT and data center manager for the company. With about 80 internal users, Quantros serves nearly three million users throughout approximately 2,500 hospitals. Its applications and virtual hosts communicate when servers send data traffic between one another over the network, Rood said. That data must be accepted while the system blocks potential intruders.

"There is this paradigm that you can secure everything or get your work done," Rood said. Too much security that's too tightly configured can make it difficult to get things done, he said. The key is finding a compromise.

Too much security that's too tightly configured can make it difficult to get things done.

When VMware Inc. showed Rood how much communication occurs between the two environments, he wondered about traffic vulnerability. An attack could occur if an intruder accessed network traffic outside Quantros' firewalls and sent acceptable commands to the hypervisor. Other applications also share data outside the network for replication and other tasks—adding to vulnerability worries.

Rood and his team tested VMware Inc.'s vShield Zones application on two virtual machines. The application works as a deep-packet inspection firewall that also allows the creation of zone-based controls for multiple applications.

"You have to make sure the way you've set up virtualization is... completely compatible from piece to piece when you turn on the firewall. We turn on the lowest level, and then increase it to be sure it's working."

Getting the network to recognize and accept desired changes has been the biggest problem, Rood said. "The security software needs to be able to follow changes so it doesn't think [they] are security problems," he said. "We have tried to implement the same security or better for our virtual environment as [we do for] our physical environment." —TODD R. WEISS

↘ SECURITY ISSUES: UNDERSTAND THE RISKS
↘ CASE STUDY
↘ NEW APPROACHES TO VIRTUALIZATION SECURITY
↘ SECURE THE RESOURCE POOL
↘ PREVENT OVER-ADMINISTRATION

(Continued from page 4)

configuration, virtual disks, snapshot files, in-memory contents and so on in the same folder by default. Keeping these files together makes it easier to track and monitor them for unauthorized access or even theft.

Since VMs are made of different files, it's easy to compromise a VM by replacing one of its virtual disks with a file containing malicious software. That's one more reason to monitor the files that make up virtual machines.

NEW APPROACHES TO VIRTUALIZATION SECURITY

Traditional security approaches still apply in the world of virtualization. You need to not only protect servers and associated applications, but also monitor who can access what in the first place. Identify people as they enter your data center infrastructure. Apply appropriate clearance levels to users who work within your IT environment and give them corresponding access rights once they have been identified.

You still have to identify that the person modifying data within your infrastructure is authorized to do so, which means you have to continue with existing security practices. If you transform all of your existing end-user service offerings into VMs and run them as VSOs, then traditional approaches to security must continue within this layer.

Unfortunately, the resource pool layer, which provides resources to VSOs, isn't designed to interact with users. Physical machines within the resource pool are simply host servers that run a virtualization engine, which means that only administrators and technicians should deal with them.

> Traditional security approaches still apply in virtualization. You need to not only protect servers and applications, but also monitor who can access what.

Each of these environments—resource pools and VSOs—runs within a given security context that's usually supported by a central directory service. Consider creating segregated security contexts for both infrastructures. After all, if resource pools are only exposed to administrators and technicians, then why should these pools share the security context of VSOs that end users can access?

In fact, end users have nothing to do with resource pools. End users don't interact with routers or switches in your network. Therefore, you need to create segregated security contexts for both the resource pool

↘ SECURITY ISSUES: UNDERSTAND THE RISKS

↘ CASE STUDY

↘ NEW APPROACHES TO VIRTUALIZATION SECURITY

↘ SECURE THE RESOURCE POOL

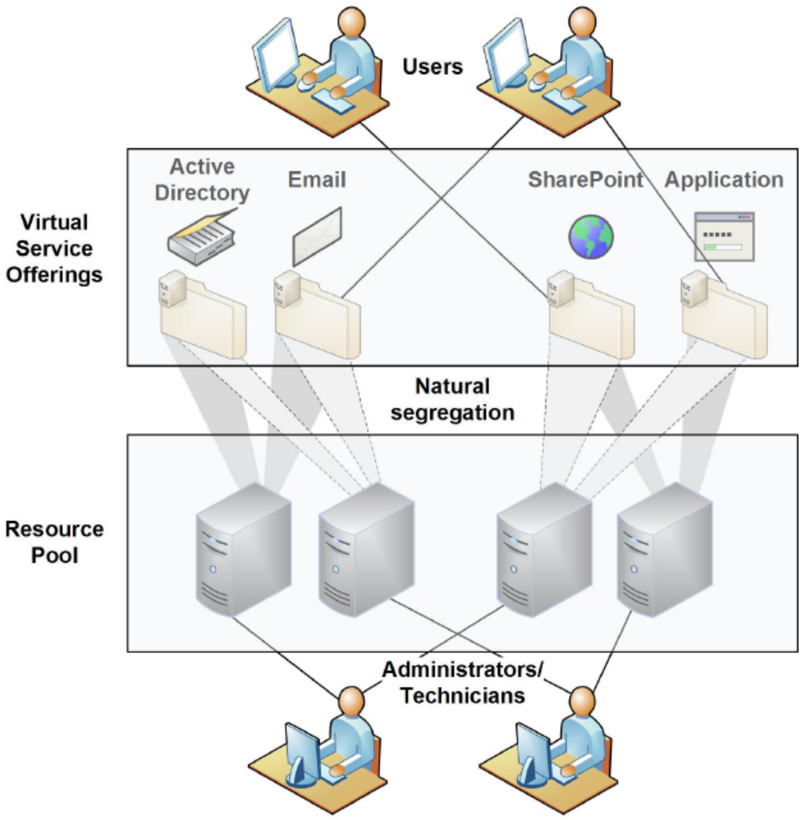
↘ PREVENT OVER-ADMINISTRATION

and the VSOs. For example, if you run VMware or Citrix hypervisors and a network of services that rely on Windows Server, then the security context of the resource pool would automatically be separate from the VSO security (FIGURE 1). That's because the host environment often runs a different OS—a custom form of Linux—than the VSOs. This segregates the two contexts naturally.

However, if you run host servers that rely on the same OS as the VMs you run, you'll need to segregate the security context of the resource pool and the VSOs. This occurs when you run a Windows network and rely on the Microsoft Hyper-V hypervisor. The same is true when you run a Linux network and rely on the hypervisor from the same Linux distribution.

FIGURE 1

Rely on natural segregation for virtual infrastructures.



SOURCE: RESOLUTIONS ENTERPRISES LTD.

In the case of a Windows network, you would have to create separate Active Directory forests for the resource pool and the VSOs, and then make sure there is no link between them. Creating this type of separate security context between the two infrastructures prevents seepage from one environment to the other (FIGURE 2).

↘ SECURITY ISSUES: UNDERSTAND THE RISKS

↘ CASE STUDY

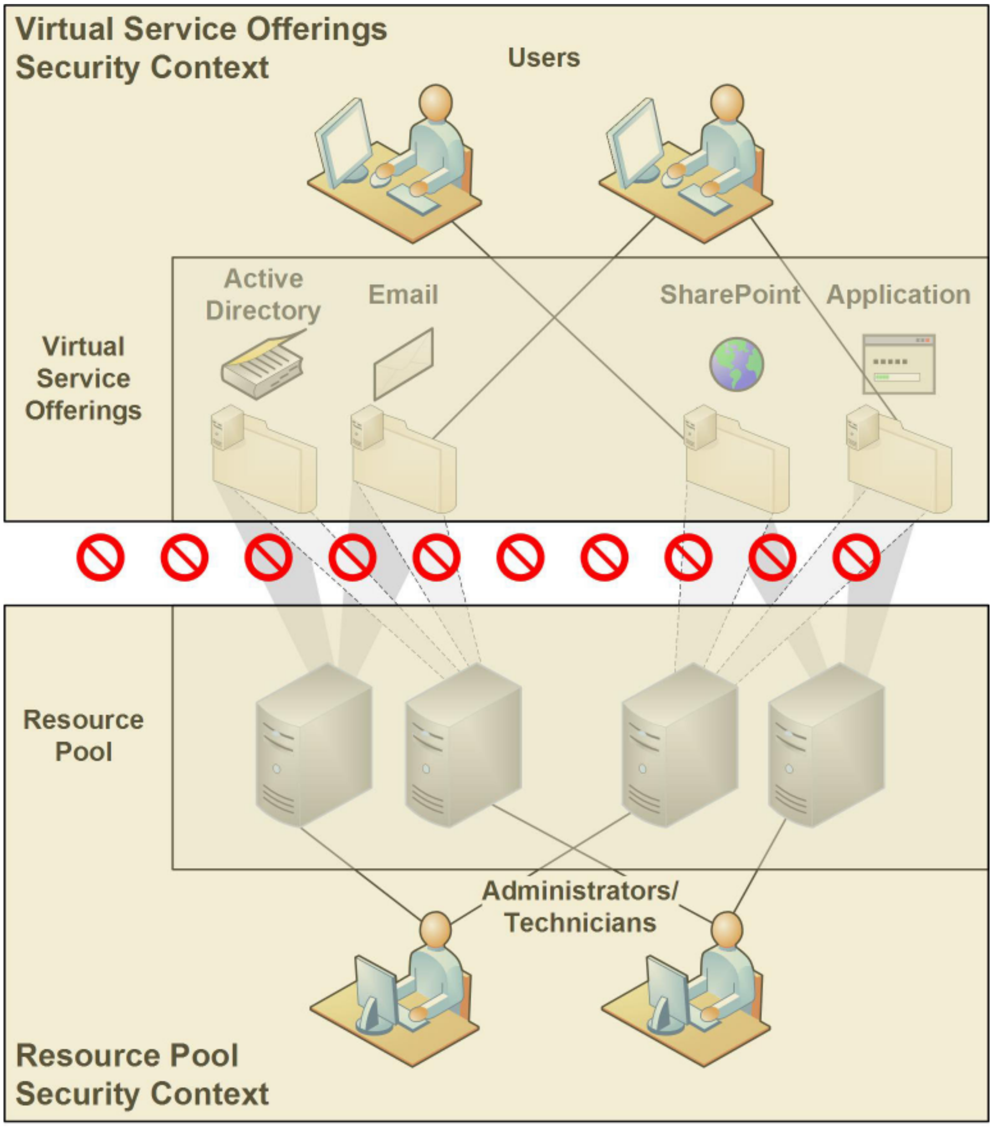
↘ NEW APPROACHES TO VIRTUALIZATION SECURITY

↘ SECURE THE RESOURCE POOL

↘ PREVENT OVER-ADMINISTRATION

FIGURE 2

Consciously segregate security contexts.



SOURCE: RESOLUTIONS ENTERPRISES LTD.

↘ SECURITY ISSUES: UNDERSTAND THE RISKS

↘ CASE STUDY

↘ NEW APPROACHES TO VIRTUALIZATION SECURITY

↘ SECURE THE RESOURCE POOL

↘ PREVENT OVER-ADMINISTRATION

SECURE THE RESOURCE POOL

Creating a segregated context for the resource pool is the first step in securing a virtual infrastructure. You should also supplement this segregation with other security measures. Here are just a few additional considerations:

- **Control access to the resource pool so that only trusted individuals have permissions for it.** Each individual accessing the resource pool should have a named account that's different from the account he or she uses to interact with the VSOs.

- **Control access to resource pool management tools.** Only trusted individuals should have access to the tools used to control resource pool components—physical servers, hypervisors, virtual networks, shared storage and any others. Allowing unauthorized access to tools is the first step in opening up your infrastructure to potential malicious behavior.

- **Manage virtual engine or hypervisor access and the virtual machines they run.** All VMs should be built and secured through administrative staff first. If end users—developers, testers or trainers—interact with VMs in your network, those machines should be built and managed by your resource pool administrators.

- **Control VM file access.** Secure all folders containing VMs and the files that comprise them with appropriate access rights. Both online and offline VM files should be tightly controlled. Ideally, you should also audit VM file access.

- **Reduce host attack surfaces by running minimal installations on your host servers.** Be sure that your hypervisor installation is as hardened as possible.

- **Implement appropriate security tools.** To support proper security policies, your infrastructure should include all of the necessary tools—systems management, inventory, auditing and monitoring tools—as well as the usual security equipment.

- **Segregate network traffic.** A proper resource pool includes private network connections for management traffic, live-motion traffic and storage traffic. All of these networks will be segregated from public network traffic in your infrastructure.

IN-DEPTH DEFENSE STRATEGIES

In addition to security context segregation, you should consider defense in-depth strategies for your virtual infrastructure. The castle defense system (CDS) model, a defense strategy endorsed by Resolutions Enterprises Ltd., an independent data cen-

↘ SECURITY ISSUES: UNDERSTAND THE RISKS

↘ CASE STUDY

↘ NEW APPROACHES TO VIRTUALIZATION SECURITY

↘ SECURE THE RESOURCE POOL

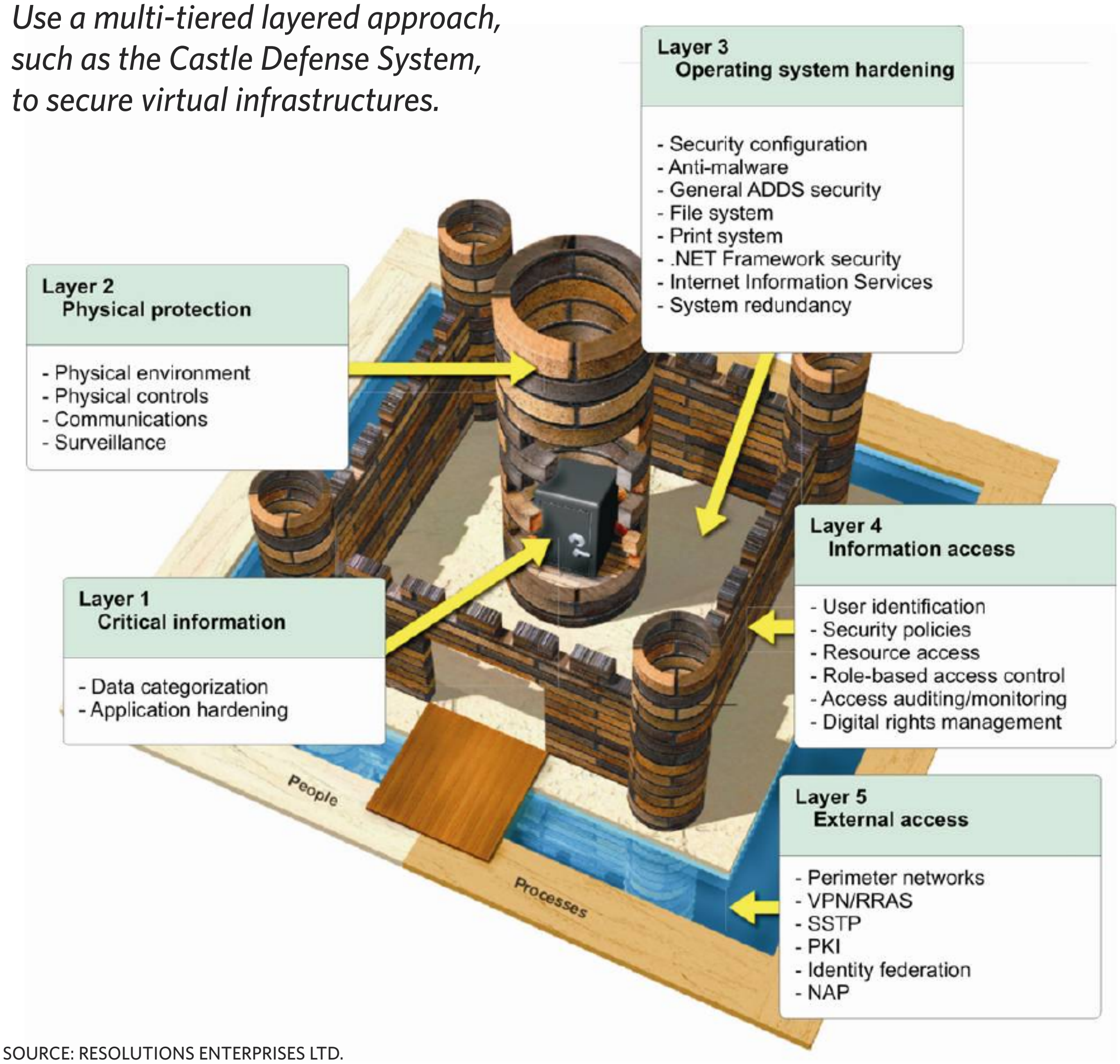
↘ PREVENT OVER-ADMINISTRATION

ter consulting group located in Victoria, British Columbia, promotes security through defense in depth. Many organizations have been using defense in-depth strategies for traditional service networks and should carry these methods over to secure the resource pool (FIGURE 3).

You can apply the CDS model to either resource pools or VSOs. TABLE 1 on page 11 outlines what you should consider in each of the five layers of the CDS when you plan to protect resource pools. The table also includes elements to consider in VSOs that allow you to compare

FIGURE 3

Use a multi-tiered layered approach, such as the Castle Defense System, to secure virtual infrastructures.



SOURCE: RESOLUTIONS ENTERPRISES LTD.

different strategies needed to protect an end-user-facing network versus a utility network such as the resource pool.

PREVENT OVER-ADMINISTRATION
Another way to improve resource pool security is to limit the number

(Continued on page 13)

LAYER-BY-LAYER CASTLE DEFENSE SYSTEM CONSIDERATIONS

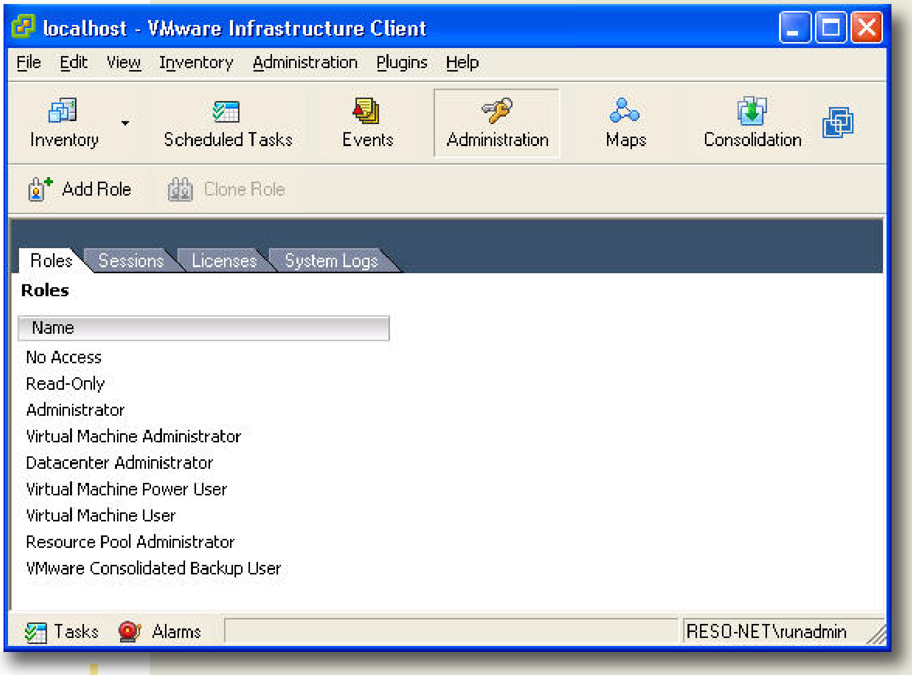
CASTLE DEFENSE LAYER	RESOURCE POOLS	VIRTUAL SERVICE OFFERINGS
Layer 1: Critical information	■ Data protection (VMs) ■ Application hardening (hypervisors)	■ Data categorization ■ Application hardening
Layer 2: Physical protection	■ Physical data center environment ■ Physical access controls ■ Communications to administrative staff ■ Surveillance	■ Physical data center environment ■ Physical access controls ■ Communications to all staff ■ Surveillance
Layer 3: Operating system hardening	■ Security configuration ■ Anti-malware/antivirus ■ Utility directory services ■ File and print systems ■ Web interfaces ■ System redundancy	■ Security configuration ■ Anti-malware ■ Production directory services ■ File and print systems ■ Web servers ■ System redundancy
Layer 4: Information access	■ Administrative user identification ■ Security policies ■ Resource access ■ Role-based access control ■ Access auditing/monitoring	■ Administrative and end-user identification ■ Security policies ■ Resource access ■ Role-based access control ■ Access auditing/monitoring ■ Digital-rights management
Layer 5: External access	■ Perimeter networks ■ VPNs/RRAs ■ SSL/PKI for all management communications	■ Perimeter networks ■ VPNs/RRAs ■ SSL/PKI ■ Identify federation ■ Network access protection

LEAST-PRIVILEDGE ACCESS PROTECTION

ONE METHOD TO secure virtual machines (VMs) that comprise virtual service offerings (VSOs) is to rely on least-privilege access. Applying this level of access in the resource pool requires a central directory service. As a rule, centralize resource pool access with any hypervisor in use to prevent inconsistencies and security breaches.

When creating a central directory service, make a utility Active Directory (AD) and link it to your host servers. This can be done with VMware vSphere or Microsoft Hyper-V. A utility directory centralizes access rights and supports delegation of administration. It requires two domain controllers—physical machines or VMs. Set VMs to autostart with host servers so they're available when you want to manage the host server infrastructure.

To create a utility directory, build a single domain forest and integrate the machines running your vCenter management interface. Then, enable Lightweight Directory Access Protocol queries to AD through the Administration -> vCenter Management Server Configuration dialog box under the AD object. You can rely on existing VMware delegation roles (see **FIGURE**) or create your own.



Roles

Name
No Access
Read-Only
Administrator
Virtual Machine Administrator
Datacenter Administrator
Virtual Machine Power User
Virtual Machine User
Resource Pool Administrator
VMware Consolidated Backup User

RESO-NET\runadmin

Creating a utility directory in Hyper-V is more complex. Create two domain controllers and appoint all host servers as member servers. Hyper-V relies on the Authorization Manager (AzMan) in Windows to provide role-based administration; the only role defined by default is Full Administrator. To assign roles, define each role by creating tasks, creating roles, assigning role definitions to role assignments and then linking roles to groups in the directory. The default AzMan store is local to the host server, so you must update it on each host. ■

↘ SECURITY ISSUES: UNDERSTAND THE RISKS

↘ CASE STUDY

↘ NEW APPROACHES TO VIRTUALIZATION SECURITY

↘ SECURE THE RESOURCE POOL

↘ PREVENT OVER-ADMINISTRATION

(Continued from page 11)

of resource pool administrators. Two administrators with full access to the environment should be enough. Then, depending on the size of your data center, you can assign appropriate delegation roles based on who needs to do what. Resource pool administrators shouldn't manage the VSO network. If you have enough personnel, it's best to segregate the roles. If you don't, then make sure that your administrators use different privileged accounts in each environment. Know that when they perform a given task in one environment, they have different responsibilities when performing an activity in a different environment.

> If you have enough personnel, it's best to segregate the roles.

Finally, protect your VMs at all times. For example, VMs that are "parked" or at rest can be at greater risk than active VMs. When VMs are in a saved state, they generate a file with the in-memory contents of the VM. This file could be analyzed to discover privileged account names and passwords. They can also be at risk if someone steals VM files and takes them out of the building. Once they have a VM in a private environment, they can break into it. ■

ABOUT THE AUTHORS

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* and *Windows Server 2008, The Complete Reference* for McGraw-Hill Osborne, as well as the *MCITP Self-Paced Training Kit (Exam 70-238): Deploying Messaging Solutions with Microsoft Exchange Server 2007*. Contact them at infos@reso-net.com.

SearchServerVirtualization.com

Cathy Gagne
Editorial Director
cgagne@techtarget.com

Christine Casatelli
Managing Editor
ccasatelli@techtarget.com

Michelle Boisvert
Managing Editor
mboisvert@techtarget.com

Martha Moore
Copy Editor

Linda Koury
Art Director of Digital Content

Marc Laplante
Publisher
mlaplante@techtarget.com