SearchSecurity

E-Guide

MANAGING VIRTUALIZATION MACHINE SECURITY FOR IN-HOUSE IAAS DEPLOYMENTS

BY DAVE SHACKLEFORD

e-guide

TechTarget

SearchSecurity

WHEN DEPLOYING AN internal Infrastructure as a Service (IaaS) cloud, there is a broad array of security considerations organizations must to take into account to not only meet security best practices but also comply with regulatory requirements. In this tip, we will specifically discuss controls for virtual machine (VM) instances, management platforms, and the network and storage infrastructure that supports an IaaS implementation.

VIRTUAL MACHINE INSTANCES

First, the operating systems and applications for virtual machines must be locked down and properly configured using existing guidelines, such as those from the Center for Internet Security (CIS). Proper VM management can also lead to more sound and consistent configuration management practices.

The key to creating and managing secure configurations on virtual machine instances is leveraging templates. It is advisable for administrators to build a "gold image" template that is used to instantiate all virtual machines within the cloud. This template should be carefully locked down and revision controls should be in place to ensure all patches and other updates are applied in a timely fashion.

Many virtualization platforms offer specific controls for securing virtual machines; organizations should certainly take advantage of these. For example, VMware Inc.'s virtual machines have configuration settings that specifically prohibit copy and paste between the VM the underlying hypervisor, which helps prevent sensitive data from being copied to hypervisor memory and clipboards. Platforms from Microsoft and Citrix Systems Inc. offer similar copy-and-paste restrictions. Other platform features can help enterprises disable unnecessary devices, set up logging parameters, and so forth.

Also when securing VM instances, be sure to segregate VMs running in different cloud segments according to standard data classification principles. Since VMs share hardware resources, running them on the same cloud segment could lead to intermingling of data in memory, although the likelihood of this is slim today.

MANAGEMENT PLATFORMS

The second key aspect to securing a virtual environment is ensuring the safety of the management platform that interacts with VMs and configures and monitors the underlying hypervisor systems in use.

These platforms, such as VMware vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), and Citrix XenCenter, come with their own local security controls that can be implemented. vCenter, for example, is often installed on Windows and inherits the local Administrator role and SYSTEM privileges unless they are changed during installation.

When it comes to management tools, ensuring the security of the management database is paramount, yet many products' default settings are not inherently secure. Most importantly, roles and privileges must be assigned for different operational roles within the management platform. While many

organizations have a virtualization team to manage VM operations within the IaaS cloud, it is critical to not grant excessive privileges within the management console. I suggest delineating privileges to storage, networking, system administration, and other teams as you would in a traditional data center environment.

For cloud management tools, such as vCloud Director and OpenStack, roles and privileges should be carefully assigned, but must include different end users of the cloud VMs. For example, development teams should have certain VMs for their job functions which are separate from the VMs used by the finance team.

All management tools should be isolated on a separate network segment, and it's a good idea to require access to these systems through a "jump box" or dedicated security proxy platform, such as HyTrust, where strong authentication and central privileged user monitoring can be established.

NETWORK AND STORAGE INFRASTRUCTURE

While securing the network and storage that facilitate the IaaS cloud is a huge area to cover, there are some general best practices that should certainly be applied.

For the storage environment, keep in mind that, just like any other sensitive file, virtual machines must be protected. Certain files store active memory or a snapshot of memory (likely the most sensitive, as they can contain user credentials and sensitive data), while other files represent the full hard disk of the system. In either case, the file can contain sensitive data. It is vital to use separate Logical Unit Numbers (LUNs) and zones/domains within the storage environment to segregate systems of different sensitivity. If storage area network (SAN)-level encryption is available, consider that if appropriate.

On the network side, be sure to keep individual segments isolated and controlled with virtual local area networks (VLANs) and access controls. Organizations may consider the use of virtual firewalls and virtual intrusion detection appliances if granular security control is necessary within the virtual environment. VMware's vCloud platform is natively integrated with its vShield virtual security appliances, and other products from traditional networking vendors are also available. In addition, consider network segments where sensitive VM data may pass in cleartext, such as the vMotion network. In this VMware environment, cleartext memory data gets carried from one hypervisor to another, leaving sensitive data vulnerable to exposure.

SearchSecurity

CONCLUSION

These three areas of control are just the tip of the iceberg when it comes to securing a virtual environment or IaaS private cloud. For additional information, VMware has a series of in-depth hardening guides that outline specific controls to evaluate, and OpenStack has a security guide available on its site. By following some fundamental practices, organizations can build their own IaaS clouds in-house and secure them to meet not only their own standards but also all other necessary industry requirements.

DAVE SHACKLEFORD is senior vice president of research and CTO at IANS, and a SANS analyst, instructor and course author. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. He is a VMware vExpert and has extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft, CTO for the Center for Internet Security, and as a security architect, analyst and manager for several Fortune 500 companies. Dave is the co-author of Hands-On Information Security from Course Technology as well as the "Managing Incident Response" chapter in the Course Technology book Readings and Cases in the Management of Information Security. Recently, Dave co-authored the first published course on virtualization security for the SANS Institute. He currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance.

SearchSecurity

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.