HYTRUST
Cloud Under Control

Learn the essentials of virtualization security

White Paper

HYTRUST
Cloud Under Control

Table of Contents

HYTRUST
Cloud Under Control

White Paper

Learn the essentials of virtualization security

Introduction

This paper is the first in a series about the essential security issues arising from virtualization and the adoption of private and public Cloud services. This series will provide the reader with an introduction to each area of security risk and provide some solutions, actions, and third-party sources to help mitigate those risks.

Virtualization and the move to private and public Clouds is well underway. The rapid pace of virtualization within the data center means that IT and security teams must adapt their existing security practices to keep up. Virtualization platforms and virtual machines are complex technologies that introduce new potential risks. The fluid nature of virtualized infrastructure and the high mobility of virtual machines (VMs) are what make virtualization and the Cloud valuable. This nature is what also brings about a broad set of security challenges; from new network security concerns to sensitive data being exposed within the VMs themselves.

Data breaches are increasing, threats are very advanced, and current virtualization technologies are a major part of the problem. The following statistics from Verizon's 2011 Data Breach Investigations Report (DBIR) underscore the current data-breach landscape:

- 76% of all data breaches came from servers
- 29% of the breaches involved physical attacks
- 92% of attacks were not difficult to accomplish

Couple that information with some statistics on virtualization:

- Through 2012, 60% of virtualized servers will be less secure than the physical servers they replace
- By the end of 2012, more than 50% of enterprise data center workloads will be virtualized

Even if we assume that the security statistics concerning virtualization are only partially accurate, we still should be concerned. We must also consider the fact

that more (and eventually most) sensitive data will be handled within these rapidly growing virtual infrastructures. Either perspective leads to the same conclusion:

Data security for virtualized servers is not a nice-to-have—it is imperative.

Hypervisor connectivity and risks

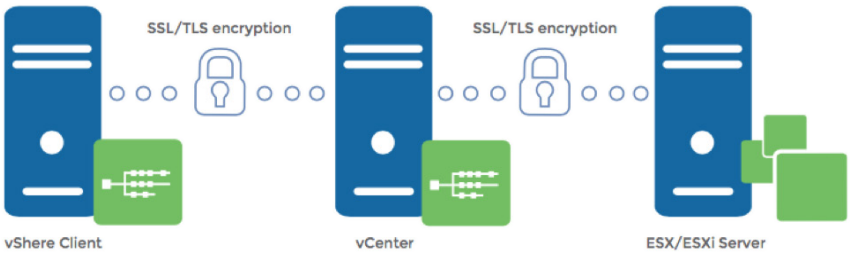
The first area of virtualization security that organizations should focus on is the hypervisor itself. Remember that Hypervisors are software just like any operating system. Accordingly, they must be kept up-to-date using consistent patch management processes and patch management tools that are capable of functioning with the appropriate hypervisor platform. For example, VMware Update Manager is a tool that VMware provides to its customers for keeping VMware's hypervisor platforms and related components current.

Any hypervisors must be configured in order to do its job, and each type of hypervisor has configuration settings that can result in a number of points of exposure. Configuration guidance sources are available for each of the major hypervisor platforms: VMware ESX and ESXi, Citrix Xen, KVM, and Microsoft Hyper-V. Sources of hardening guidance include the Center for Internet Security, the Defense Information Systems Agency, and the platform vendors. The hardening guides describe specific configuration settings related to user and group management, network settings and local firewall use, file permissions, logging, and numerous additional areas. In general, the hypervisor should be as locked down as possible without sacrificing any critical business functionality.

Multi-tenancy risks

Another key area of risk for organizations deploying virtualization platforms is the inherent multi- tenant nature of these systems. Multi-tenancy creates the possibility that multiple types of systems, potentially owned and maintained by different business units, end up on the same physical infrastructure and/or having their data co-mingled on the same storage device. Virtualization makes it easy to (sometimes unknowingly) intermingle applications and data that would have never operated on the same host or in the same storage in the old physical data center. For example, many organizations unknowingly host sensitive or compliance-related applications on the same hypervisor host as less sensitive applications, potentially exposing the sensitive data to intermingling or leakage through access by less sensitive systems or other resources.

As an organization moves beyond basic server virtualization to a more fluid private and public cloud infrastructure, the co-mingling of applications and data can become a much larger issue. Different organizations' data might be hosted on the same platform, necessitating local protection mechanisms that prevent data from exposure in the virtual network. Most virtual networking components are inherently isolated from each other; for example, standard virtual switches cannot be cascaded together without a virtual machine acting as a proxy between the two. However, native virtual switches from all the major vendors do not afford much more protection than standard Layer-2 Virtual LANs (VLANs), so additional segmentation controls likely need to be installed as virtual appliances or add-ons to the existing hypervisor.



Management and operational network risks

One overlooked area of security for a virtualization infrastructure is the management network that connects administrators to management servers and the management servers to the hypervisor plat- forms themselves. The simple network diagram depicted in Figure 1 demonstrates a typical installation scenario in a VMware environment.

In this diagram, the two network segments related to management traffic should be carefully protected with encryption, which is usually present by default. Another essential control to implement is adequate network segmentation of the management connections. Any management servers should be on a separate management VLAN or physical network, and clients that connect to these management servers should ideally be on this separate network as well. One simple best practice is to install a server with the management client installed on the management network as a "bastion host" that administrators can connect to with Remote Desktop or other secure remote access protocols. This provides a single point of connectivity that can be adequately protected and monitored.

Storage risks

Storage environments are critical for large-scale virtualization deployments, as virtual machines can- not migrate from one host to another without a shared storage medium, and large numbers of virtual machines require a significant amount of storage space in general. However, many storage environments are not well secured. Network File System (NFS) and Network Attached Storage (NAS) systems as well as iSCSI and Fibre Channel SANs are known to have many security issues if they are not configured properly. NFS is a clear-text protocol with few access controls built in, and both iSCSI and Fibre Channel are susceptible to a number of well-known issues, as well. Fibre Channel environments send traffic in clear-text, and often leverage a weak node identification system built on World Wide Names (WWNs), an 8-byte value that uniquely identifies host bus adapters (HBAs). Attackers can easily spoof WWNs, and these are often the only access controls protecting storage resources. Storage volumes are usually identified by logical unit numbers (LUNs), and "hiding" LUNs is commonly done on the hypervisor HBA instead of elsewhere in the network, allowing an attacker who gains access to the hypervisor platform to unmask the LUN and access storage volumes that were "hidden". iSCSI environments suffer from many of the same issues, but implemented differently.

The virtual machines themselves are an attractive target for attackers because a virtual machine is simply a set of files, so stealing a machine is as easy as copying the files. How to protect virtual machines? Virtual machines are operating systems that can benefit from the same protective controls as physical machines, including OS

patch management and common configuration standards that lock down the OS. The resources mentioned above for hypervisor configuration guidance (CIS, DISA, various vendors) apply in the case of OS security configuration management.

Beyond patching and general configuration management for the OS and applications, a few controls exist that are specific to virtual machines. For example, in VMware environments, a virtual machine (here called "VM") contains a number of specific files:

- VM.vmx: VM config file
- VM.vmdk: Virtual disk config file
- VM-flat.vmdk: Actual VM hard disk
- VM.nvram: VM's BIOS file
- VM*.log: VM log files
- VM.vswp: The VM Swap file
- VM.vmsn/vmsd: VM snapshot metadata
- VM0000001-delta.vmdk: Real-time snapshot write file
- VM-***.vmss: Suspended VM memory data

Not all of these exist at any given time; they depend on the state of the VM. All of these files are important, but some, if unprotected, can expose sensitive data. For example, the VM swap file (vswp) and VM suspension file (vmss) might contain passwords, crypto keys, or sensitive application data, and an at- tacker could access and steal this data while these files are in storage. From a configuration standpoint, the .vmx file is the most critical, and a number of specific settings within this file can help to secure the VM, with controls ranging from logging parameters to hypervisor interaction.

Some important controls to consider include the following:

- **VM host copy/paste:** This control determines whether remote clipboard content is available to VM users. To disable this potentially dangerous functionality, enter the following statements:
  - isolation.tools.copy.disable true
  - isolation.tools.paste.disable true
  - isolation.tools.setGUIOptions.enable false
- V**M logging:** Limit VM log file size to prevent a VM disk from filling up. Configuring the number of distinct log files to retain is also an important consideration. These can be configured as follows:
  - log.rotateSize 100000 (sets logs to 100KB in size)
  - log.keepOld 10 (keeps 10 distinct log files)

- **Disable unauthorized devices:** Security best practices dictate that any unnecessary devices and ports should be disabled whenever possible. The following settings disable floppy disk drives, serial ports, and parallel ports (where <x> is a device number starting with 0):
  - floppy<x>.present FALSE
  - serial<x>.present FALSE
  - parallel<x>.present FALSE
- **Disable drag-and-drop functionality:** This control disables drag-and-drop functionality between the VM and hypervisor system, which is not found on most enterprise systems. When it is, drag-and-drop functionality between the VM and the console operator can lead to potential data leakage and communication channel compromise. Disable it with the following statement:
  - isolation.tools.dnd.disable FALSE

There are many additional considerations for virtual machine security. For example, are the virtual disks protected while being stored on the central SAN or NAS devices? Operationally, encrypting virtual machine disk files is much different than standard full disk encryption (FDE), as the VMDK (virtual disk file) and similar files need to be manipulated and managed by hypervisor platforms in a number of ways, ranging from simple disk reads for OS interaction to performance metric calculation by the hypervisor and virtualization solution in use.

Virtual machine mobility risks within the data center

As organizations look to enhance their virtualization implementations by moving to a private or hybrid cloud, securing the mobility of virtual machines within the cloud needs to be addressed. Several key points to consider are:

- **Clear-text data in transit:** Using vMotion and similar VM migration techniques, a migration operation exposes VM memory in transit, potentially allowing application data or file data to be accessed by anyone monitoring the network over which this data traverses.
- **Multi-tenancy:** Multiple VMs hosted on the same hypervisor can potentially lead to sensitive data exposure if the same classification of systems is not adhered to during data and VM migration. Many organizations do a poor job of data classification, and complex cloud environments could easily have numerous VM migration operations occurring simultaneously. If proper policies and controls are not in place, serious data exposure could occur. For example, a VM hosting payment card data processing applications could be migrated to a hypervisor hosting much less sensitive systems, opening up a new avenue of exposure. Organizations should take care to ensure that VMs with similar data sensitivity levels are kept together on specific hypervisor platforms during migration.
- **Data-at-rest security:** Virtual machines are sets of files that usually exist on shared storage, and are usually protected by the often minimal security that is in place within the storage environment itself. Accessing

these sets of files at the storage layer can usually happen without the knowledge and controls put in place within the virtual infrastructure layer.

To solve these security problems, many in the security community are looking for new security mechanisms where security policy and enforcement stays with the virtual machine as it travels. To be effective, security policies need to be created and applied within a virtualization solution and be recognized by each hypervisor hosting the virtual machine as the virtual machine travels. Examples of this functionality include localized VM identification policy (for multi-tenancy consideration and evaluation) as well as VM encryption capabilities.

Conclusion

There are many pieces to the puzzle of virtualization security, ranging from hypervisor configuration to network security measures and storage. The ultimate security consideration, however, lies with the virtual machines themselves. The inherently fluid and mobile nature of the virtualized environment requires security to travel with the virtual machine and protect its data. Therefore, the security of a virtual machine's data cannot simply be where it happens to reside at the moment. Encryption, access control, and audit are central to protecting the virtual machine and its data both inside the data center.

About the author

Dave Shackleford is Founder and Principal Consultant at Voodoo Security. Director, Risk & Compliance and Director, Security Assessments at Sword & Shield Enterprise Security, Inc. Chief Security Strategist, EMC Ionix at EMC, Chief Security Officer at Configuresoft. SANS Instructor - teaches virtualization security to hundreds of companies every year.

HyTrust - Cloud Under Control.
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040, USA
Phone: 1-844-681-8100
International: 1-650-681-8100