CHAPTER 11

Auditing Virtualized Environments

Innovations in operating system virtualization and server hardware permanently changed the footprint, architecture, and operations of data centers. This chapter discusses auditing virtualized environments, and begins with an overview of common virtualization technologies and key controls. The virtualization audit combines the concerns of the hypervisor and the guest operating systems. Although the focus of this chapter is the hypervisor and server virtualization, you can apply many of the same steps and concepts to desktop virtualization. We make the assumption that these system components are under your control. You should reference Chapter 14, "Auditing Cloud Computing and Outsourced Operations" for guidance on how to ensure outsourced virtualized environments are properly managed and secured.

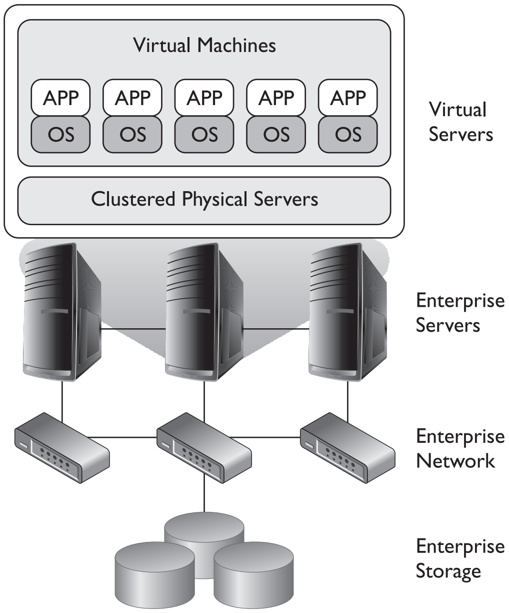
This chapter covers the following:

- A brief technical overview of virtualization
- How to audit the virtualization environment
- Tools and resources for enhancing your virtualization audits

Background

Virtualization allows the separation of the operating system from the hardware, using a layer called a *hypervisor* to sit between the hardware and the operating system. The hypervisor abstracts the physical hardware and presents the hardware you specify to the operating system. The resulting abstraction of the operating system from the specific physical server provides tremendous creative freedom for backing up, copying, restoring, and moving running operating systems, complete with their installed applications. Figure 11-1 illustrates the separation of virtual machines from the physical hardware. Notice that complete abstraction from the hardware allows for some interesting hardware clustering scenarios and also enables the groundwork for sharing hardware resources with an outside cloud computing environment.

Figure 11-1 Virtualization model



Virtualization software can be installed onto a bare metal server or as an application on top of another operating system. Many vendors allow the hypervisor to be installed either way, on top of the OS or by itself, without the hassle and overhead of the OS. The software is designed to utilize embedded processor instructions specifically designed to support multiple operating systems. Processor manufacturers led this charge a few years ago, and the highly customized hardware packages by Cisco Systems, VMware, and other global players foretell the intent to package as much power, security, and management as possible into the hardware to support virtual infrastructures. Gartner believes—and the readers of this book will know—that by the time this book is published and distributed, more than 50 percent of the world's servers will be virtualized.

Commercial and Open Source Projects

Several commercial players are in this market, including VMware, Microsoft, Citrix, Oracle, Parallels, Red Hat, and Novell. Some of these players maintain open source projects, including Xen by Citrix and VirtualBox by Oracle-Sun Microsystems. KVM is a popular open source virtualization project for Linux. Links to each of these projects are located in "Knowledge Base" at the end of the chapter.

Virtualization Auditing Essentials

To understand the material in this chapter, you need a basic understanding of the components that make up the virtualization environment. Your role as an auditor and advisor will significantly improve if you understand major technology trends challenging virtualization models.

Security models, business alignment, capacity planning, and performance management are more important than ever before in virtual environments. Smaller environments may have a few virtually hosted servers running on a single powerful physical server, whereas larger environments support hundreds or thousands of virtually hosted servers and desktops running on a complex infrastructure of clustered servers connected to a massive Storage Area Network (SAN). The scale may change the scope or approach to the audit, but the same business requirements and controls exist. Resource management and monitoring of each of the components separately and collectively enable the virtual environment to function.

Figure 11-2 illustrates an example collective environment and several audit considerations. Notice that these considerations also apply to a normal server or storage audit. What's different? What are the security concerns that keep administrators awake? What should auditors explore? The hypervisor has control requirements similar to those found in a server, but it also has unique requirements to ensure that the hosted environment doesn't present additional control weaknesses to the guest operating systems. The guest operating systems have unique control requirements because of the necessity to keep appropriate segregation controls in place between servers. Mildly complicating this mix are different conceptual approaches to creating the virtual environment.

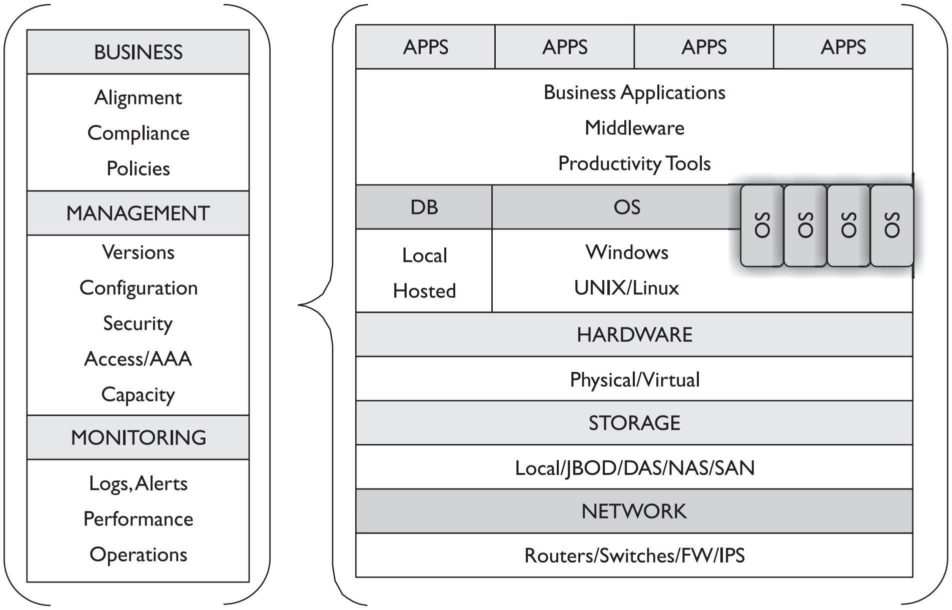


Figure 11-2 Example virtualization audit model

Test Steps for Auditing Virtualization

The virtualization audit covered here is designed to review critical controls that protect the confidentiality, integrity, or availability of the environment for the supported operating systems and users that rely on the environment. Each of the following steps applies to some extent; however, use your judgment to determine the depth to which you decide to take any one step. For example, an auditor reviewing high-performance environments supporting a business-critical application might spend more time asking questions and reviewing vendor-specific analysis output that verifies that the virtualized environment has the capacity and performance necessary to handle peak loads.

NOTE This audit focuses on the hypervisor and management of the virtual environment, regardless of where the hypervisor is installed. If the hypervisor is installed as an application on another operating system, audit the underlying operating system separately using the appropriate test steps in Chapter 6, "Auditing Windows Operating Systems," or Chapter 7, "Auditing UNIX and Linux Operating Systems."

Note that there are several excellent hardening guides and configuration checking utilities, and we encourage the use of these tools to help provide consistency across the environment. Vendors have different approaches for shipping products. Some vendors include unnecessary services and product features enabled. Others ship their products in a hardened state whereby the administrator must enable additional services. Note many of the hardening guides have a narrow scope that focus on the compromise of the hypervisor as opposed to ensuring that controls support business processes and objectives. This is the value provided by Control Objectives for IT (COBIT).

Setup and General Controls

1. Document the overall virtualization management architecture, including the hardware and supporting network infrastructure.

The team responsible for managing virtualization should maintain documentation illustrating the virtualization architecture and how it interfaces with the rest of the environment. Documentation should include supported systems, management systems, and the connecting network infrastructure. This information will be used by the auditor to help interpret the results of subsequent audit steps.

How

Discuss and review existing documentation with the administrator. As applicable, verify that document structure and management are aligned with corporate standards. Verify the entire environment, including management, storage, and network components, are properly documented.

2. Obtain the software version of the hypervisor and compare with policy requirements.

Review the software version to ensure that the hypervisor is in compliance with policy. Older software may have reliability, performance, or security issues that can increase the difficulty in managing the virtualization platform(s). Additionally, disparate software versions may increase the scope of administrator's responsibilities as he or she attempts to maintain control over the different hypervisors and their feature, control, and administration differences.

How

Work with the administrator to obtain this information from the system and review vendor documentation. Ensure that the software is a version the vendor continues to support and does not contain widely known and patchable vulnerabilities that would bypass existing controls. Also verify that the current running version does not contain performance or reliability issues that would affect your environment. Review any mitigating factors with the administrator, such as issues that have not been fixed but are not applicable to the environment.

3. Verify that policies and procedures are in place to identify when patches are available and to evaluate and apply applicable patches. Ensure that all approved patches are installed per your policy requirements.

Most virtualization vendors have regularly scheduled patch releases. You should be prepared for the scheduled releases so that you can plan appropriately for testing and installation of the patches. If all the patches are not installed, widely known security vulnerabilities or critical performance issues could exist.

How

Interview the administrator to determine who reviews advisories from vendors, including timely notifications about new vulnerabilities and zero-day attacks, what steps are taken to prepare for the patches, and how the patches are tested before being applied to the production systems. Ask to review notes from the previous patching cycle.

Obtain as much information as possible about the latest patches through conversations with the administrator and review of vendor documentation, and determine the scope of the vulnerabilities addressed by the patches. Compare the available patches with the patches applied to the hypervisor. Talk with the administrator about steps taken to mitigate potential risk if the patches are not applied in a timely manner.

4. Determine what services and features are enabled on the system and validate their necessity with the system administrator.

Unnecessary services and features increase risk exposure to misconfigurations, vulnerabilities, and performance issues and complicate troubleshooting efforts.

How

Today's virtualization systems range from the very simple to the extremely complex. Work closely with the virtualization administrator to discuss enabled services and their applicability to the environment. Review and evaluate procedures for assessing vulnerabilities associated with necessary services and features and keeping them properly configured and patched.

Account and Resource Provisioning and Deprovisioning

Administrative accounts in the virtual environment must be managed appropriately, as should the provisioning and deprovisioning of virtual machines.

5. Review and evaluate procedures for creating administrative accounts and ensuring that accounts are created only when a legitimate business need has been identified. Also review and evaluate processes for ensuring that accounts are removed or disabled in a timely fashion in the event of termination or job change.

Effective controls should govern account creation and deletion. Inappropriate or lacking controls could result in unnecessary access to system resources, placing the integrity and availability of sensitive data at risk.

How

Interview the system administrator, and review account-creation procedures. This process should include some form of verification that the user has a legitimate need for access. Take a sample of accounts and review evidence that they were approved properly prior to being created. Alternatively, take a sample of accounts and validate their legitimacy by investigating and understanding the job function of the account owners.

Review the process for removing accounts when access is no longer needed. This process could include a component driven by the company's human resources (HR) department providing information on terminations and job changes. Or the process could include a periodic review and validation of active accounts by the system administrator and/or other knowledgeable managers. Obtain a sample of accounts and verify that they are owned by active employees and that each employee has a legitimate business requirement for administrative access.

6. Verify the appropriate management of provisioning and deprovisioning new virtual machines, including appropriate operating system and application licenses.

Written policies should govern the process used to create new virtual machines, manage users, and allocate software licenses. The ease of spinning up new servers for development and testing has created a new challenge for managing hardware and license resources.

Policies or procedures should also exist for "cleaning up" or removing virtual machines, rights, and licenses that are no longer needed when a project is completed.

Failure to manage virtual host allocation could unnecessarily expend virtualization capacity and software licenses.

Virtual machines should be accountable to specific groups or users. Failure to govern rights management may allow users that should no longer have access to hosts to maintain inappropriate levels of access.

How

Discuss policies and procedures for provisioning and deprovisioning new hosts and accounts with the virtualization administrator, including license allocation, user management, and host ownership. Several tools help manage this process, particularly in development environments where server sprawl tends to become a problem. For example, VMware's Lab Manager allows the provisioning administrator to set time limits for how long a virtual machine can be active. Lab Manager provides a control that protects the virtualization resources from becoming overrun with virtual machines that consume resources from the virtual hosts that really need those resources.

Virtual Environment Management

The virtual environment must be managed appropriately to support existing and future business objectives. Resources must be monitored and evaluated for capacity and performance. Resources must also support the organization's Business Continuity/Disaster Recovery objectives.

7. Evaluate how hardware capacity is managed for the virtualized environment to support existing and future business requirements.

Business and technical requirements for virtualization can change quickly and frequently, driven by changes in infrastructure, business relationships, customer needs, and regulatory requirements. The virtualization hardware and infrastructure must be managed to support existing business needs and immediate anticipated growth. Inadequate infrastructure places the business at risk and may impede critical business functions that need more hardware capacity.

How

Virtual machine capacity is managed by the hypervisor to allocate a specific amount of storage, processor, and memory to each host. Verify that capacity requirements have been documented and that customers have agreed to abide by them. Capacity allocation may directly affect performance. Review processes for monitoring capacity usage for storage, memory, and processing, noting when they exceed defined thresholds. Evaluate processes in place for responding and taking action when capacity usage exceeds customer-approved thresholds. For example, some organizations utilize cloud bursting to offload increases in demand for internal computing capacity, whereby a service provider makes additional capacity available as needed. Discuss the methods used to determine present virtualization requirements and anticipated growth. Review growth plans with the administrator to verify that the hardware can meet the performance requirements, capacity requirements, and feature requirements to support infrastructure and business growth.

8. Evaluate how performance is managed and monitored for the virtualization environment to support existing and anticipated business requirements.

Virtualization performance of the infrastructure as a whole and for each virtual machine is driven by several factors, including the physical virtualization media, communication protocols, network, data size, CPU, memory, storage architecture, and a host of other factors. Inadequate virtualization infrastructure places the business at risk of losing access to critical business applications. It's possible to have adequate capacity but incorrectly configured and underperforming virtual machines that fail to deliver on the Service Level Agreement (SLA).

How

Verify that regular periodic performance reviews of the processor, memory, and bandwidth loads on the virtualization architecture are performed to identify growing stresses on the architecture. A common performance measurement for virtual environments is based on Input/Output Operations Per Second (IOPS). Verify that performance requirements have been documented and that customers have agreed to abide by them. Review processes for monitoring performance and noting when performance falls below defined thresholds. Evaluate processes in place for responding and taking action when performance falls below customer-agreed thresholds. Discuss the methods used to determine present performance requirements and anticipated changes.

NOTE A review of capacity management and performance planning is essential to this audit. Be careful to ensure that the administrator has a capacity management plan in place and verifies that performance needs are appropriate for the organization.

9. Evaluate the policies, processes, and controls for data backup frequency, handling, and offsite management.

Processes and controls should meet policy requirements, support Business Continuity/Disaster Recovery (BC/DR) objectives, and protect sensitive information. Data backups present monumental challenges for organizations, particularly when it comes to the central data repositories in the organization, namely the databases and virtualization platforms. Vendors offer several solutions to manage the frequency, handling, and offsite delivery of data and system backups. The implemented solution should be appropriate to meeting the stated goals of the BC/DR plans.

How

Review policy requirements for meeting Recovery Point Objectives (RPOs), which affect how much data might be lost from a disaster, and Recovery Time Objectives (RTOs), which affect how long it will take to restore data after a disaster occurs. The RPOs and RTOs, shown in Figure 11-3, for virtualized hosts should be aligned with the BC/DR programs. Discuss the relative priority to other systems based on business criticality and dependencies. Verify that an appropriate Service Level Agreement (SLA) is in place

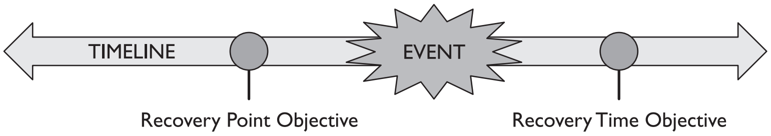


Figure 11-3 Recovery Point Objective and Recovery Time Objective

that supports your stated RPO/RTO objectives if part of this process is outsourced or handled by another party. You should also ensure that sensitive data is encrypted prior to offsite storage.

10. Review and evaluate the security of your remote hypervisor management.

Secure remote hypervisor management protects the hypervisor from remote attacks that might otherwise disrupt the hypervisor or hosted virtual machines. Each of the hypervisors has its own management tools designed to allow remote administration of the hypervisor and virtual machines. Many of these commercial tools can manage other commercial hypervisors in an effort to manage heterogeneous virtual environments seamlessly. Despite their obvious differences, the areas that should be reviewed have some commonalities.

Unused services, accessible APIs, and installed applications may subject the hypervisor to additional attack vectors if a security flaw is discovered. In addition, remote users should be forced to access the system using accounts that can be tied to a specific user for logging and tracking. The difference between this step and step 4 is the careful analysis of network-accessible components for the hypervisor with regard to remote management. Unless specifically required and appropriately controlled, network-accessible features should not be enabled. Enable only those components that are necessary and appropriately configured for remote management.

How

Each vendor provides specific security guides for enabling remote management. These security guides are generally easy to read and should be reviewed in detail prior to beginning the audit. The execution of this step consists of a policy review, account permissions review, and a configuration review.

Review remote access policies and access methods with the administrator. Verify that all remote access is logged to a system separate from the environment. Question the need for any clear-text communications used for remote access. Identify and validate the appropriateness of administrative accounts that have remote access.

NOTE The use of secure protocols is particularly important in a DMZ and other high-risk environments. It is also advisable to use secure protocols for management on internal networks to minimize internal attack vectors. Attackers will use a single compromised beachhead system to learn about the environment, pivot, and attack other systems from within.

Obtain vendor appropriate guidance for configuring secure remote hypervisor access. These should be used to identify and verify that the environment is securely configured for remote access. This process can be conducted manually, but we highly recommend using one of the several available versions of configuration checking tools. For example, the Tripwire-VMware developed tool verifies the following which may also assist you with other parts of this audit:

- Virtual network labeling
- Port Group settings
- Network isolation for VMotion and iSCSI
- NIC Mode settings / Layer 2 Security settings
- MAC address parameters
- VMware ESX Service Console security settings
- SAN resource masking and zoning
- Disk partitioning for Root File System
- VirtualCenter database configuration
- Configuration changes

Additional Security Controls

11. Review and evaluate the security around the storage of virtual machines.

Virtual machines are stored and manipulated as files that are easily transported, copied, and viewed. Shared storage for virtual machines should have controls in place to isolate sensitive virtual machines and content from the rest of the environment.

Some environments might encrypt data-at-rest. Encryption of data-at-rest involves encrypting data as it is stored on disk. Encryption of data-at-rest is more important than other forms of encryption because the lifetime of data on disk is much longer than the lifetime of data on the network. If you look at where data is most likely to be stolen, you'll find it is most likely to be taken directly from the storage while at rest and not while traversing the network.

This step isn't appropriate for all environments and may be covered by other controls or applications.

How

Ensure virtual machines are stored in such a manner that sensitive virtual machines are isolated from the rest of the network and that only appropriate administrators have access. Consideration must also be given to managing and auditing administrative access to a storage environment containing sensitive virtual machines.

Verify that encrypted data is encrypted properly. Additionally, review the location where the encryption keys are stored because the strength of encryption relies on the strength of protection of the encryption keys. If the encryption keys are stored with the encrypted data, an attacker can subvert the security simply by extracting the encryption keys.

If encryption is used, then verify the disaster recovery plan contains encryption key management. A mistake you do not want your administrator to make is to implement encryption features but fail to include key management in the backup procedures. Failing to back up encryption keys properly may result in the inability to recover a backup.

12. Verify that network encryption of data-in-motion is implemented where appropriate.

Policy requirements may require that traffic be encrypted for applications that contain sensitive information or for backing up some virtualized hosts to another location. Network encryption serves two main purposes: to protect authentication credentials as they move across the network, and to protect the actual data as it moves over the network. The network is not a secure environment—IP addresses can be spoofed, and network traffic can be redirected and sniffed.

How

Work with the administrator to verify that encrypted protocols are used for remote administration of the virtual environment. Review policy requirements with the administrator and determine if any of the virtualization data is required to be encrypted in transit. If the virtual hosts contain sensitive data, verify that network traffic used to backup or replicate the hosts is encrypted.

Given the additional potential complexity derived from dedicated networks for storage, backup, management, failover, and so on, an auditor might want to document the data flow between these components for the virtual environments. This may have been accomplished in step 1.

13. Evaluate the low-level and technical controls in place to segregate or firewall highly sensitive data on critical virtual machines from the rest of the virtualization environment.

Controls should exist that restrict access between virtual machines to protect sensitive information such as cardholder data (CHD), personally identifiable information (PII), source code, and other types of proprietary data, including administrative rights to the host. Each of the hypervisors has specific settings and controls that can be implemented to assist with the segregation of data between hosts. Commonly discussed threats specifically include the use of shared folders and the ability to copy and paste between a host operating system and the hosted virtual machine. If encryption is used, describe it here and evaluate the handling of keys, including the granting and revocation of rights, keys, and certificates.

How

Review with the virtualization administrator the controls in place to isolate virtual machines that have different classification levels. Identify technical and administrative controls that force separation between sets of data. Strong controls will prevent comingling of disparate data types, and create actionable, nonrepudiated logs when these controls are bypassed. Sensitive virtual machines should not be directly accessible by the rest of the environment.

Review auditing and log management procedures governing administrative access to the virtualization environment that could bypass intended controls. Consider compensating controls such as data encryption.

The detail of configuration options between the variant hypervisors to protect virtual machines from each other and the host (when installed on a hosted OS) requires that the auditor gather additional knowledge to identify vendor-recommended best practices. Discuss specific options with the administrator in the business context of environmental risk and compensating controls.

There are several resources available. One particularly well-written resource readily found online is from McAfee/Foundstone titled *How Virtualization Affects PCI DSS: Part 2: A Review of the Top 5 Issues*. Figure 11-4 illustrates the use of firewalls to segment virtualized components. This particular example was created for the PCI-SSC Virtualization Information Supplement for a discussion around segmenting sensitive credit card data from other virtual machines in a multitenant environment. Note that firewalls and switches may be virtualized as well and appropriate controls must be verified for these components.

14. Review and evaluate system administrator procedures for security monitoring.

The virtualization administrator should regularly monitor the environment for changes and periodically review the environment for security vulnerabilities. A poor monitoring program could allow security incidents to occur without the administrator's knowl-

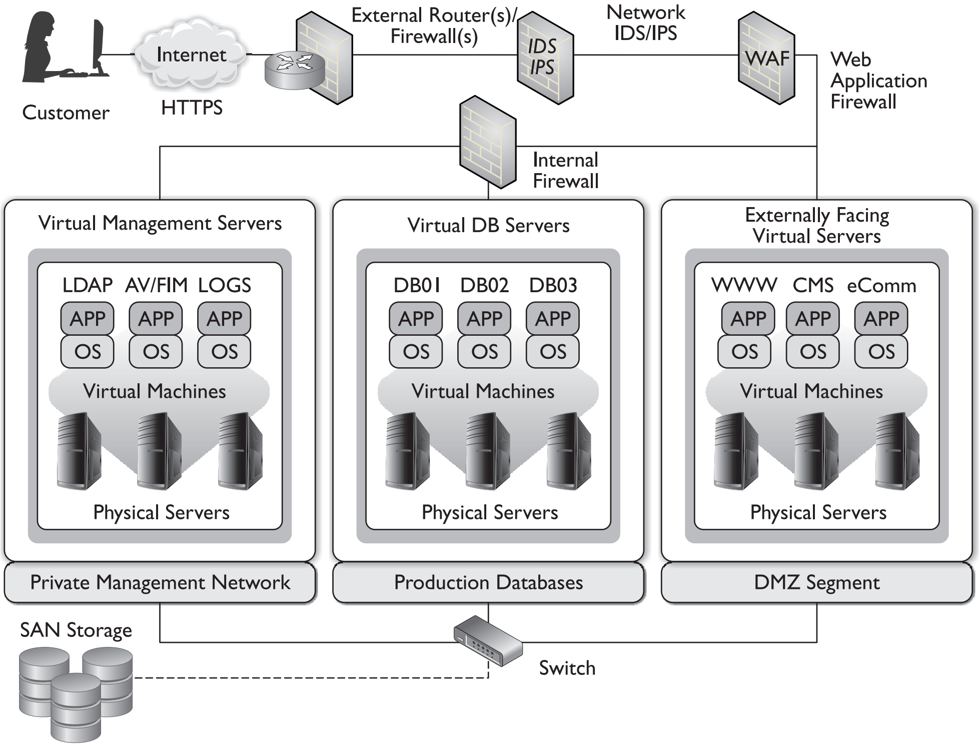


Figure 11-4 Segmenting virtual machines with firewalls

edge. *Monitoring* in this case means actively watching for issues (detection) and actively searching them out (identifying and mitigating vulnerabilities).

How

Interview the system administrator and review relevant documentation to gain an understanding of log monitoring practices. Several methods of log monitoring may be performed. The level of monitoring should be consistent with the criticality of the system and the inherent risk of the environment (for example, a virtualization environment supporting critical financial data should have robust security monitoring). The system administrator is responsible for monitoring the environment to identify activity and trends that might allow the prevention of critical issues. Several robust and excellent tools are available for monitoring virtual environments.

If security event monitoring is performed using an Intrusion Prevention System (IPS) or similar system to identify malicious events, assess the frequency of the monitoring and the quality with which it is performed. Look for evidence that the security monitoring tools are actively used. It may be possible to review recent events and determine whether the events were investigated. Leverage the results of the rest of the audit in performing this assessment. For example, if you found significant issues in an area the administrator was supposedly monitoring, you might question the effectiveness of that monitoring.

PART II

15. Evaluate the use of baseline templates and the security of hosted virtual machines as appropriate to the scope of the audit.

Baseline templates allow you to provision configured virtual machines quickly. One of the best ways to propagate security throughout an environment is to ensure that new systems are built correctly before moving into testing or production. In addition, if the scope of the audit includes evaluating hosted virtual machines, refer to Chapters 6 and 7.

How

Through interviews with the system administrator, determine the methodology used for building and deploying new systems. If a standard build is used, consider auditing a newly created system using the steps in Chapters 6 and 7. It's a good practice to include your baseline configurations as part of your normal audit routines.

16. Perform the steps from Chapter 4, "Auditing Data Centers and Disaster Recovery," and Chapter 10, "Auditing Storage," as they pertain to the environment you are auditing.

In addition to auditing the logical controls of the system, you must ensure that appropriate environmental controls are in place to provide for system protection and availability. Also consider a deep review of the storage environment to ensure that data is protected and that capacity and performance are managed.

How

Reference the steps from Chapter 4, and perform those that are relevant to the system being audited. For example, the following topics are likely to be pertinent:

- Asset inventory
- Physical security

- Environmental controls
- Capacity planning
- Change management
- System monitoring
- Backup processes
- Disaster recovery planning

Reference the steps from Chapter 10 and perform those that are relevant to the system being audited. For example, the following topics are likely to be pertinent:

- Capacity management
- Performance management
- Data protection

Knowledge Base

Following are additional resources that can offer information about virtual environments and related controls. Vendors include a tremendous amount of information on their websites for general consumption. In addition, the community of helpful enthusiasts, open source projects, and forums continues to grow daily.

Hypervisors

Hypervisor	Website
VMware	www.vmware.com
Microsoft Hyper-V	www.microsoft.com/virtualization
Open Source (XenServer) (Citrix is a major contributor)	www.xen.org www.citrix.com/xenserver/overview
Open Source by Oracle (OracleVM)	www.oracle.com/technologies/virtualization
Open Source by Sun Microsystems (VirtualBox) (Owned by Oracle)	www.virtualbox.org
Open Source Linux (KVM)	www.linux-kvm.org

Tools

Tool	Website
VMware's Open Source Tools	http://open-vm-tools.sourceforge.net/faq.php
VMware Security Utilities	www.vmware.com/technical-resources/security/utilities.html
CIS Benchmarks	www.cisecurity.org/tools2/vm/CIS_VM_Benchmark_v1.0.pdf
DISA ESX STIG Guidelines	http://iase.disa.mil/stigs/stig/esx_server_stig_v1r1_final.pdf
VMware Security Advisories	www.vmware.com/security/advisories/

Tool	Website
VMware Security Guidelines	www.vmware.com/resources/techresources/726 www.vminformer.com/ www.vkernel.com/download/free-vm-tools
RSA enVision	www.rsa.com

Master Checklists

The following checklist summarizes the steps for auditing virtualization.

Checklist for Auditing Virtualization	
❑	1. Document the overall virtualization management architecture, including the hardware supporting network infrastructure.
❑	2. Obtain the software version of the hypervisor and compare with policy requirements.
❑	3.Verify that policies and procedures are in place to identify when patches are available and to evaluate and apply applicable patches. Ensure that all approved patches are installed per your policy requirements.
❑	4. Determine what services and features are enabled on the system and validate their necessity with the system administrator.
❑	5. Review and evaluate procedures for creating administrative accounts and ensuring that accounts are created only when a legitimate business need has been identified. Also review and evaluate processes for ensuring that accounts are removed or disabled in a timely fashion in the event of termination or job change.
❑	6.Verify the appropriate management of provisioning and deprovisioning new virtual machines, including appropriate operating system and application licenses.
❑	7. Evaluate how hardware capacity is managed for the virtualized environment to support existing and future business requirements.
❑	8. Evaluate how performance is managed and monitored for the virtualization environment to support existing and anticipated business requirements.
❑	9. Evaluate the policies, processes, and controls for data backup frequency, handling, and offsite management.
❑	10. Review and evaluate the security of your remote hypervisor management.
❑	11. Review and evaluate the security around the storage of the virtual machines.
❑	12.Verify that network encryption of data-in-motion is implemented where appropriate.
❑	13. Evaluate the low-level and technical controls in place to segregate or firewall highly sensitive data on critical virtual machines from the rest of the virtualization environment.
❑	14. Review and evaluate system administrator procedures for security monitoring.
❑	15. Evaluate the use of secure baseline templates and the security of hosted virtual machines as appropriate to the scope of the audit.
❑	16. Perform the steps from Chapter 4, "Auditing Data Centers and Disaster Recovery," and Chapter 10, "Auditing Storage," as they pertain to the environment you are auditing.