ADC9521: Surviving Regulatory Compliance in the Virtual Infrastructure

Patrick Daigle, VCP, VMware
Operations Team Lead,
CGI/ITM

John Y. Arrasjid, VCP, Sr.
Consulting Architect, VMware

VMWORLD 2006

Agenda

- Compliance Rules For Sarbanes-Oxley
- Implications for VMware Implementations
- Case Study
- Control Weaknesses
- Overcoming Security Issues: Security Pods
- Overcoming Audit Issues
- Compliance Checklists
- Questions and Answers

How Does Compliance Impact You?

- *Define baseline security requirements in alignment with industry standards*
- *Develop ITIL-compliant processes to implement security standards*
- *Ensure systems are compliant (hardening)*
- *Develop ITIL-compliant processes to document and approve exceptions*
- *Verify systems for compliance (internal and external audit)*
- *Provide evidence for all of the above*

Compliance Rules for Sarbanes-Oxley Compliance

Required activities for Sarbanes-Oxley & CICA5970 evidence

- Clean up server access lists
  - Simplified by VirtualCenter with central corporate accounts in a Microsoft Active Directory infrastructure
- Strengthen formal access control management processes
- Standardize server configuration
  - Server hardening and automated deployment through scripted installs for ESX Server and templates for virtual machines
- Demonstrate continued process compliance
- Maintain documentation of processes and changes

Implications for VMware Implementations

- VMware Dynamic Resource Scheduling (VMware DRS), VMotion, and VMware High Availability (VMware HA) must be factored into compliance processes
- Risk should be mitigated by including a task for the implementer to update documentation in your Change Management Request template
  - Key items related to Virtual Infrastructure include target host and current resource assignment.
- For VMware DRS and VMotion, deviations should be addressed by pre-approval for specific VMs to be migrated between pre-defined ESX Server hosts
- For HA, change control approval and documentation is required to satisfy compliance
  - Pre-approval may be possible

Case Study Overview

- Customer Industry
  - Provider of end-to-end IT and business process services
- Concerns
  - Prepare for audit for internal financial data
  - Prepare and assist clients for their audit needs
  - Maintenance window approval for ESX Server patching
- Architecture
  - Enterprise-secured and isolated management VLAN as host to VirtualCenter communications
  - Dedicated non-routed VLAN for VMotion
- Results
  - ESX Server recognized as a quick win in the overall hardening process because the virtualization layer means no impact on services provided
  - Achieved compliance by deadline on September 30

Control Weaknesses

Problem: Improper account provisioning with segregation of duties

Solution: Use VirtualCenter to lock down access to Virtual Infrastructure Hosts (ESX Server/GSX Server/VMware Server) and virtual machines

Case Study Examples:

- Each user required to have a unique account with appropriate restrictions
- Ensure that only one super-user (root) account exists on each host
- Use VirtualCenter for all access controls of hosts and virtual machines
- VM Remote Console access reserved for specific console use only
- Use of RDP (Remote Desktop Protocol) or SSH to prevent sharing of restricted information

Control Weaknesses

Problem: Insufficient controls for change management

Solution: Integrate VirtualCenter with existing processes

- Identify levels of change
- Clone pre-change environment
- Take snapshots of each step of the change
- Notify change management upon use of VMotion
- Require signoff for any change affecting network and disk access or addition/changes to user accounts

Case Study Examples:

- Software updates must be installed from a pre-approved source
- Documentation of all changes must be recorded
- Acceptance testing must be completed and recorded

Control Weaknesses

Problem: Lack of understanding of correct system configurations

Solution: VMware Certified Professional (VCP) certification to ensure understanding of configuration settings and implications of incorrect settings

- Begin with Consulting Services to identity correct system configurations
- Validate system configurations in a health check 3-6 months following implementations
- Leverage a Technical Account Manager for ongoing assistance

Case Study Example:

All support staff VCP certified to ensure operational readiness.

Control Weaknesses

Problem: Audit logs not reviewed and no tracking of audit reviews

Solution: Ensure that your team reviews all logs on a regular basis including VirtualCenter and service console logs

- Aggregate log files from many servers in a shared mapped drive
- Require new logon access to the logs (separate from the server)

Case Study Examples:

- Schedule reviews of logs
- Monitor VirtualCenter logs
- Tie SNMP traps to other monitoring systems
- Follow log retention guidelines based on your compliance requirements and your corporate legal guidelines

Control Weaknesses

Problem: Abnormal transactions not identified in a timely manner and/or violation of security policies within the network

Solution: Identify changes in VirtualCenter access controls using combination of VirtualCenter and Domain controls

- With internal 802.1q trunking, place a virtual sniffer on the ESX Server
- Add internal firewall software
- Add IDS/IPS systems to ensure security policies are followed

Case Study Example:

•Automated analysis and notification of changes to access controls.

Control Weaknesses Summary

Ensure that the following weaknesses do **NOT** exist at your site

- ✓ Improper account provisioning without segregation of duties
- ✓ Insufficient controls for change management
- ✓ Lack of understanding/training around key system configurations
- ✓ Audit logs not reviewed nor audit reviews tracked
- ✓ Abnormal transactions not identified in a timely manner and/or violation of security policies within the network

Overcoming Security Issues: General

- Standardize based on industry best practices for OS security
  - Center for internet security (CIS) benchmark for Windows and Linux
  - Vendor recommendations (VMware, Microsoft)
- Adjust operational standards
- Deviations must be identified and justified
  (DRS and HA are two examples as they introduce changes that require change approval)
- Use VLAN and trunking protocols internal to the VMware/Virtual servers/switches and to external applications

Overcoming Security Issues: Security Pods

Definition: Security pods are logical groupings of virtual machines (VM) that require a similar level of regulatory compliance controls

- Consolidate all related VM files into one directory and use roles and privileges to control access using VI3
- Segregate networks with Virtual Switch configurations
- Segregate storage volumes into security zones
- Implement access level controls through VirtualCenter *Virtual Machine Groups* and specific admin groups
- Enforce process by creating VirtualCenter groupings that reflect actual operational and regulatory compliance implementations
- Enforce established security relationships within and across security pods

Overcoming Security Issues: Patch Policy

- The urgency to apply security patches should be determined based on vulnerability level
- Recommend and implement a systematic, quarterly application of (N – 1) level updates from VMWare
- Patch testing is crucial!
  - Virtual Infrastructure provides a flexible framework for testing

Case Study Example:

•The latest approved patches must be installed from a known source.

Overcoming Audit Issues

- It is essential to have a documented change management process and show evidence that the process was enforced to provide auditors with:
  - Proof that due process was followed
  - An example of how the process is implemented in every day affairs
- Never volunteer any information
- Vague questions should be narrowed down to questions you can answer with yes or no; help the auditor make his question more precise

Overcoming Audit Issues

Required activities for Sarbanes-Oxley and CICA5970 evidence

- Clean up server access list (simplified by VirtualCenter with central corporate Active Directory Accounts)
- Strengthen formal access control management processes
- Standardize server configuration (server hardening and automated deployment through scripted installs for ESX Server and templates for virtual machines)
- Demonstrate process compliance
- Document maintenance

Compliance Checklists

- **Divided into four major categories**
  - Account management
  - File and directory security
  - System configuration
  - Logging

Checklists: Account Management

- Use VirtualCenter to control access to Virtual Infrastructure Hosts (ESX Server, GSX Server, and VMware Server) and virtual machines
  - VirtualCenter can manage through users access roles and privileges
    - An access role defines what privileges an associated user will have
    - A privilege defines an allowable action
  - VirtualCenter provides centralized user and administrator account management
  - Move account management to an enterprise Microsoft Active Directory (MSAD) environment
    - Simplifies enforcement of stronger password policies by using the same global account policies established within MSAD
    - This includes password aging, password length and composition

Checklists: Account Management (continued)

- Security access levels can also be maintained through the use of the same controls implemented within Active Directory
- Do not use shared accounts for changes to the environment
  - This can prevent identifying change control points

- **Change Management approval requirements**
  - Changes to access permissions

Case Study Examples:

- Enforce password lifetime of minimum 2 days maximum 45 days
- Enforce account lockout after 5 unsuccessful attempts

Checklists: File and Directory Security

- Limit access to the VirtualCenter server only through the Virtual Infrastructure client (no Remote Desktop Protocol)
- Use access policies for users and groups tied to Active Directory and based on your compliance guidelines for file/directory access
- Use security pods for the virtual disks. i.e: grouping VMs tied to a security zone onto a set of VMFS volumes defined for their use
- Minimize use of remote console sessions as concurrent users share identical views of data

Checklists: File and Directory Security

- Security pods are handled differently in VI2 vs. VI3
  - VI3: All files (configuration, virtual disk, nvram, snapshots, and logs) are kept within one directory simplifying controls
  - VI2: Multiple locations for files can result in higher management overhead to meet regulatory compliance

- **Change Management approval requirements:**
  - Changes to disks including disk modes, permissions, and locations

Case Study Example:

• Access to system log files (read or write) should be restricted to administrator account.

Checklists: System Configuration

- **Installation**
  - Use scripted installs to enforce a standard (documented) build as well as an approved source for installation
  - Installation should include (as part of the standard build or as a post-install step) application of the latest corporate-approved patch level

Case Study Example:
•Use scripted Kickstart installations for consistency.

Checklists: System Configuration

- **Services**
  - Remote access to the VMware Service Console is locked down by default in version 3.x
    - SSH restricted to non-root users
  - ESX Server 3.x includes a built-in firewall to assist in lockdown of the environment
    - No outbound SSH access from the service console
    - Many services are disabled (SNMP, NTP, etc.)

Case Study Examples:
•Disable telnet, nfs, ftp, remote root login (all disabled by default in VI3)
•Create legal banner for remote access

Checklists: System Configuration

- **Change Management approval requirements:**
  - Changes to virtual machine configurations
  - Changes to virtualization platform or virtual infrastructure

Checklists: Logging

- Ensure proper auditing
  - VirtualCenter provides a centralized event log for Virtual Machine events as well as some Virtual Infrastructure Host events
  - A centralized syslog service can be used to automate parsing and reviewing of logs with tools like Swatch

Links

- VMWare updates download pages
  - www.vmware.com/download/esx/
  - www.vmware.com/download/vi/
- Center for Internet Security
  - www.cisecurity.org
- Swatch
  - swatch.sourceforge.net
- NT Syslog
  - ntsyslog.sourceforge.net

References

- VMworld '05 Presentations
  - SLN138: Security Management in a VMware Virtual Infrastructure Environment
  - SLN241: Virtualization Streamlines Regulatory Compliance
- VMware PSO Virtual Infrastructure Security (VIS) engagement material
- Related VMworld '06 Presentations
  - ADC9938: An Aggressive Approach Using P2V to Address Disaster Recovery and Business Continuity Planning
  - MED0119: Ensuring Sarbanes Oxley Compliance with WYSE and VDI
  - MED9960: Provisioning Hosted Desktops for Centralized Access, Management, Improved Security, Compliance, and Disaster Recovery
  - LAB3805: Securing and Monitoring VMware Infrastructure 3
  - MDC9523: How Virtualization Changes the Security Equation
  - TACO162: How to Secure VMware ESX Server Virtual Machines

Presentation Download

Please remember to complete your
session evaluation form
and return it to the room monitors
as you exit the session

The presentation for this session can be downloaded at
http://www.vmware.com/vmtn/vmworld/sessions/

Enter the following to download (case-sensitive):

Username: cbv_rep
Password: cbvfor9v9r

Some or all of the features in this document may be representative of feature areas under development. Feature commitments must not be included in contracts, purchase orders, or sales agreements of any kind. Technical feasibility and market demand will affect final delivery.

VMWORLD 2006