



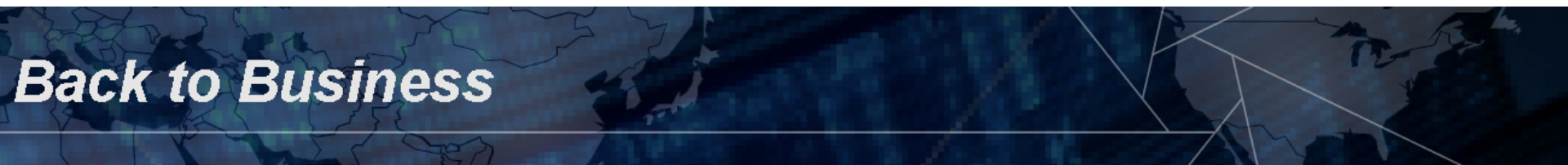
S24 – Virtualization Security from the Auditor Perspective

Rob Clyde, CEO, Adaptive Computing; former CTO, Symantec

David Lu, Senior Product Manager, Trend Micro

Hemma Prafullchandra, CTO/SVP Products, HyTrust

November 7-9, 2011



Back to Business

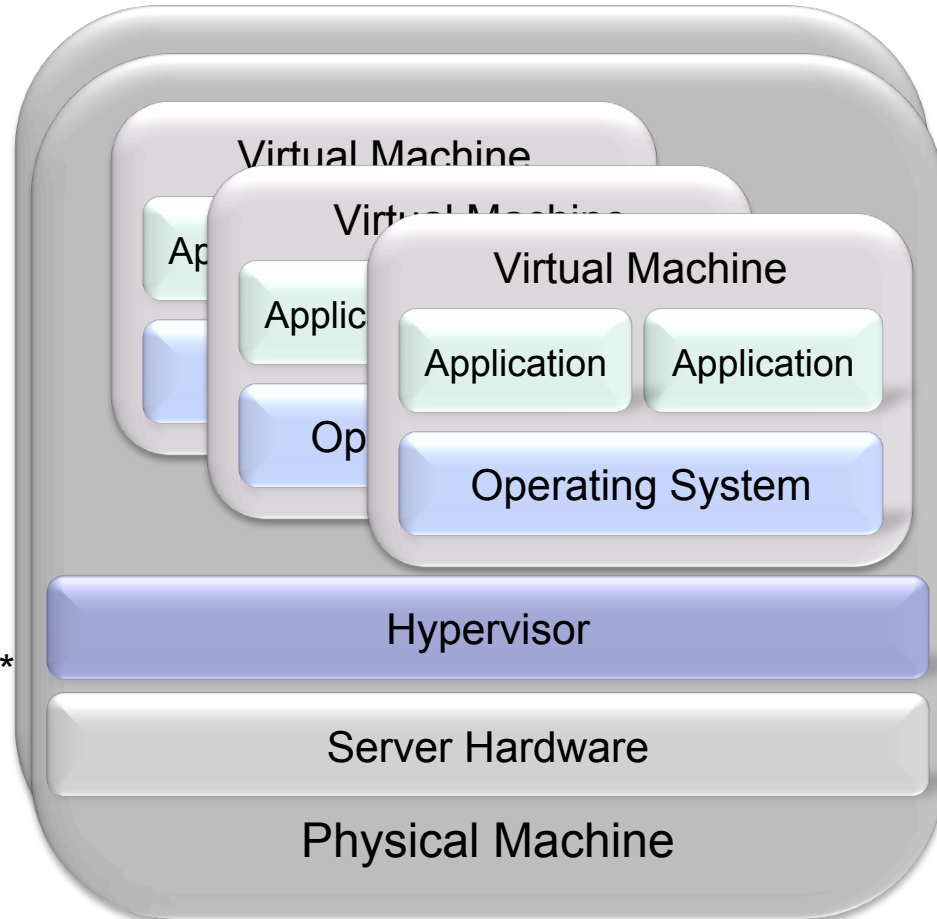
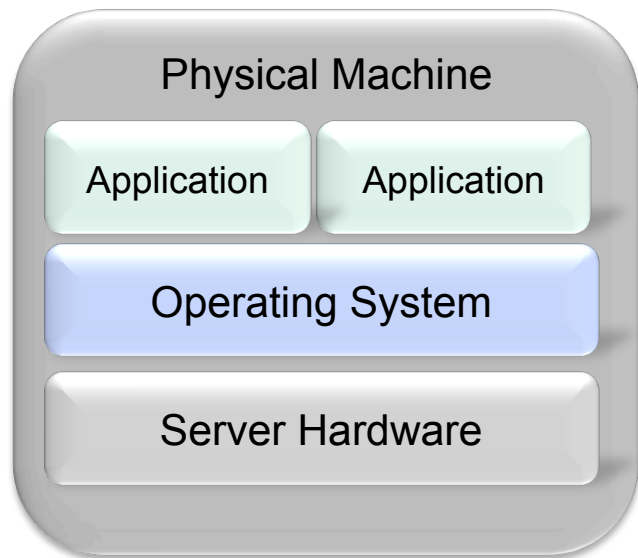
Agenda

- Virtualization Overview & Security Challenges
- Industry Best Practices
 - ISACA/COBIT Virtualization Security Checklist
 - Center for Internet Security (hardening best practices)
 - Payment Card Industry (Data Security Standard & Virtualization Information Supplement)
 - NIST Virtualization Guidance
- End-to-End Security and Compliance Guidance
- Q & A
- Resources

Agenda

- Virtualization Overview & Security Challenges

What is Virtualization?

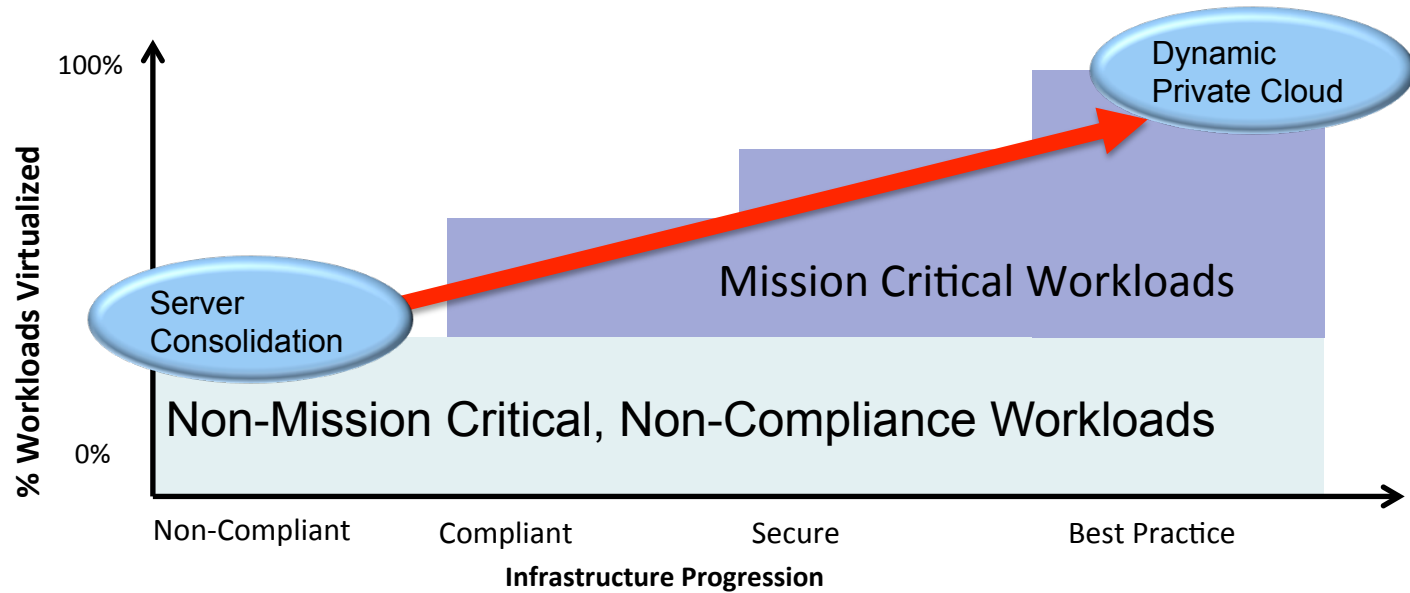


Virtualization is highly compelling:

- 60% reduction in capital expenditure per app*
- Half as many human resources require per app*
- 80% reduction in Datacenter outage costs*
- Key to implementation of cloud computing

* VMware Analysis 2010

Virtualization Progression



Despite high ROI, barriers to adoption remain

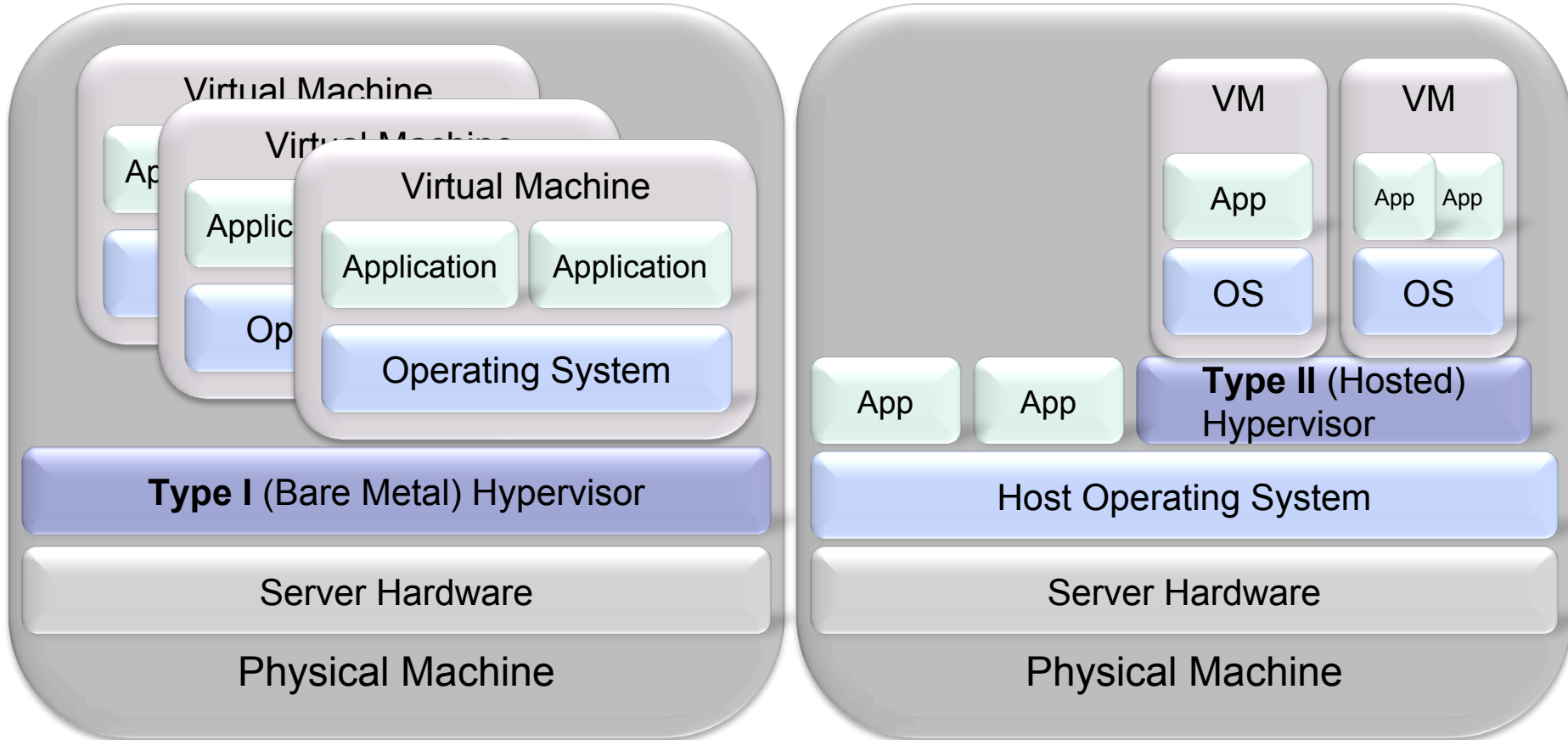
- 46% cite security as primary reason that adoption can be slowed*
- 35% worry about insider threats‡
- 28% “very” or “extremely” concerned with security in virtual environment‡‡

* Jeff Burt, eWeek Article, Sept. 2009

‡ Prism Microsystems Survey of 300 orgs, 2010

‡‡ Info Pro 2010 Security Study

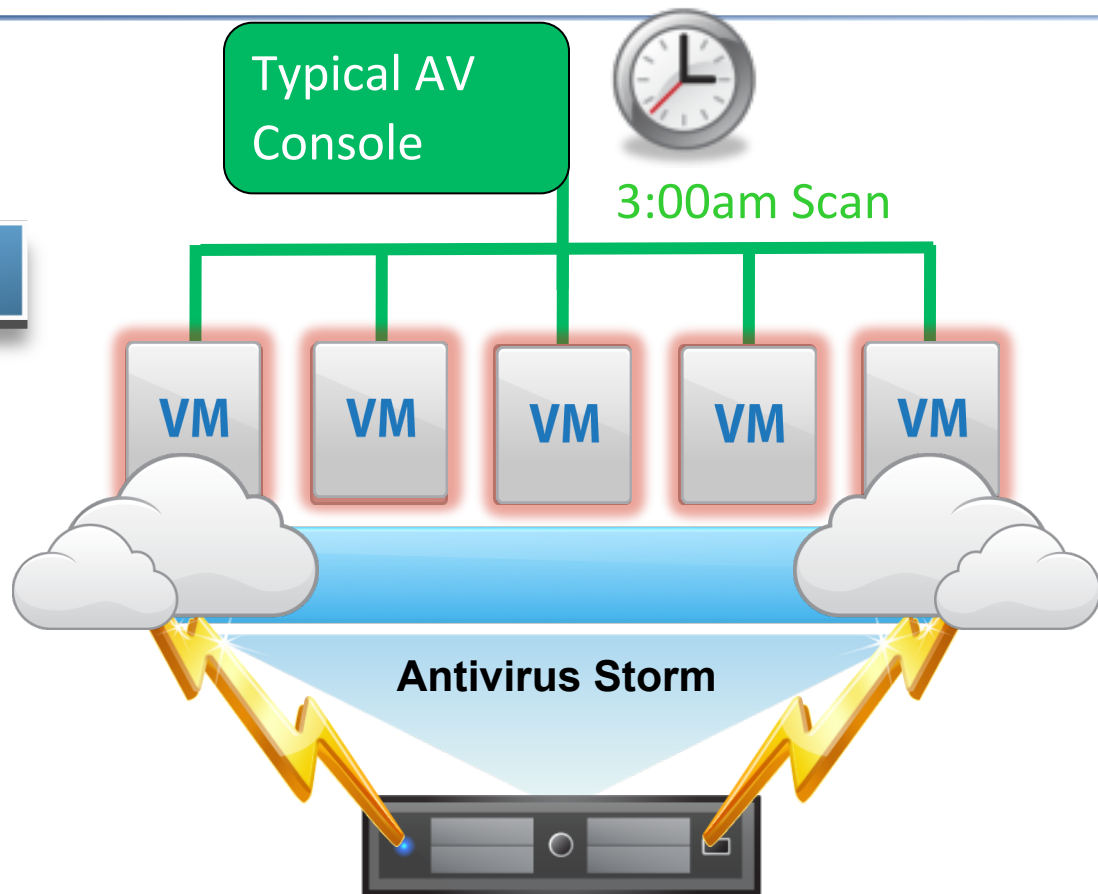
Challenge: Not All Hypervisors are Equal



Security Challenge: Resource Contention

1

Resource Contention

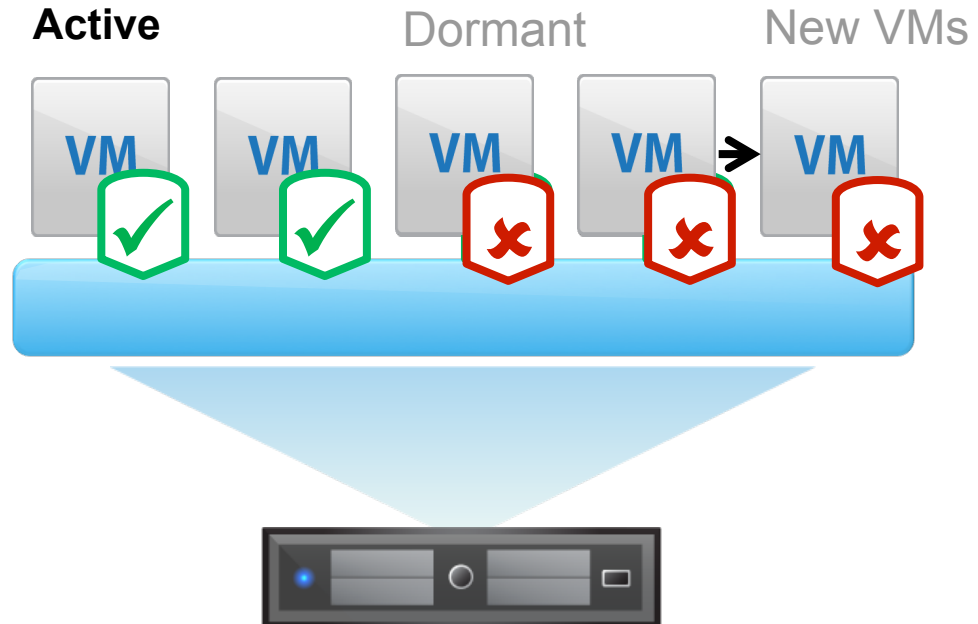


**Antivirus scans & updates
overburden the Hypervisor & SAN**

Security Challenge: Instant-on Gaps

1 Resource Contention

2 Instant-on Gaps



Dormant VMs will be missing critical patches and contain out-of-date security controls and are subject to exploitation and compromise

Security Challenge: Inter-VM Attacks

1

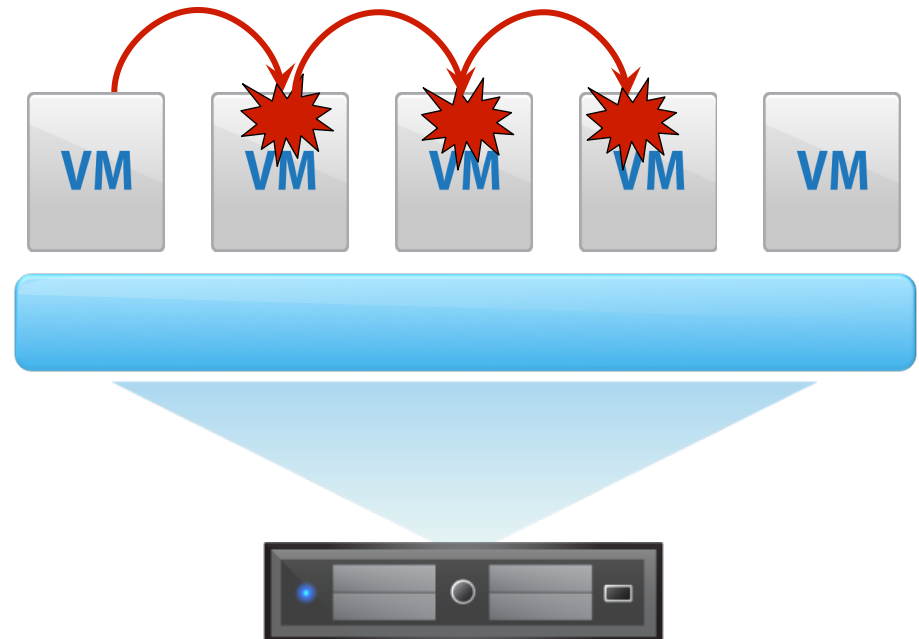
Resource Contention

2

Instant-on Gaps

3

Inter-VM Attacks / Blind Spots



Attacks can spread across VMs

Security Challenge: Management

1 Resource Contention

2 Instant-on Gaps

3 Inter-VM Attacks / Blind Spots

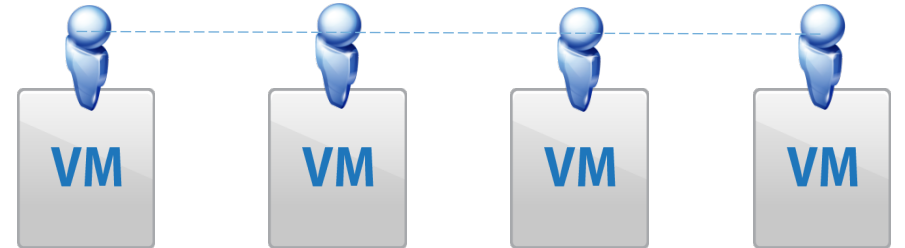
4 Complexity of Management

Provisioning
new VMs

VM
Migration

Patching
Complexity

Private
Cloud



VM sprawl inhibits compliance

Agenda

- Industry Best Practices
 - ISACA/COBIT Virtualization Security Checklist
 - Center for Internet Security (hardening best practices)
 - Payment Card Industry (Data Security Standard & Virtualization Information Supplement)
 - NIST Virtualization Guidance

ISACA Checklist Mapping To	COBIT Control Objective(s)
1. Securing the virtualization platform	
a. Platform and installation requirements	
1.a.1 Limit physical access to the host: only authorized administrative personnel should have physical access to the host system to prevent unauthorized changes.	PO4.9, DS12.3
1.a.2 Verify integrity of files prior to installation: verify the hash values of system files, as provided by the vendor, prior to installation to ensure integrity.	PO2.4, AI3.2
1.a.3 Load and enable only required operating system components and services: no unnecessary operating systems components (e.g., drivers) should be loaded, and no unnecessary services should be enabled (e.g., printing services, file sharing services).	AI3.2
1.a.4 BIOS, bootloader passwords: passwords should be used for BIOS and bootloaders (e.g., GRUB) for both hosts and guests.	DS5.3

Source: ISACA Virtualization-Security-Checklist-26Oct2010-Research.pdf

Center for Internet Security (CIS)

- Working on VMware vSphere 4.1 benchmark, schedule dependent on volunteers
- vSphere 5 already released, no hardening guide from vendor or CIS or NSA or DISA stigs...
- Use vendor supplied benchmark: more current and vendor aligned with CIS and government requirements

Automate Configuration Compliance Reporting

Compliance History

Summary

Hosts

Details

Templates

☐ View All
 Showing 1 to 8 of 8
 << < 1 > >>

Date/Time	Template	Host	Compliance
05/18/2011 1:38:19 PM	PCI-ESXi	esxi4a.toyshack.com	89%
05/18/2011 1:38:16 PM	PCI-ESXi	esxi3a.toyshack.com	89%
05/18/2011 1:38:10 PM	PCI-ESXi	esxi1a.toyshack.com	89%
05/18/2011 1:38:09 PM	PCI-ESXi	esxi2a.toyshack.com	89%
05/16/2011 10:15:06 AM	PCI-ESXi	esxi4a.toyshack.com	22%
05/16/2011 10:15:05 AM	PCI-ESXi	esxi3a.toyshack.com	22%
05/16/2011 10:15:05 AM	PCI-ESXi	esxi2a.toyshack.com	22%

Compliance Test Results

Export as CSV

Showing 1 to 9 of 9

<< < 1 > >>

Name	Description	Date/Time	Result
vm_snapshot		05/18/2011 1:37:43 PM	Passed
PCI 2.2		05/18/2011 1:37:50 PM	Passed
PCI 2.2		05/18/2011 1:37:54 PM	Passed
PCI 7.1		05/18/2011 1:38:02 PM	Passed
PCI 7.2		05/18/2011 1:38:07 PM	Passed
PCI 7.2		05/18/2011 1:38:10 PM	Passed
PCI 10.2	Syslog.Remote.Host =	05/18/2011 1:38:12 PM	Failed
PCI 10.4		05/18/2011 1:38:15 PM	Passed
PCI 10.7		05/18/2011 1:38:19 PM	Passed

Automate Comprehensive Compliance Reporting

Summary Report
superadmin
Log Out

General Compliance Policy Configuration Maintenance Help

General > HTA Report Configuration > Summary Report

Summary Report

PDF CSV

PCI DSS Version 2 Summary Report

Report Generated: October 17, 2011 10:41:25 AM

Date Range: From: October 17, 2011 To: October 17, 2011
Scope: Infrastructure Label: All VM Label: All
Templates: ESX: PCI ESXi: PCI-ESXi

Overview

vSphere and HyTrust Operations	Authorized: 3; Denied: 2	Number of Authorized and Denied operations for vSphere and HyTrust Appliance (HTA)
Number of Virtual Machines with Label	44	Number of VMs with the selected label
Trend Micro Status (Overall)	Trend Micro is Enabled	Trend Micro Deep Security Server Configuration
Number of Resources with Label	204	Number of vSphere resources with the selected label
Number of Hosts that Failed Configuration Checks	3	Number of hosts with configuration checks that failed

Summary

	Violations (V)	Potential Violations (P)	Satisfied Controls (S)	Monitored Controls (M)	
	380	133	46		
Requirement 1	82	46	6	25072	Install and maintain a firewall configuration to protect cardholder data
Requirement 2	54	0	26	76	Do not use vendor-supplied defaults for system passwords and other security parameters
Requirement 3	67	19	0	314	Protect stored cardholder data
Requirement 5	60	0	7	0	Use and regularly update antivirus software or programs
Requirement 6	1	19	0	1	Develop and maintain secure systems and applications
Requirement 7	0	22	3	2	Restrict access to cardholder data by business "need to know"
Requirement 8	13	22	1	1	Assign a unique ID to each person with computer access
Requirement 9	12	0	0	0	Restrict physical access to cardholder data
Requirement 10	91	5	3	50	Track and monitor all access to network resources and cardholder data
Requirement 1: Firewalls Violations: 82; Potential Violations: 46; Satisfied Controls: 6; Monitored Controls: 25072					
Firewall Active Count	Not Activated (V): 41; N/A or On with No Rules (P): 23; On, with Rules (S): 3				Firewall Status
Firewall rules Assigned	Firewall Rules (M): 71				Number of Assigned Firewall Rules
Firewall Events	Firewall Events (M): 22326				Number of Firewall Events
Deep Packet Inspection Status	Not Activated (V): 41; N/A or Prevent with No Rules (P): 23; Prevent, with Rules (S): 3				Deep Packet Inspection Status
Deep Packet Inspection Rules	DPI Rules (M): 2642				Number of Assigned Deep Packet Inspection Rules
Deep Packet Inspection Events	DPI Events (M): 0				Number of Deep Packet Inspection Events
Firewall Activated Hosts	Hosts with Active Firewalls (M): 0				Number of ESX hosts with firewalls configured to policy
Detected Virtual Firewalls	Virtual Firewalls Detected (M): 0				Virtual Machines that are labeled as firewalls

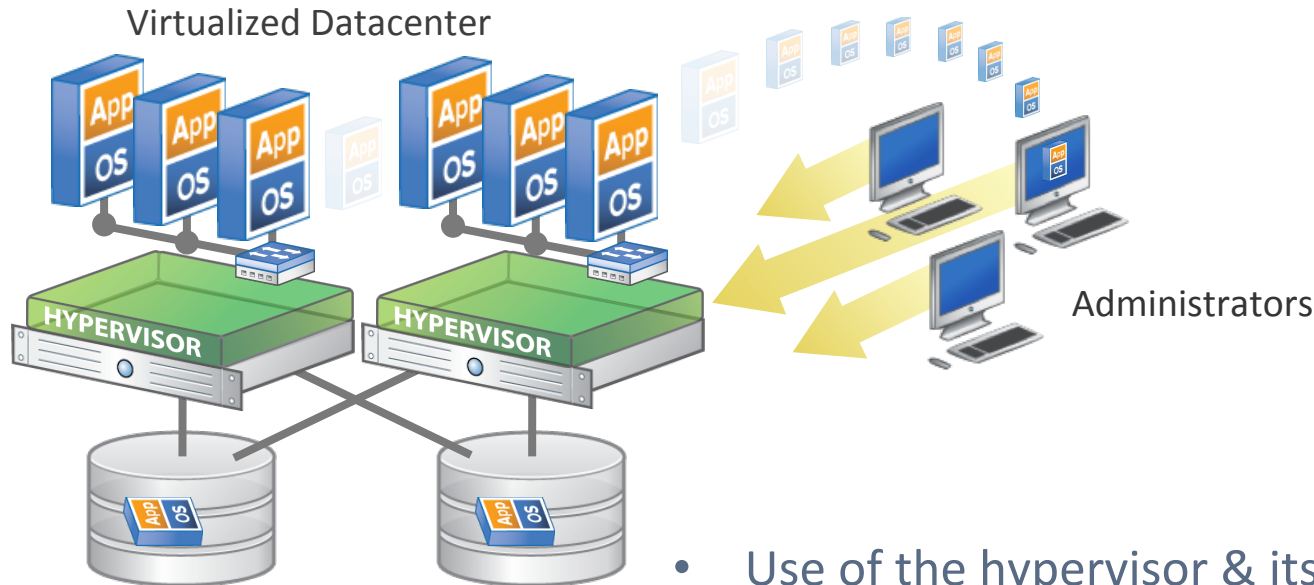
PCI Data Security Standard

- PCI Data Security Standard for protecting Cardholder Data
- Changes in PCI Data Security Standard version 2.0
 - Released October 2010; all assessments from Jan. 1, 2012 must be against 2.0
 - Explicitly states that System components include any virtualization components
 - Detailed virtualization guidance released as an Information Supplement in July 2011



Source: PCI DSS 2.0 Quick Reference Guide

Challenges & Concerns When Virtualizing CDE



- Scope: identify & consider 'included in or connected to'
- Segmentation of different security/trust zones and workload tiers
- Use of the hypervisor & its management systems/interfaces/ consoles
- Storage of cardholder data
- Access control & separation of duties
- Logging and alerting

CDE Virtualization Checklist

- Take a risk-based approach: identify all CDE system components and note if virtual or physical, and their primary function and owner
 - Consider the risk aggregated when running multiple in-scope virtual machines/appliances/security appliances on a single or cluster of hypervisors and implement adequate PCI DSS controls
 - Secure the hypervisor as it is most critical system component (including its management system/interfaces/consoles)
 - Manage complete life-cycle of in-scope VMs
 - Secure VM-to-VM traffic that remains within the hypervisor(s)
 - Ensure in-scope VMs or other objects are not moved to non-compliant environments
 - Leverage optimized, virtualization-aware firewall and anti-virus solutions
- Update processes to account for the greater management flexibility
 - Pay attention to roles definition, access control and logging
 - Privileged access to the hypervisor

Virtualization and Security Concerns

- Additional layers of technology
- Many systems on a physical system
- Sharing pool of resources
- Lack of visibility
- Dynamic environment
- May increase the attack surface

Recommendations for Security for Full Virtualization Technologies

- Risk-based approach
- Secure all elements of a full virtualization solution and perform continuous monitoring
- Restrict and protect administrator access to the virtualization solution
- Ensure that the hypervisor is properly secured
- Carefully plan the security for a full virtualization solution before installing, configuring, and deploying it

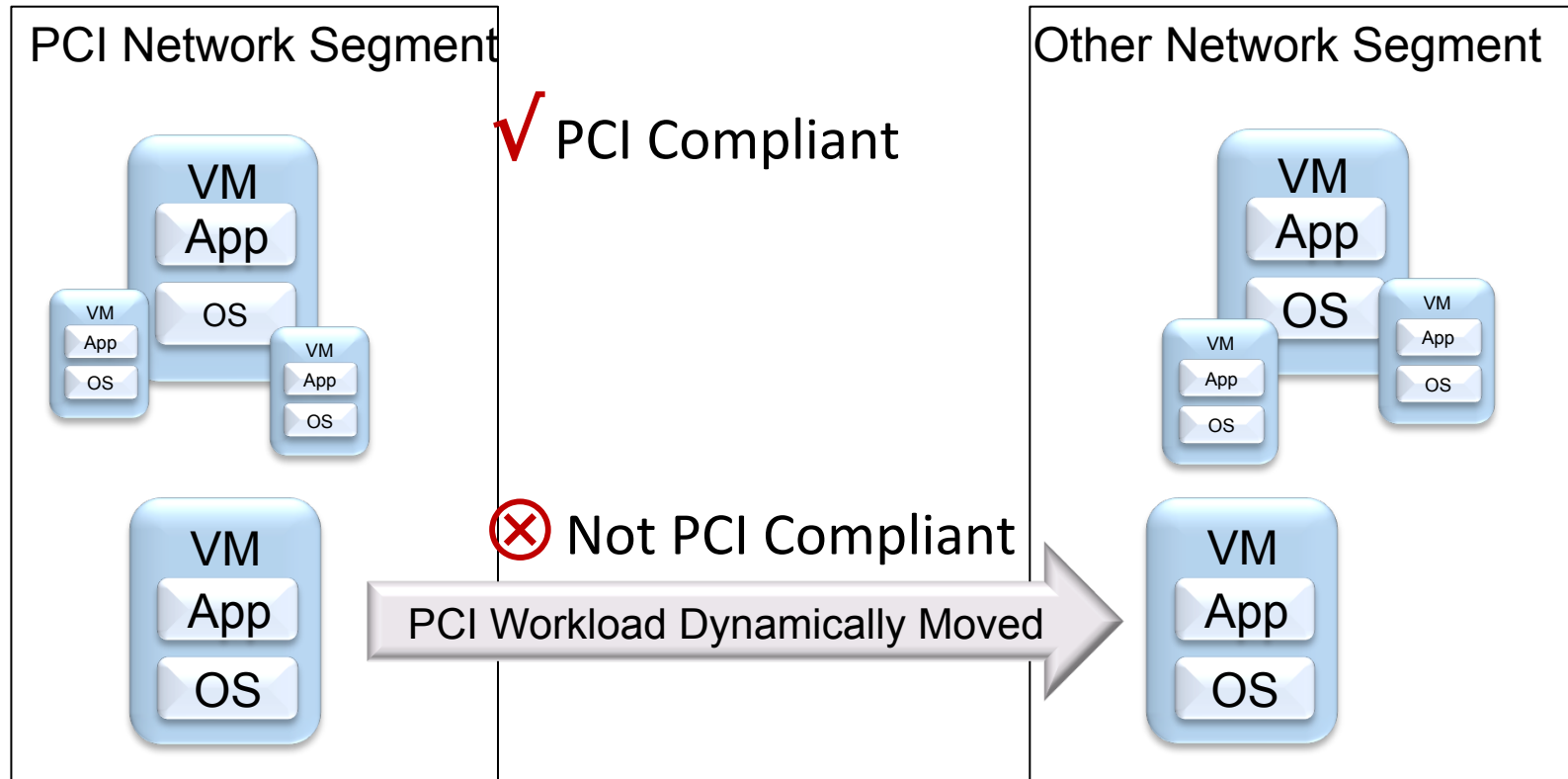
Summary of Threats and Countermeasures

- Intra-guest vulnerabilities
 - Hypervisor partitioning
- Lack of visibility in the guest OS
 - Hypervisor instrumentation and monitoring
- Hypervisor management
 - Protect management interface, patch management, secure configuration
- Virtual workload security
 - Management of the guest OS, applications, data protection, patch management, secure configuration, etc
- Virtualized infrastructure exposure
 - Manage access control to the hardware, hypervisors, network, storage, etc.

Agenda

- End-to-End Security and Compliance Guidance

Compliance Challenge: Moving Workloads



PCI = Payment Card Industry Data Security Standard

Non-Compliant VM Movement

The screenshot shows the vSphere Client interface for 'vc2.topsports.com'. The left sidebar displays a tree view of the inventory, including 'TopSports DC', 'eCommerce Cluster', and 'Development'. The 'Omniure' VM is selected, and a context menu is open, showing options like 'Power', 'Guest', 'Snapshot', 'Open Console', 'Edit Settings...', 'Migrate...', 'Clone...', 'Template', 'Fault Tolerance', 'Add Permission...', 'Alarm', 'Report Performance...', 'Rename', and 'Open in New Window...'. The 'Migrate...' option is highlighted. The main pane shows the 'General' tab for the 'Omniure' VM, displaying details such as 'Guest OS: Microsoft Windows Server 2003, Standard E..', 'VM Version: 7', and 'CPU: 1 vCPU'. The 'Resources' tab is also visible, showing 'Consumed Host CPU: 0 MHz', 'Consumed Host Memory: 27.00 MB', 'Active Guest Memory: 0.00 MB', 'Provisioned Storage: 24.36 MB', 'Not-shared Storage: 328.73 KB', and 'Used Storage: 328.73 KB'. A table below the storage information shows the 'Datastore' 'NAS' with a 'Status' of 'Normal' and a 'Capacity' of '196.86 GB'.

Datastore	Status	Capacity
NAS	Normal	196.86 GB

Network	Type	Status
eCommerce Netw...	Standard switch network	✓

VM is now moved to the wrong cluster!

vc2.topsports.com

- TopSports DC
 - eCommerce Cluster
 - esxi1b.topsports.co
 - esxi2b.topsports.co
 - Customer DB
 - Inventory DB
 - Omniture
 - Development Cluster
 - esxi3b.topspo
 - esxi4b.topsports.co
 - Active Directory
 - Nexus1KV
 - splunk

Omniture

Summary | Resource Allocation | Performance | Tasks

General

Guest OS: Microsoft Windows Server 2003, S
VM Version: 7
CPU: 1 vCPU
Memory: 16 MB
Memory Overhead: 86.46 MB
IP Address:
DNS Name:
EVC Mode:
State:
Host: esxi2b.topsports.com
Active Tasks: Migrate virtual machine

Commands

Open Console

Annotations

Notes:

Recent Tasks

Name	Target	Status
Migrate virtual machine	Omniture	78%

Require Policy-based Controls for all Change Management Activity

topsports.com

- TopSports DC
 - eCommerce Cluster
 - esxi1b.topsports.co
 - esxi2b.topsports.co
 - Customer DB
 - Inventory DB
 - Development Cluster
 - esxi3b.topspo
 - esxi4b.topsports.co
 - Active Directory
 - Nexus1KV
 - Omniture
 - splunk

Omniture

Summary | Resource Allocation | Performance | Tasks

General

Guest OS: Microsoft Windows Ser
VM Version: 7
CPU: 1 vCPU
Memory: 16 MB
Memory Overhead: 84.96 MB
VMware Tools: Not installed
IP Addresses:
DNS Name:
EVC Mode: N/A
State: Powered On
Host: esxi4b.topsports.com
Active Tasks:

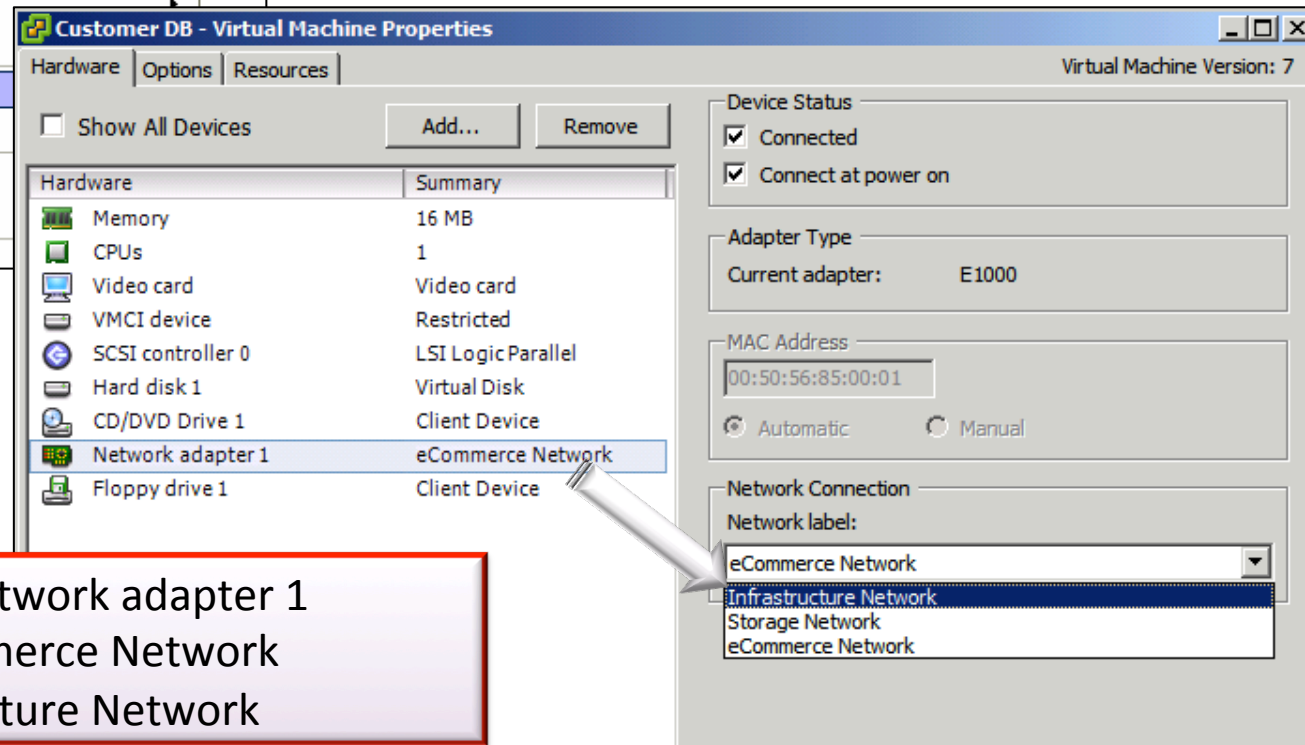
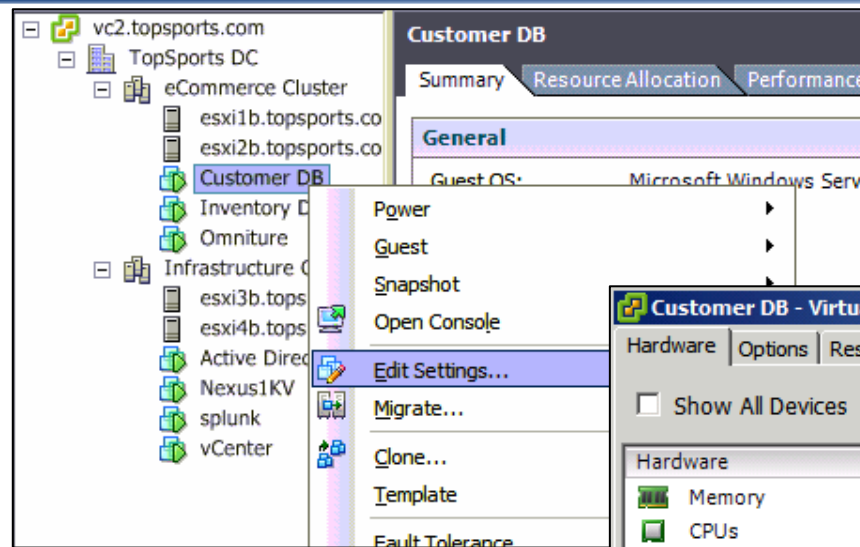
Commands

Power Off
Suspend
Reset
Edit Settings
Open Console

Name	Target	Status
Migrate virtual machine	Omniture	Completed

VM reconfiguration: network change

Require Policy-based Controls to ensure that authorized users do not accidentally/intentional break compliance



Changing Network adapter 1
From eCommerce Network
To Infrastructure Network

Compliance Challenge: Insufficient Logging

The screenshot shows the VMware vCenter console interface. On the left, a tree view displays the hierarchy: vc2.topsports.com > TopSports DC > eCommerce Cluster > Customer DB. The main pane shows the 'Customer DB' task log. The 'View' tab is set to 'Tasks'. A table lists several tasks, all of which are 'Completed'. The 'Task Details' section for the first task, 'Reconfigure virtual machine', shows it was initiated by TOPSPORTS\phil and completed successfully. The 'Related Events' section shows two events from 5/31/2011 11:00:01 AM and 11:00:03 AM, both indicating the task was completed on esxi1b.topsports.com in TopSports DC. Notably, the logs do not contain any IP addresses or specific details about the network adapter configuration.

Name	Target	Status	Details
Reconfigure virtual machine	Customer DB	Completed	
Migrate virtual machine	Customer DB	Completed	
Reconfigure virtual machine	Customer DB	Completed	
Migrate virtual machine	Customer DB	Completed	
Migrate virtual machine	Customer DB	Completed	
Migrate virtual machine	Customer DB	Completed	
Reconfigure virtual machine	Customer DB	Completed	
Power On virtual machine	Customer DB	Completed	

Task Details

Name: **Reconfigure virtual machine** Target: **Customer DB** Initiated by: **TOPSPORTS\phil**

Status: **Completed**

Related Events: [Hide](#)

- 5/31/2011 11:00:01 AM, Task: Reconfigure virtual machine
- 5/31/2011 11:00:03 AM, Reconfigured CustomerDB on esxi1b.topsports.com in TopSports DC

Missing IP address and no indication that the network adapter was reconfigured

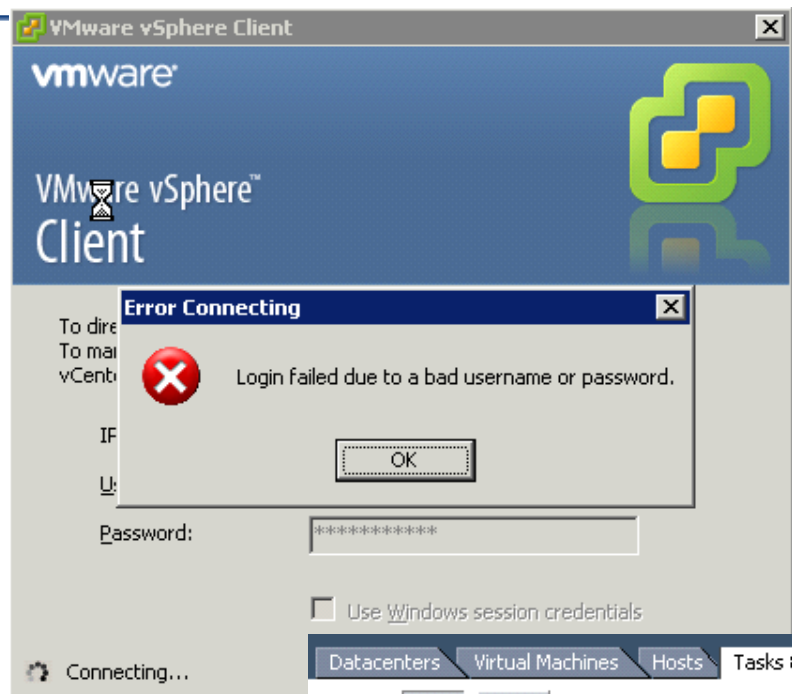
Insufficient Logging

Confusing host logs with insufficient details to identify specific action, no IP address or user

```
May 31 10:54:29 192.168.10.151 May 31 18:03:07 Hostd: [2011-05-31 18:03:07.855  
6938EB90 verbose 'DvsManager'] PersistAllDvsInfo called  
host=splunk.topsports.com | sourcetype=esxi_hosts | source=udp:514  
May 31 10:54:28 192.168.10.151 May 31 18:03:06 Vpxa: [2011-05-31 18:03:06.175  
1BFD6B90 verbose 'App'] [VpxaHalServices] HostChanged Event Fired, properties changed  
[]  
host=splunk.topsports.com | sourcetype=esxi_hosts | source=udp:514  
May 31 10:54:28 192.168.10.151 May 31 18:03:06 Vpxa: [2011-05-31 18:03:06.172  
1BFD6B90 verbose 'VpxaHalCnxHostagent'] [VpxaHalCnxHostagent:  
updates from 124750 to 124751 (at 124750)  
host=splunk.topsports.com | sourcetype=esxi_hosts | source=udp:514  
May 31 10:54:28 192.168.10.151 May 31 18:03:06 Vpxa: [2011-05-31 18:03:06.172  
1BFD6B90 verbose 'VpxaHalCnxHostagent'] Received callback in  
host=splunk.topsports.com | sourcetype=esxi_hosts | source=udp:514  
May 31 10:54:28 192.168.10.151 May 31 18:03:06 Vpxa: [2011-05-31 18:03:06.172  
1BFD6B90 verbose 'App'] [VpxaInvHost] Increment master gen.  
LicenseManager:VpxaInvHostLicenseManagerListener::LicenseCha  
host=splunk.topsports.com | sourcetype=esxi_hosts | source=udp:514  
May 31 10:54:28 192.168.10.151 May 31 18:03:06 Vpxa: [2011-05-31 18:03:06.172  
1BFD6B90 verbose 'App'] [VpxaHalServices] LicenseManagerChange Event fired  
host=splunk.topsports.com | sourcetype=esxi_hosts | source=udp:514  
May 31 10:54:28 192.168.10.151 May 31 18:03:06 Vpxa: [2011-05-31 18:03:06.172  
1BFD6B90 verbose 'VpxaHalCnxHostagent'] [VpxaHalCnxHostagent::ProcessUpdate] Applying  
updates from 124749 to 124750 (at 124749)  
host=splunk.topsports.com | sourcetype=esxi_hosts | source=udp:514
```

Require log records with sufficient details for all virtual admin actions to allow for monitoring/investigation/forensics

Compliance Challenge: Insufficient Log Records



The screenshot shows the VMware vSphere Client interface. A modal dialog box titled "Error Connecting" is displayed in the foreground. It contains a red "X" icon and the text "Login failed due to a bad username or password." with an "OK" button. Below the dialog, the login fields for "Username" and "Password" are visible, with the password masked by asterisks. The "Use Windows session credentials" checkbox is unchecked. The background interface shows the "Tasks & Events" tab selected, with a search bar and a table header.

Require Log Records of all Change Management Activity (denied/failed and allowed)

View: **Tasks** Events [Scheduled Tasks](#)

Name, Target or Status contains: Clear

Name	Target	Status	Details	Initiated by
------	--------	--------	---------	--------------

No log message is recorded.
Violates most policies and standards.

End-to-End Security & Compliance Guidance

- Virtualization increases the risk and complexity of compliance so engage your auditors early to streamline the audit process
- Look beyond traditional security vendors for solutions that address virtualization specific requirements (hypervisor/VM controls)
- View virtualization as an **opportunity to improve your current processes**
 - reporting, monitoring, inter-VM controls, etc.
 - achieve objectives that you always wanted in physical environments but could not afford or were restricted by legacy infrastructure
- Embrace virtualization with a virtualization by default approach and build compliance into the default mode of operation

Questions?

Resources

- ISACA Virtualization Checklist -
<http://www.isaca.org/Knowledge-Center/Research/Documents/Virtualization-Security-Checklist-26Oct2010-Research.pdf>
- <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Virtualization-Benefits-and-Challenges.aspx>
- PCI Security Standards Council:
<https://www.pcisecuritystandards.org/index.php>
- NIST: <http://csrc.nist.gov/publications/index.html>
- Adaptive Computing: <http://www.adaptivecomputing.com>
- HyTrust: <http://www.hytrust.com/resources/main>
- Trend Micro:
<http://us.trendmicro.com/us/solutions/enterprise/security-solutions/compliance/>