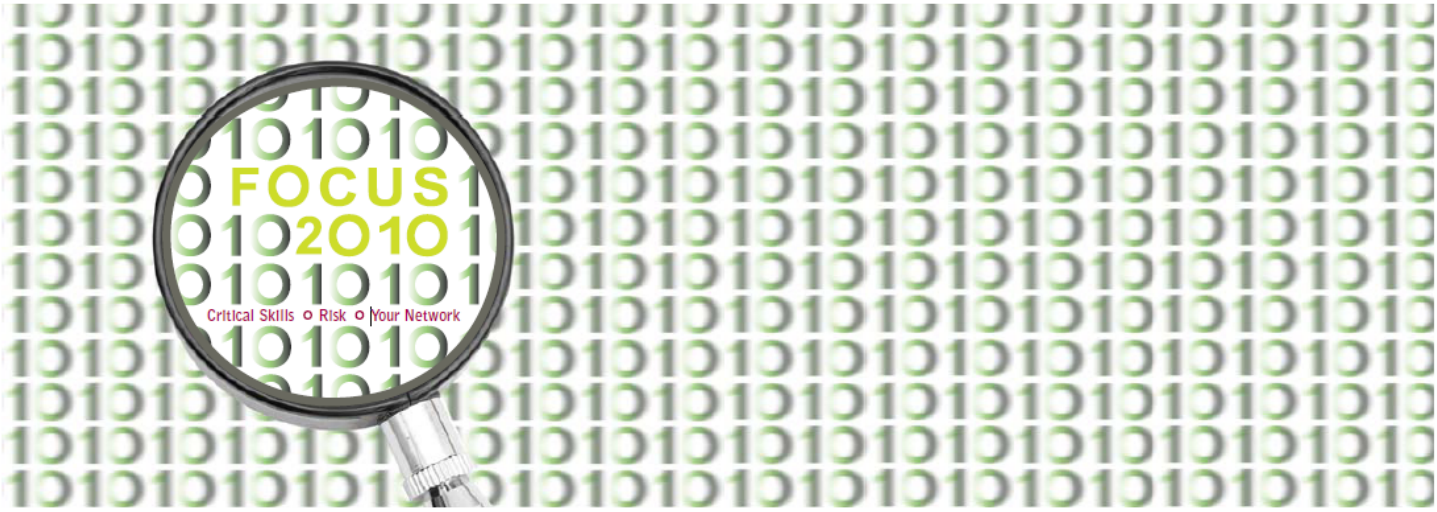
10th Annual SF ISACA Fall Conference

October 4 – 6, 2010



T12: Virtualization: IT Audit and Security Perspectives

Jason Chan, VMware

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

Virtualization: IT Audit and Security Perspectives

Jason Chan

Director of Security, VMware

Agenda

- Background and Disclaimers
- Virtualization Basics and Business Drivers
- Audit and Security Topics of Interest
- New Attack Vectors
- Architectural Options and Opportunities
- Summary

Background and Disclaimers

- I work at VMware
  - In IT (not R&D or Marketing)
- Security consulting and audit background
  - @stake, Symantec, iSEC Partners

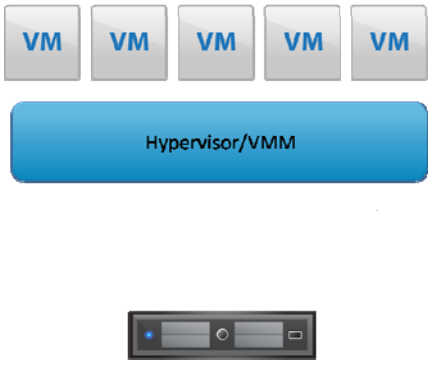
Presentation Focus

- x86 server virtualization
  - Application, desktop, storage virtualization (while interesting) are not covered
- Not VMware-specific
- Not comprehensive
- **What is interesting about server virtualization from a security and IT audit perspective?**

Virtualization Basics and Business Drivers

Server Virtualization in 30 secs

- Virtualization: Separation of the service request from the underlying physical service delivery
- Abstraction of hardware to allow multiple “virtual machines” to co-exist on single physical system
- The hypervisor manages VM & hardware interaction



Common Virtualization Terminology

- Host
- Guest
- Hypervisor Types
  - Type 1/Bare Metal/Non-Hosted/Native
  - Type 2/Hosted
- Paravirtualization
- VM Migration

Server Virtualization in the Real World

- General implementation order:
  - Dev and Test
  - LOB
  - Production/Mission Critical
- Overall workload virtualization is estimated around 16% as of 10/2009
- Expected to be ~50% by 2012

Business Drivers: Cost

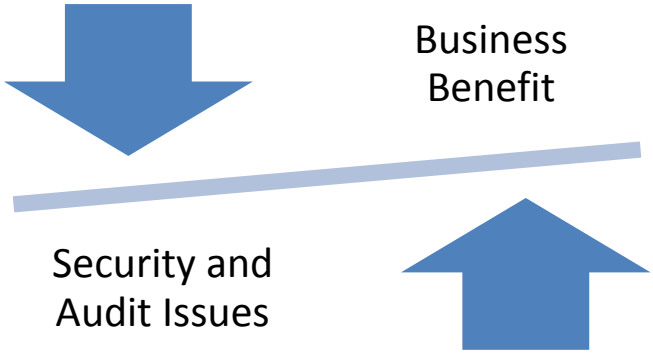
- Do more with less
  - Centralize administration
  - Drive a higher server/admin ratio
- Hardware, space, and power
  - Consolidate and contain infrastructure
  - Less hardware, fewer racks
  - Lower power and cooling costs

Business Drivers: Agility

- Flexibility and ease of deployment and change
  - Simple provisioning
  - Multiple OS on a single server
  - Easily scale up, down, in, and out
- High availability
  - Simple clustering
  - Location-independent agility for DR

Mapping Business Drivers to Security and Audit Concerns

- Or, there's no such thing as a free lunch



Mapping Business Drivers to Security and Audit Concerns

Business Drivers

- Server consolidation
- Centralized administration
- Higher server/admin ratio
- Quick provisioning
- Simple reconfiguration
- Multiple OS on single platform
- Agility across locations

Concerns

- Management infrastructure
- SoD/RBAC
- "Physical" access
- Licensing compliance
- Change management
- Capacity/SLA planning
- Platform security, hardening & isolation

Audit and Security Topics

Segregation of Duties

- Hypervisor and virtualization infrastructure are new components to manage
- Server, storage, network, and security duties are collapsed
- Critical considerations:
  - Role-mapping within IT
  - RBAC capabilities of virtualization platform
  - Layered controls (prevent, detect, respond)
- **Unfortunately, often given short shrift because of deployment patterns**

Physical Security?!?

- Consider traditional data center controls in a virtual context
  - Cameras – prevent theft, monitor physical access
  - Biometrics, guards, man traps – control physical access
  - Locked racks – prevent theft of physical assets

Virtual Corollaries to Physical Security

- Virtual console
  - Accessible without respect to physical location
  - Protect with idle timeouts, access control
- Storage of virtual disks
  - "Theft" of a system possible without physical access
  - Maintain control of virtual machine files (including templates and backups)
- "Rack and stack"
  - Rogue provisioning without data center access
  - Emphasize management infrastructure access controls and monitoring

Change and Configuration Management

- Virtualization enables fast and highly automated provisioning and change
  - Responsibilities may be consolidated
- Licensing compliance can become an issue without adequate controls
- Process needs to keep pace to leverage advantages while managing risk
  - Ramifications for CMDB?
- Emphasize both preventative and detective controls

Capacity Management

- Virtual capacity is a new discipline for capacity and scalability engineers
  - Power, network, CPU, etc.
- Dynamic capabilities of virtual workloads puts increased importance on planning
- HA, DR and planned maintenance can cause capacity issues if not properly addressed at design-time

Infrastructure Hardening

- Hypervisor/VMM system hardening
- Security of administrative and support infrastructure
  - Service accounts, networking
- Management network isolation
  - Consolidation of functions makes this even more critical
- Virtual network configuration

Platform Security

- Security characteristics and capabilities of your virtualization platforms and vendors
- Software security quality
- Resource isolation across VMs
  - Memory, disk, CPU, network
- Resource limits and reservations
- Management infrastructure
  - RBAC, monitoring, remote administration, APIs

Security Advantages and Opportunities

- Interesting options for control placement and implementation
  - Patching, firewalls, IPS, DLP, etc.
- Centralized view of resources
  - Management, monitoring, etc.
- Full system lifecycle management and visibility
  - Actions on system state are traceable
  - Decommissioning is auditable
- Templates provide new opportunities for configuration management and refresh

New Attack Vectors

VM Escape

- Considered “holy grail” of virtualization exploits
- “Escaping” through the virtualization layer to attack:
  - The host
  - Other virtual machines (out of band)
- Cloudburst
  - Presented at Black Hat 2009

Hyperjacking

- VMBRs (Virtual Machine Based Rootkits)
- Inserting a hypervisor underneath a running OS
- Can target a physical or virtual system
- Relies on hardware virtualization extensions
- Blue Pill, SubVirt, Vitriol

VM Migration Attacks

- HA/DR/maintenance feature
- Involves moving a VM across hardware
  - Server, cluster, storage
- Attacks involve sniffing, capturing, and/or modifying VM traffic during migration

Virtualization and Security Architecture

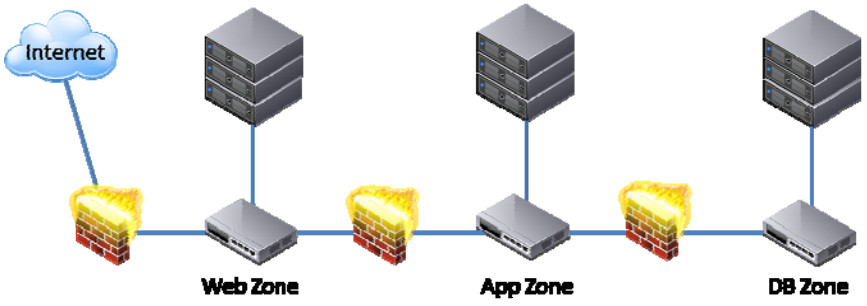
Traditional Architectural Drivers

Populations – Hi to Lo Trust
- Employees
- Contractors/Consultants
- Partners
- Public
- Competitors

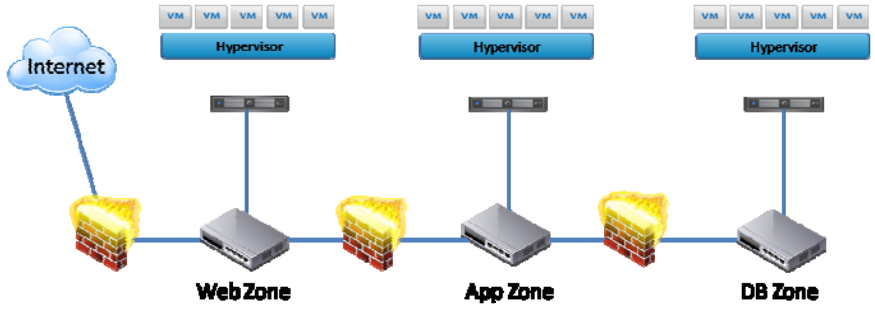
Environments – Hi to Lo Trust
- Mission Critical
- Intranet
- Extranet
- DMZ
- Internet

These considerations are key drivers for:
- Security policy and standards
- Network design and segmentation
- Access controls
- Etc . . .

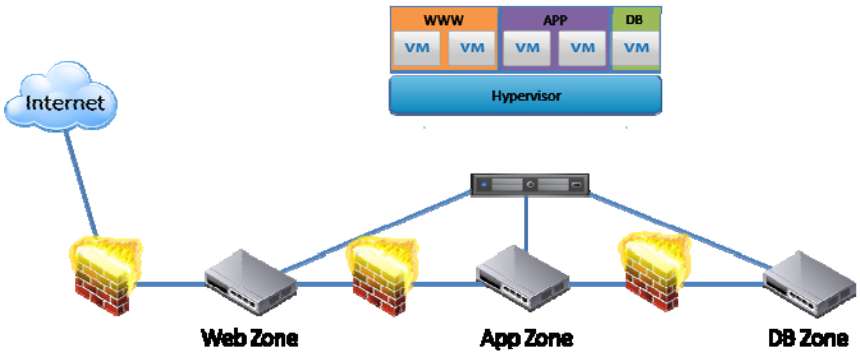
All Physical (Traditional)



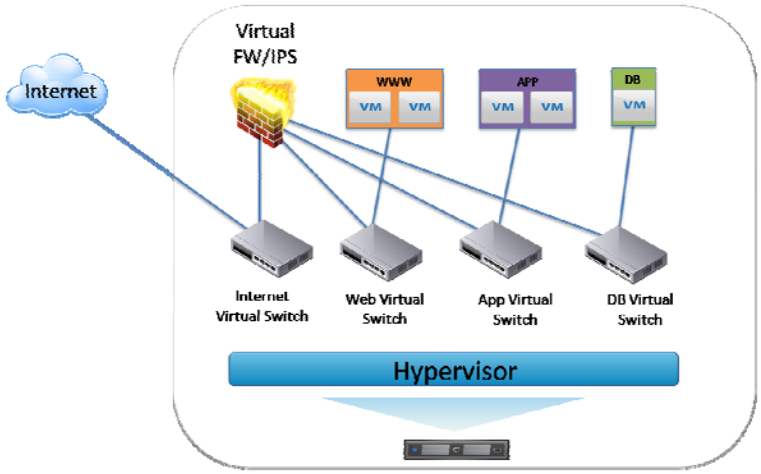
Virtualization Within Trust Zones



Virtualization Across Trust Zones



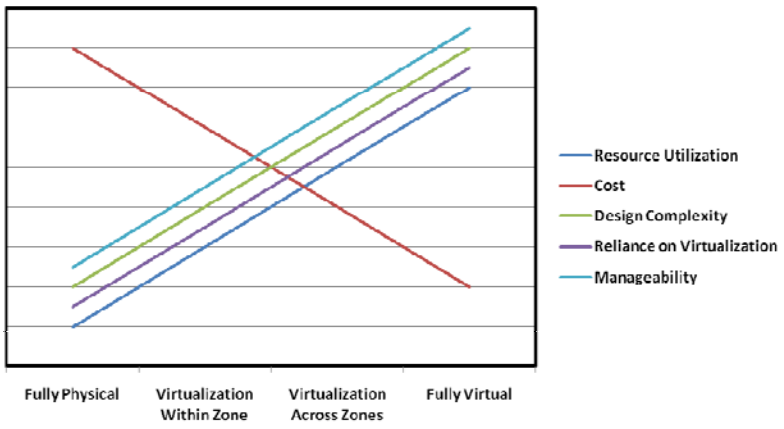
Fully Virtualized



What Considerations Arise?

- Degree of resource utilization
- Cost to acquire and operate
- Complexity of design
- Reliance on virtualization
- Manageability of environment
- The "right" answers depend on organizational capabilities and risk management approach

Comparison of Approaches



* For discussion purposes only – not to scale

Recommendations

- Understand:
  - Virtualization security concerns and possibilities
  - How existing processes and controls can be leveraged and will need to be enhanced
  - Security controls offered by your virtualization platforms
- Have the architectural conversations
  - Determine what's organizationally appropriate

References

- http://www.gartner.com/it/page.jsp?id=1211813
- http://www2.catbird.com/pdf/press/Catbird_ComputerTechnologyReview_Feb4,2009%5B1%5D.pdf
- http://www.vmware.com/files/pdf/dmz_virtualization_vmware_infra_wp.pdf
- http://www.virtualizationpractice.com/blog/?p=5726
- http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-PAPER.pdf
- http://www.eecs.umich.edu/virtual/papers/king06.pdf
- http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf
- Martin Carbone, Wenke Lee, Diego Zamboni. “Taming Virtualization”. IEEE Security & Privacy. Jan/Feb 2008.