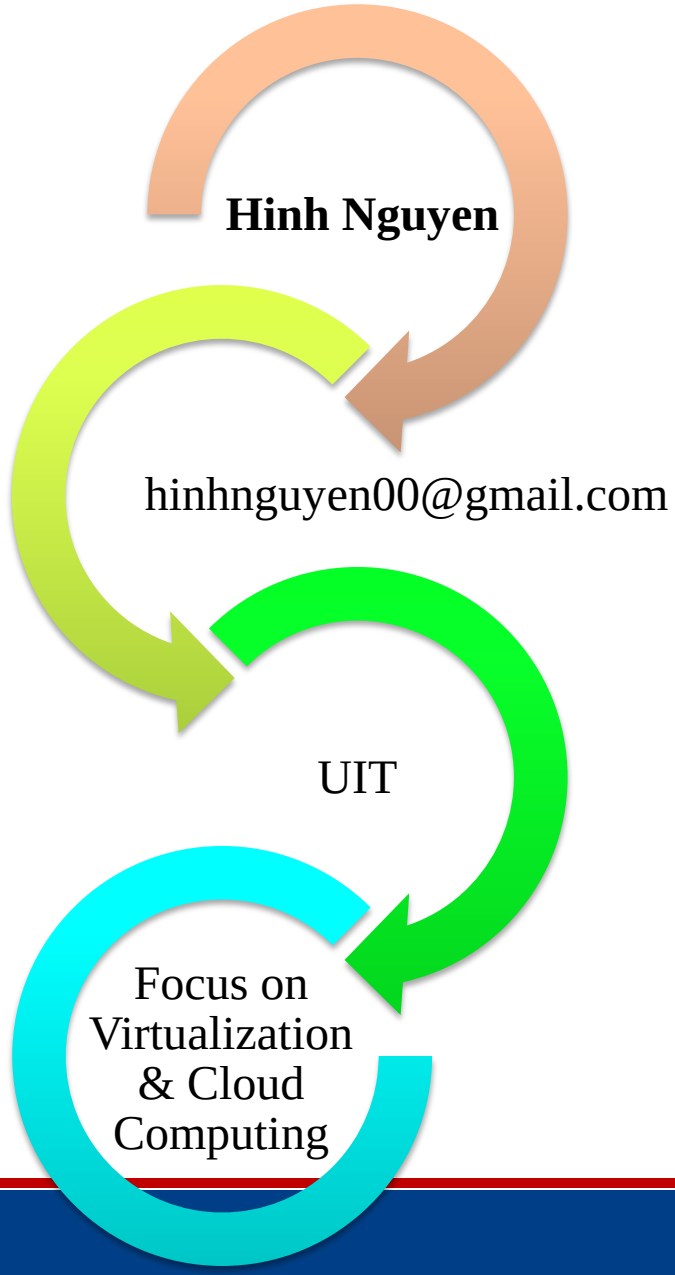
Common issues of Virtualization Security

Nguyễn Hinh | hinhnguyen00@gmail.com


Hinh Nguyen
hinhnguyen00@gmail.com
UIT
Focus on Virtualization & Cloud Computing

About Me

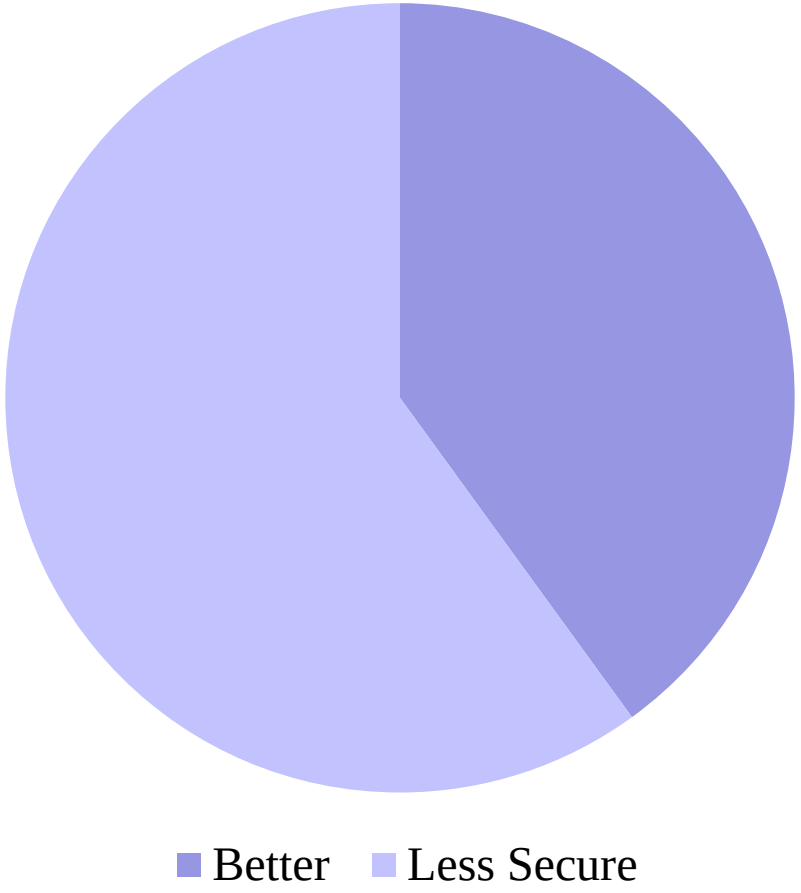
Content

Virtualization Overview

With vMotion instances launching every second, there are more VMs in motion globally than actual aircraft.” -- Paul Maritz, CEO, VMware

Virtualization Security Overview

- Gartner: 60% of VMs will be **LESS SECURE** than the Physical Servers they replace (through 2012)



http://www.gartner.com/it/page.jsp?id=1322414

Why???

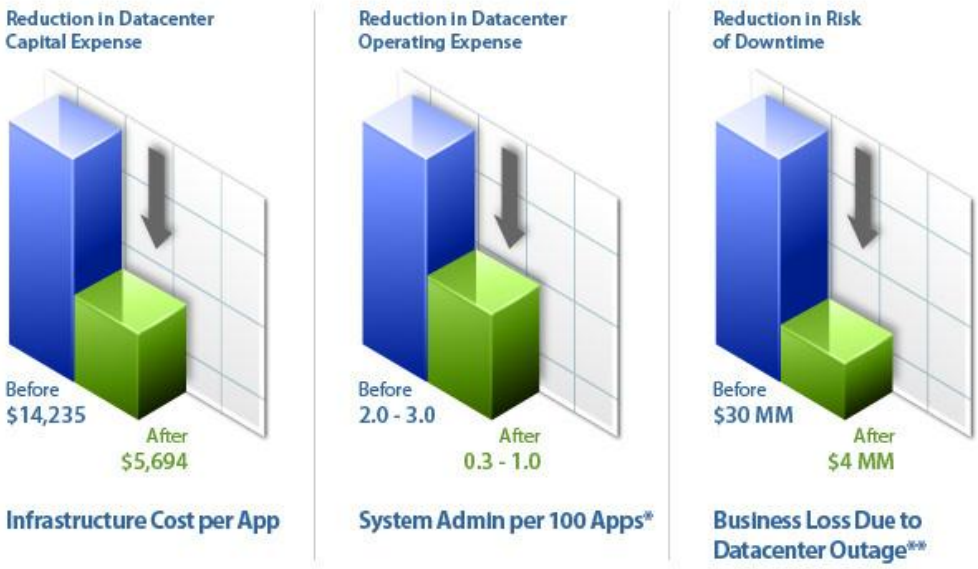
Why - "Hypervisor creates new attack surface"

- Designer/Operator


II. BENEFITS OF VIRTUALIZATION
The Journey to Your Cloud.

II.1. Reduce cost

- Reduce maintenance cost, save power
- Reduce quantity of hardware & software to purchase
- **Reduce "server sprawl"**



II.2. More Secure

Sandboxing

- unstable app & compromised server
- Risk: “VM Escape”

Disaster Recovery & HA

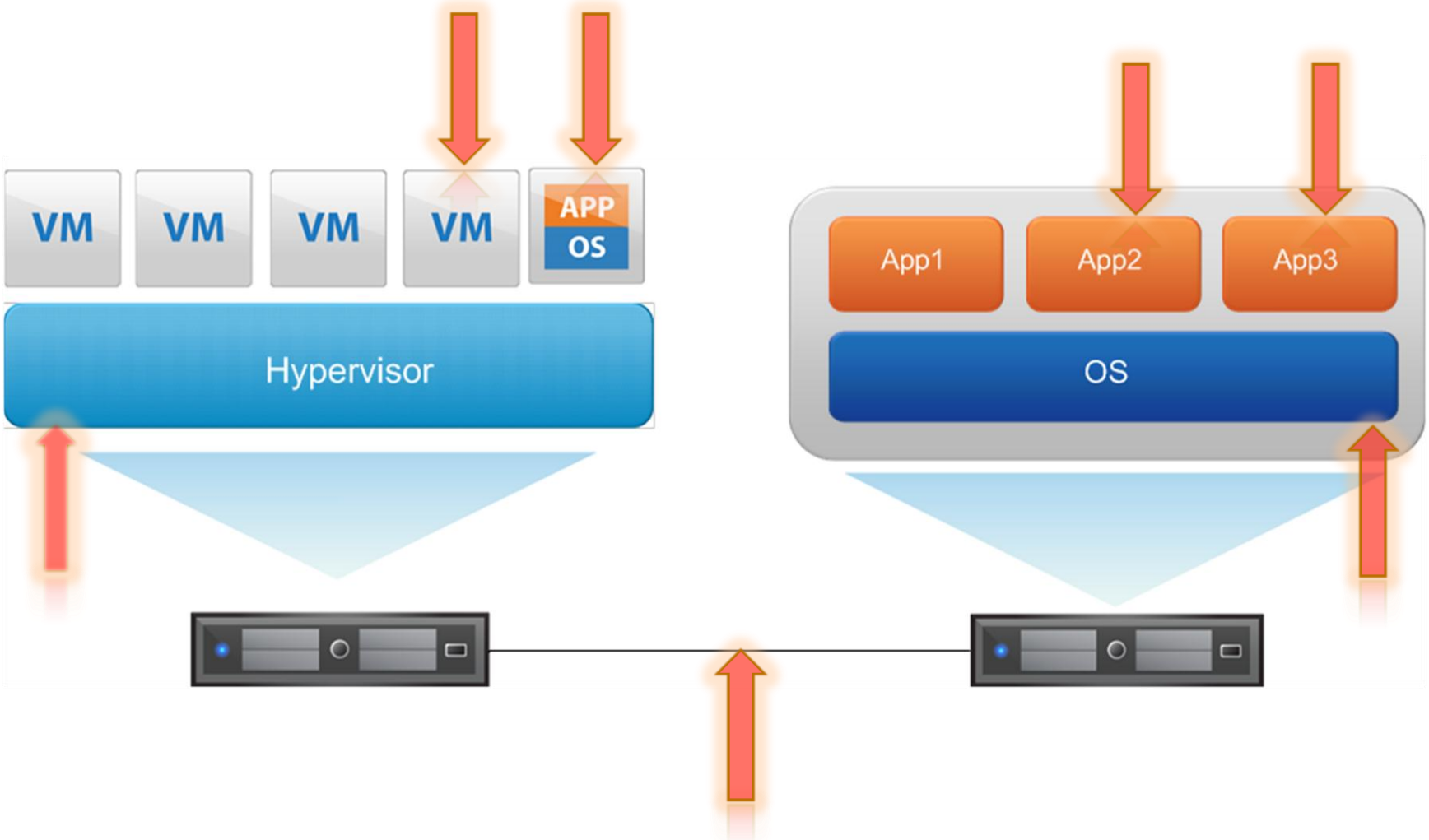
- HA, FT, ….
- Mixed: 1 physical server (master) – VMs (slave)

Forensic analysis capabilities

- snapshot

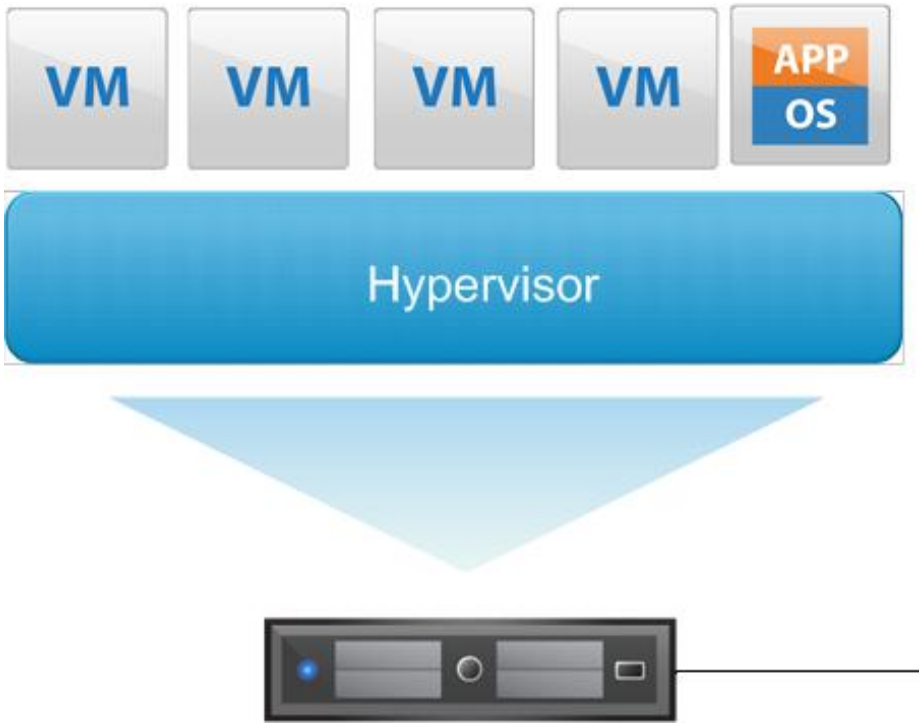
III. RISKS FOR VIRTUALIZED ENVIRONMENTS

III. Risks for Virtualized Environments



III. Risks for Virtualized Environments

- Hypervisor
- Host/platform
- Communication
- Isolation between guest and guest
- Isolation between guest and host




IV. RECOMMENDATIONS
The Journey to Your Cloud.

IV. Recommendations

- Restrict physical access
- Implement defense in depth
- Enforce least privilege and separation of duties
- Harden the hypervisor
- Harden virtual machines and other components

CODE	NAME
HCM01	Do not use default self-signed certificates for ESXi communication.
HCM02	Disable managed object browser.
HCM03	Ensure that ESXi is configured to encrypt all sessions.
HLG01	Configure remote syslog.
HLG02	Configure persistent logging.
HLG03	Configure NTP time synchronization.
HMT01	Control access by CIM-based hardware-monitoring tools.
HMT02	Ensure proper SNMP configuration.
HCN02	Enable lockdown mode to restrict root access.
HCN04	Disable Tech Support Mode.
HCP01	Use a directory service for authentication.
NAR01	Ensure that vSphere management traffic is on a restricted network.
NAR02	Ensure that vMotion traffic is isolated.
NAR04	Maintain strict control of access to management network.
NCN03	Ensure that the "MAC address change" policy is set to "reject."
NCN04	Ensure that the "forged transmits" policy is set to "reject."
NCN05	Ensure that the "promiscuous mode" policy is set to "reject."

Table 27. Security Hardening ESXi – Implementation

CODE	NAME
HST03	Mask and zone SAN resources appropriately.
HIN01	Verify integrity of software before installation.
HMT03	Establish and maintain configuration file integrity.
HCN01	Ensure that only authorized users have access to the DCUI.
HCN03	Avoid adding the root user to local groups.
NCN06	Ensure that port groups are not configured to the value of the native VLAN.
NCN07	Ensure that port groups are not configured to VLAN 4095 except for virtual guest tagging.
NCN08	Ensure that port groups are not configured to VLAN values reserved by upstream physical switches.
NCN10	Ensure that port groups are configured with a clear network label.
NCN11	Ensure that all dvSwitches have a clear network label.
NCN12	Fully document all VLANs used on dvSwitches.
NCN13	Ensure that only authorized administrators have access to virtual networking components.
NPN01	Ensure that physical switch ports are configured with STP disabled.
NPN02	Ensure that the *non-negotiate* option is configured for trunk links between external physical switches and virtual switches in VST mode.
NPN03	Ensure that VLAN trunk links are connected only to physical switch ports that function as trunk links.

Table 28. Security Hardening ESXi – Operational

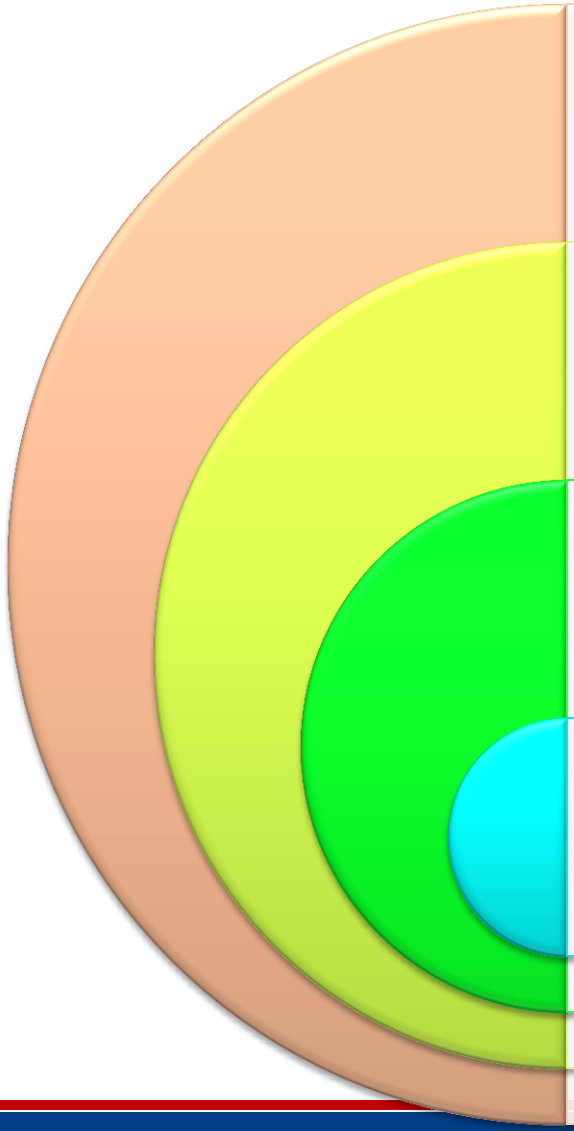
CODE	NAME
VMX02	Prevent other users from spying on administrator remote consoles.
VMX10	Ensure that unauthorized devices are not connected.
VMX11	Prevent unauthorized removal, connection and modification of devices.
VMX12	Disable virtual machine-to-virtual machine communication through VMCI.
VMX20	Limit virtual machine log file size and number.
VMX21	Limit informational messages from the virtual machine to the VMX file.
VMX24	Disable certain unexposed features.
VMP03	Use templates to deploy virtual machines whenever possible.
VMP05	Minimize use of the virtual machine console.

Table 29. Security Hardening Virtual Machine – Operational

vSphere 5.0 security guide


CloudInfraAr


Hardening vSphere



VM

- Update OS,… like physical server
- Limit sharing console: 2
- Control access resource, disconnet unauthorized device

ESXi

- Use AD, verify “ESX Admin” group
- passwork policy
- Config FW (SSH), NTP, SNMP…
- SSL for NFC

vCenter

- Assign role to specific users
- Verify vSphere plug-in
- Client connect vCenter by SSL with trusted CA-signed cert
- Disable datastore browser

vNetwork

- Management, vMotion & storage traffic is isolated
- Forged Transmits & MAC address change policy: reject
- Port groups are not native VLAN

Q & A


THANKS FOR YOUR ATTENTION
I HOPE YOU LIKED AYA
MEMECREATOR.NET