

# How to Secure VMware ESX

Alex Bakman

Ecora Software

[www.ecora.com](http://www.ecora.com)

Founder, Chairman, CTO



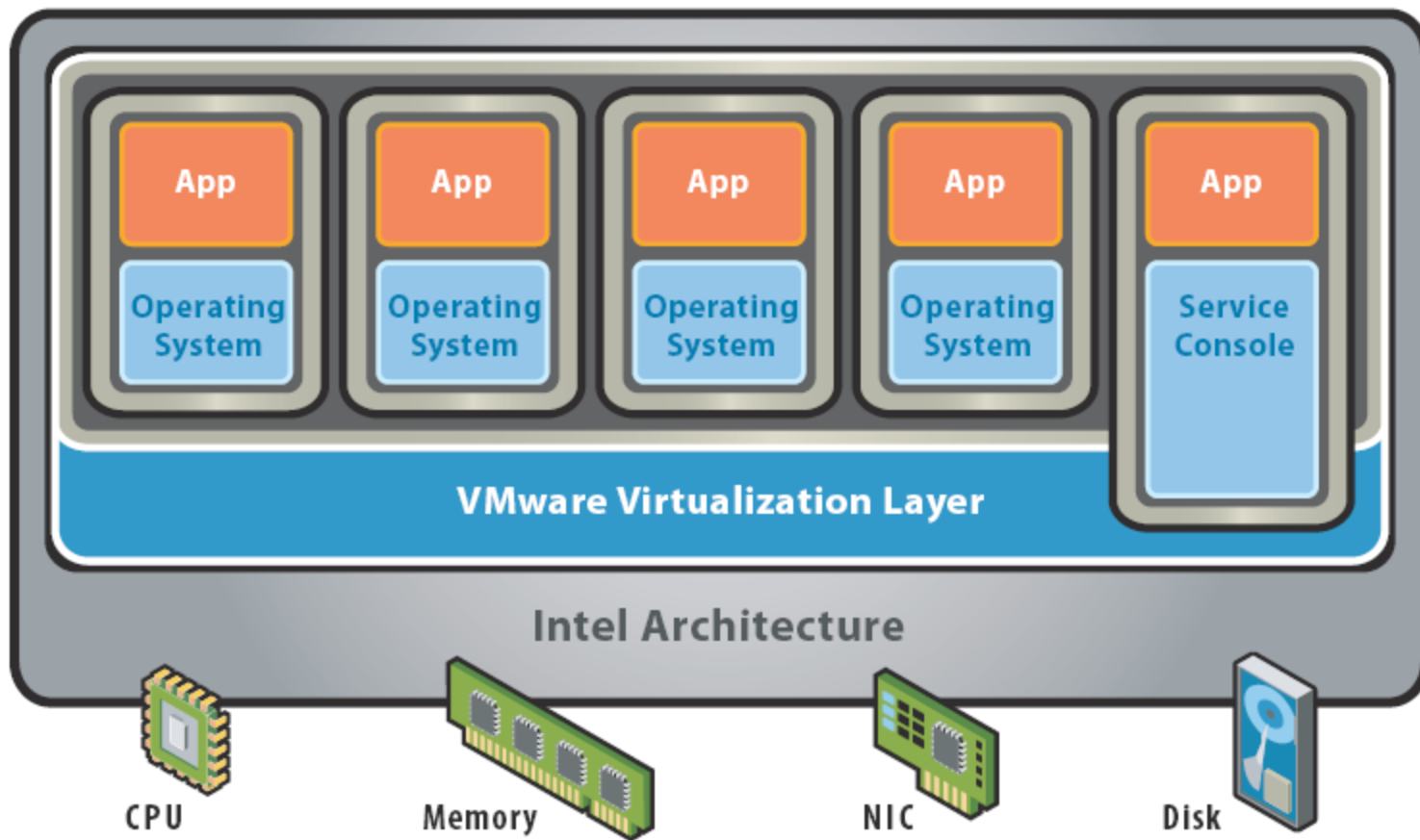
**VMWORLD 2006**

## Agenda

- Why do we care about security?
- ESX security architecture
- ESX role-based access control
- Security deployment models
- Top 10 Security recommendations
- Change and Configuration Reporting using Ecora Auditor
- Additional Resources

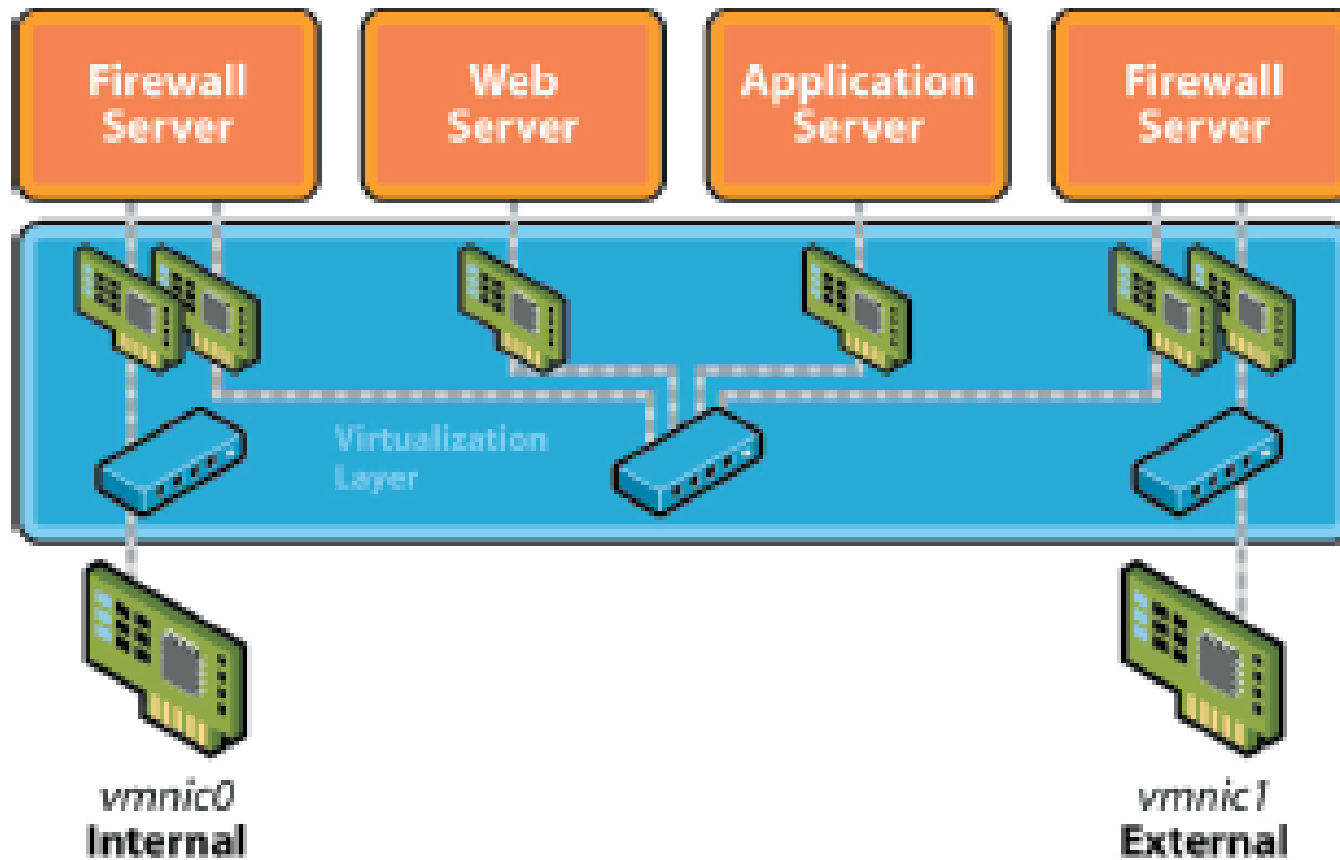
## Why Do We Care About Security?

- Data center environment
- Pass regulatory audits: SOX, PCI DSS, etc
- Protect our customers' valuable data
- Keep your company's reputation clean
- Keep your company in business



## ESX Architecture

- Virtual Machines are highly secured - hardware isolation
- vmkernel has no public interfaces to connect to
- Virtual machines can only communicate through the network
- Isolation by performance. e.g. set cpu for a particular machine to consume < 10% CPU

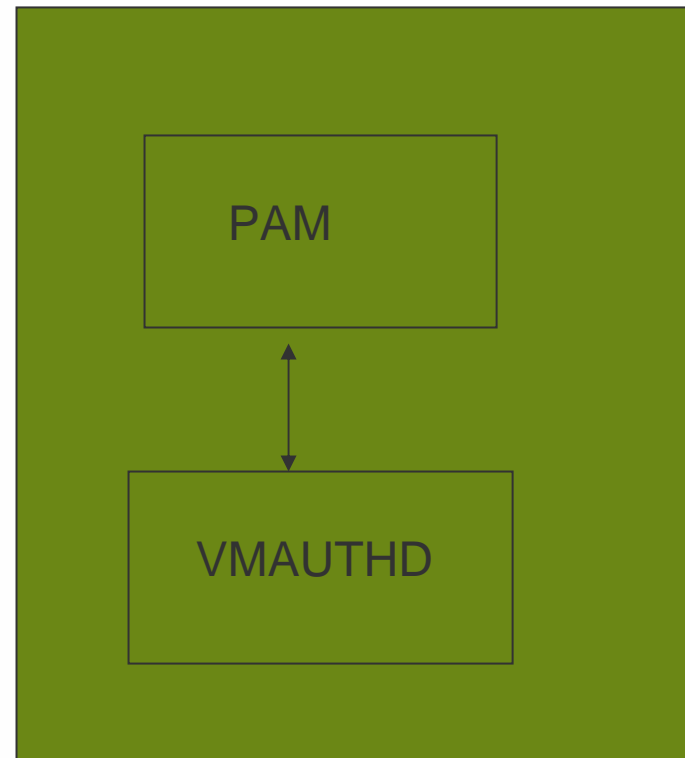


## Access to COS

MUI →

Command line →

VirtualCenter →



## PAM

- Any operation on ESX server requires user authentication
- PAM allows processes to authenticate to account databases
- All forms of access: MUI, command line, etc, go through PAM
- Very flexible and customizable

## Default Role-Based Access in ESX Servers

- Read only
  - No access to log into MUI
  - May only view vmkusage stats
- Guest OS owner
  - Ability to log into MUI
  - View only its own VMs
  - Control power function on its own machines
  - Access owned machines remotely
  - Given r-x access writes to the VM configuration file

# Default Role-Based Access in ESX Servers

- VMWARE Admin
  - Control power of all guests
  - Remote console feature on all guests
  - Create and delete virtual machines
  - Modify vm hardware configuration
  - Change access permissions of guests
  - Limited access to COS by using SUDOers file
- Root
  - Create and remove users and groups
  - Modify resource allocations for guests
  - Modify all ESX settings
  - Full control over COS
  - Assigned by default to root user when ESX is installed
  - Users must be in a “wheel” group to escalate to root using SU

# Single Customer Deployment

## ESX Server Configuration

Feature	Config	Comments
Service console and MUI share physical network with VMs?	No <sup>3</sup>	The service console and MUI traffic should be on a physically separate network.
VMs share physical network?	Yes	All VMs are on the same physical network, separate from the service console's physical network
NIC sharing?	Partial	All VMs share NICs with each other, but NICs aren't shared between the VMs and the Service Console
HBA sharing?	Yes	
VMFS sharing?	Yes	All .dsk files reside within one VMFS partition
Security Level?	Medium	Allow FTP access to the service console
VM Memory Overcommitment?	Yes	Total memory for VMs can be configured to be greater than the total physical memory
COM/Perl API access?	Yes	

# Single Customer Deployment

## User Accounts on ESX Server

Category	Total number of accounts
Site admins	1
Customer admins	0
System admins	0
Business users	0

## Access Chart

Feature	Site Admin	System Admin
Root access	•	
Service Console secure shell (SSH) access	•	
MUI and Remote Console access	•	
Create and edit VMs	•	
Terminal access to VMs	•	•

# Restrictive Multi-Customer Deployment

## ESX Server Configuration

Feature	Config	Comments
Service console and MUI share network with VMs?	No	The service console and MUI traffic should be on a physically separate network from the VMs.
VMs share physical network?	Partial	VMs from the same customer are on the same physical network. Multiple customers do not share the same physical network.
NIC sharing?	Partial	VMs from the same customer share NICs, but multiple customers never share NICs.
HBA sharing?	Yes	
VMFS sharing?	No	Each customer has their own VMFS partition, and their VM .dsk files reside on this partition. The partition can span multiple LUNs
Security Level?	High	No FTP access
VM Memory Over committment?	Yes	Total memory for VMs can be configured to be greater than the total physical memory
COM/Perl API access?	Yes	

# Restrictive Multi-customer Deployment

## User Accounts on ESX Server

Category	Total number of accounts
Site admins	1
Customer admins	10
System admins	0
Business users	0

## Access Chart

Feature	Site Admin	Customer Admin	System Admin
Root access	•		
Service Console secure shell (SSH) access	•	•	
MUI and Remote Console access	•	•	
Create and edit VMs	•	•	
Terminal access to VMs	•	•	•

## Recommendation #1

- Use Firewall and Antivirus software for COS
  - Just like any other OS
  - Provides basic protection

## Recommendation #2

- Use VLANs to segment physical network so that only machines that need to see each other can
  - Huge help with compliance audits
  - Run COS on a a separate network

## Recommendation #3

When installing ESX use security=high

- This is the default settings
- All traffic is encrypted
- Username and password never sent in clear text
- No FTP access

## Recommendation #4

- Do not allow root level access over SSH and use secure commands
  - don't worry MUI and console access will still work
  - Forces users to have an audit trail
  - Have users use SU command. Use wheel group to control SU usage
  - SUDO is a great way to accomplish this

## Recommendation #5

- Disable all unnecessary services in COS
  - No NFS
  - Use PuTTY for secured shell access
  - Use WinSCP and scp to copy files

## Recommendation #6

- Use VirtualCenter to help you manage granular security access
  - Must have if you have more than a handful of hosts
  - Replaces the native ESX model role-based access model and stores users and acls in the database
  - Permissions can be assigned at any level of granularity within organization
  - Audit trails for compliance
  - Root account is not used
  - If external authentication with AD is important, VC makes it a lot easier

## Recommendation #7

- Patching
  - Stay current with patches, especially security patches
  - Test patches in development environment
  - Subscribe to vmware email alerts

## Recommendation #8

- Secure Guest OSes
  - It is just like securing a physical machine
  - Shut down unnecessary daemons and services
  - Close unused ports
  - Harden configurations
  - Patch frequently

## Recommendation #9

- Control User Level access using VirtualCenter
  - VMware's native "flagship" model is too weak for role-based access
  - Use unique IDs supports Sarbanes Oxley "segregation of duties" model and enables traceability
  - Audit logs for individual access are key

## Recommendation #10

- Document and Monitor configurations changes in your environment, especially changes in security settings.
  - Changes happen daily
  - Avoid problems proactively
  - Must do for compliances: SOX, PCI DSS, HIPPA, etc
  - Proof for Auditors

## About Ecora

- Founded in 1999, Portsmouth, NH
- The industry's only agentless solution for automating detailed configuration and change reporting of IT systems Components
- Customers: Fortune Global 1,000 customers in all key verticals
- Hundreds of companies used Ecora Auditor to verify and proof compliance to SOX, PCI, GLBA, FISMA and other regulatory requirements
- The Only CMDB Vendor with Nearly 8,000 users Worldwide
- Recognized in 2005 on the Deloitte & Touche Fast 500 and Software 500
- Partnerships with HP, BMC, Microsoft





## Ready Made Reports

[Documentation Report](#)

[Baseline Report](#)

[Change Report](#)

## Fact Finding Reports:

[Kernel and Memory Information](#)

[ESX Security Settings](#)

[Virtual Machine Permissions](#)

[VMFS Files](#)

[Virtual Machines Summary](#)

[Virtual Machine Hardware Summary](#)

[Physical NIC and Virtual Switches](#)

[Storage Configuration SCSI](#)

[Kernel and Memory Information](#)

[Memory and Swap File Information](#)

[Virtual Machine Hardware](#)

## Consolidated Change Log Reports:

[Virtual Machines](#)

## Virtual Machine Permissions

*Prepared For: administrator <root@sampleOrg.com>  
 Prepared On: Wednesday, July 19, 2006 11:52:30 AM  
 Prepared By: Ecora Auditor Professional 4.0 - VMware Module  
 Prepared Using: FFR Definition 'Virtual Machine Permissions'  
 Prepared Time Criteria: Last 20 month(s)*

*Copyright © 2006 SampleOrg.com  
 All rights reserved.*

- [Permissions](#)

*This report shows permissions for Virtual Machines*

**Table 1. Permissions**

Host Name	Account Name	Account Type	Read	Execute	Write
chmserver	BUILTIN\Administrators	Alias	Yes	Yes	Yes
	BUILTIN\Users	Alias	Yes	Yes	No
	NT AUTHORITY\SYSTEM	Group	Yes	Yes	Yes
vm-server		Other	Yes	No	No
	root	Group	Yes	Yes	No
	root	User	Yes	Yes	Yes

## ESX Security Settings

Prepared For: administrator <root@sampleOrg.com>  
Prepared On: Wednesday, July 19, 2006 11:52:05 AM  
Prepared By: Ecora Auditor Professional 4.0 - VMware Module  
Prepared Using: FFR Definition 'ESX Security Settings'  
Prepared Time Criteria: Last 20 month(s)

Copyright © 2006 SampleOrg.com  
All rights reserved.

- [Security Settings](#)

This report shows ESX Server security settings

**Table 1. Security Settings**

Host Name	Management Interface SSL Enabled	Remote Console SSL Enabled	SSH Enabled	FTP Enabled	Telnet Enabled	NFS File Sharing Enabled
BigBoy	Yes	Yes	Yes	No	No	No
BigBoy	Yes	Yes	Yes	Yes	No	No

Host Name	Partition	File Name	Size	Permissions	Owner	Group	Type	Last Modified	Mapped Disk
BigBoy	vmhba1:12:0:5	Ecora.vmdk.gz	299	rw-r--r--	0	0		May 3 02:50	
		SwapFile.vswp	16000	rw-----	0	0	swap	May 1 08:37	
		SwapFile2.vswp	200	rw-----	0	0	swap	Mar 22 04:33	
		SwapFile3.vswp	200	rw-----	0	0	swap	Mar 22 04:36	
		SystemDisk.vmdk.filepart	1478	rw-r--r--	0	0		Mar 22 04:10	
		Untitled.vmdk	4000	rw-----	0	0	disk	Mar 22 09:54	
		vm1.vmdk	8000	rw-----	0	0	disk	May 1 08:28	
		vm2.vmdk	8000	rw-rw----	0	507	disk	May 1 08:29	
		vmk3.vmdk	4000	rw-----	0	0	disk	Apr 4 09:53	
		Windows 2003 std.vmdk	5000	rw-----	0	503	disk	Feb 17 11:55	

## Additional Resources

- [http://www.vmware.com/pdf/esx\\_lun\\_security.pdf](http://www.vmware.com/pdf/esx_lun_security.pdf)
- [http://www.vmware.com/pdf/esx\\_authentication\\_AD.pdf](http://www.vmware.com/pdf/esx_authentication_AD.pdf)
- [http://www.vmware.com/pdf/esx2\\_security.pdf](http://www.vmware.com/pdf/esx2_security.pdf)
- [www.cert.org](http://www.cert.org)
- “VMware ESX Server: Advanced Technical Design Guide” by Ron Oglesby and Scott Herold
- “Hacking Exposed: Network Security Secrets and Solutions” 4<sup>th</sup> Edition by Stuart McClure, Joel Scambray, George Kurtz

## 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**

**VMWORLD 2006**

