How to Secure VMware ESX

Alex Bakman
Ecora Software
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
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

Diagram:
- PAM
- VMAUTHD
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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Config</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service console and MUI share physical network with VMs?</td>
<td>No³</td>
<td>The service console and MUI traffic should be on a physically separate network.</td>
</tr>
<tr>
<td>VMs share physical network?</td>
<td>Yes</td>
<td>All VMs are on the same physical network, separate from the service console's physical network.</td>
</tr>
<tr>
<td>NIC sharing?</td>
<td>Partial</td>
<td>All VMs share NICs with each other, but NICs aren’t shared between the VMs and the Service Console.</td>
</tr>
<tr>
<td>HBA sharing?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>VMFS sharing?</td>
<td>Yes</td>
<td>All .dsk files reside within one VMFS partition.</td>
</tr>
<tr>
<td>Security Level?</td>
<td>Medium</td>
<td>Allow FTP access to the service console.</td>
</tr>
<tr>
<td>VM Memory Overcommitment?</td>
<td>Yes</td>
<td>Total memory for VMs can be configured to be greater than the total physical memory.</td>
</tr>
<tr>
<td>COM/Perl API access?</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
## Single Customer Deployment

### User Accounts on ESX Server

<table>
<thead>
<tr>
<th>Category</th>
<th>Total number of accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site admins</td>
<td>1</td>
</tr>
<tr>
<td>Customer admins</td>
<td>0</td>
</tr>
<tr>
<td>System admins</td>
<td>0</td>
</tr>
<tr>
<td>Business users</td>
<td>0</td>
</tr>
</tbody>
</table>

### Access Chart

<table>
<thead>
<tr>
<th>Feature</th>
<th>Site Admin</th>
<th>System Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root access</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Service Console secure shell (SSH) access</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>MUI and Remote Console access</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Create and edit VMs</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Terminal access to VMs</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Feature</td>
<td>Config</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Service console and MUI share network with VMs?</td>
<td>No</td>
<td>The service console and MUI traffic should be on a physically separate network from the VMs.</td>
</tr>
<tr>
<td>VMs share physical network?</td>
<td>Partial</td>
<td>VMs from the same customer are on the same physical network. Multiple customers do not share the same physical network.</td>
</tr>
<tr>
<td>NIC sharing?</td>
<td>Partial</td>
<td>VMs from the same customer share NICs, but multiple customers never share NICs.</td>
</tr>
<tr>
<td>HBA sharing?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>VMFS sharing?</td>
<td>No</td>
<td>Each customer has their own VMFS partition, and their VM.dsk files reside on this partition. The partition can span multiple LUNs</td>
</tr>
<tr>
<td>Security Level?</td>
<td>High</td>
<td>No FTP access</td>
</tr>
<tr>
<td>VM Memory Over committement?</td>
<td>Yes</td>
<td>Total memory for VMs can be configured to be greater than the total physical memory</td>
</tr>
<tr>
<td>COM/Perl API access?</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Restrictive Multi-customer Deployment

User Accounts on ESX Server

<table>
<thead>
<tr>
<th>Category</th>
<th>Total number of accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site admins</td>
<td>1</td>
</tr>
<tr>
<td>Customer admins</td>
<td>10</td>
</tr>
<tr>
<td>System admins</td>
<td>0</td>
</tr>
<tr>
<td>Business users</td>
<td>0</td>
</tr>
</tbody>
</table>

Access Chart

<table>
<thead>
<tr>
<th>Feature</th>
<th>Site Admin</th>
<th>Customer Admin</th>
<th>System Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root access</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Console secure shell (SSH) access</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>MUI and Remote Console access</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Create and edit VMs</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Terminal access to VMs</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>
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 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

This report shows permissions for Virtual Machines

Table 1. Permissions

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Account Name</th>
<th>Account Type</th>
<th>Read</th>
<th>Execute</th>
<th>Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>chmserver</td>
<td>BUILTIN\Administrators</td>
<td>Alias</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>BUILTIN\Users</td>
<td>Alias</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>NT AUTHORITY\SYSTEM</td>
<td>Group</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>vm-server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>Group</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>root</td>
<td>User</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>root</td>
<td>User</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
ESX Security Settings

This report shows ESX Server security settings

Table 1. Security Settings

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Management Interface SSL Enabled</th>
<th>Remote Console SSL Enabled</th>
<th>SSH Enabled</th>
<th>FTP Enabled</th>
<th>Telnet Enabled</th>
<th>NFS File Sharing Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>BigBoy</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>BigBoy</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Host Name</td>
<td>Partition</td>
<td>File Name</td>
<td>Size</td>
<td>Permissions</td>
<td>Owner</td>
<td>Group</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>---------------------------</td>
<td>------</td>
<td>-------------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>BigBoy</td>
<td>vmhba1:12:0:5</td>
<td>Ecora.vmdk.gz</td>
<td>299</td>
<td>rw-r--r--</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SwapFile.vswp</td>
<td>16000</td>
<td>rw--------</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SwapFile2.vswp</td>
<td>200</td>
<td>rw--------</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SwapFile3.vswp</td>
<td>200</td>
<td>rw--------</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SystemDisk.vmdk.filepart</td>
<td>1478</td>
<td>rw-r--r--</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Untitled.vmdk</td>
<td>4000</td>
<td>rw--------</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vm1.vmdk</td>
<td>8000</td>
<td>rw--------</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vm2.vmdk</td>
<td>8000</td>
<td>rw-rw----</td>
<td>0</td>
<td>507</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vmk3.vmdk</td>
<td>4000</td>
<td>rw--------</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows 2003 std.vmdk</td>
<td>5000</td>
<td>rw--------</td>
<td>0</td>
<td>503</td>
</tr>
</tbody>
</table>
**Additional Resources**

- www.cert.org

- “VMware ESX Server: Advanced Technical Design Guide” by Ron Oglesby and Scott Herold

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/](http://www.vmware.com/vmtn/vmworld/sessions/)

Enter the following to download (case-sensitive):

**Username:** cbv_rep  
**Password:** cbvfor9v9r