Securing the Data Center against vulnerabilities & Data Protection
Agenda

Virtual Virtualization Technology
How Virtualization affects the Datacenter Security
Keys to a Secure Virtualized Deployment and Data Protection
The Future of Datacenter Security
Centralized Management

VMware VirtualCenter

SHARED STORAGE
Centralized Management

Centrally manage your infrastructure from a single console

1. Virtual Machine Management
2. Server Provisioning
3. Workload Migration
4. Resource Management
5. System Monitoring
6. Rich Security and Access Controls
7. Programmatic Interfaces
A template is a master copy of a VM used to create and provision new VMs.
A clone is a copy of a VM plus customization.
About Snapshots

A snapshot preserves the state of the virtual machine, allowing you to return to it repeatedly.

Linear Process

Windows operating system
snapshot 1
snapshot 2
snapshot 3
snapshot 4
snapshot 5

Process Tree

Windows operating system
baseline
IE base
Foxfire base

SP1
IE base1
You Are Here

SP2
Foxfire base2

IE base2
**Guided Consolidation**

- **DISCOVER**
  - Automatically discovers physical servers

- **ANALYZE**
  - Analyzes utilization and usage patterns
  - Converts physical servers to VMs placed intelligently based on user response

- **CONVERT**
  - Lowers training requirements for new virtualization users
  - Steers users through the entire consolidation process
ESXi: Thin, Hardware-Integrated Hypervisor

- 32MB footprint: Increased security and reliability
- No installation: From server boot to running VMs in minutes
From server boot to running VMs in Minutes

1. Power on server and boot into hypervisor
2. Configure Admin Password
3. (optional) Modify network configuration
4. Connect VI Client to IP Address or manage with VirtualCenter
ESXi Enables ‘Plug-and-Play’ Datacenter

- DRS + ESXi: “Hot add” of compute capacity
- Standardized and optimized servers as stateless compute nodes
- Plug-and-Play capacity management

ESXi: 32MB thin, production-proven, OS-independent, secure hypervisor
Traditional ESX Server

98%

Agent
Agent
RPM

RHEL3-based Service Console

Disk Footprint: 2 GB
Percent of Patches: >50%

RPM 2%

App
App
App

OS
OS
OS

VMkernel

Helpers
VMM
VMM
VMM

Storage
Networking
Resource Management
HAL and Device Drivers

Disk Footprint: 32 MB
ESXi Server: Thin Virtualization!

- **Agent**: 98%
- **RPM**: 2%

**RHEL3-based Service Console**

**Disk Footprint:**
- 2 GB
- >50% Percent of Patches

**Disk Footprint:**
- 32 MB

**VMkernel**
- **Helpers**
- **VMM**
- **Storage**
- **Networking**
- **Resource Management**
- **HAL and Device Drivers**
Agenda

Virtual Virtualization Technology

How Virtualization affects the Datacenter Security

Keys to a Secure Virtualized Deployment and Data Protection

The Future of Datacenter Security
How Virtualization Affects Datacenter Security

Abstraction and Consolidation
- ↑ Capital and Operational Cost Savings
- ↓ New infrastructure layer to be secured
- ↓ Greater impact of attack or misconfiguration

Collapse of switches and servers into one device
- ↑ Flexibility
- ↑ Cost-savings
- ↓ Lack of virtual network visibility
- ↓ No separation-by-default of administration
How Virtualization Affects Datacenter Security

Faster deployment of servers
- ↑ IT responsiveness
- ↓ Lack of adequate planning
- ↓ Incomplete knowledge of current state of infrastructure

VM Mobility
- ↑ Improved Service Levels
- ↓ Identity divorced from physical location

VM Encapsulation
- ↑ Ease of business continuity
- ↑ Consistency of deployment
- ↑ Hardware independence
- ↓ Outdated offline systems
Biggest Security Risk: Misconfiguration

Neil MacDonald – “How To Securely Implement Virtualization”

Gartner

“Like their physical counterparts, most security vulnerabilities will be introduced through misconfiguration and mismanagement”
Agenda

Virtual Virtualization Technology
How Virtualization affects the Datacenter Security
Keys to a Secure Virtualized Deployment and Data Protection
The Future of Datacenter Security
VMware Update Manager

Automates patch management for ESX Server hosts and select Microsoft and RHEL virtual machines

- Scans and remedies online as well as offline virtual machines* and online ESX Server hosts
- Snapshots virtual machines prior to patching and allows rollback to snapshot

> Eliminates manual tracking of patch levels of ESX Server hosts and virtual machines
> Automates enforcement of patch standards
> Reduces risk through snapshots and offline virtual machine patching

* Note: RHEL guests can only be scanned, not remediated
Non-disruptive ESX Server Patching with Update Manager and DRS

- Update Manager patches entire DRS clusters
  - Each host in the cluster enters DRS maintenance mode, one at a time
  - VMs are migrated off, host is patched & rebooted if required
  - VMs are migrated back on
  - Next host is selected

- Automates patching of large number of hosts with zero downtime to virtual machines
Data and System Protection – Physical vs. Virtual

Data and system protection with physical infrastructure
- Separate processes for protecting data and system disks
- Require identical hardware for guaranteed restore
- Complex processes to ensure protection

Data and system protection with VMware Infrastructure
- Same process for data and system disks
  - Entire system stored as data
  - Hardware-independent virtual machines are easy to restore to any hardware
What to Backup in an ESX Server?

- VM 1
  - App
  - Operating System
  - .vmx
  - .redo
  - .vmdk

- VM 2
  - App
  - Operating System
  - .vmx
  - .vmdk

- VM 3
  - App
  - Operating System
  - .vmx
  - .redo
  - .vmdk

- VMFS
- RDM

- ESX Server
- Service Console
Approaches when Performing Backup

> Run backup software inside a virtual machine
> Perform off-line backups

VMware Consolidated Backup
VMware Consolidated Backup

- Backup load off ESX Server
- Backup traffic off the LAN
- Backup agents off virtual machines
VCB Software

- VCB Software is **not** a replacement for backup software
- VCB Software integrates with existing backup tools and technologies already in place
Securing Virtual Machines

Provide Same Protection as for Physical Servers

Host
- Anti-Virus
- Patch Management

Network
- Intrusion Detection/Prevention (IDS/IPS)

Edge
- Firewalls
Secure Design for Virtualization Layer

Fundamental Design Principles

- **Isolate all management networks**
- **Disable all unneeded services**
- **Tightly regulate all administrative access**
Enforce Strong Access Controls

Security Principle | Implementation in VI
--- | ---
Least Privileges | Roles with only required privileges
Separation of Duties | Roles applied only to required objects

Joe

Harry

Anne

- Administrator
- Operator
- User
Security Advantages of Virtualization

Ease of maintenance

> Test patches on multiple configurations in contained environment before rolling them out

> Use snapshots to save the known good state of a virtual machine before trying out something risky

> Production VM can be cloned and then modified off-line while the original one still runs.
  - Updated VMs can be brought up in parallel with the previous version
  - Both can be kept running as long as necessary to validate the new configuration
Security Advantages of Virtualization

Better Lifecycle Controls

Request Document -> Create -> Approve -> Publish or Retract -> Audit Usage -> Retain

Request for VM Provisioning -> Deploy from Template -> Route for Audit/Approval -> Power-On or Suspend -> Monitor & Adjust Resources

Archive

Dispose

Delete
Agenda

Virtual Virtualization Technology
How Virtualization affects the Datacenter Security
Keys to a Secure Virtualized Deployment and Data Protection

The Future of Datacenter Security
New Solutions for Reduced Downtime

- Fault Tolerance
  - Zero downtime, zero data loss, continuous availability

- Data Recovery
  - Integrated backup and recovery appliance
VMware Fault Tolerance

- Single identical VMs running in lockstep on separate hosts
- Zero downtime, zero data loss failover for all virtual machines in case of hardware failures
- Integrated with VMware HA/DRS
- Zero downtime, zero data loss
- No complex clustering or specialized hardware required
- Single common mechanism for all applications and OS-es
Transforming Availability Service Levels

Hardware Failure Tolerance

CONTINUOUS

AUTOMATED RESTART

UNPROTECTED

0% 10% 100%

Application Coverage

VMware FT

with VMware HA

0% 10% 100%
1. **Backup**

- Schedule backups via VC
- Snapshots taken
- Data de-duped and stored

**VirtualCenter**

Agent-less, disk-based backup and recovery of your VMs

VM or file level restore

Incremental backups and data de-dupe to save disk space

2. **Restore**

- VM goes down
- Select VM images/files to recover
- Restore...VM running in seconds

**VirtualCenter**

Quick, simple and complete data protection for your VMs

Centralized Management through VirtualCenter

Cost Effective Storage Management
VMware VMsafe

API that enables protection of VMs by inspection of virtual components in conjunction with hypervisor

- Isolation of protection engine from malware
- Broad ranging coverage of virtual machine CPU, memory, storage and network

Application

Operating System

Protection Engine

VMware Infrastructure
Ecosystem Enablement with VMware VMsafe

Multi-function Security Appliance

- Agent-less deployment of partner security services
- Single security VM for multiple security services AV, Firewall, IPS
- Security policy and state moves with virtual machine

- Integrated, more effective, comprehensive security solutions within the virtual infrastructure
- Better security than physical servers!
VMsafe: Broad Security Industry Support

Enterprise to SMB

End-points to Gateways

Anti-Virus to IPS

Networks to Host

Audit to Patching

And Anywhere in between…
Thank You

http://www.vmware.com/go/security