ISACA®

Trust in, and value from, information systems

San Francisco Chapter

San Francisco, California

Virtualization Security and Audit

(server virtualization focusing on VMware ESX 3.5)

Thursday, March 4, 2010

Michael T Hoesing

CISA,CISSP, CCP, ACDA, CIA, CFSA, CMA, CPA

University of Nebraska at Omaha

a CAE IAE institution

mhoesing@mail.unomaha.edu

m-hoesing@cox.net

Disclaimer: *While every effort is made to present accurate and non-harmful material, the presenter nor the sponsor can know all the aspects of your environment. Therefore, none of the content herein should be implemented by attendees without complete testing and other due diligence in their environment and attendees accept all liability for any adaptation of this content into their environment.*

For the attorneys in the audience, even those who will not admit they are an attorney, don't sue me, I have no money.

Any opinion expressed during this presentation are those of the presenter and do not represent positions of employers, clients, or other associates past, present, or future.

Key Points

I. Background

II. Risks

III. Security Techniques & Controls

IV. Security Products

V. Assessing ESX

VI. An Example – Look for Sprawl

VII. vShpere (aka ESX 4.0)

VIII. Clouds (you can’t go on the speaker circuit without discussing this)

IX. Compliance, Other, References, QA

I Background

Why

Scope

An Example

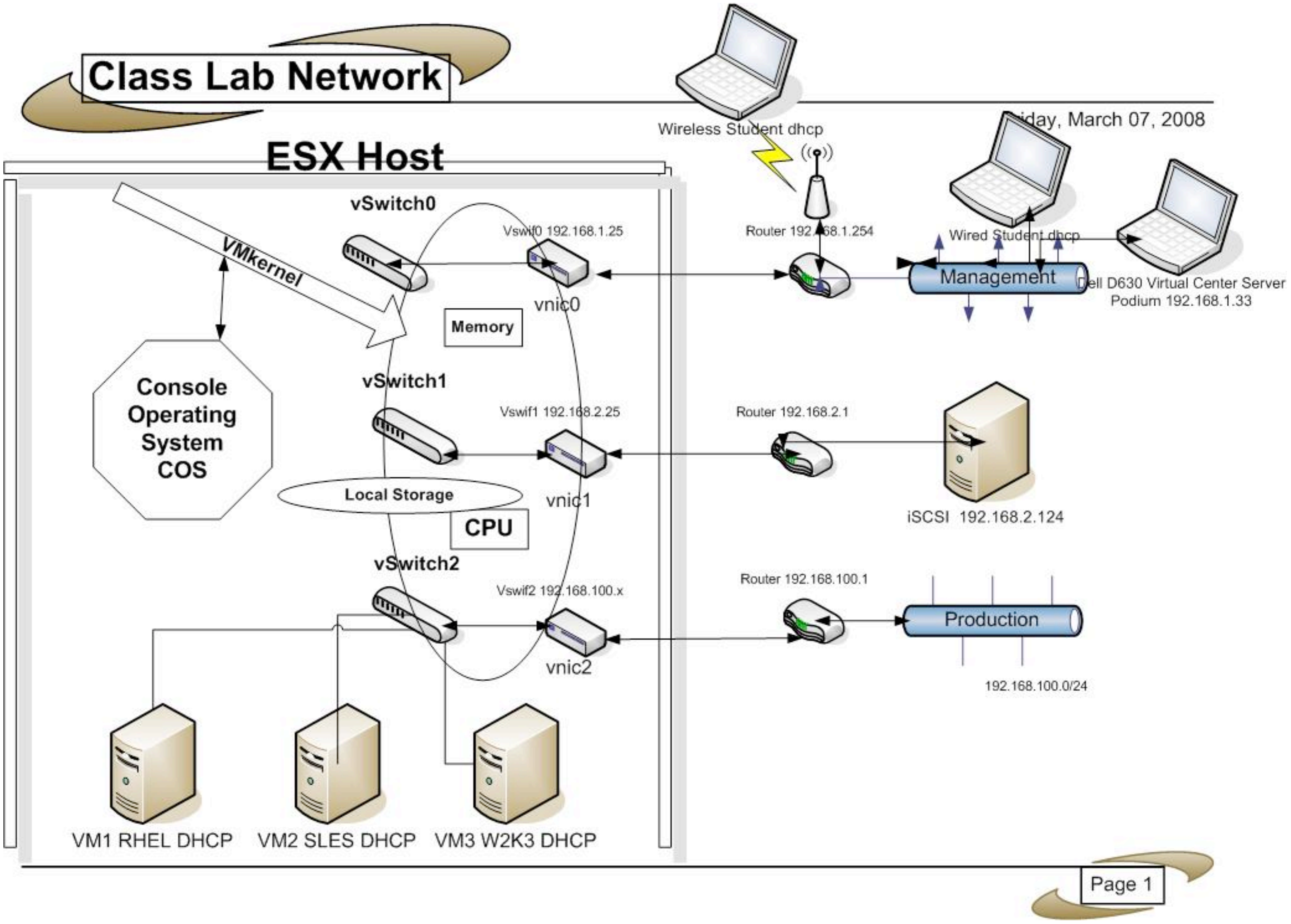
Why

- Hardware Consolidation resulting possibly in:
  - Hardware cost savings (less recently)
  - Data center floor space reduction (hosting costs)
  - Power Consumption ("green")
- Speed to Deployment (virtual servers= no AP, less logistics, cloning, templating…)
- Flexible Movement (vMotion, vStorageMotion)

Scope

- Virtualization Scope – ESX 3.5 servers hosting guests
- Not Included – (not
  because they are not
  important, only so
  much can be done
  in an
  ho
  u
  r) VDI, Hyper-V, Xen (Citrix & other variants), clusters
- Some topics expand beyond ESX (policy, process, procedure) if you are going to
  secur
  e
  an ESX environment you must think beyond the COS
- Some topics should be in scope but their

An Example


Class Lab Network
iday, March 07, 2008
ESX Host
VMkernel
vSwitch0
Vswif0 192.168.1.25
vnic0
Memory
Console Operating System COS
vSwitch1
Vswif1 192.168.2.25
vnic1
Local Storage
CPU
vSwitch2
Vswif2 192.168.100.x
vnic2
VM1 RHEL DHCP
VM2 SLES DHCP
VM3 W2K3 DHCP
Wireless Student dhcp
Router 192.168.1.254
Wired Student dhcp
Management
Dell D630 Virtual Center Server
Podium 192.168.1.33
Router 192.168.2.1
iSCSI 192.168.2.124
Router 192.168.100.1
Production
192.168.100.0/24
Page 1

II Risks

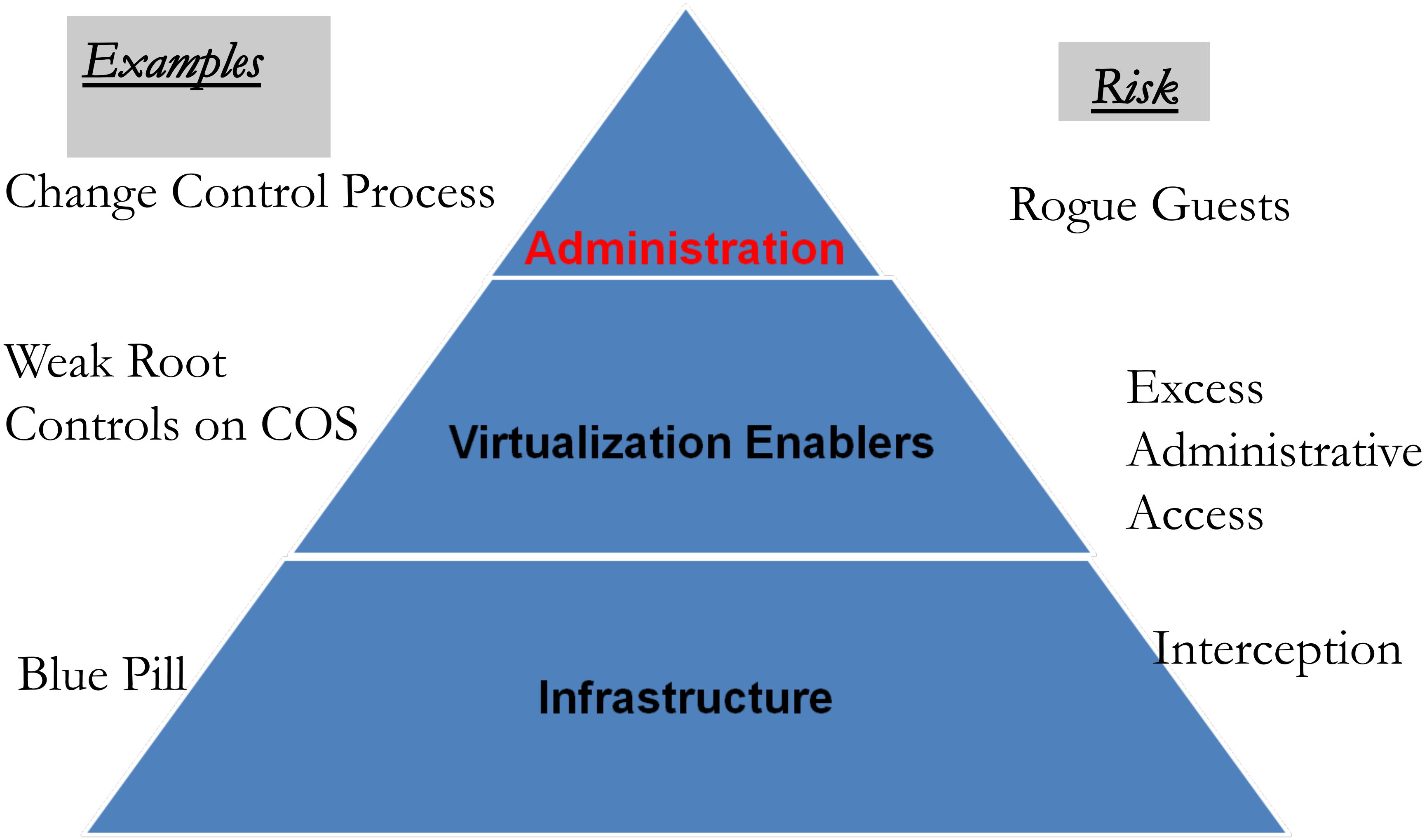
Overview

A List of Ten

Example of Each of the Ten

A Risk ~~not~~ on my List

Risk Overview



Examples

Risk

Administration

Change Control Process

Rogue Guests

Virtualization Enablers

Weak Root Controls on COS

Excess Administrative Access

Infrastructure

Blue Pill

Interception

10 (but not all)Risks of Virtualization

- Rogue (Sprawl), Possibly Misconfigured, Guests
- Network Segmentation
- Access Roles
- Infrastructure Integration
- Internal Skills

- Misconfigured Hosts
- Remote Access
- Single Point of Failure, (Additional Point of Failure)
- CPU (Blue Pill)
- Software Licensing
- (I lied, #11 = appliances)

Risk Examples

- Rogue (Sprawl), Possibly Misconfigured ,Guests – a VM is created for research purposes, disassociated with the host but not deleted from the VMFS, as time passes the greater the risk that this dormant guest will miss patches or configuration changes increases, and if this dormant out of compliance and the VM is re-associated with the host in production, the weakness may affect this or other VMs
- Misconfigured Hosts – changing default configurations (such as not allowing promiscuous mode on a virtual switch portgroup) , activating services such as FTP, or altering the rules associated with the Iptables firewall built into the ESX COS, could breach confidentiality and disrupt continuity

Risk Examples

- Network Segmentation – production and management traffic on the same segment coupled with weak root access control could result in elevated privileges and prohibit recovery, data traffic in the clear on an unauthorized network could impact confidentiality
- Remote Access – altering default configurations (leave default SSH configuration to prohibit direct root access), or failing to add (SSL certificates, banners) configuration items could lead to remote users gaining more access than intended

Risk Examples

- Access Controls– role descriptions in vCenter assigned to inappropriate users, lack of strong password controls over the COS root account, could lead to elevation when coupled with remote access weaknesses
- Single Point of Failure –without speedy recovery of the host, vCenter, License Server, database, continuity is diminished, given recent economic events the risk of disgruntled staff disrupting operations has increased

Risk Examples

- Infrastructure Integration – features based on certain hardware requirements may not function properly if hardware is not consistent/compatible (VMotion, but improvements have been made), particularly critical if your BCP relies on VMotion
- CPU – if an unauthorized malicious OS can run in a core or ring undetected by the second production OS, confidentiality could be compromised (Blue Pill)

Risk Examples

- Skills
  - if the networking configuration capabilities enabled by the hypervisor are in the hands of staff untrained in networkin

A Risk ~~Not~~ On My List - Guest Escape

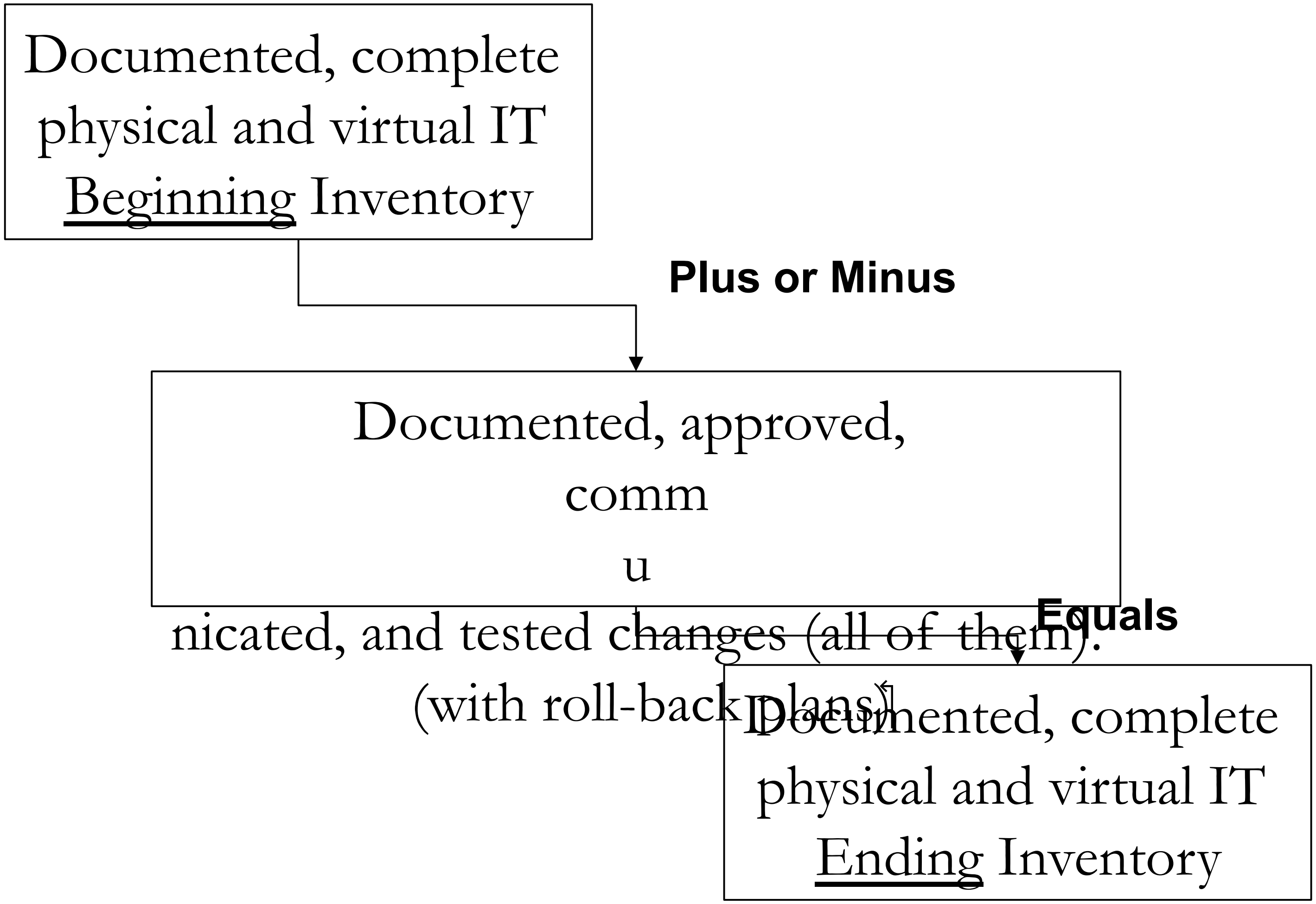
- while it is software controlling resource allocation, and software is subject to human error, ~~no documented case of one guest inappropriately accessing another~~

III Security Techniques & Conrols

Mantra

10 Risks, 10 Controls

Security Techniques – Overriding Mantra



Documented, complete physical and virtual IT Beginning Inventory

Plus or Minus

Documented, approved, communicated, and tested changes (all of them). (with roll-back plans)

Equals

Documented, complete physical and virtual IT Ending Inventory

Security Techniques & Controls

- Rogue (Sprawl), Possibly Misconfigured ,Guests –
  - A mature, documented , change control policy and process with authorization , testing, communication and roll-back requirements for every Guest creation, change,

Security Techniques & Controls

- Misconfigured Hosts –
  - Establish a build standard(s) appropriate for the intended use of the host and underlying guests starting with promulgated standards (CIS http://cisecurity.org , DISA, NSA, VMware White Papers) tailored to organizational needs and risk appetite
  - Establish independent (preferably automated) assessment processes to compare current configuration of the authorized inventory (see previous slide) to the adopted standard(s)
  - Risk rank guests and place them with other similarly ranked guests on a host

Security Techniques & Controls

- Network Segmentation –
  - Segregate production and management traffic on separate network segment
  - Segregate iSCSI clear traffic on separate network segment
  - Restrict access to VMotion and Storage VMotion (which is in the clear traffic)
  - Leave default vSwitch promiscuous mode in default “Reject" mode

Security Techniques & Controls

- Remote Access –
  - Leave the default setting off for root access to SSH
  - Alterations of the default ports allowed by the COS iptables rules should reconcile back to the authorized & documented change control process
  - Replace default SSL certificates

Security Techniques & Controls

- Access Controls– role descriptions in vCenter assigned to inappropriate users, vCenter roles are editable enforce change

Security Techniques & Controls

- Infrastructure Integration – features based on certain hardware requirements may not function properly if hardware is not consistent/compatible (VMotion, but improvements have been made EVC), particularly critical if your BCP relies on Vmotion, use devices on the vendors certification list
- CPU – if an *unauthorized* sniffing OS can run in a core or ring undetected by the second production OS, confidentiality could be compromised , physical security over hosts networking devices management consoles

Security Techniques & Controls

- Skills – if the networking configuration capabilities enabled by the hypervisor are in the hands of staff untrained in

IV Security Products

(for awareness, and re-use if IT or InfoSec has already purchased these)

Security Products - Overview

- In 2 Hours All I can do is Name-drop, you do the research in your environment/strategy/risk appetite
- Not a Bake-off, not a Best-of, I can only relate what worked in

Security Products – Network/Firewall

- Some Products have a Virtual Appliance (FW, IPS, Combined)
- Some Products have both Physical and Virtual Appliance
- Research = Stonegate, Reflex, Catbird, Apani (encryption)
- See Chris Hoff for key
  questi
  o
  ns http://rationalsecurity.typepad.com/blog/2008/04/the-four-horsem.html

  i. extra resources are consumed by the security v-appliance
  ii. moving a guest may detach it from the security v-appliance
  iii. may result in multiple v-appliances (firewall, IPS/IDS, AV, patch) from different vendors
     incr
     e
     asing administration complexity and exacerbating (i.) above
  iv. cost may not decrease because you may still
     hav
     e

Security Products – Configuration

- Most Products Compare Configuration Status Metrics to published standards (CIS, PCI, ...)
- Most products allow for custom built rules/measurements
- Some Products are agent-less some have an agent
- Some Products just report status (assessment focus)
- Some Products facilitate configuration changes when non-compliance is detected (administration focused)
  - ✓ Usually these products have multiple

Security Products – Backups

- (many,
  ma
  n
  y hours to explain this one, so I will name drop but not expand)
- VCB by VMware – patch this up to date VMSA-2008-0014
- Traditional backup agents inside each guest still work
- Snapshots, backing up raw storage rather than VMs, are options
- Research = vRangerPro, esXpress, NetApp, Veeam (backup)

Security Products – Other

- Monitoring –
  Veeam
  Monitor,
  Vkernel
  Optimization
  Pack, Vkernel
  SearchMyVM,
  S
  p
  lunk for logs, Astaro UTM, eG Monitor for VMware, vFogLight
- Hypervisor
  API
  Le
  v
  el – VMsafe in ESX 4 (Symantec, TrendMicro, CheckPoint, ISS)
- Virtual Appliance Level –
  BlueLane is now owned by VMware

Honorable Mention

Akorri Balance Point

BMC Performance Manager

CA ASM (Unicenter)

eG Innovations Enterprise Suite

Embotics V-Commander

HP Operations Orchestration

IBM Tivoli Monitoring for Virtual Servers

ManageIQ EVM Suite

Netuitive SI for Vmware

Quest vFoglight

Symantec Altiris

Tideway Foundation

Veeam (nworks)

SPI for Vmware

Veeam (nworks) Mgmt Pack for Microsoft MOM/SCOM

V Assessment/Audit Techniques

Overview Considerations
Tools to Gather Metrics:
a.) Free & Close to free
b.) Commercial

Assessment/Audit Tools for ESX

- Free Tools – great price, don’t scale well
- Some tools inventory the Virtual Center database, some tools enumerate raw data (like rogue guests [sprawl] whether assigned to a host or not)
- No one tool does everything

Assessment Process – Gathering Metrics

- Interviewing and Document Review for policies, standards, procedures, training
- Free Tools –
  - console CLI
  - **!CIS-CAT 2.1.0(for members) ESX 3.5 benchmark test script ~~draft~~,! [published, see speaker]**
  - VIToolkit & Powershell, (now called vSphere PowerCLI 4.0 U1)
  - esxcfg-xxx commands various (i.e. esxcfg-firewall –q)
  - esxcfg-info – dump of everything, load into ACL and search

Assessment Process – Gathering Metrics (continued)

- More Free Tools:
  - vmware-vim-cmd hostsvc/ = grep /net/info or grep /storage/info (careful, many of these commands change settings, stick with the ones with the word ‘info’)
  - Configuresoft (Ionix) ComplianceChecker, Tripwire configcheck,
  - From VMware - VI API, VIX API (allows files xfer from guest) , Perl API, CIM API (risks of rolling your own = script storage security, stored passwords, change management, version management)

Assessment Process – Gathering Metrics (continued)

- More Free Tools:
  - Bastille – remember to run in the –assess mode, not the harden mode
  - DISA – SRR (security readiness review evaluation script) watch these, they may harden if not run correctly
  - LSAT – works, but the MD5 process will try to analyze the very large vmdk disk files, this is time consuming and could crash running guests (ctrl + c to exit)

Assessment Process –
Gathering Metrics (continued)

- Existing Management
  Tools -
  (v
  C
  enter, Update Mgr, Lifecycle Mgr, Veeam & others)

- Security Tools (Reflex, Catbird, ~~BlueLane~~ & others)

- Commercial
  To
  o
  ls – (Configursoft [Ionix], Ecora, Tripwire, & others)
  - Hy-Trust - won a bunch at
    VMw
    o

VI Example – Look for Sprawl

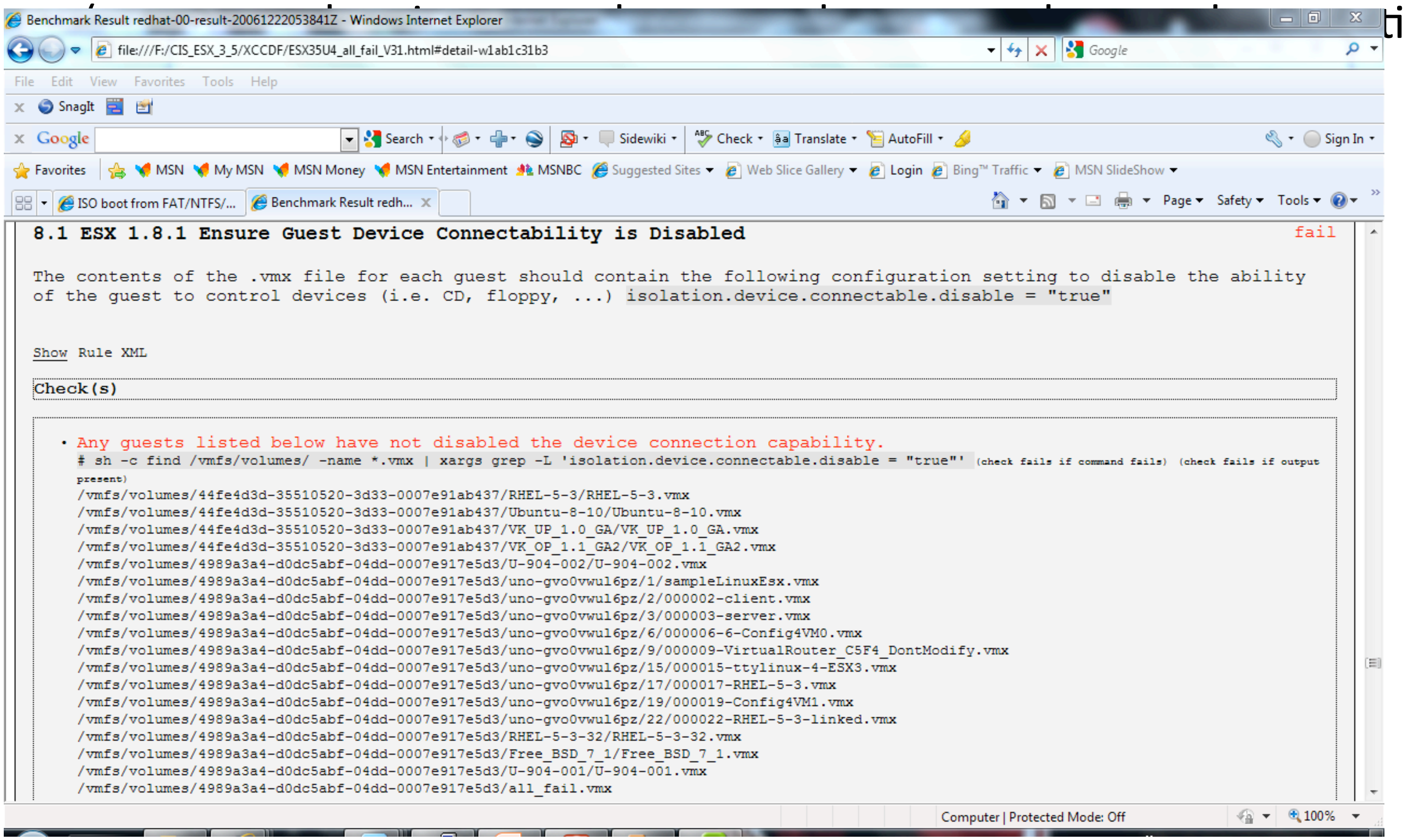
Example – Sprawl

- Free Tools – Command Line Interface (CLI)
  ls –lR /vmfs/volumes/* | grep vmdk (or vmx)
- Or the ‘find’ command (does not follow sym links)

```
•   -rwxrwxrwx    1 root     root     4831838208 Jul  7  2007 BLVS-flat.vmdk
•   -rwxrwxrwx    1 root     root            331 Jul  7  2007 BLVS.vmdk
•   -rwxrwxrwx    1 root     root     8589934592 Jul  7  2007 BLVSMgr-flat.vmdk
•   -rwxrwxrwx    1 root     root            336 Jul  7  2007 BLVSMgr.vmdk
•   -rw-------    1 root     root     872415232 Sep 23 10:10 Reflex-VSA-Template-flat.vmdk
•   -rw-------    1 root     root           480 Sep 23 10:10 Reflex-VSA-Template.vmdk
•   -rw-------    1 root     root     4294967296 Oct  8 11:37 Reflex-vsc-flat.vmdk
•   -rw-------    1 root     root           499 Oct  8 00:50 Reflex-vsc.vmdk
•   -rw-------    1 root     root     6442450944 Sep 29 01:59 RHEL-4-4-ES-flat.vmdk
•   -rw-------    1 root     root           339 Sep 29 01:57 RHEL-4-4-ES.vmdk
•   -rw-------    1 root     root     16791552 Mar 17  2008 SLES10-SP1-000001-delta.vmdk
•   -rw-------    1 root     root           252 Mar 17  2008 SLES10-SP1-000001.vmdk
•   -rw-------    1 root     root     6442450944 Mar 17  2008 SLES10-SP1-flat.vmdk
•   -rw-------    1 root     root           338 Mar 17  2008 SLES10-SP1.vmdk
•   -rw-------    1 root     root     4294967296 Oct  5  2007 Ubuntu-7-04-server-flat.vmdk
•   -rw-------    1 root     root           345 Oct  5  2007 Ubuntu-7-04-server.vmdk
•   -rw-------    1 root     root     3221225472 Aug 14  2007 Vkernel-B3_1-flat.vmdk
•   -rw-------    1 root     root           440 Aug 14  2007 Vkernel-B3_1.vmdk
```

Example – Rogue Guests (cont)

- Free Tools CIS-CAT 2.1.1 (~~when~~ Released 2/2010! ESX benchmark test xccdf xml file is released) will list VMs with non compliant vmx config file
  s
  tion)



Benchmark Result redhat-00-result-20061222053841Z - Windows Internet Explorer
file:///F:/CIS_ESX_3_5/XCCDF/ESX35U4_all_fail_V31.html#detail-w1ab1c31b3
Google
File Edit View Favorites Tools Help
SnagIt
Google Search Sidewiki Check Translate AutoFill Sign In
Favorites MSN My MSN MSN Money MSN Entertainment MSNBC Suggested Sites Web Slice Gallery Login Bing™ Traffic MSN SlideShow
ISO boot from FAT/NTFS/... Benchmark Result redh...
Page Safety Tools
Computer | Protected Mode: Off
100%

8.1 ESX 1.8.1 Ensure Guest Device Connectability is Disabled fail

The contents of the .vmx file for each guest should contain the following configuration setting to disable the ability of the guest to control devices (i.e. CD, floppy, ...) `isolation.device.connectable.disable = "true"`

Show Rule XML

Check(s)

- Any guests listed below have not disabled the device connection capability.

```
# sh -c find /vmfs/volumes/ -name *.vmx | xargs grep -L 'isolation.device.connectable.disable = "true"' (check fails if command fails) (check fails if output present)
/vmfs/volumes/44fe4d3d-35510520-3d33-0007e91ab437/RHEL-5-3/RHEL-5-3.vmx
/vmfs/volumes/44fe4d3d-35510520-3d33-0007e91ab437/Ubuntu-8-10/Ubuntu-8-10.vmx
/vmfs/volumes/44fe4d3d-35510520-3d33-0007e91ab437/VK_UP_1.0_GA/VK_UP_1.0_GA.vmx
/vmfs/volumes/44fe4d3d-35510520-3d33-0007e91ab437/VK_OP_1.1_GA2/VK_OP_1.1_GA2.vmx
/vmfs/volumes/4989a3a4-d0dc5abf-04dd-0007e917e5d3/U-904-002/U-904-002.vmx
/vmfs/volumes/4989a3a4-d0dc5abf-04dd-0007e917e5d3/uno-gvo0vwul6pz/1/sampleLinuxEsx.vmx
/vmfs/volumes/4989a3a4-d0dc5abf-04dd-0007e917e5d3/uno-gvo0vwul6pz/2/000002-client.vmx
/vmfs/volumes/4989a3a4-d0dc5abf-04dd-0007e917e5d3/uno-gvo0vwul6pz/3/000003-server.vmx
/vmfs/volumes/4989a3a4-d0dc5abf-04dd-0007e917e5d3/uno-gvo0vwul6pz/6/000006-6-Config4VM0.vmx
/vmfs/volumes/4989a3a4-d0dc5abf-04dd-0007e917e5d3/uno-gvo0vwul6pz/9/000009-VirtualRouter_C5F4_DontModify.vmx
/vmfs/volumes/4989a3a4-d0dc5abf-04dd-0007e917e5d3/uno-gvo0vwul6pz/15/000015-ttylinux-4-ESX3.vmx
/vmfs/volumes/4989a3a4-d0dc5abf-04dd-0007e917e5d3/uno-gvo0vwul6pz/17/000017-RHEL-5-3.vmx
/vmfs/volumes/4989a3a4-d0dc5abf-04dd-0007e917e5d3/uno-gvo0vwul6pz/19/000019-Config4VM1.vmx
/vmfs/volumes/4989a3a4-d0dc5abf-04dd-0007e917e5d3/uno-gvo0vwul6pz/22/000022-RHEL-5-3-linked.vmx
/vmfs/volumes/4989a3a4-d0dc5abf-04dd-0007e917e5d3/RHEL-5-3-32/RHEL-5-3-32.vmx
/vmfs/volumes/4989a3a4-d0dc5abf-04dd-0007e917e5d3/Free_BSD_7_1/Free_BSD_7_1.vmx
/vmfs/volumes/4989a3a4-d0dc5abf-04dd-0007e917e5d3/U-904-001/U-904-001.vmx
/vmfs/volumes/4989a3a4-d0dc5abf-04dd-0007e917e5d3/all_fail.vmx
```

Example – Rogue Guests (cont)

- Free Tools -VI Tools for Windows & Powershell now named vSphere PowerCLI 4.0 (partial script)

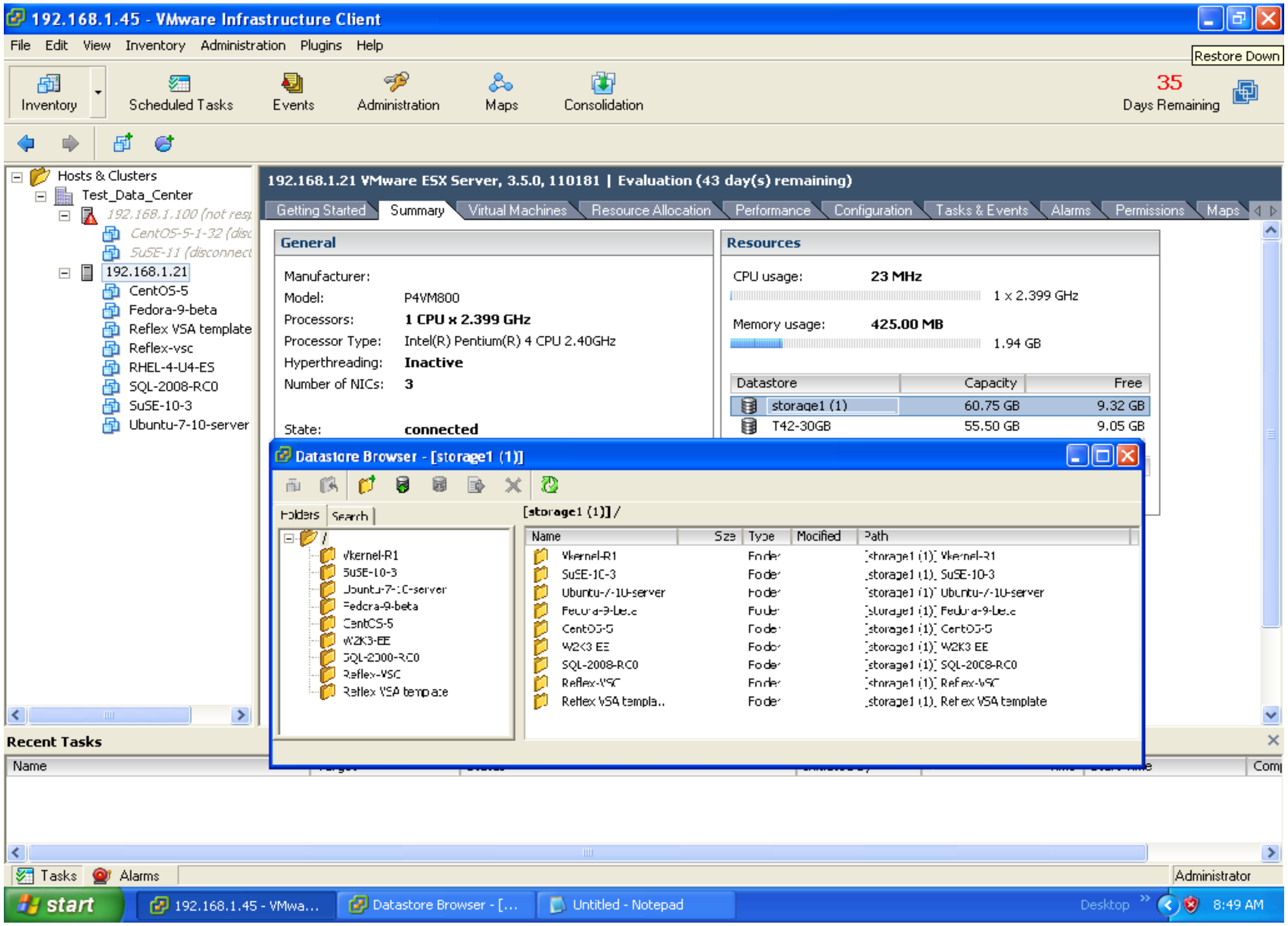
```
# academic only, don't do the next line
$VC = Connect-VIServer 192.168.1.21 -User XXXXXX -Password XXXXXX
#
$VMs = Get-VM | format-table -property name
$Datastores = Get-Datastore | Format-Table -property Name
$VMXlist = " "
$i = 1; while ($i -le $Datastores.length-4)
{
        $Datastore = Read-Host "Enter Data Store Name, like storage1*  from the list above "

        Get-Datastore $Datastore | New-DatastoreDrive -name dstemp
        cd dstemp:
        get-childitem -recurse -include *.vmx | format-table -property name >> c:\vmxlist
        cd c:\
        Remove-PSDrive dstemp
        $i +=1
}
```

Then compare the two files (VM list and vmx list) with diff, ACL, or manually

Example – Sprawl

- Existing Management Tools - Virtual Center



192.168.1.45 - VMware Infrastructure Client

192.168.1.21 VMware ESX Server, 3.5.0, 110181 | Evaluation (43 day(s) remaining)

General

Manufacturer:	
Model:	P4VM800
Processors:	1 CPU x 2.399 GHz
Processor Type:	Intel(R) Pentium(R) 4 CPU 2.40GHz
Hyperthreading:	Inactive
Number of NICs:	3
State:	connected

Resources

CPU usage: 23 MHz — 1 x 2.399 GHz

Memory usage: 425.00 MB — 1.94 GB

Datastore	Capacity	Free
storage1 (1)	60.75 GB	9.32 GB
T42-30GB	55.50 GB	9.05 GB

Datastore Browser - [storage1 (1)]

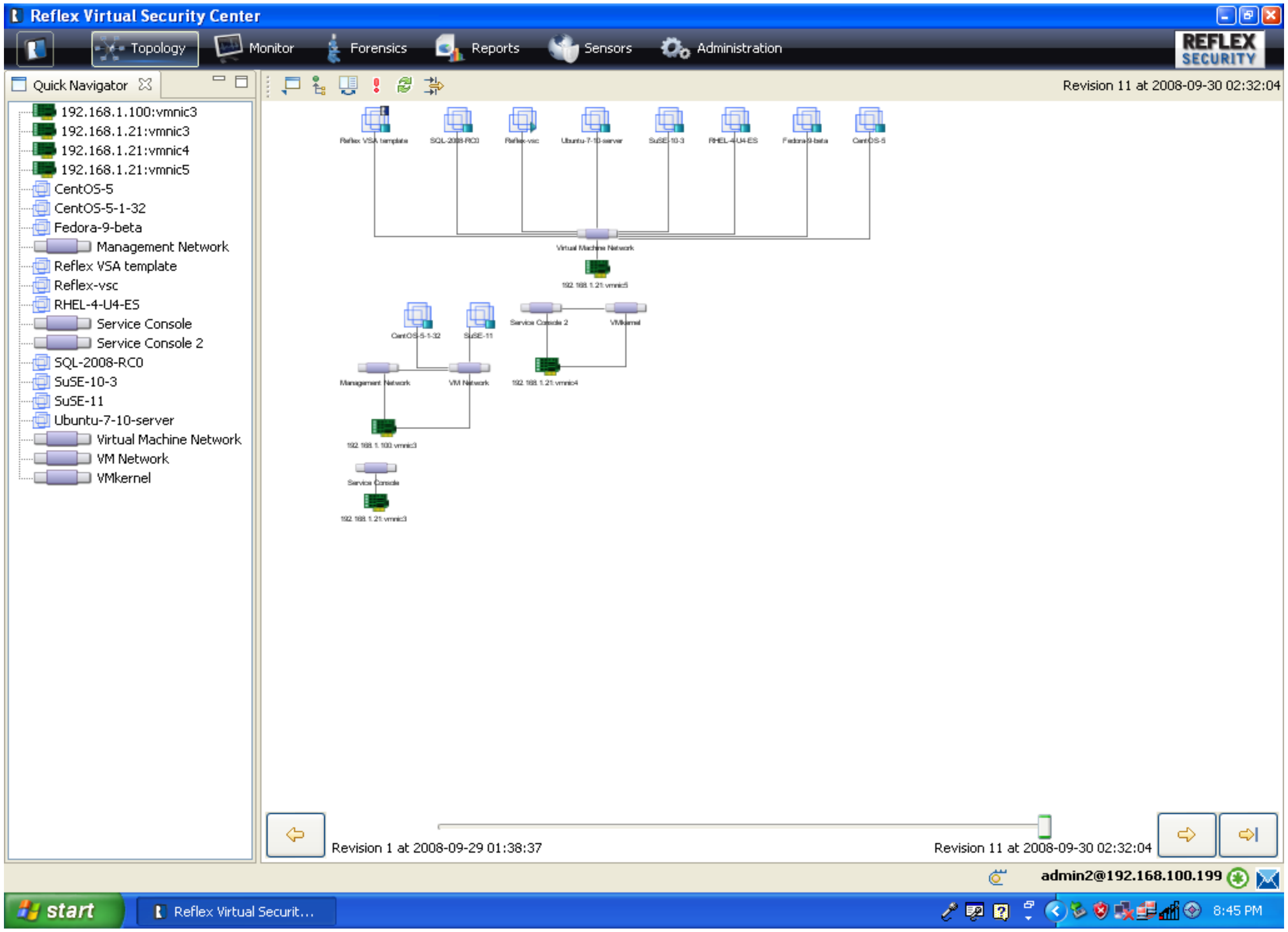
[storage1 (1)] /

- /
  - Vkernel-R1
  - SuSE-10-3
  - Ubuntu-7-10-server
  - Fedora-9-beta
  - CentOS-5
  - W2K3-EE
  - SQL-2008-RC0
  - Reflex-VSC
  - Reflex VSA template

Name	Size	Type	Modified	Path
Vkernel-R1		Folder		[storage1 (1)] Vkernel-R1
SuSE-10-3		Folder		[storage1 (1)] SuSE-10-3
Ubuntu-7-10-server		Folder		[storage1 (1)] Ubuntu-7-10-server
Fedora-9-beta		Folder		[storage1 (1)] Fedora-9-beta
CentOS-5		Folder		[storage1 (1)] CentOS-5
W2K3 EE		Folder		[storage1 (1)] W2K3 EE
SQL-2008-RC0		Folder		[storage1 (1)] SQL-2008-RC0
Reflex-VSC		Folder		[storage1 (1)] Reflex-VSC
Reflex VSA templa...		Folder		[storage1 (1)] Reflex VSA template

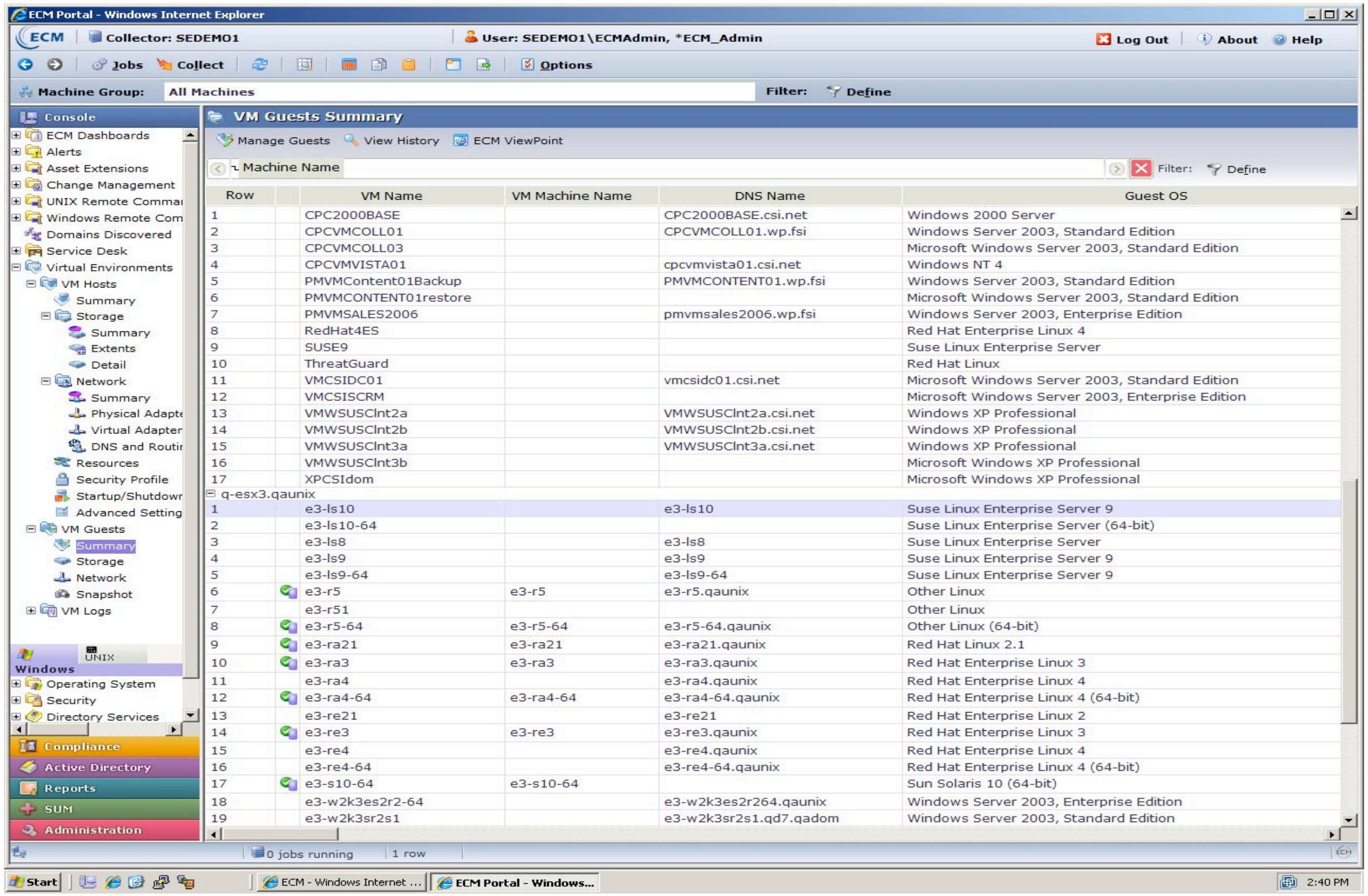
Example – Sprawl(cont)

- Third Party Security Tools – Reflex



Example – Sprawl (cont)

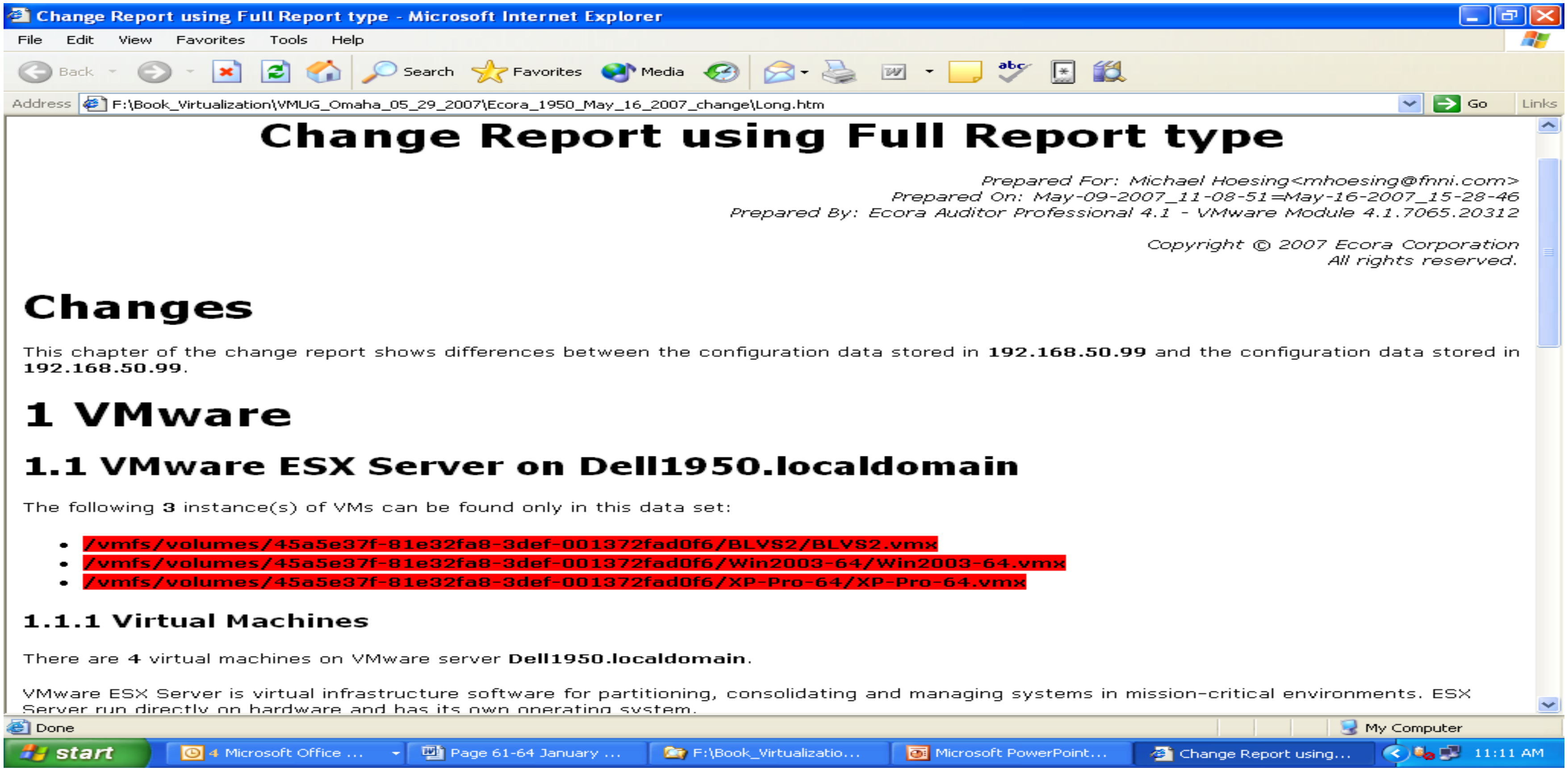
- Commercial Tools – Configuresoft (Ionix)



Row		VM Name	VM Machine Name	DNS Name	Guest OS
1		CPC2000BASE		CPC2000BASE.csi.net	Windows 2000 Server
2		CPCVMCOLL01		CPCVMCOLL01.wp.fsi	Windows Server 2003, Standard Edition
3		CPCVMCOLL03			Microsoft Windows Server 2003, Standard Edition
4		CPCVMVISTA01		cpcvmvista01.csi.net	Windows NT 4
5		PMVMContent01Backup		PMVMCONTENT01.wp.fsi	Windows Server 2003, Standard Edition
6		PMVMCONTENT01restore			Microsoft Windows Server 2003, Standard Edition
7		PMVMSALES2006		pmvmsales2006.wp.fsi	Windows Server 2003, Enterprise Edition
8		RedHat4ES			Red Hat Enterprise Linux 4
9		SUSE9			Suse Linux Enterprise Server
10		ThreatGuard			Red Hat Linux
11		VMCSIDC01		vmcsidc01.csi.net	Microsoft Windows Server 2003, Standard Edition
12		VMCSISCRM			Microsoft Windows Server 2003, Enterprise Edition
13		VMWSUSClnt2a		VMWSUSClnt2a.csi.net	Windows XP Professional
14		VMWSUSClnt2b		VMWSUSClnt2b.csi.net	Windows XP Professional
15		VMWSUSClnt3a		VMWSUSClnt3a.csi.net	Windows XP Professional
16		VMWSUSClnt3b			Microsoft Windows XP Professional
17		XPCSIdom			Microsoft Windows XP Professional
⊟ q-esx3.qaunix					
1		e3-ls10		e3-ls10	Suse Linux Enterprise Server 9
2		e3-ls10-64			Suse Linux Enterprise Server (64-bit)
3		e3-ls8		e3-ls8	Suse Linux Enterprise Server
4		e3-ls9		e3-ls9	Suse Linux Enterprise Server 9
5		e3-ls9-64		e3-ls9-64	Suse Linux Enterprise Server 9
6	✓	e3-r5	e3-r5	e3-r5.qaunix	Other Linux
7		e3-r51			Other Linux
8	✓	e3-r5-64	e3-r5-64	e3-r5-64.qaunix	Other Linux (64-bit)
9	✓	e3-ra21	e3-ra21	e3-ra21.qaunix	Red Hat Linux 2.1
10	✓	e3-ra3	e3-ra3	e3-ra3.qaunix	Red Hat Enterprise Linux 3
11		e3-ra4		e3-ra4.qaunix	Red Hat Enterprise Linux 4
12	✓	e3-ra4-64	e3-ra4-64	e3-ra4-64.qaunix	Red Hat Enterprise Linux 4 (64-bit)
13		e3-re21		e3-re21	Red Hat Enterprise Linux 2
14	✓	e3-re3	e3-re3	e3-re3.qaunix	Red Hat Enterprise Linux 3
15		e3-re4		e3-re4.qaunix	Red Hat Enterprise Linux 4
16		e3-re4-64		e3-re4-64.qaunix	Red Hat Enterprise Linux 4 (64-bit)
17	✓	e3-s10-64	e3-s10-64		Sun Solaris 10 (64-bit)
18		e3-w2k3es2r2-64		e3-w2k3es2r264.qaunix	Windows Server 2003, Enterprise Edition
19		e3-w2k3sr2s1		e3-w2k3sr2s1.qd7.qadom	Windows Server 2003, Standard Edition

Example – Sprawl (cont)

- Commercial Assessment Tools – Ecora



Change Report using Full Report type

Prepared For: Michael Hoesing<mhoesing@fnni.com>
Prepared On: May-09-2007_11-08-51=May-16-2007_15-28-46
Prepared By: Ecora Auditor Professional 4.1 - VMware Module 4.1.7065.20312

Copyright © 2007 Ecora Corporation
All rights reserved.

Changes

This chapter of the change report shows differences between the configuration data stored in **192.168.50.99** and the configuration data stored in **192.168.50.99**.

1 VMware

1.1 VMware ESX Server on Dell1950.localdomain

The following **3** instance(s) of VMs can be found only in this data set:

- /vmfs/volumes/45a5e37f-81e32fa8-3def-001372fad0f6/BLVS2/BLVS2.vmx
- /vmfs/volumes/45a5e37f-81e32fa8-3def-001372fad0f6/Win2003-64/Win2003-64.vmx
- /vmfs/volumes/45a5e37f-81e32fa8-3def-001372fad0f6/XP-Pro-64/XP-Pro-64.vmx

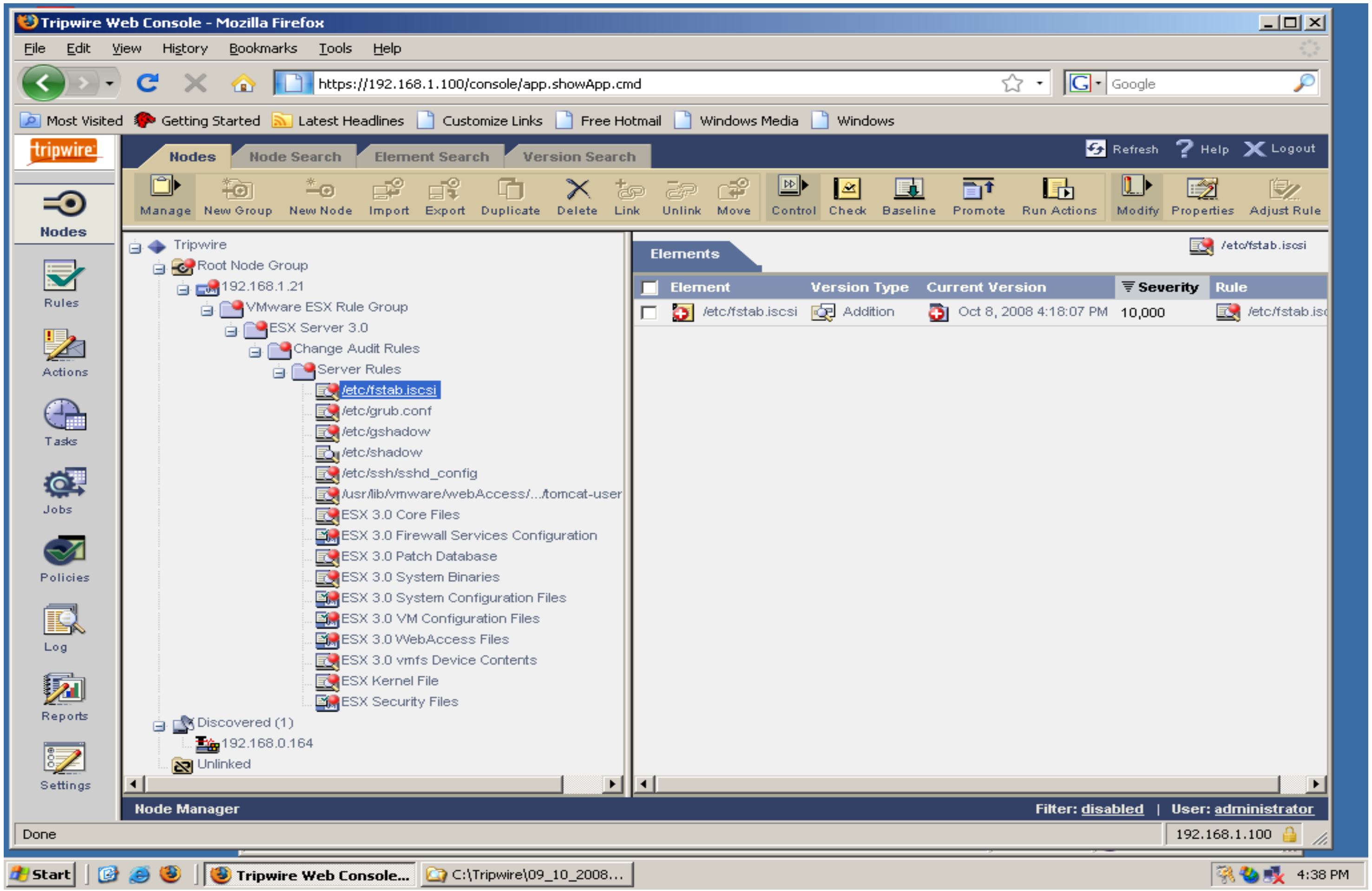
1.1.1 Virtual Machines

There are **4** virtual machines on VMware server **Dell1950.localdomain**.

VMware ESX Server is virtual infrastructure software for partitioning, consolidating and managing systems in mission-critical environments. ESX Server run directly on hardware and has its own operating system.

Example – Sprawl (cont)

- Commercial Assessment Tools – Tripwire


Tripwire Web Console - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google
Most Visited Getting Started Latest Headlines Customize Links Free Hotmail Windows Media Windows
tripwire
Nodes Node Search Element Search Version Search
Refresh Help Logout
Manage New Group New Node Import Export Duplicate Delete Link Unlink Move Control Check Baseline Promote Run Actions Modify Properties Adjust Rule
Nodes
Rules
Actions
Tasks
Jobs
Policies
Log
Reports
Settings
Tripwire
Root Node Group
192.168.1.21
VMware ESX Rule Group
ESX Server 3.0
Change Audit Rules
Server Rules
/etc/fstab.iscsi
/etc/grub.conf
/etc/gshadow
/etc/shadow
/etc/ssh/sshd_config
/usr/lib/vmware/webAccess/.../tomcat-user
ESX 3.0 Core Files
ESX 3.0 Firewall Services Configuration
ESX 3.0 Patch Database
ESX 3.0 System Binaries
ESX 3.0 System Configuration Files
ESX 3.0 VM Configuration Files
ESX 3.0 WebAccess Files
ESX 3.0 vmfs Device Contents
ESX Kernel File
ESX Security Files
Discovered (1)
192.168.0.164
Unlinked
Elements
/etc/fstab.iscsi
Node Manager
Start
Tripwire Web Console...
C:\Tripwire\09_10_2008...
4:38 PM

https://192.168.1.100/console/app.showApp.cmd

□	Element	Version Type	Current Version	Severity	Rule
□	/etc/fstab.iscsi	Addition	Oct 8, 2008 4:18:07 PM	10,000	/etc/fstab.is

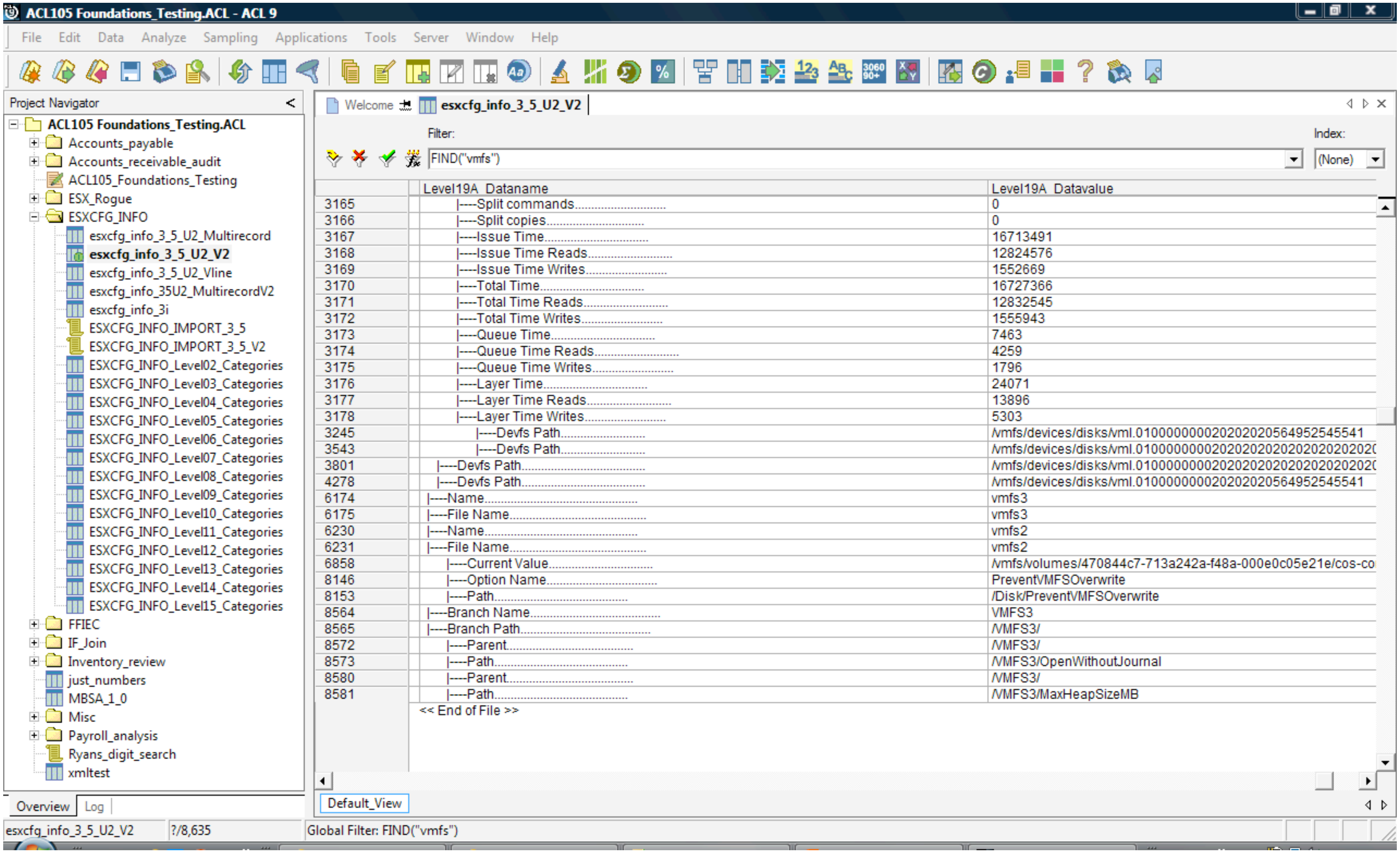
Filter: disabled | User: administrator

Done

192.168.1.100

Example – Sprawl (cont)

Combo: Commercial & Free Tools – esxcfg-info read into ACL


ACL105 Foundations_Testing.ACL - ACL 9
File Edit Data Analyze Sampling Applications Tools Server Window Help
Project Navigator
Welcome
esxcfg_info_3_5_U2_V2
Filter:
Index:
(None)
Overview
Log
Default_View

```
ACL105 Foundations_Testing.ACL
  Accounts_payable
  Accounts_receivable_audit
  ACL105_Foundations_Testing
  ESX_Rogue
  ESXCFG_INFO
    esxcfg_info_3_5_U2_Multirecord
    esxcfg_info_3_5_U2_V2
    esxcfg_info_3_5_U2_Vline
    esxcfg_info_35U2_MultirecordV2
    esxcfg_info_3i
    ESXCFG_INFO_IMPORT_3_5
    ESXCFG_INFO_IMPORT_3_5_V2
    ESXCFG_INFO_Level02_Categories
    ESXCFG_INFO_Level03_Categories
    ESXCFG_INFO_Level04_Categories
    ESXCFG_INFO_Level05_Categories
    ESXCFG_INFO_Level06_Categories
    ESXCFG_INFO_Level07_Categories
    ESXCFG_INFO_Level08_Categories
    ESXCFG_INFO_Level09_Categories
    ESXCFG_INFO_Level10_Categories
    ESXCFG_INFO_Level11_Categories
    ESXCFG_INFO_Level12_Categories
    ESXCFG_INFO_Level13_Categories
    ESXCFG_INFO_Level14_Categories
    ESXCFG_INFO_Level15_Categories
  FFIEC
  IF_Join
  Inventory_review
  just_numbers
  MBSA_1_0
  Misc
  Payroll_analysis
  Ryans_digit_search
  xmltest
```

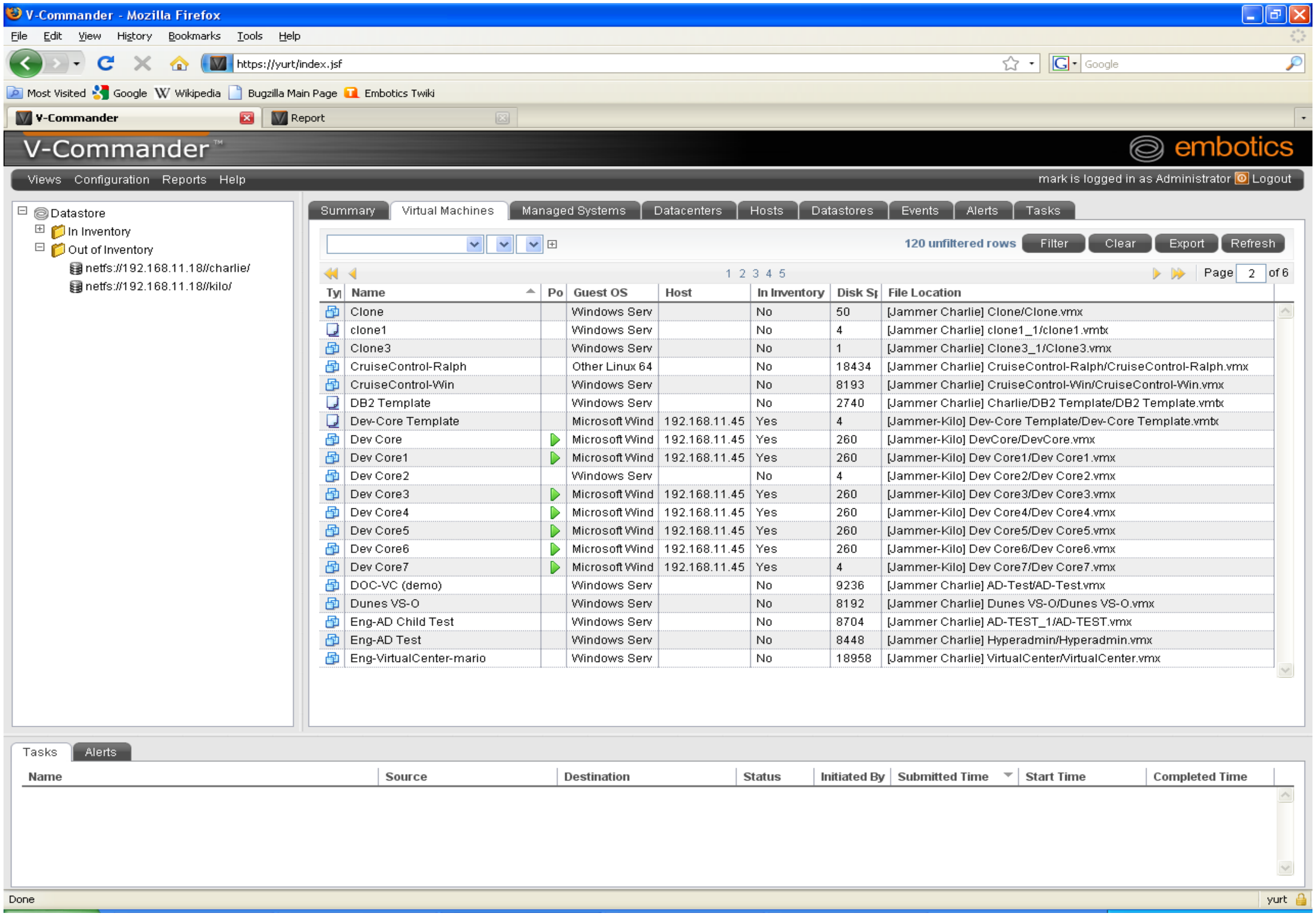
Filter: FIND("vmfs")

```
        Level19A  Dataname                                   Level19A  Datavalue
3165              |----Split commands..........................  0
3166              |----Split copies............................  0
3167              |----Issue Time..............................  16713491
3168              |----Issue Time Reads........................  12824576
3169              |----Issue Time Writes.......................  1552669
3170              |----Total Time..............................  16727366
3171              |----Total Time Reads........................  12832545
3172              |----Total Time Writes.......................  1555943
3173              |----Queue Time..............................  7463
3174              |----Queue Time Reads........................  4259
3175              |----Queue Time Writes.......................  1796
3176              |----Layer Time..............................  24071
3177              |----Layer Time Reads........................  13896
3178              |----Layer Time Writes.......................  5303
3245                  |----Devfs Path..........................  /vmfs/devices/disks/vml.010000000020202020564952545541
3543                  |----Devfs Path..........................  /vmfs/devices/disks/vml.0100000000202020202020202020202
3801          |----Devfs Path..................................  /vmfs/devices/disks/vml.0100000000202020202020202020202
4278          |----Devfs Path..................................  /vmfs/devices/disks/vml.010000000020202020564952545541
6174        |----Name..........................................  vmfs3
6175        |----File Name.....................................  vmfs3
6230        |----Name..........................................  vmfs2
6231        |----File Name.....................................  vmfs2
6858            |----Current Value.............................  /vmfs/volumes/470844c7-713a242a-f48a-000e0c05e21e/cos-co
8146            |----Option Name...............................  PreventVMFSOverwrite
8153            |----Path......................................  /Disk/PreventVMFSOverwrite
8564        |----Branch Name...................................  VMFS3
8565        |----Branch Path...................................  /VMFS3/
8572            |----Parent....................................  /VMFS3/
8573            |----Path......................................  /VMFS3/OpenWithoutJournal
8580            |----Parent....................................  /VMFS3/
8581            |----Path......................................  /VMFS3/MaxHeapSizeMB
        << End of File >>
```

esxcfg_info_3_5_U2_V2 | ?/8,635 | Global Filter: FIND("vmfs")

Example – Sprawl (cont)

- Commercial Assessment Tools : V-Commander by Embotics



V-Commander - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://yurt/index.jsf

Most Visited · Google · Wikipedia · Bugzilla Main Page · Embotics Twiki

V-Commander · Report

V-Commander™ embotics

Views Configuration Reports Help

mark is logged in as Administrator Logout

Datastore
- In Inventory
- Out of Inventory
  - netfs://192.168.11.18//charlie/
  - netfs://192.168.11.18//kilo/

Summary · Virtual Machines · Managed Systems · Datacenters · Hosts · Datastores · Events · Alerts · Tasks

120 unfiltered rows · Filter · Clear · Export · Refresh

1 2 3 4 5 · Page 2 of 6

Ty	Name	Po	Guest OS	Host	In Inventory	Disk Sp	File Location
	Clone		Windows Serv		No	50	[Jammer Charlie] Clone/Clone.vmx
	clone1		Windows Serv		No	4	[Jammer Charlie] clone1_1/clone1.vmtx
	Clone3		Windows Serv		No	1	[Jammer Charlie] Clone3_1/Clone3.vmx
	CruiseControl-Ralph		Other Linux 64		No	18434	[Jammer Charlie] CruiseControl-Ralph/CruiseControl-Ralph.vmx
	CruiseControl-Win		Windows Serv		No	8193	[Jammer Charlie] CruiseControl-Win/CruiseControl-Win.vmx
	DB2 Template		Windows Serv		No	2740	[Jammer Charlie] Charlie/DB2 Template/DB2 Template.vmtx
	Dev-Core Template		Microsoft Wind	192.168.11.45	Yes	4	[Jammer-Kilo] Dev-Core Template/Dev-Core Template.vmtx
	Dev Core	▶	Microsoft Wind	192.168.11.45	Yes	260	[Jammer-Kilo] DevCore/DevCore.vmx
	Dev Core1	▶	Microsoft Wind	192.168.11.45	Yes	260	[Jammer-Kilo] Dev Core1/Dev Core1.vmx
	Dev Core2		Windows Serv		No	4	[Jammer-Kilo] Dev Core2/Dev Core2.vmx
	Dev Core3	▶	Microsoft Wind	192.168.11.45	Yes	260	[Jammer-Kilo] Dev Core3/Dev Core3.vmx
	Dev Core4	▶	Microsoft Wind	192.168.11.45	Yes	260	[Jammer-Kilo] Dev Core4/Dev Core4.vmx
	Dev Core5	▶	Microsoft Wind	192.168.11.45	Yes	260	[Jammer-Kilo] Dev Core5/Dev Core5.vmx
	Dev Core6	▶	Microsoft Wind	192.168.11.45	Yes	260	[Jammer-Kilo] Dev Core6/Dev Core6.vmx
	Dev Core7	▶	Microsoft Wind	192.168.11.45	Yes	4	[Jammer-Kilo] Dev Core7/Dev Core7.vmx
	DOC-VC (demo)		Windows Serv		No	9236	[Jammer Charlie] AD-Test/AD-Test.vmx
	Dunes VS-O		Windows Serv		No	8192	[Jammer Charlie] Dunes VS-O/Dunes VS-O.vmx
	Eng-AD Child Test		Windows Serv		No	8704	[Jammer Charlie] AD-TEST_1/AD-TEST.vmx
	Eng-AD Test		Windows Serv		No	8448	[Jammer Charlie] Hyperadmin/Hyperadmin.vmx
	Eng-VirtualCenter-mario		Windows Serv		No	18958	[Jammer Charlie] VirtualCenter/VirtualCenter.vmx

Tasks · Alerts

Name	Source	Destination	Status	Initiated By	Submitted Time	Start Time	Completed Time

Done · yurt

Assessment/Audit Techniques

- One more Rogue Guest Tool – vminformer
- 61 questions an auditor/assessor could ask **http://members.cox.net/m-d-hoesing/ESX_Audit_Program_3_5.doc** (there are more ideas, have my class at your local iSACA chapter, one and 2 day versions are available)

VII vSphere aka ESX 4.0

What is NOT New
What is New
What is Different

vSphere - What is Not New

- This release added new functionality to 3.5, and did not substantially alter the core vmkernel and console operating system (but see what's different slide)
- Many of the assessment/management/security tools in the prior slides work well with vSphere
- Knowledge from 3.5 transfers to 4.0
- Risk are similar (although a few more)

vSphere - What is New (Added)

- Host Profiles – can create & copy Host Golden Image
- vCenter Cluster – can group mgmt consoles
- vShields Zones – group hosts by security class
- VMsafe – enables security products (i.e. A-V) to sit on the host while protecting guests
- Thin Disks – expand as needed
- Linked Clones – similar VM’s share a base set of bytes
- Distributed Virtual Networking (DVN) – a virtual switch that serves many ESX hosts

vSphere - What is New (Added) (cont)

- Fault Tolerance – mirroring (HA is failover, DRS is processing load balancing, DPM is kilowatt load balancing)
- Pluggable Storage Arrays – multi pathing
- VM Direct Path – guests directly accessing hardware
- VMCI – messaging between VM’s and between VM’s and their ESX host

vSphere - What is New (Added) (cont)

- vOrchestrator – workflow
- Hot add memory & networking
- DR Data Recovery – backup and recovery
- Mutual CHAP – 2 way authentication

- Not yet – vProbes
- Not yet - ConfigControl

vSphere - What is Different

- C Compiler is gone LSAT will not install (but Java, make, rpm still present)
- No Web access direct to the ESX host (use VI client)
- Boot services changes:
  - pegasus to sfcbd-watchdog
  - added = slpd service location protocol, nfs (rpcgssd and rpcidmapd), lm_sensors, ip6tables, restorecond from SE Linux
- Firewall config file has many active lines regarding rule change saving /etc/sysconfig/iptables.config
- COS kernel is now 2.6

VIII Clouds

(gotta cover this or the young-uns will think I am out of touch)

Clouds - Background

- Usually deployed using virtualization
- Third party hosts the physical hardware (there is always hardware if you dig deep enough)
- Third party allocates resources dynamically based on your (and your neighbor's) needs
- The dynamic movement of your programs and data may span several data centers
- You are sharing hardware with an (unknown) neighbor
- Popular as a cost saving method
- Sensible when hardware needs are either temporary or unpredictable (testing environments)

Clouds – Risks

- Where is your data/applications/operating system" and is that location(s) safe? (many can't tell you)
- Who is your neighbor in the Cloud, and how segregated are they? And how safe are they?
- Is exit easy? Many cloud providers use proprietary management tools to create, dynamically allocate and move resources between customers.
- What is your providers capacity? (too much and they go broke, too little and they can not handle you dynamic needs)
- What is their continuity posture?

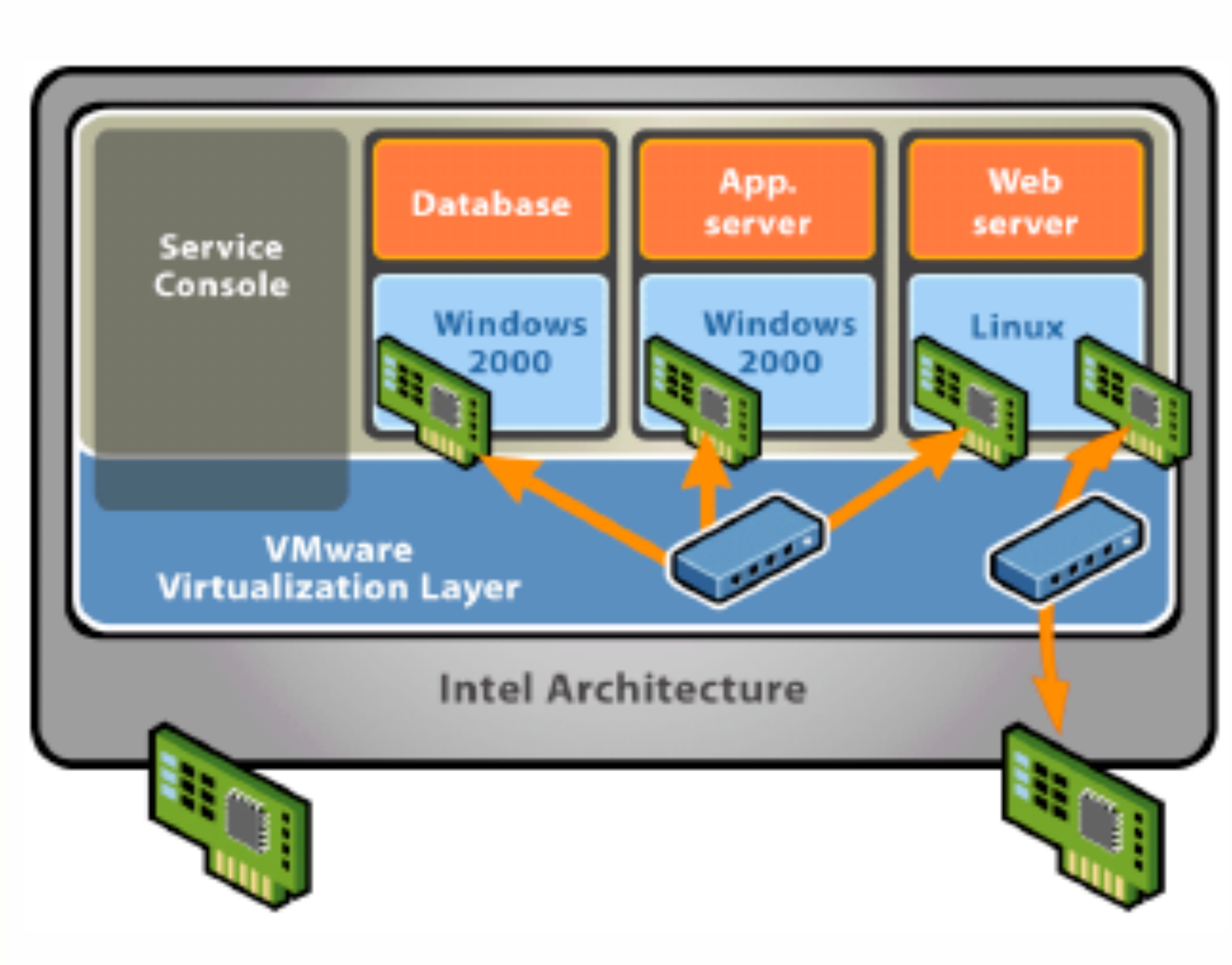
Clouds – Controls & Audit

- Strong contract with SLA's and penalties.
  - Cover continuity
  - Cover security
  - Cover de-conversion
  - Cover Reporting/Logging
- SAS 70, pen tests, right to on-site audit
- Audit Approach – like a vendor management audit

IX Compliance, References, Other, Q&A

Virtual Network Tiering

source: John Hall VMworld 2006



PCI/DSS Assessments Big 3

- Protect root access to the ESX host COS
  - Strong password, use SUDO
- Protect remote access
  - “High” in ESX 2.x, don’t change ESX 3 defaults (i.e. no active telnet, no root access via ssh, default firewall)
- Tiered Networks, ensure you can show your assessor the following:

PCI/DSS Assessments

- No password history or complexity for the COS (modify PAM)
- SNMP default community string is “public” (change to “password”) [1]
- NTP is not enabled (enable this)
- DSS v1.2 section 5.1 Oct 2008 – “systems commonly affected by malware” need AV, ESX? COS? PCICouncil White Paper Q1 2009

No warning banners or minimum days life of a password are required by PCI/DSS, but both are a good idea to add

» [1] auditor levity

Resources

The Source http://www.VMware.com

Technology network
http://www.VMware.com/community/index.jspa

Security topics
http://www.VMware.com/vmtn/technology/security/

Security Response
http://www.VMware.com/support/policies/security_response.html

Compliance Center http://www.vmware.com/technology/security/compliance/index.html

Books by Ogelby & Herold and Edward Haletky

http://www.amazon.com/VMware-ESX-Server-Advanced-Technical/dp/0971151067
http://www.amazon.com/VMware-ESX-Server-Enterprise-Virtualization/dp/0132302071
http://www.amazon.com/VMware-vSphere-Virtual-Infrastructure-Security/dp/0137158009

Resources

The **CIS** ESX benchmark and the general Virtualization benchmarks are both at (Xen also) http://www.cisecurity.org

DISA orangebook virtualization final at
http://iase.disa.mil/stigs/stig/esx_server_stig_v1r1_final.pdf

NSA VMware ESX Server Configuration Guide
http://www.nsa.gov/snac/support/I733-009R-2008.pdf

Gartner Research # **G00144828** must be a member **www.gartner.com**

Blogs
http://www.virtualization.info/2003/09/virtualization-sites-blogs.html

Mailing list
http://searchsecurity.techtarget.com/topics/0,295493,sid14_tax306899,00.html

http://searchvmware.com

LinkedIn **VM People VM**

Other

- Managing heterogeniality
- The rise of Hyper –V (maybe)
- VCP – VM Certified Professional (VCI, VCDX)
- vExpert – 300 picked by the vendor
- If storage fails or under performs, Hosts & VM will fail or under perform
- Hardware Cost story: requirement - 10 servers , 2 CPU's, 4gb Memory, 40GB storage
  - A = buy ten R410s 2 Xeon 1.8, 4gb, 160GB, 2 nics Gig $1,466 x 10 = $14,660
  - B = buy one R905 2 socket six core Opterons 2.6, 450GB SCSI, 64GB, 4 nics Gig $9,317

Summary

- Many
  Ri
  s
  ks are Traditional Carryovers from Physical Server s
- Change Control is More
  Imp
  o
  rtant Now Over Guests, particularly Dormant Guests
- Segregate Network Traffic
- Plan Security Tools Outside & Inside the Host (or both)
- Document Configuration Standards
- Assess/Audit Configuration Standard Compliance
- Collaboration Critical Amongst
  Security,
  S
  erver, Network, Storage, Legal, & Application teams

??? Q and A ???