Sense of Security Pty Ltd
(ABN 14 098 237 908)
306, 66 King St
Sydney NSW 2000
Australia

Tel: +61 (0)2 9290 4444
Fax: +61 (0)2 9290 4455
info@senseofsecurity.com.au

Securing Virtualised Environments - Focus on the Fundamentals

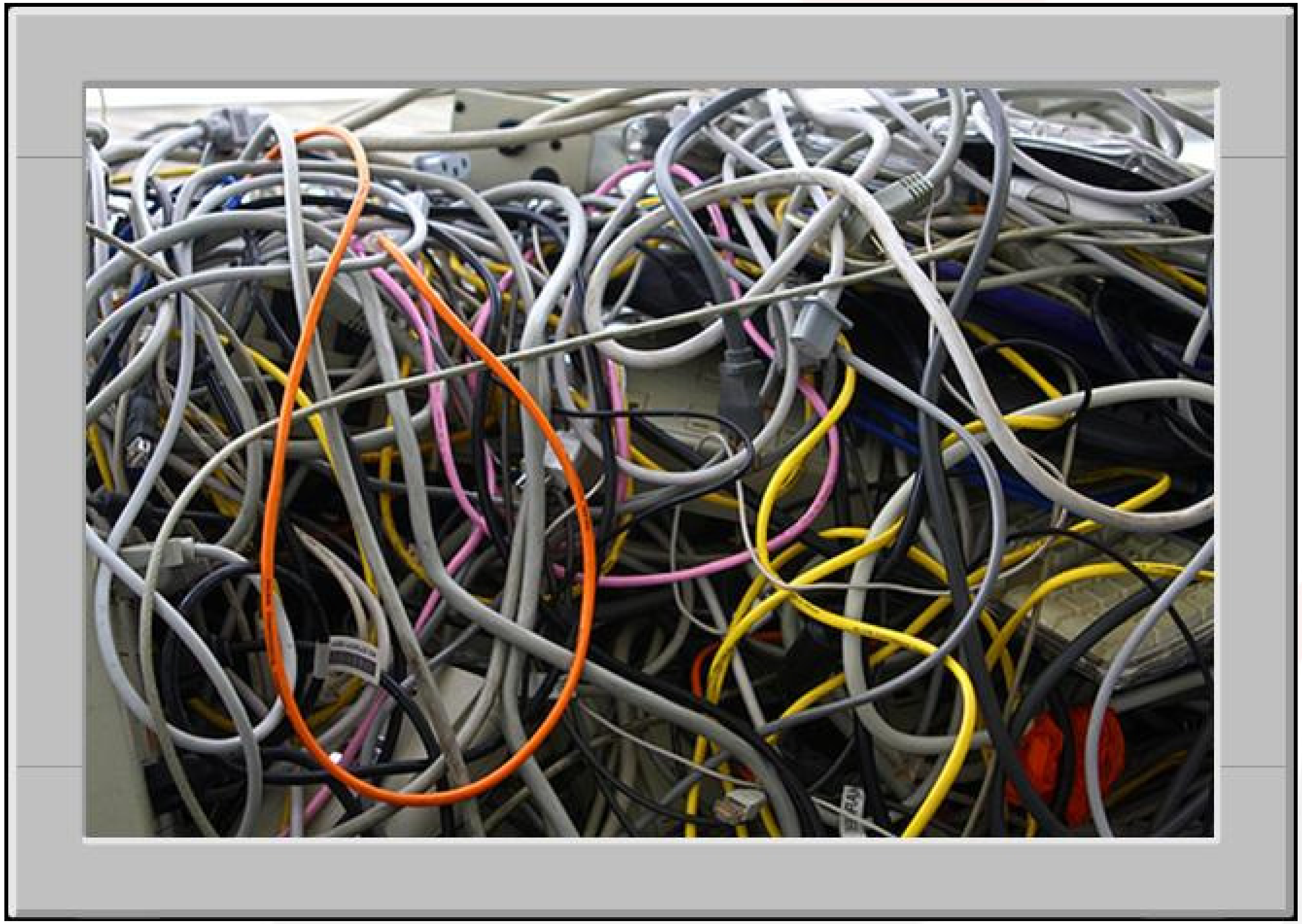
Jul 2010

Agenda

- Why people love Virtualisation
- What to look out for
- Identify security weaknesses
- Be prepared
- Conclusion

Virtualization Benefits

The problem



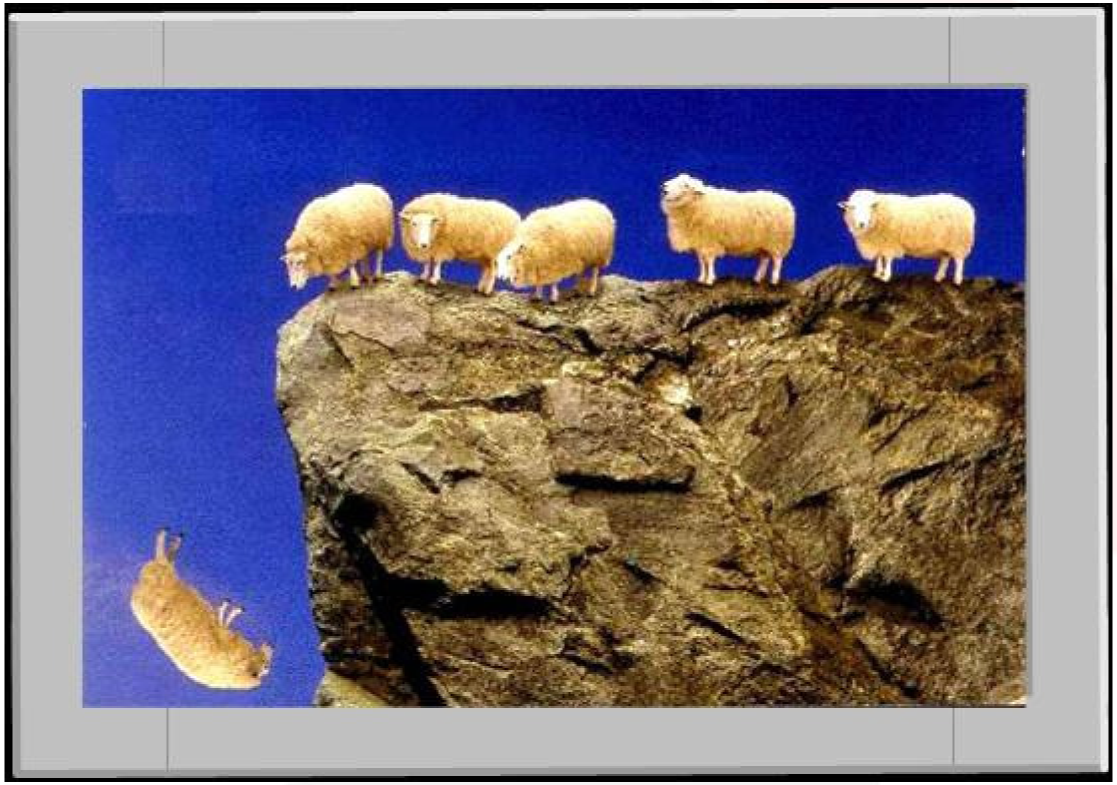
Sense of Security

Security that enables business

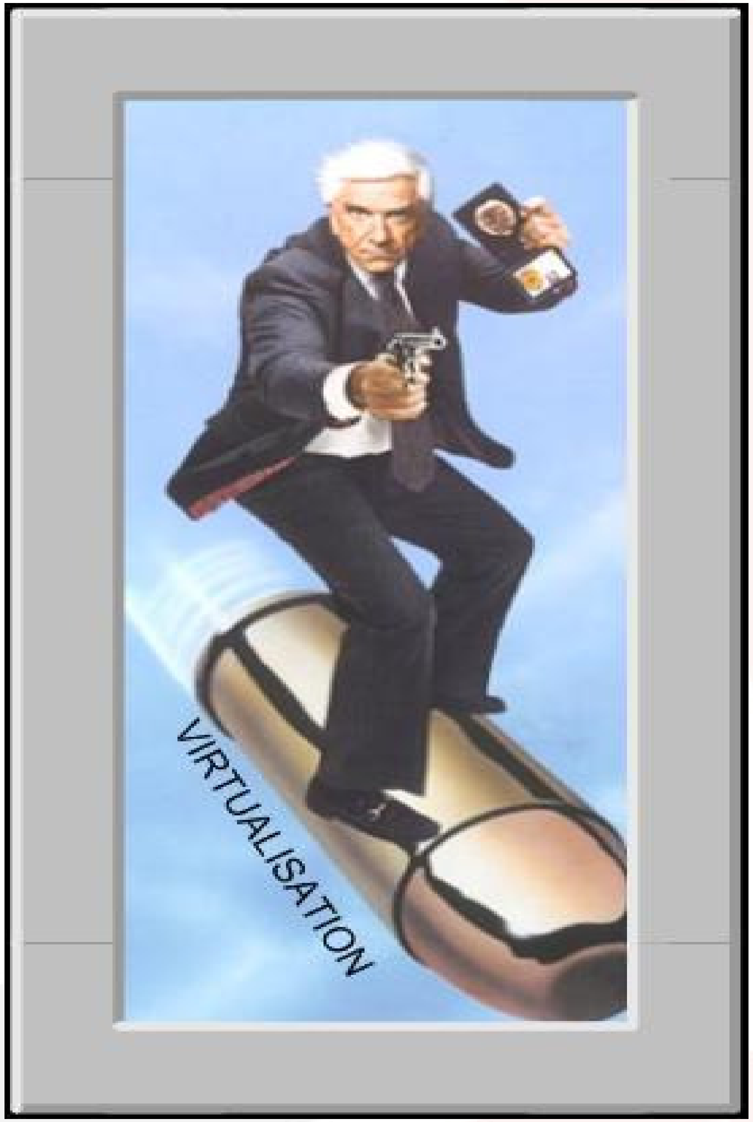
The dream

The solution? A virtualisation Project?

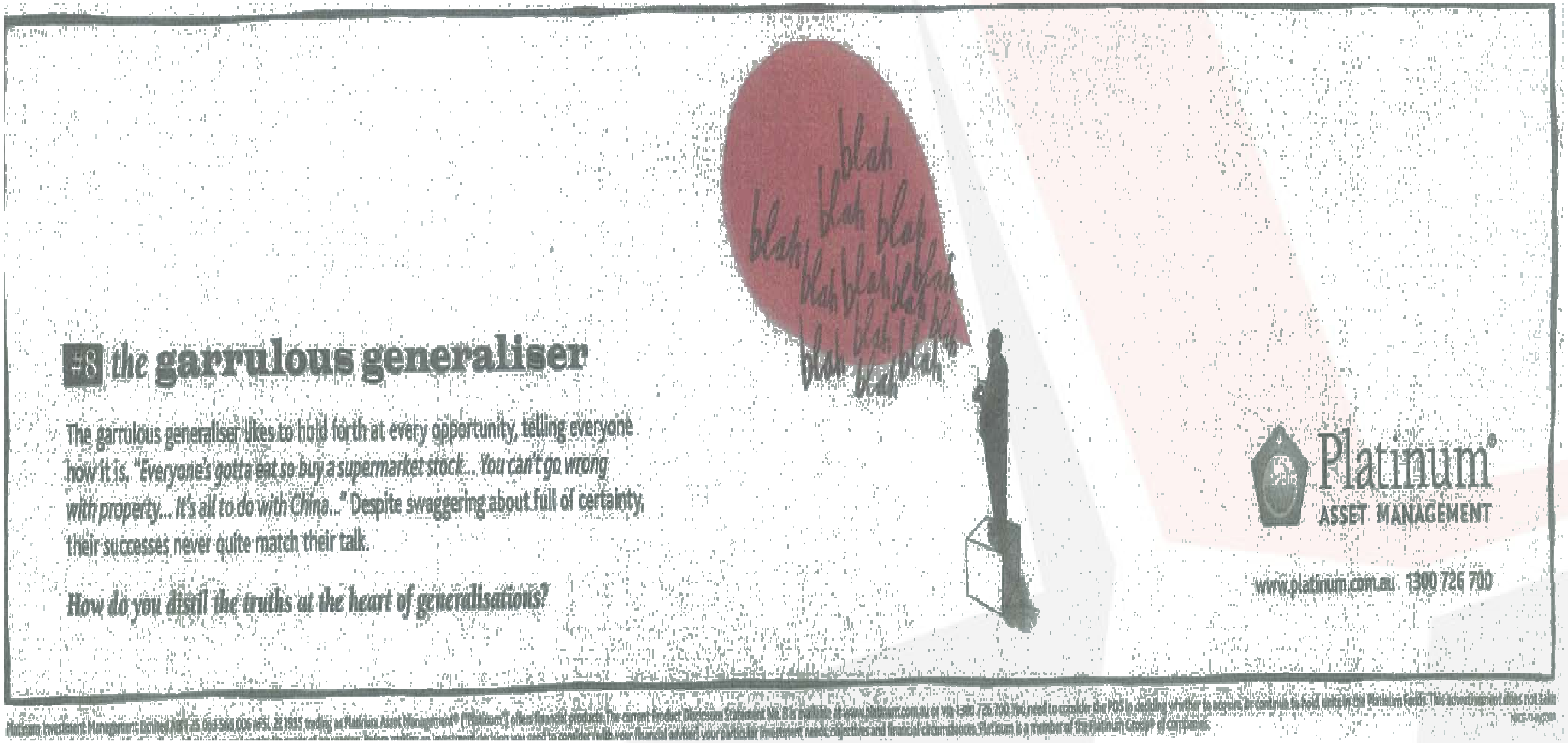
Follow me



Riding the Virtualisation Silver Bullet



It is hard with all the Blah Blah Blah


blah blah blah blah blah blah blah blah blah blah blah blah blah

#8 the garrulous generaliser

The garrulous generaliser likes to hold forth at every opportunity, telling everyone how it is. *"Everyone's gotta eat so buy a supermarket stock... You can't go wrong with property... It's all to do with China..."* Despite swaggering about full of certainty, their successes never quite match their talk.

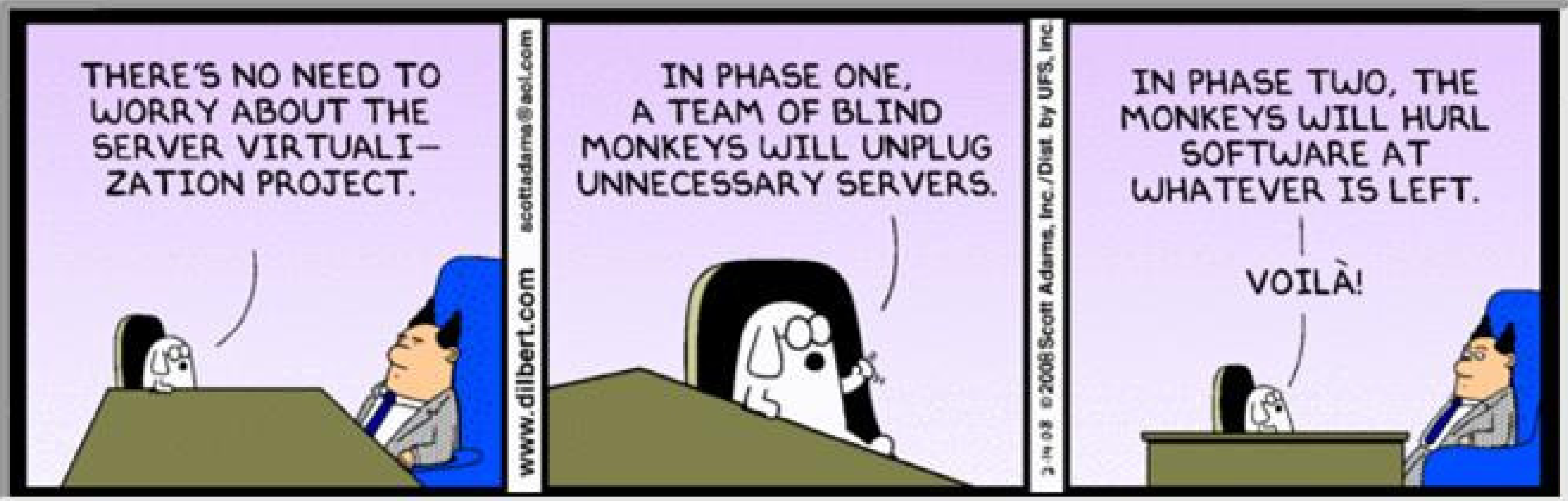
How do you distil the truths at the heart of generalisations?

Platinum®
ASSET MANAGEMENT

www.platinum.com.au 1300 726 700

Platinum Investment Management Limited ABN 25 063 565 006 AFSL 221935 trading as Platinum Asset Management® ("Platinum") offers financial products. The current Product Disclosure Statement No. 8 is available at www.platinum.com.au or via 1300 726 700. You need to consider the PDS in deciding whether to acquire, or continue to hold, units in the Platinum Funds. This advertisement does not take [illegible] Before making an investment decision you need to consider (with your financial adviser) your particular investment needs, objectives and financial circumstances. Platinum is a member of the Platinum Group® of companies.

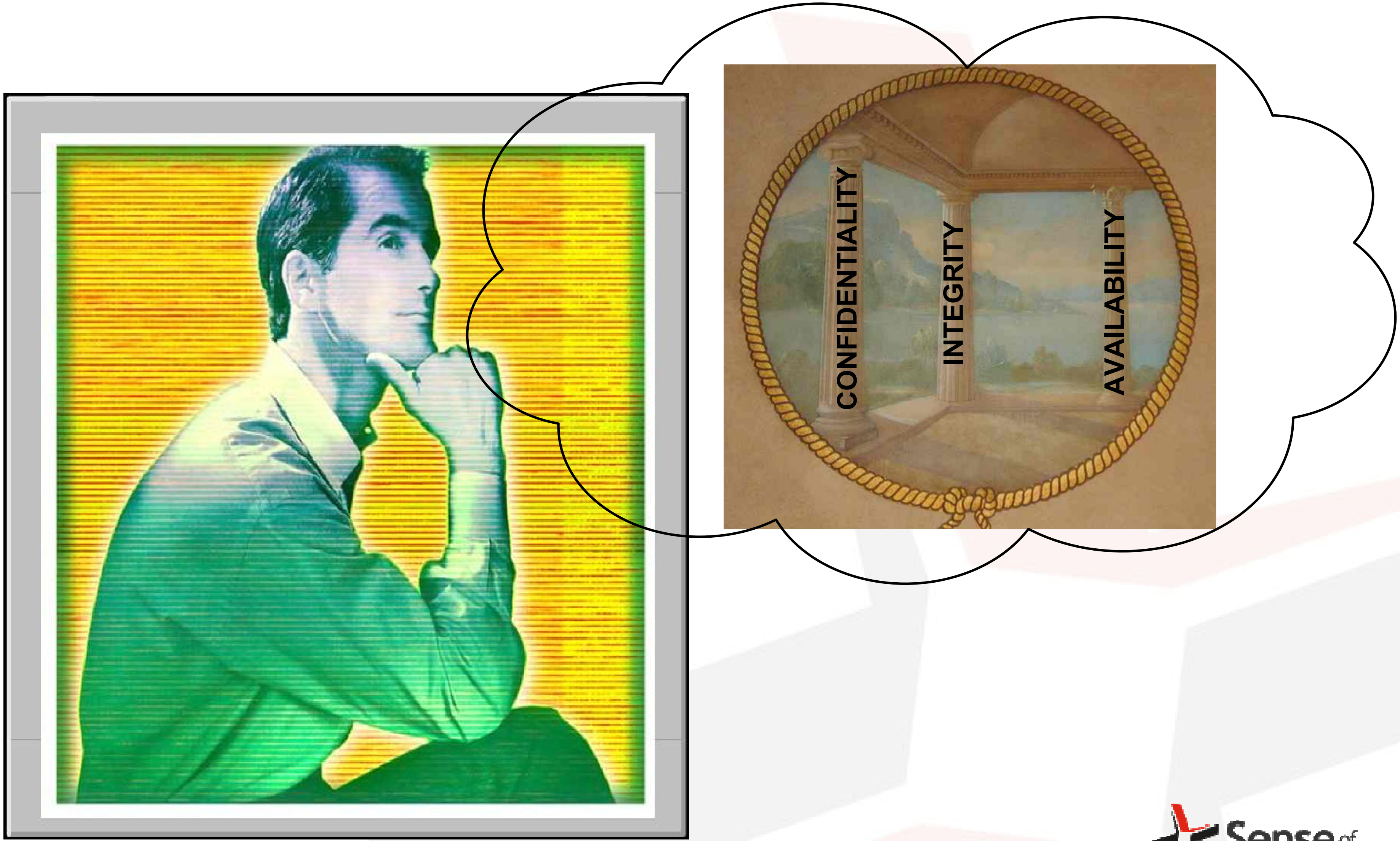
Even Dilbert's boss is onto this!


THERE'S NO NEED TO WORRY ABOUT THE SERVER VIRTUALI-ZATION PROJECT.
IN PHASE ONE, A TEAM OF BLIND MONKEYS WILL UNPLUG UNNECESSARY SERVERS.
IN PHASE TWO, THE MONKEYS WILL HURL SOFTWARE AT WHATEVER IS LEFT.
VOILÀ!
scottadams@aol.com
www.dilbert.com
3-19-08 © 2008 Scott Adams, Inc./Dist. by UFS, Inc.

Copyright acknowledged

Are we doomed?

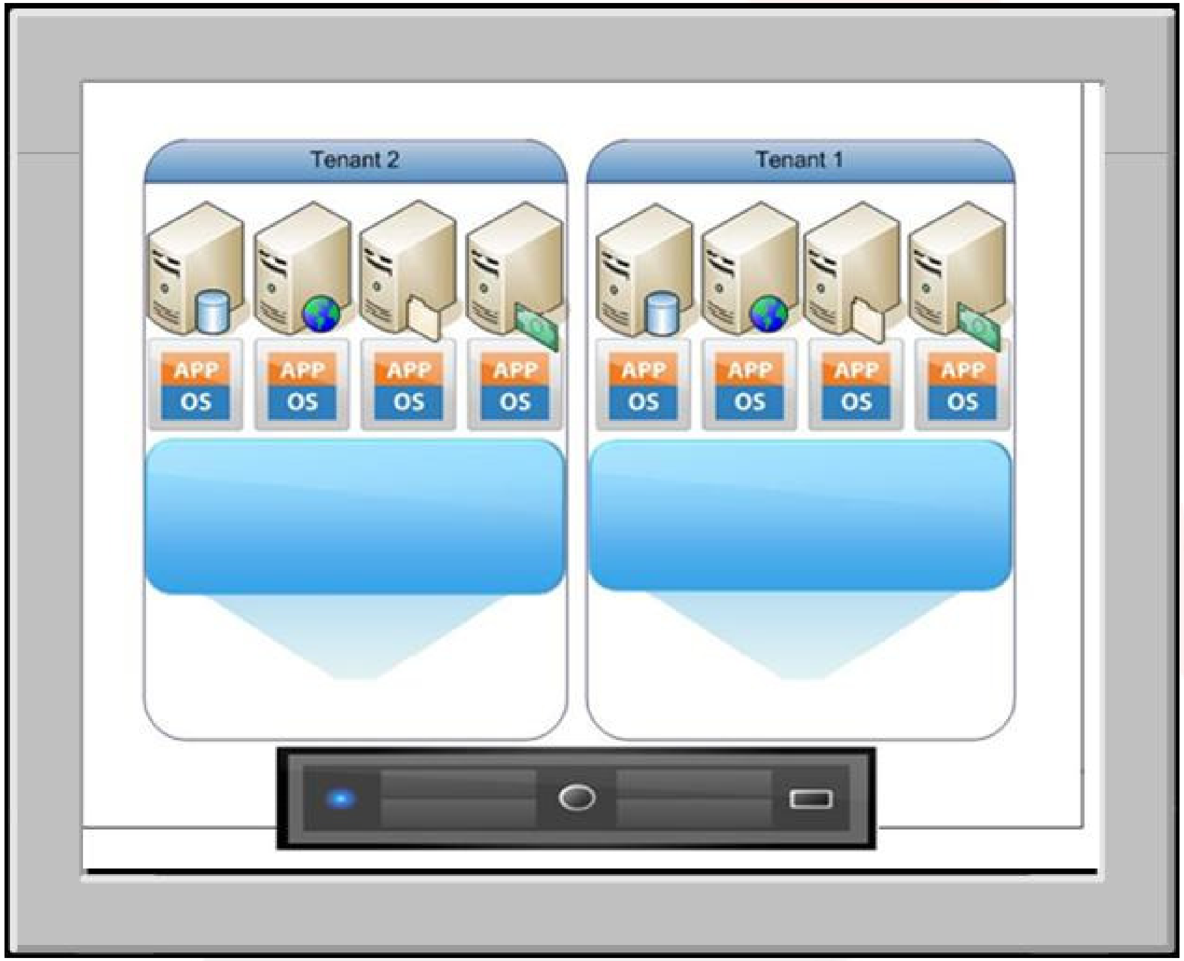
STOP


CONFIDENTIALITY
INTEGRITY
AVAILABILITY

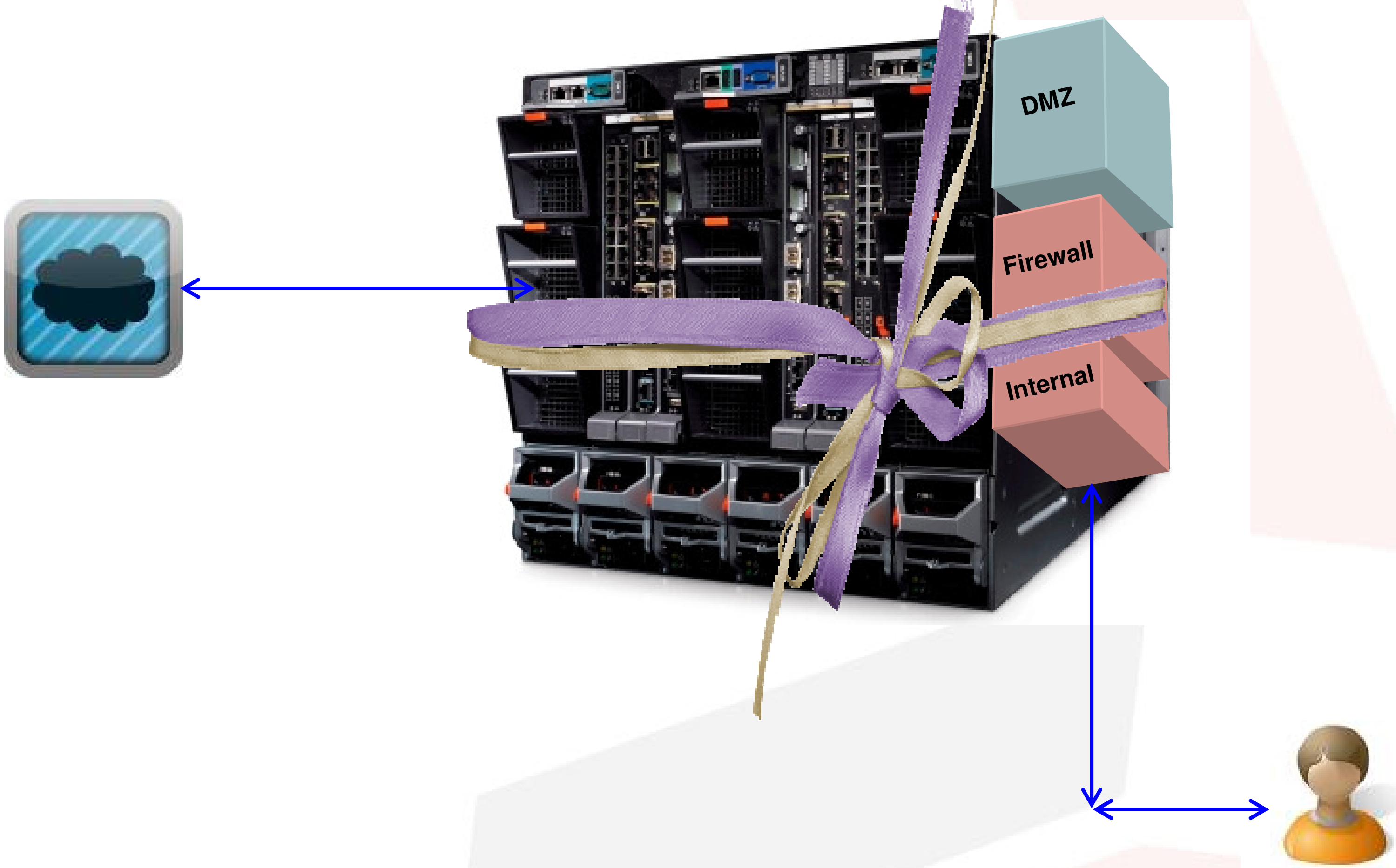
The Real Agenda

- We need to be able to evaluate and measure the security of the deployment in terms of C I A

Confidentiality



Company in a box



Is it getting crowded in there?

Stealing a Physical Machine

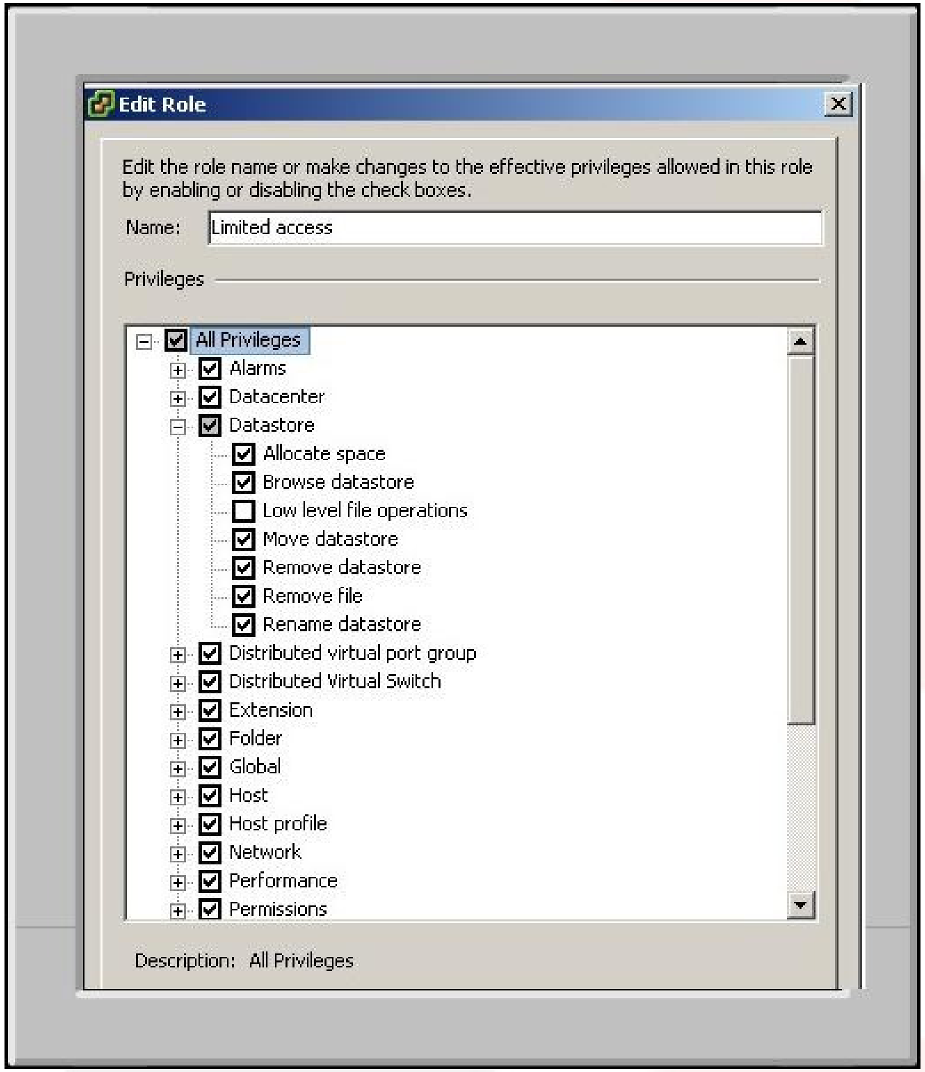
VERY DIFFICULT

Stealing a Virtual Machine

See Link to Video Content

http://vimeo.com/14631581

Confidentiality cont…



Edit Role

Edit the role name or make changes to the effective privileges allowed in this role by enabling or disabling the check boxes.

Name: Limited access

Privileges

- ☑ All Privileges
  - ☑ Alarms
  - ☑ Datacenter
  - ☑ Datastore
    - ☑ Allocate space
    - ☑ Browse datastore
    - □ Low level file operations
    - ☑ Move datastore
    - ☑ Remove datastore
    - ☑ Remove file
    - ☑ Rename datastore
  - ☑ Distributed virtual port group
  - ☑ Distributed Virtual Switch
  - ☑ Extension
  - ☑ Folder
  - ☑ Global
  - ☑ Host
  - ☑ Host profile
  - ☑ Network
  - ☑ Performance
  - ☑ Permissions

Description: All Privileges

Who manages the system?

“ An ESX virtual switch supports copying packets to a mirror port. By using what is called promiscuous mode, ESX Server makes a virtual switch port act as a SPAN port or mirror port. This capability makes it possible to debug using a sniffer or to run monitoring applications such as IDS.”

“Forged transmit blocking, when you enable it, prevents virtual machines from sending traffic that appears to come from nodes on the network other than themselves”

ref [http://www.vmware.com/files/pdf/virtual_networking_concepts.pdf]

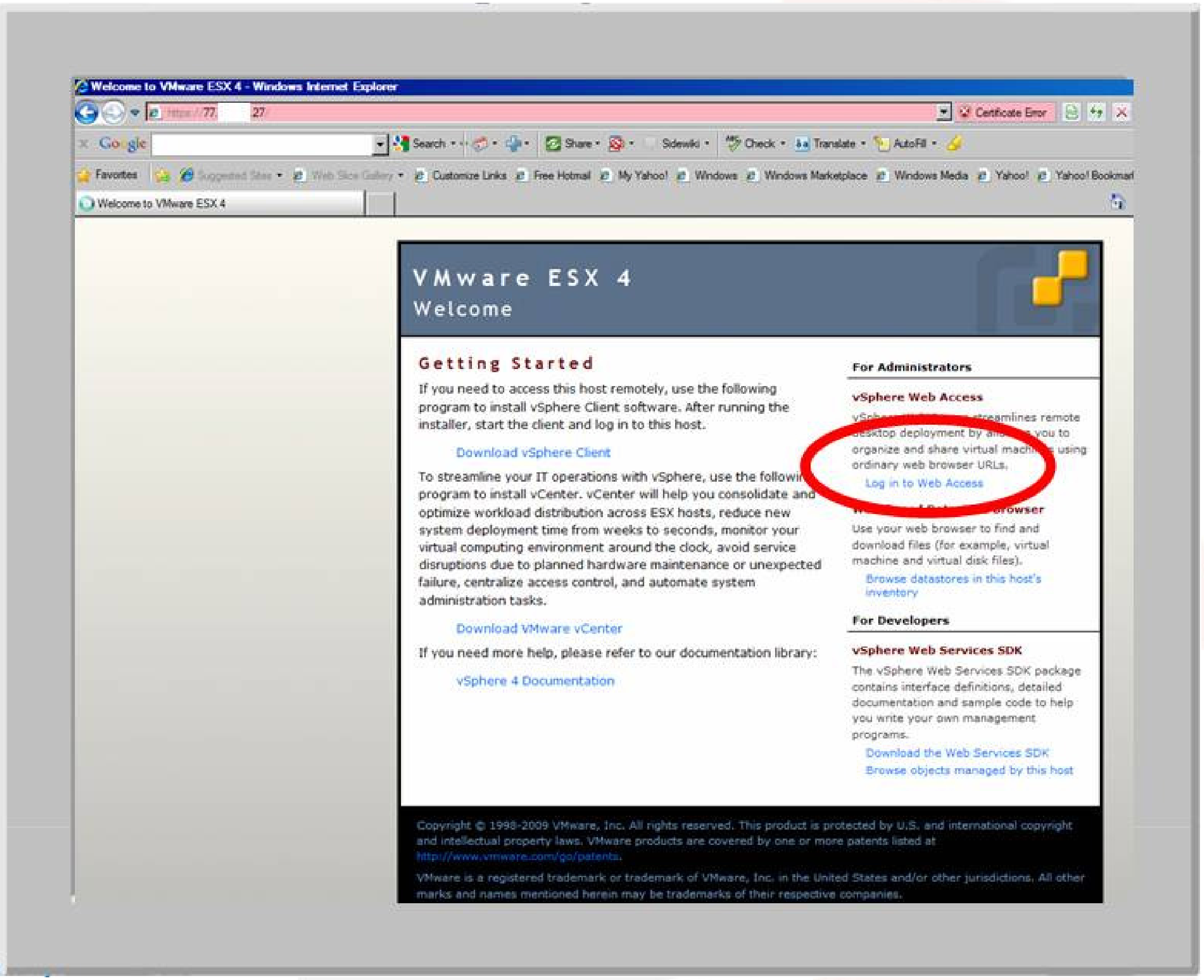
Virtual System may be administered by someone who is neither a network nor a security expert!

Integrity

- Just like any other software virtual platforms are and have been buggy
  - VMSA-0008-0002.1 (Virtual Center Tomcat 5.5.7.1)
  - CVE-2007-1321 (Heap Overflow in Xen network Driver)
  - CVE-2008-0923 (Path Traversal vulnerability in VMware's shared folders implementation)
  - CVE-2009-2968 (VMware Studio 2 directory traversal)

- Patch Management Framework in place?

Integrity cont…



VMware ESX 4

Welcome

Getting Started

If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.

Download vSphere Client

To streamline your IT operations with vSphere, use the followi program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.

Download VMware vCenter

If you need more help, please refer to our documentation library:

vSphere 4 Documentation

For Administrators

vSphere Web Access

vSph streamlines remote esktop deployment by al you to organize and share virtual mach using ordinary web browser URLs.

Log in to Web Access

W d Dat rowser

Use your web browser to find and download files (for example, virtual machine and virtual disk files).

Browse datastores in this host's inventory

For Developers

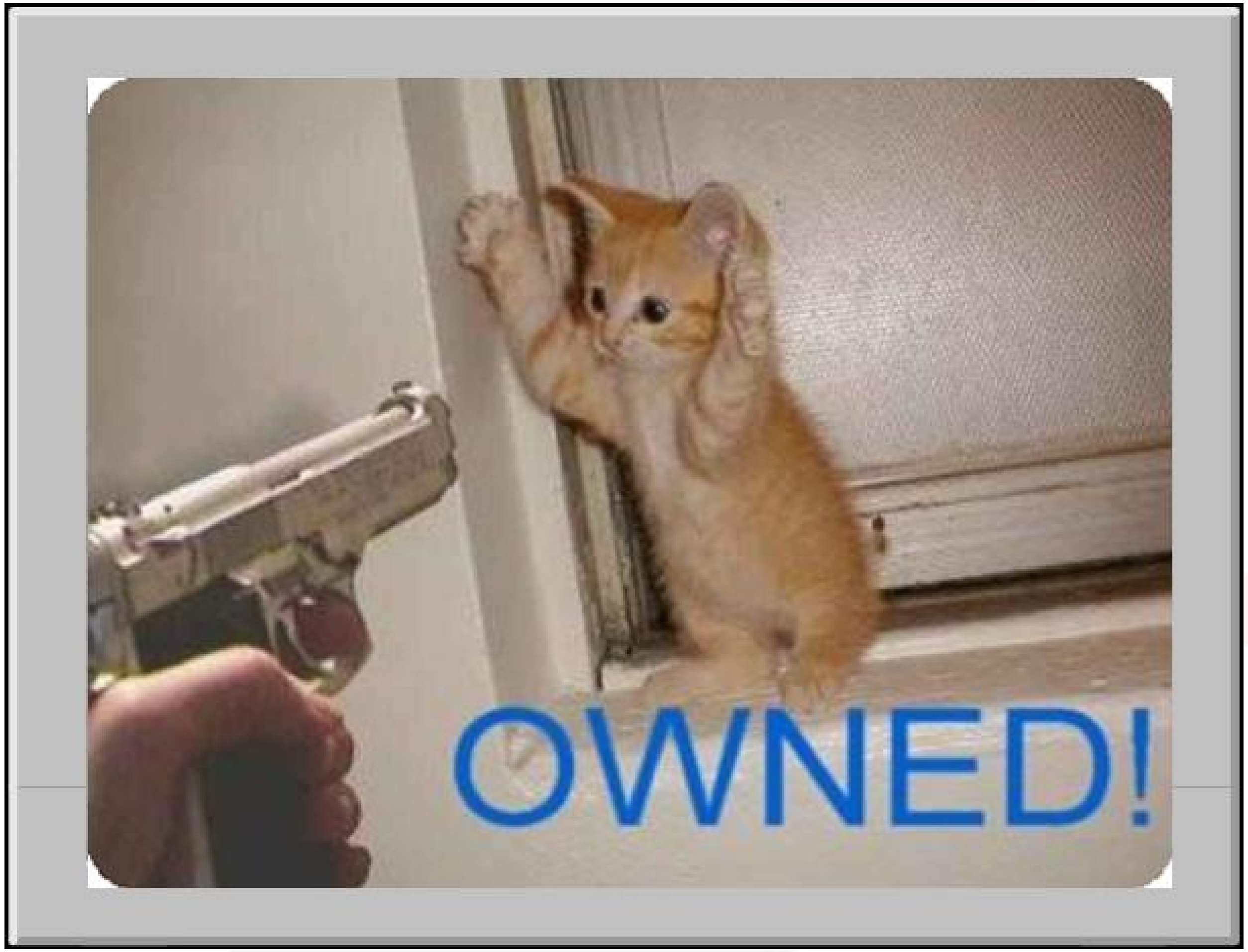
vSphere Web Services SDK

The vSphere Web Services SDK package contains interface definitions, detailed documentation and sample code to help you write your own management programs.

Download the Web Services SDK

Browse objects managed by this host

This is a good start to getting ….



Integrity cont…

- Man in the Middle Attacks
- Various VMWare clients susceptible
- Including vi client
  - Configuration of the clients.xml file

Segregation of Duties

- Server, storage, network, and security duties are collapsed
- Critical considerations:
  - Role-mapping within IT
  - RBAC capabilities of virtualisation platform
  - Layered controls (prevent, detect, respond)
- Roles and Responsibilities
  - Review of 75 discrete responsibilities assigned to 3 or 4 roles

    (Per VMWare)

Infrastructure hardening

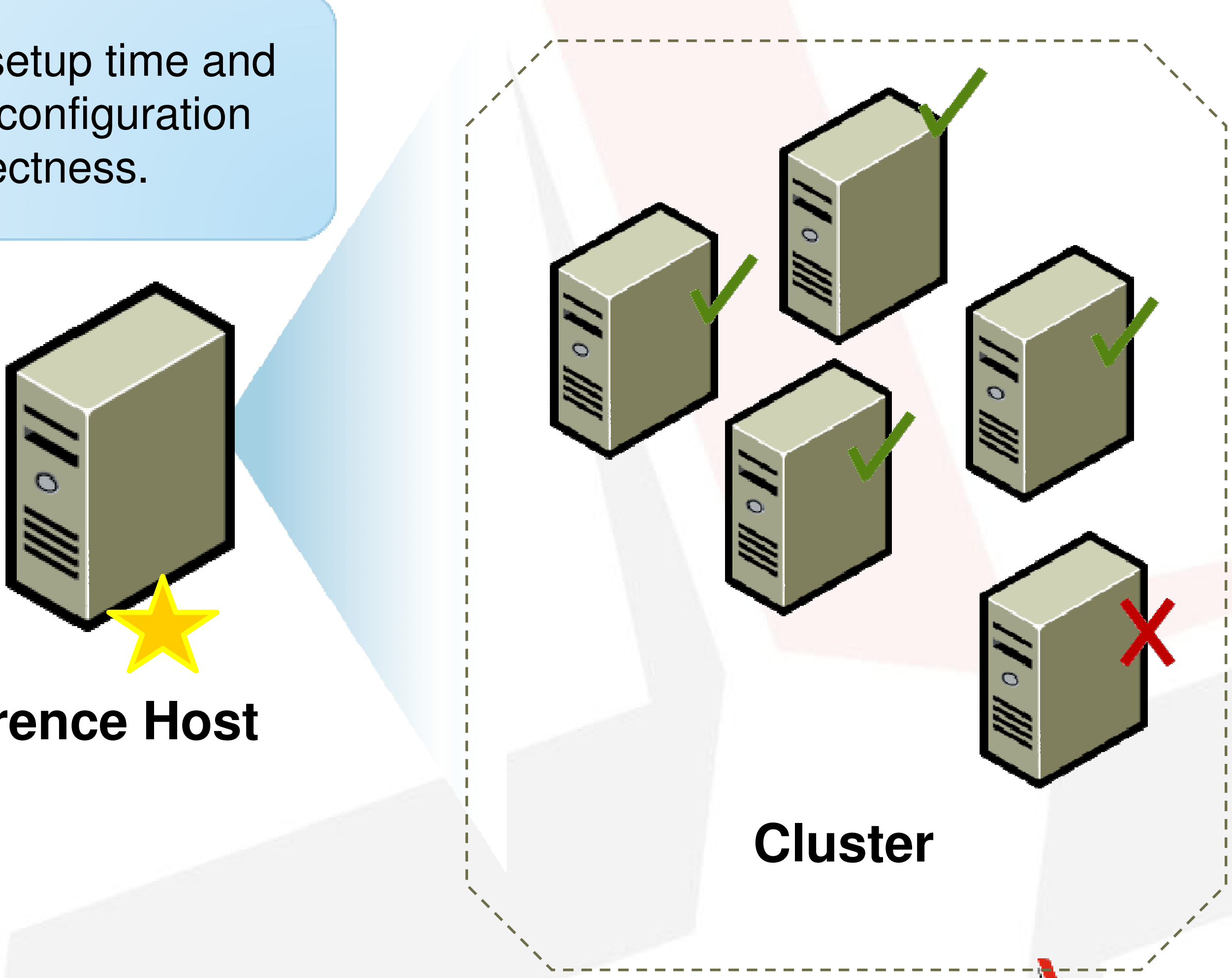
- Hypervisor Protection
- Management Interfaces
- Zones of Trust
- Virtual Network Configuration
- Consolidation of functions

Auditing

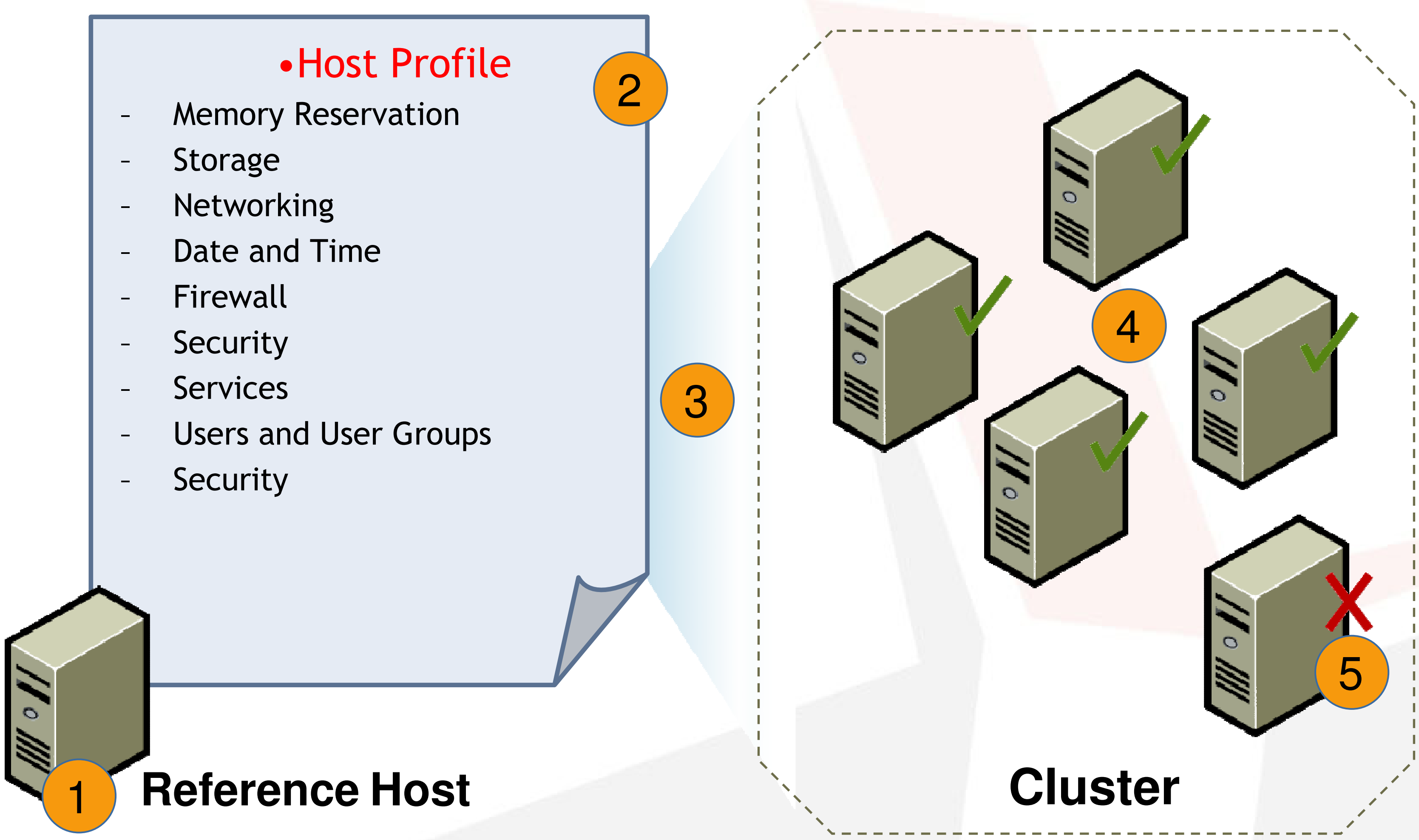
- The entire environment should be auditable
- All activity should be logged and monitored
- Administrators/Auditors should be able to produce compliance reports at any point in time
- Native and Commercial tools can be used

VMWare Native Tool – Host Profiles

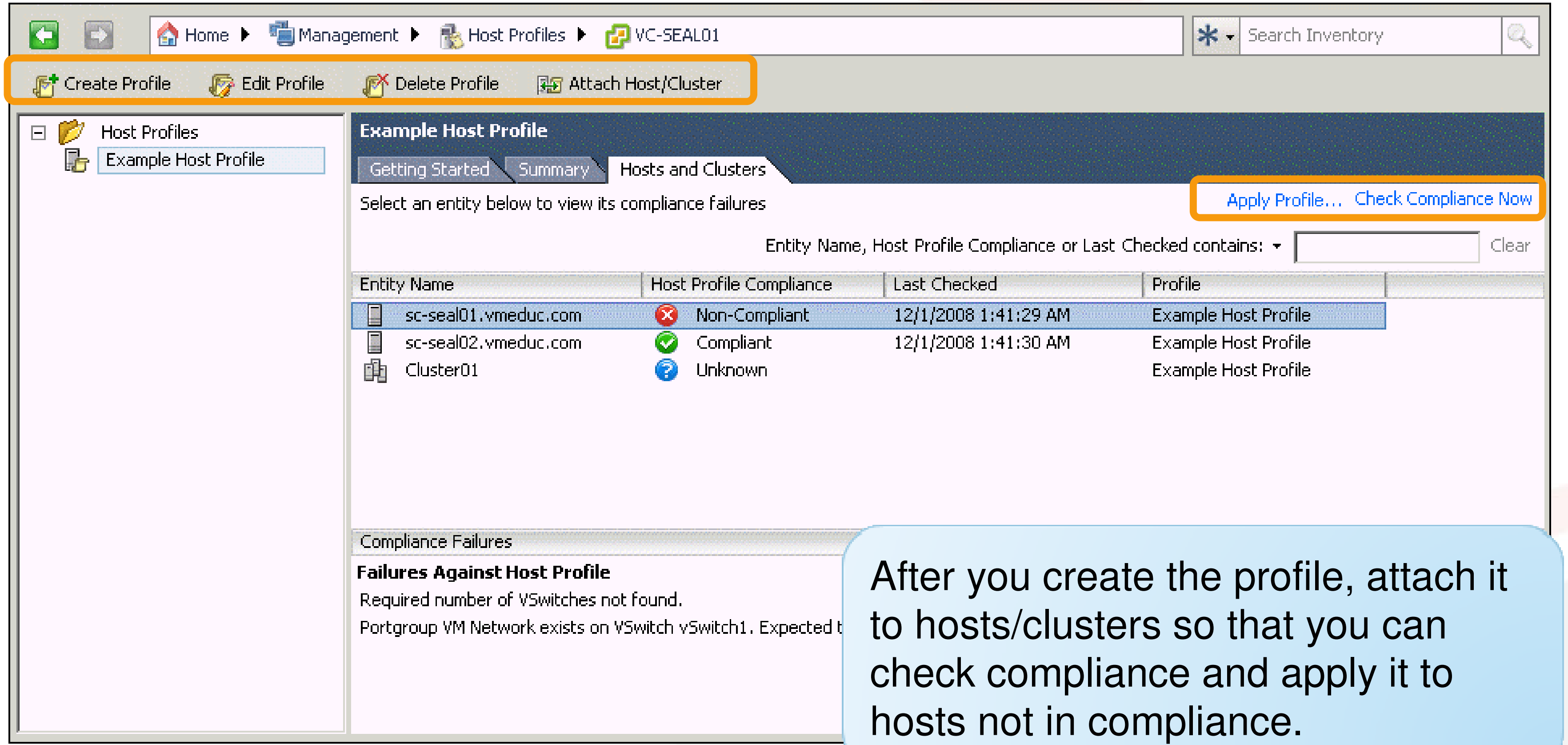
Host profiles reduce setup time and allow you to manage configuration consistency and correctness.



Basic Workflow to Implement Host Profiles



- Host Profile
  - Memory Reservation
  - Storage
  - Networking
  - Date and Time
  - Firewall
  - Security
  - Services
  - Users and User Groups
  - Security



Example Host Profile

Select an entity below to view its compliance failures

Entity Name, Host Profile Compliance or Last Checked contains:

Entity Name	Host Profile Compliance	Last Checked	Profile
sc-seal01.vmeduc.com	✗ Non-Compliant	12/1/2008 1:41:29 AM	Example Host Profile
sc-seal02.vmeduc.com	✓ Compliant	12/1/2008 1:41:30 AM	Example Host Profile
Cluster01	? Unknown		Example Host Profile

Compliance Failures

Failures Against Host Profile

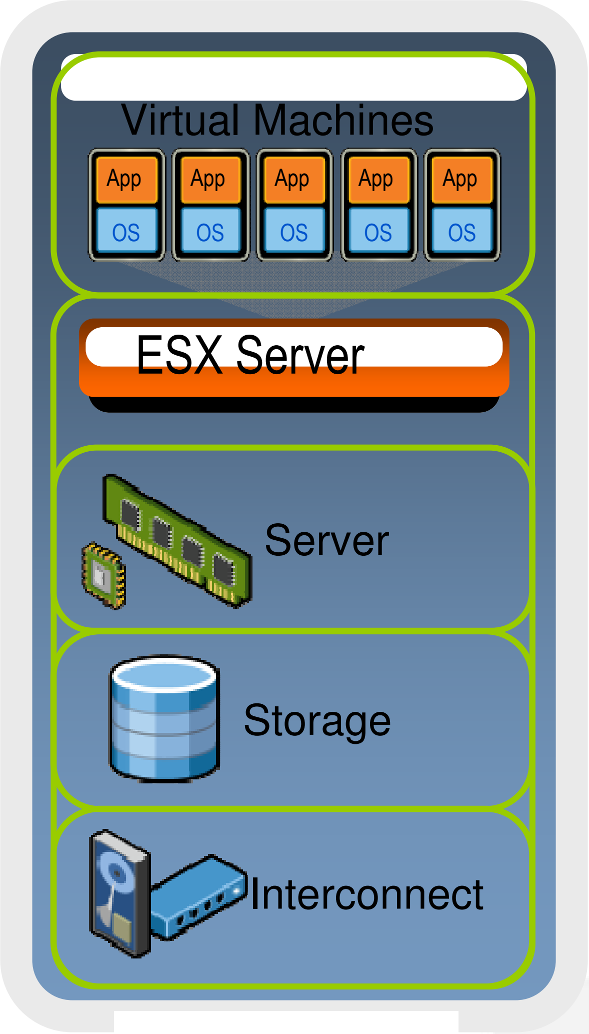
Required number of VSwitches not found.

Portgroup VM Network exists on VSwitch vSwitch1. Expected t

After you create the profile, attach it to hosts/clusters so that you can check compliance and apply it to hosts not in compliance.

Availability

- How is Availability delivered?
- Active Active
- Active Passive
- Fault Tolerance
- System Maintenance
- Patch Management (access to dormant VM's)



Planned Downtime	Unplanned Downtime
	VM Failure Monitoring
VMotion	HA – High Availability FT – Fault Tolerance
Storage VMotion	VCB / VADR
Network Redundancy	NIC & HBA Teaming

Availability: Speed, Latency, Capacity

- Can software-based virtual appliances deliver to level expected of purpose built hardware?
- Many vendors have elected not to deliver L3 capability in virtual appliances.
- Do you want a Virtual UTM?

Key Issues to Think About

- Going in blind with no plan – is not a plan!
- Inadequate Protection to the Hypervisor
- Blind Spot - Lack of Visibility and Control to Virtualised Network and VM’s
- Collapsed Fabric – Virtualising across zones of trust
- Segregation of Duties – not defined
- Administration – Availability, Patch Management
- Ensure overall system is auditable

Thank You

Murray Goldschmidt

Chief Operating Officer

Sense of Security

murrayg@senseofsecurity.com.au

+61 2 9290 4444

www.senseofsecurity.com.au