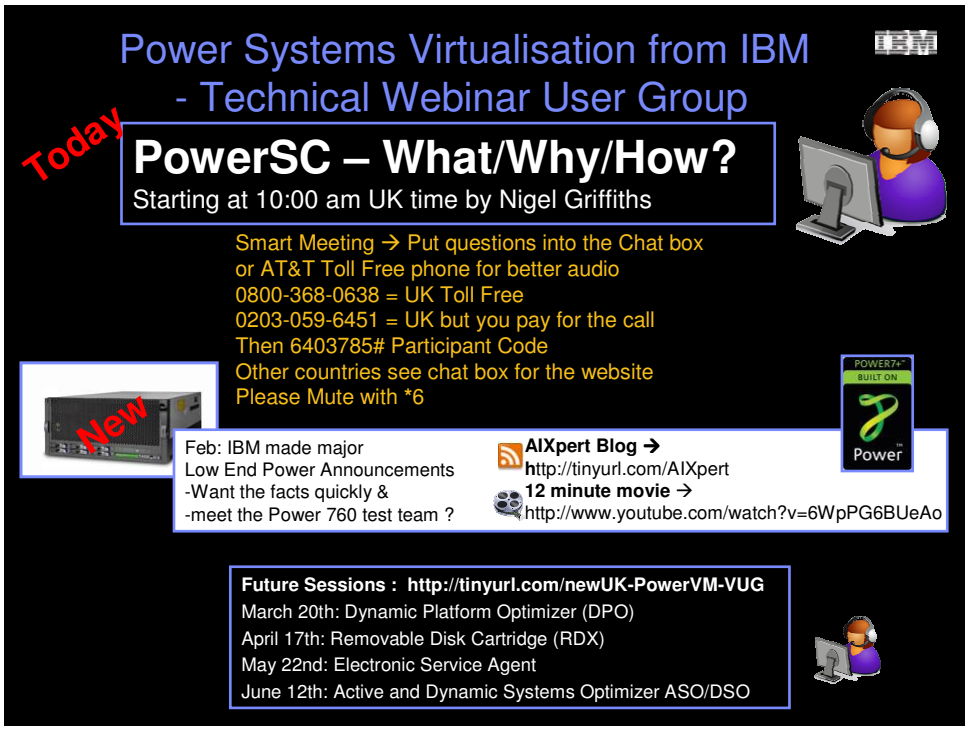
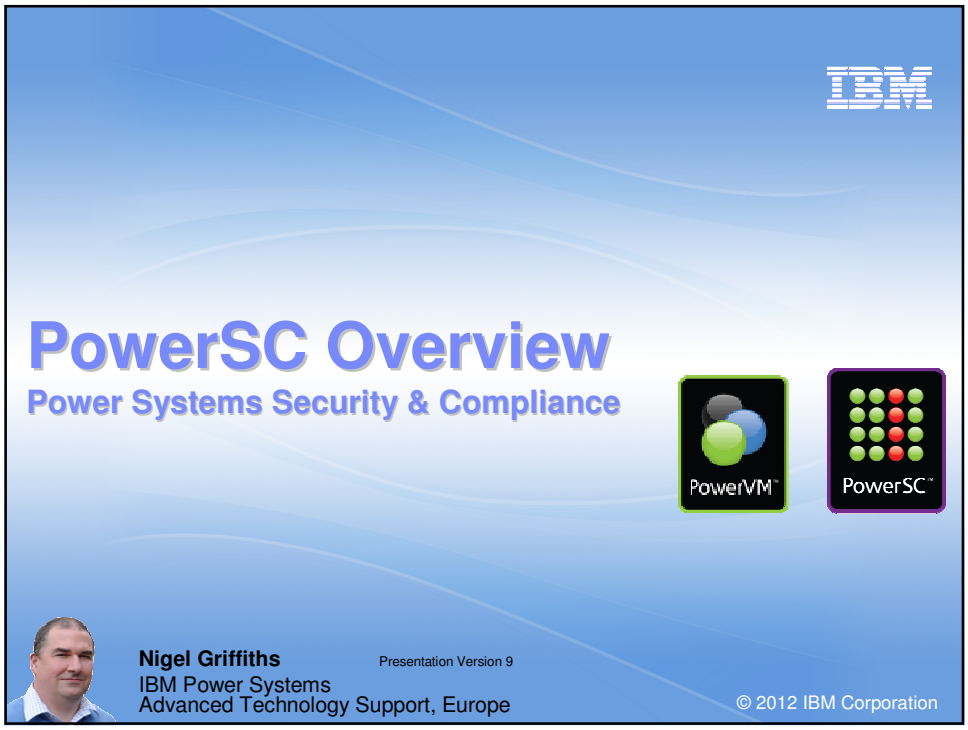
Selling IBM STG Systems Software to
Business Partners



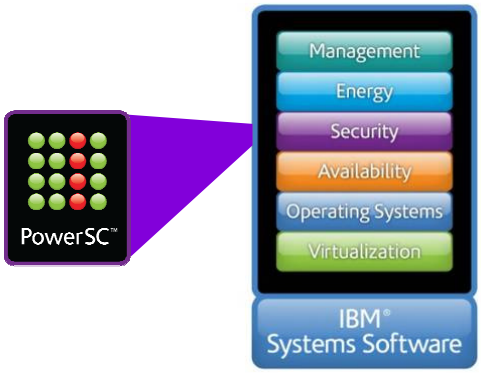


IBM

PowerSC → **Security** + **Compliance** designed to protect data centers virtualized with PowerVM **enabling** Higher Quality Services

Client Benefits

- ***Simplifies management*** *and measurement of security & compliance*
- ***Reduces cost*** *of administrating security & compliance*
- ***Improves detection*** *and reporting of security exposures*
- ***Reduces time and skills*** *needed for the* ***audit capability*** *to satisfy reporting requirements*
- *Provides* ***"virtualization aware"*** *security extensions*



© 2012 IBM Corporation

IBM

PowerSC Editions

- **PowerSC Express**
  - *Basic compliance for AIX*
- **PowerSC Standard**
  - *Security and compliance for virtual & cloud environments*

Trusted Surveyor ##
Separate LPP & price

PowerSC Editions	Express	Standard
Security & Compliance Automation	✓	✓
Trusted Logging		✓
Trusted Boot**		✓
Trusted Firewall ##		✓
Trusted Network Connect & Patch Mgmt		✓
Real Time Compliance	✓	

** Requires POWER7 System with eFW7.4
Supports IBM i & Power Linux

PowerSC GBP/core	Express	Standard
Small Blade up to 750	£91.75 £15.53	£111.67 £22.34
Medium Power 770	£229.38 £39.17	£281.41 £56.28
Large Power780 & 795	£458.77 £77.99	£558.35 £111.67

Top=1st Year License + 1 year SWMA
Bottom=Subsequent years = SWMA

UK List prices from mid-2012 = only indicative of a ball-park.

Please ask for a current price in your country & currency.

© 2012 IBM Corporation

IBM

IBM Power System : Secure Virtualization

Designed to provide a secure virtualized environment and lower overall TCO

-**Power Systems Hypervisor has never had a single reported security vulnerability; A perfect security record.† No downtime forced by security patches.**

-**Software based hypervisors such as VMware (93† security vulnerabilities) have a high number of security concerns.**

Customer Benefits
- **Improved efficiency through consolidation**
- **Secure sharing of common resources such as processors, I/O and memory**
- **Reduced IT costs**
- **Flexibility to instantly respond to workload changes**

- The Power Systems hypervisor is designed for security and isolation plus performance hence using a hardware based hypervisor & LPARs.
- Only hardware firmware (digitally signed by IBM) can be loaded into the Power Systems hypervisor.
- In addition to its proven security record, Power Systems have all of the functionality and management control required to operate in a public cloud environment:
  - Live partition mobility
  - Proven resource isolation between partitions
- Power Virtualization including the hypervisor and the Virtual I/O server has be certified for EAL4+ Common Criteria

† US Gov and Mitre tracking of Common Vulnerabilities and Exposures
http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=VMware
http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=PowerVM

© 2012 IBM Corporation

IBM

AIX Security is already excellent

Hands up those that think IT Security is exciting? Typically not many ☺

- But it is absolutely important if it is your bank account, credit card, pension, medical records, personal details …!

Actually AIX has excellent security features you are/should be using already

- ssh / sftp
- RBAC = Roll based Access Control
- Encrypted JFS2 filesystems
- Extended passwords & secondary challenge response additions
- aixpert, ARTEX, IP filters, permissions manager, user check …..

- Provided it is … **AIX 6 & 7** and **up to date on TL/service pack**

No amount of security software can fix users/sysadmin using telnet or ftp?

© 2012 IBM Corporation

IBM i - Built-in Security

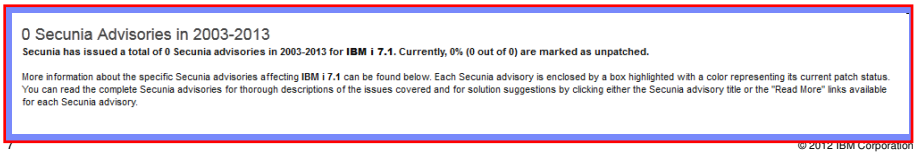
Security was designed as an integral part of the system

- Virus resistant, object-based architecture
- Integrated security features
- Integrated Cryptography and Key management
- Integrated User Management Interfaces
- Intrusion Detection
- Object based authority
- Native IBM i Audit Journal
- SSL
- VPN
- Encrypted backup
- Encrypted data at rest
- IBM i EAL4+ CAPP certified
- Wealth of ISV applications

Learn more at
http://www.ibm.com/systems/power/software/i/security

No advisories (no security warnings) for IBM i 7.1:

- www.secunia.com → Vulnerability Report: IBM i 7.1 :


0 Secunia Advisories in 2003-2013

Secunia has issued a total of 0 Secunia advisories in 2003-2013 for IBM i 7.1. Currently, 0% (0 out of 0) are marked as unpatched.

More information about the specific Secunia advisories affecting **IBM i 7.1** can be found below. Each Secunia advisory is enclosed by a box highlighted with a color representing its current patch status. You can read the complete Secunia advisories for thorough descriptions of the issues covered and for solution suggestions by clicking either the Secunia advisory title or the "Read More" links available for each Secunia advisory.

© 2012 IBM Corporation

PowerSC and IBM i

Supported PowerSC features:

- Work on all operating Systems (AIX / IBM i / Linux):
  - **Trusted Firewall** ✓
  - **Trusted Surveyor** ✓

Some equivalent functionality already in the base IBM i:

- PowerSC Trusted Audit Data Repository – ~**Trusted Logging**
  - Very similar to IBM i audit features
  - QAUDJRN journal & associated journal receivers are **read-only** objects cannot be modified by any user
- PowerSC Trusted Digital Signature Verification – ~**Trusted Boot**
  - IBM i allows digital signing and verifying of any executables
  - CHKOBJITG command
  - IBM i LIC, OS, LICPGMs are digitally signed by IBM
- IBM i has built-in features to setup/monitor/enforce – ~**Trusted Security**
  - Password security
  - Authorizations to files/programs/
  - Manage users/system wide security settings
- ISV solutions for security & compliance provide additional advanced capabilities

No equivalent IBM i functionality:

- Trusted Network Connect & Patch Management

More info in the You and i blog entry - PowerSC and IBM i: Integration of Security:
http://ibmsystemsmag.blogs.com/you_and_i/2012/10/powersc-and-ibm-i-integration-of-security.html

© 2012 IBM Corporation

IBM

PowerSC has Five Components

1 Trusted Boot
Be sure that boot media & AIX has booted in a known-trusted state

2 Trusted Network Connect
When an LPAR attempts to join a VLAN, ensure a minimum AIX level

3 Trusted Firewall
Pass packets securely between LPARs without an external firewall

4 Trusted Logging
Secure audit files away and safe from malicious modification

5 Compliance Automation
Raise alerts if any of 100's of settings of a security policy are violated

Announced late in 2012 two more tools

6. **Real-time alerts** – no more periodic script running/polling
7. **Trusted Surveyor** – checks all LPARs on a VLAN + reports changes

© 2012 IBM Corporation

IBM

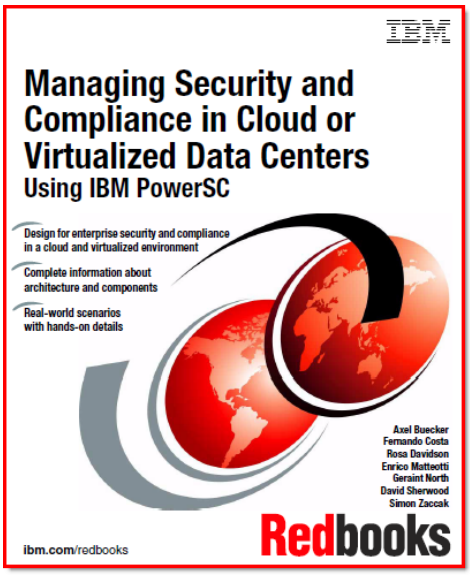
PowerSC Redbook

Obfuscated name!

Big = 350 pages

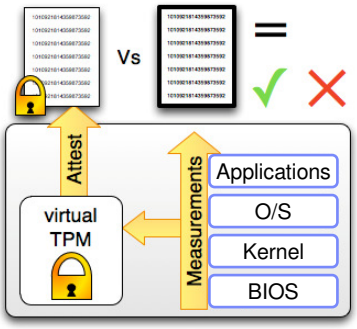
Contents:

- Part 1 Business drivers and solution overview
- Chapter 1. IT security and compliance management business context
- Chapter 2. Introducing the IBM PowerSC solution
- Part 2 Technical concepts and deployment guidelines
- Chapter 3. Security and Compliance Automation
- Chapter 4. Real Time Compliance
- Chapter 5. Trusted Logging
- Chapter 6. Trusted Network Connect and Patch Management
- Chapter 7. Trusted Boot
- Chapter 8. Trusted Firewall
- Chapter 9. Trusted Surveyor



© 2012 IBM Corporation

PowerSC – Trusted Boot and Trusted Execution



How PowerSC works:
1.Measure the boot process and securely store the results in a Virtual Trusted Platform Module (VTPM)
2.Provide a sealed set of measurements to the requestor
3.Verify these measurements against a reference manifest

Overview

Challenge: Ensure that every virtual machine image in your datacenter hasn't been altered either by accident or maliciously (commonly called a RootKit attack).

PowerSC Solution: Trusted Boot forms the core root of trust for the image, i.e. a foundation for trust. Each stage of the boot process measures the next, starting at the firmware.

Benefits

- PowerSC offers the only solution on the market to form a chain of trust for VMs all the way from boot to OS!
- Improve QoS by reducing the risk of accidental or malicious image tampering
- Reduce the time it takes to ensure that every VM in your datacenter is running authorized and trusted software.

© 2012 IBM Corporation

Trusted Boot Pre-Requisites

POWER7 C model (or later) for firmware 740-xxx

AIX 6 TL7 or AIX 7 TL1 (and VIOS 2.2.1.4)

- Sorry: no Linux or IBM i

PowerSC documentation page 11-16

http://pic.dhe.ibm.com/infocenter/aix/v6r1/topic/com.ibm.aix.powersc/powersc_pdf.pdf

IBM

Trusted Boot Architecture

While booting the firmware, boot loader & AIX we save details in the VTPM

- Virtual Trusted Platform Module

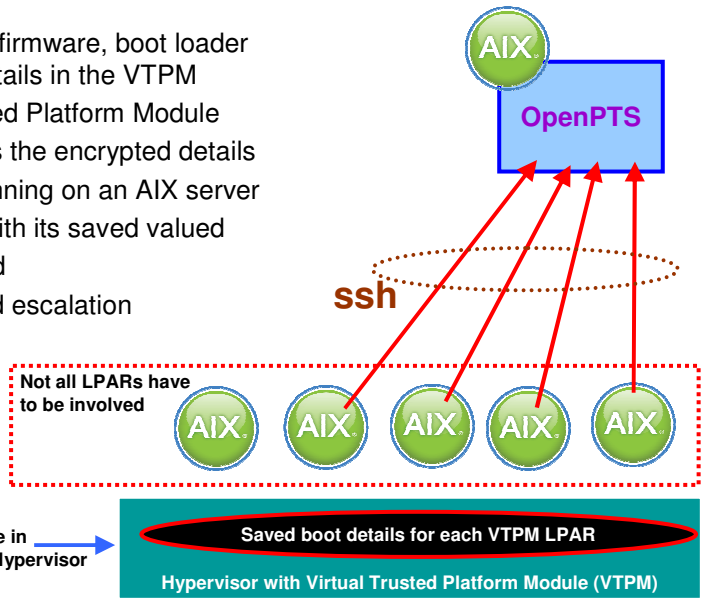
OpenPTS extracts the encrypted details

- Software running on an AIX server

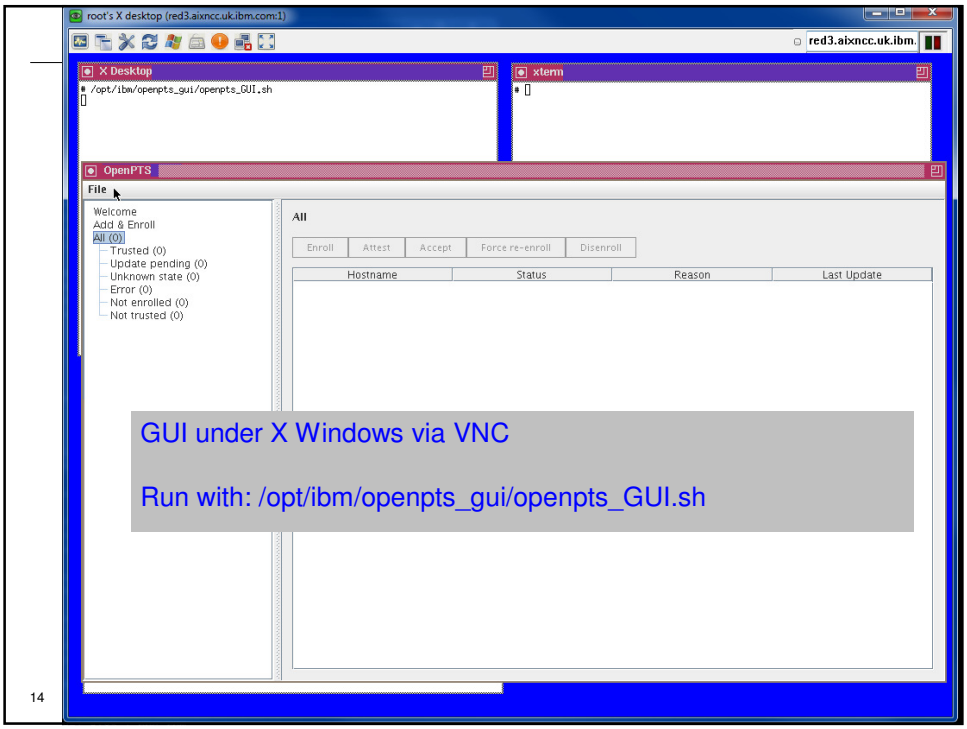
Then compared with its saved valued

If the same = Valid

If different = Need escalation



13

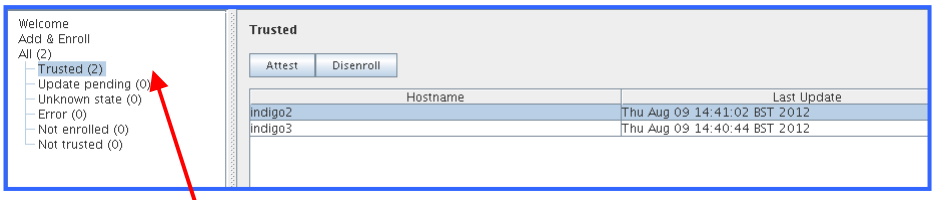


14

IBM

Setup ssh and Enrol you AIX LPARs

"Enrol" captures current VTPM encrypted settings = Master



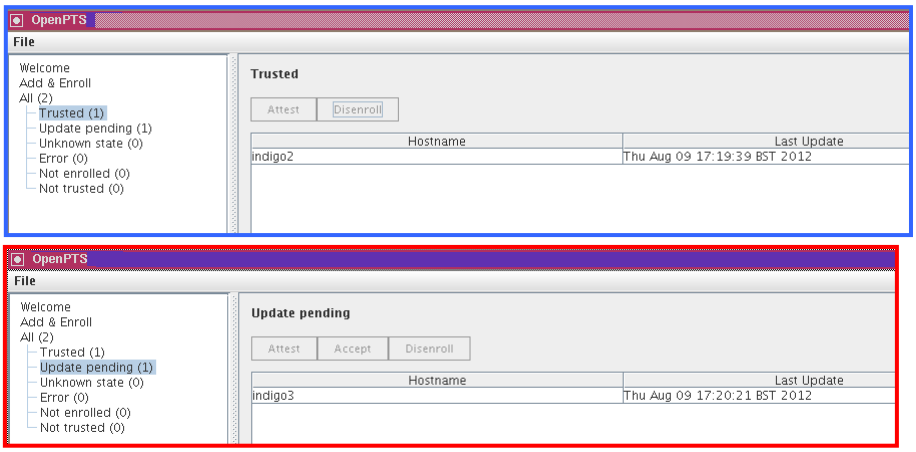
List of Trusted hosts = Good

© 2012 IBM Corporation

IBM

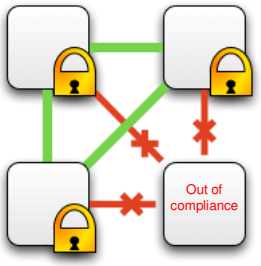
Modified a boot image → it is noticed

Ran bosboot on one LPAR – Can you tell which?



© 2012 IBM Corporation

PowerSC – Trusted Network Connect and Patch



How PowerSC works:
• An image that does not meet trusted patch levels will trigger an alert to the administrator
• It is not allowed access to the protected network as it's a known weakness (missing security enhancements)
• Can automatically update by NIM then allowed

Overview

Challenge: Ensure that images are trusted and at the proper patch level when they connect to the network.

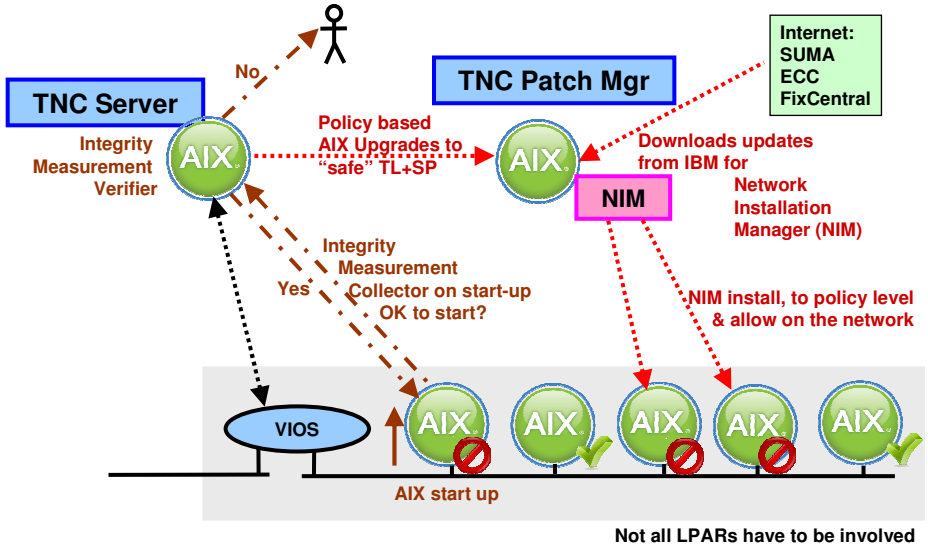
PowerSC Solution: Trusted Network Connect and Patch Management detects noncompliant virtual machines during activation and alerts administrators immediately. Offers automated updating of AIX (via NIM)

Benefits

- Reduce business risk by active notification of down level systems via email and SMS.
- Lower admin costs by automatically spotting non compliant systems within the virtual data center and cloud environments
- Lower costs of demonstrating compliance. Monitoring at virtual machine activation proves compliance to patch policy

© 2012 IBM Corporation

Trusted Network Connect (TNC) Architecture

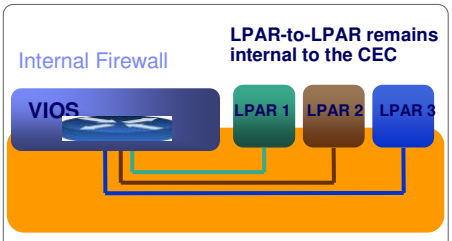


Not all LPARs have to be involved

All communication uses ssh
TNC Server and Patch Manager can be the same machine

© 2012 IBM Corporation

PowerSC – Trusted Firewall



How PowerSC works:

Provides network isolation and layer 2,3,4 firewalling between workloads

This Firewall will be provided within the VIOS & between Virtual Networks

Overview

Challenge: No LPAR-to-LPAR firewall protection so all network traffic must be routed via an external Firewall and hairpin turn back into the Power System. Customer needs to purchase high bandwidth router based Firewall hardware

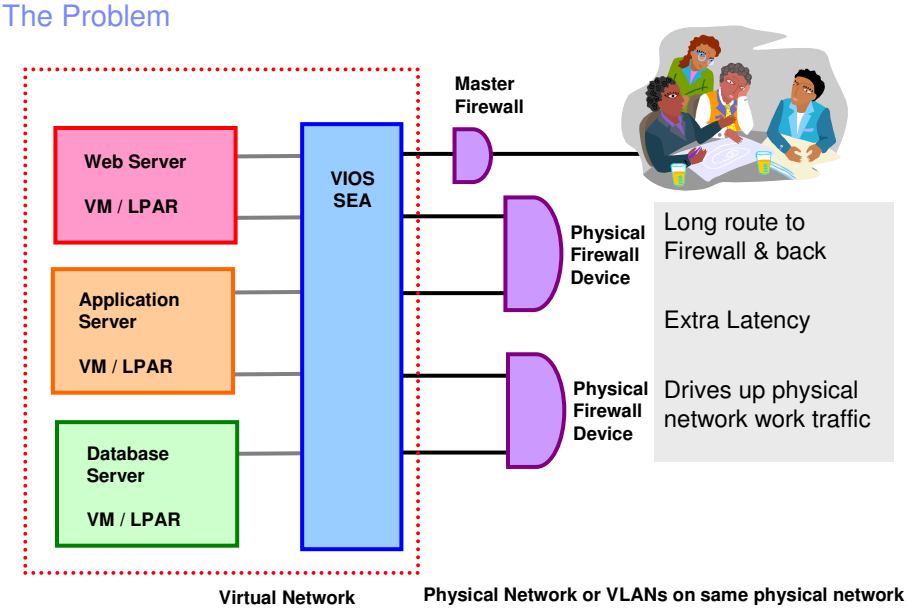
Power SC Solution: Provide a VIOS based Firewall managed by VIOS.

Benefits

- Provides network firewall services within the local server virtualization infrastructure to control network traffic between virtual workloads
- Improves performance by providing network firewall services within the server, which does not require an external firewall for VM-to-VM traffic on the same server
- Reduces network resource consumption by eliminating the need to use the external network for VM-to-VM traffic when virtual machines are running on the same server

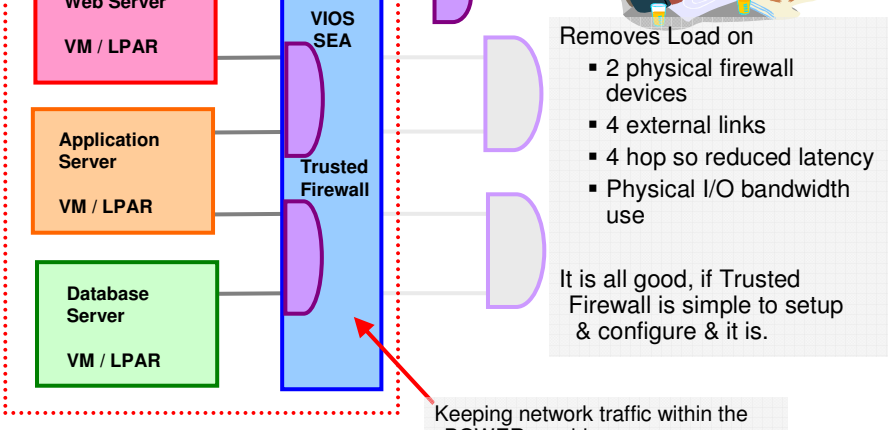
© 2012 IBM Corporation

The Problem



© 2012 IBM Corporation

The Trusted Firewall Solution



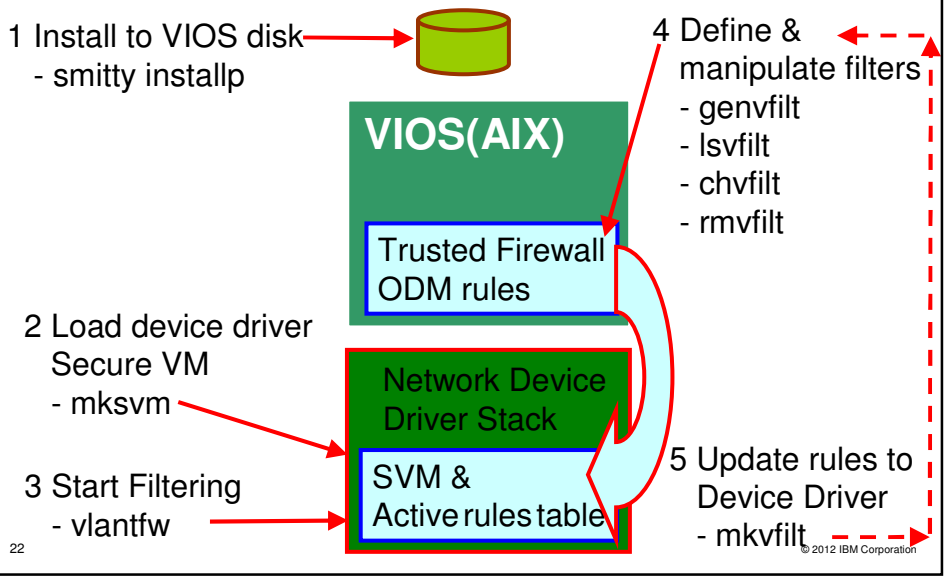
Removes Load on
- 2 physical firewall devices
- 4 external links
- 4 hop so reduced latency
- Physical I/O bandwidth use

It is all good, if Trusted Firewall is simple to setup & configure & it is.

Virtual I/O Server 2.2.1.4
Any supported OS as it is internal to VIOS

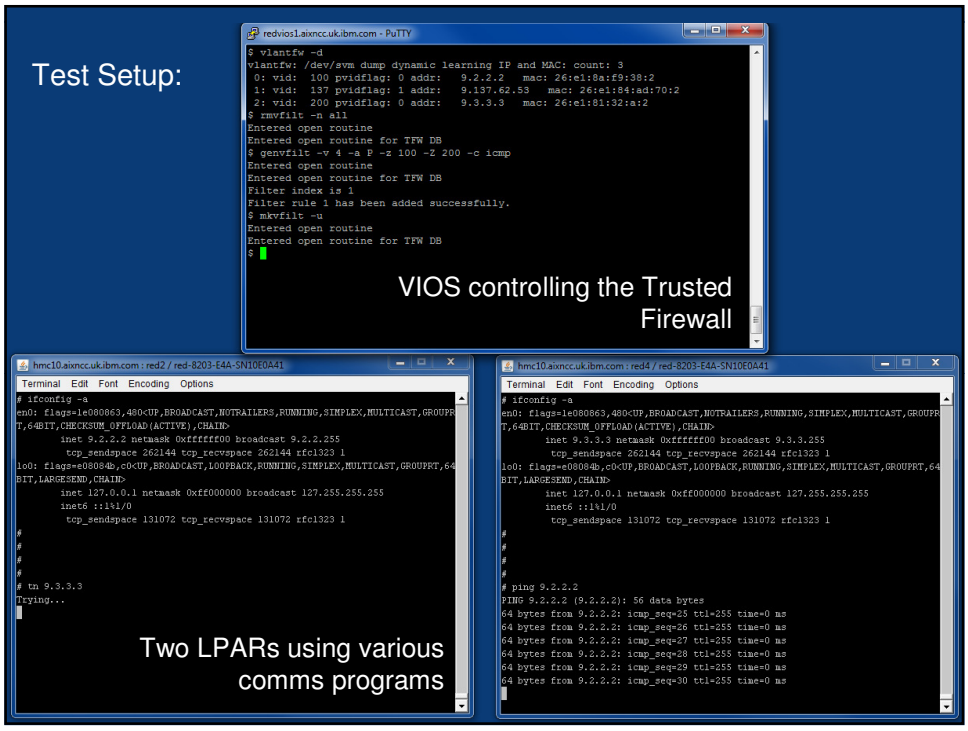
© 2012 IBM Corporation

Five stages to get the Firewall configured



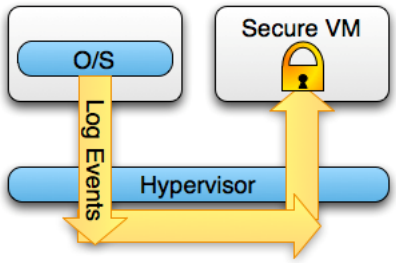
© 2012 IBM Corporation

Selling IBM STG Systems Software to Business Partners



PowerSC Standard Edition

PowerSC – Trusted Logging



How PowerSC works:
- Trusted Logging provides tamperproof secure centralized protection for AIX audit and system logs and is integrated with PowerVM virtualization
- Limited access to the Secure VM (VIOS) to a few privileged super users
- Guest VM logs can be managed and backed up from a single location within each physical server
- Log scraping agents and reporting agents can be removed from guest OS

Overview

Challenge: Prevent malicious users from "covering their tracks."

Power SC Solution: Move log events to a secure external VM via the hypervisor. Centralized logging ensures that even when virtual machines are discarded the audit logs remain on the central location for audit purposes.

Benefits

- Discourage malicious activity by ensuring individual accountability; trace actions to authenticated individuals.
- Reduce the time it takes to identify tampering and/or unauthorized changes
- Reduce the time it takes to demonstrate Security Compliance by maintaining strict control over audit logs.

© 2012 IBM Corporation

IBM

Trusted Logging Pre-Requisites

Virtual I/O Server 2.2.1.0
- Latest = currently 2.2.1.4 recommended

AIX 6 TL7+

AIX 7 TL1+
- With all service packs recommended

Any hardware that runs the above

PowerSC documentation page 22 -24
http://pic.dhe.ibm.com/infocenter/aix/v6r1/topic/com.ibm.aix.powersc/powersc_pdf.pdf

VIOS Documentation page 144 - 149
http://pic.dhe.ibm.com/infocenter/powersys/v3r1m5/topic/p7hb1/p7hb1.pdf

© 2012 IBM Corporation

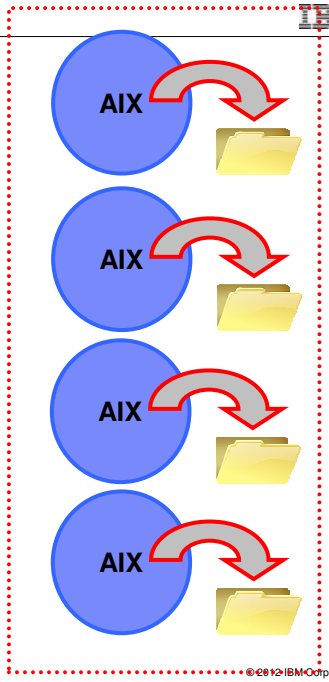
IBM

Logging Alternatives

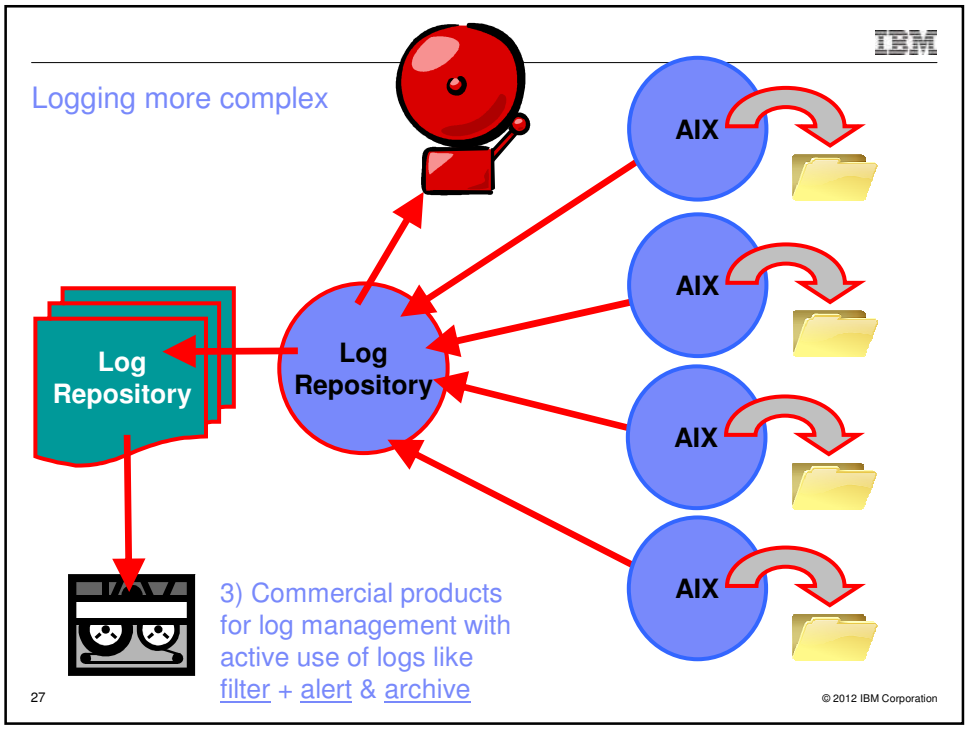
1) Local default AIX Logging

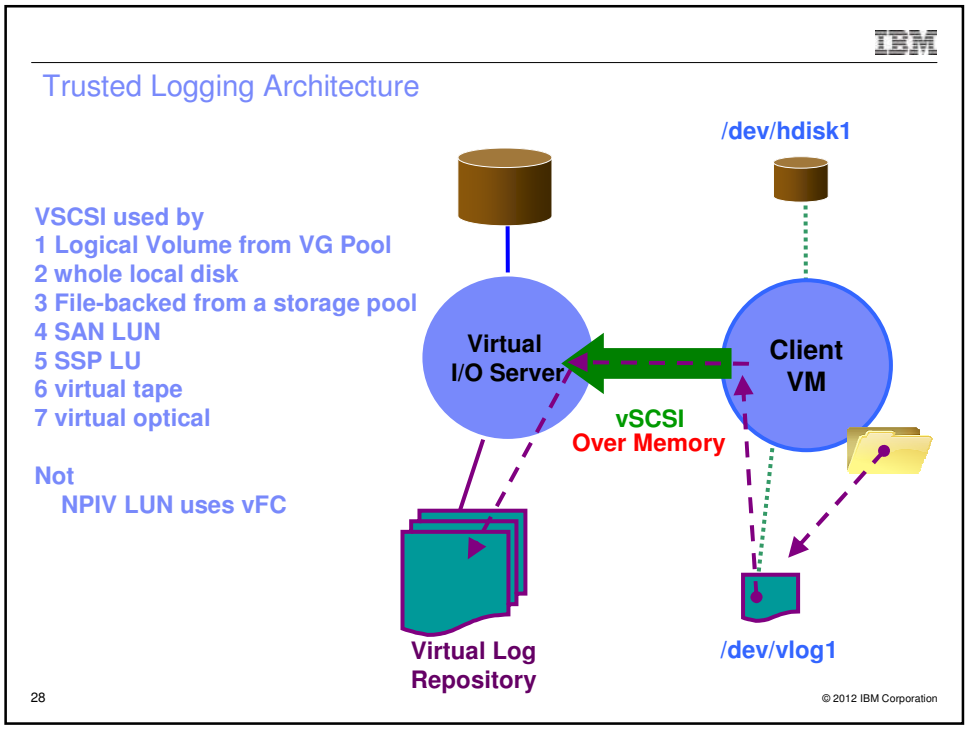
Risks: Your nasty hacker could
- shuts down logging
- removes log
- edits log
- destroys the LPAR and
  we will never work out how/why!

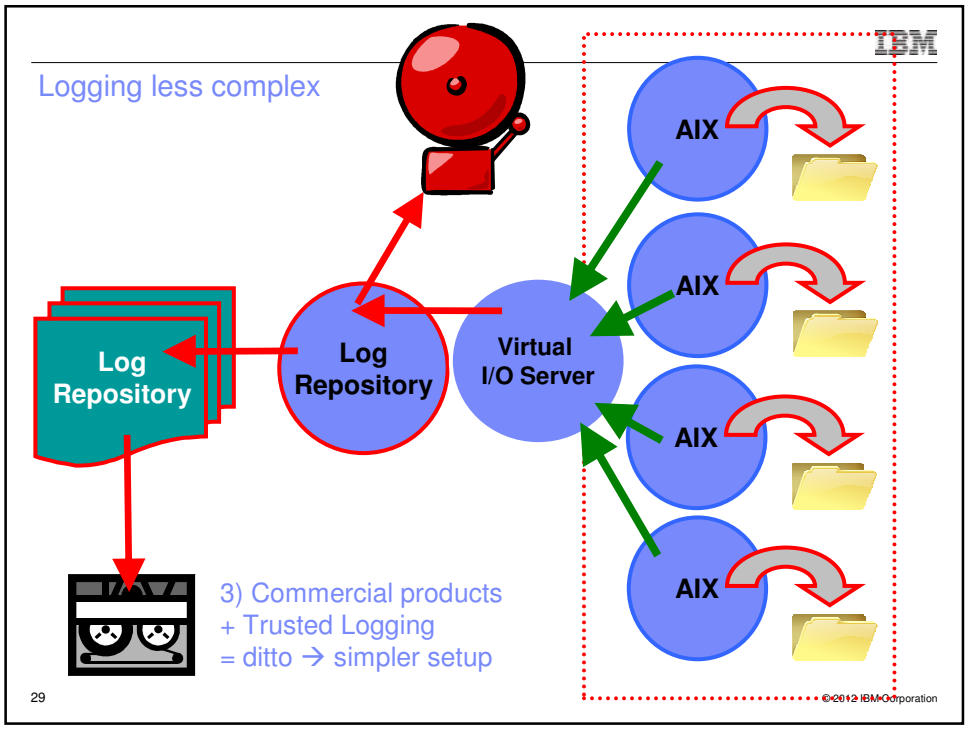
= No post-mortem analysis

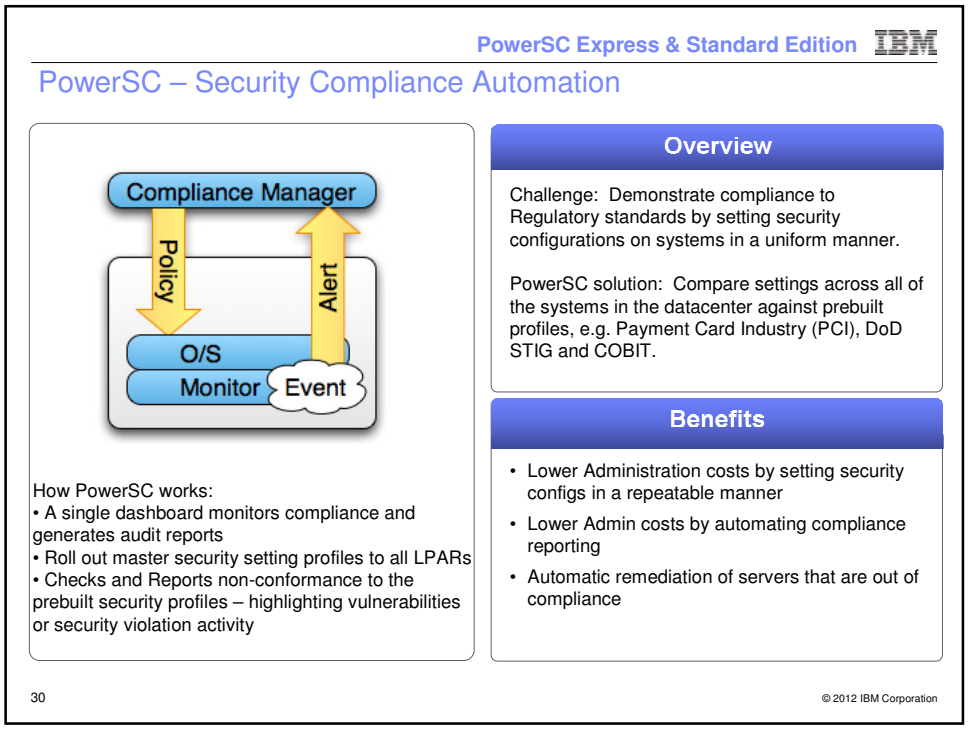


© 2012 IBM Corporation


IBM
Logging more complex
AIX
AIX
AIX
AIX
Log
Repository
Log
Repository
3) Commercial products
for log management with
active use of logs like
filter + alert & archive
27
© 2012 IBM Corporation


IBM
Trusted Logging Architecture
/dev/hdisk1
VSCSI used by
1 Logical Volume from VG Pool
2 whole local disk
3 File-backed from a storage pool
4 SAN LUN
5 SSP LU
6 virtual tape
7 virtual optical
Not
NPIV LUN uses vFC
Virtual
I/O Server
Client
VM
vSCSI
Over Memory
Virtual Log
Repository
/dev/vlog1
28
© 2012 IBM Corporation

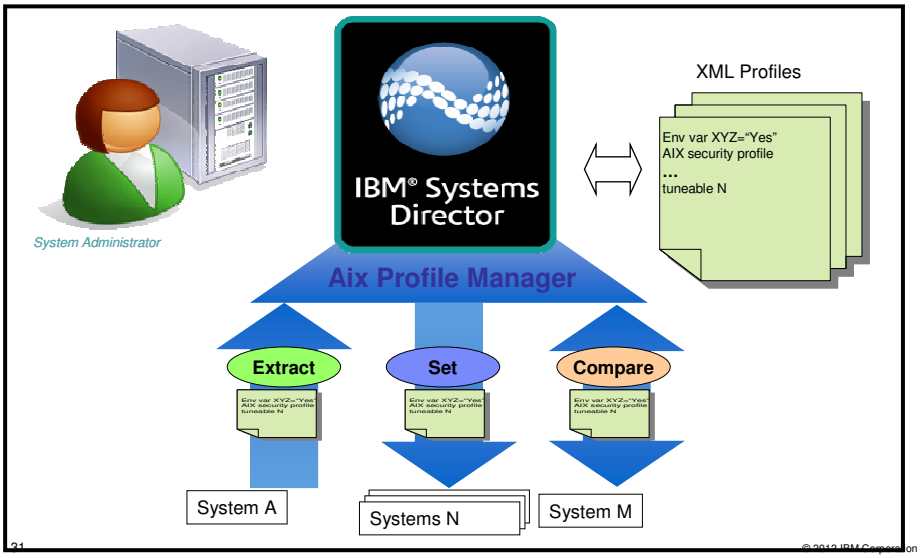

Logging less complex
AIX
AIX
AIX
AIX
Log Repository
Log Repository
Virtual I/O Server
3) Commercial products
+ Trusted Logging
= ditto → simpler setup
29
© 2012 IBM Corporation


PowerSC Express & Standard Edition
PowerSC – Security Compliance Automation
Compliance Manager
Policy
Alert
O/S
Monitor
Event
How PowerSC works:
• A single dashboard monitors compliance and generates audit reports
• Roll out master security setting profiles to all LPARs
• Checks and Reports non-conformance to the prebuilt security profiles – highlighting vulnerabilities or security violation activity
Overview
Challenge: Demonstrate compliance to Regulatory standards by setting security configurations on systems in a uniform manner.
PowerSC solution: Compare settings across all of the systems in the datacenter against prebuilt profiles, e.g. Payment Card Industry (PCI), DoD STIG and COBIT.
Benefits
• Lower Administration costs by setting security configs in a repeatable manner
• Lower Admin costs by automating compliance reporting
• Automatic remediation of servers that are out of compliance
30
© 2012 IBM Corporation

IBM

AIX Profile Manager Architecture

A Systems Director plug-in simple & consistency across multiple systems



© 2012 IBM Corporation

IBM

Security and Performance Profiles

XML paragraphs of setting used by 2 AIX commands

- ARTEX is the performance settings command
- aixpert is the security setting command

Capture the settings from a "reference" machine

Profiles for IT standard requirements supplied with PowerSC Express

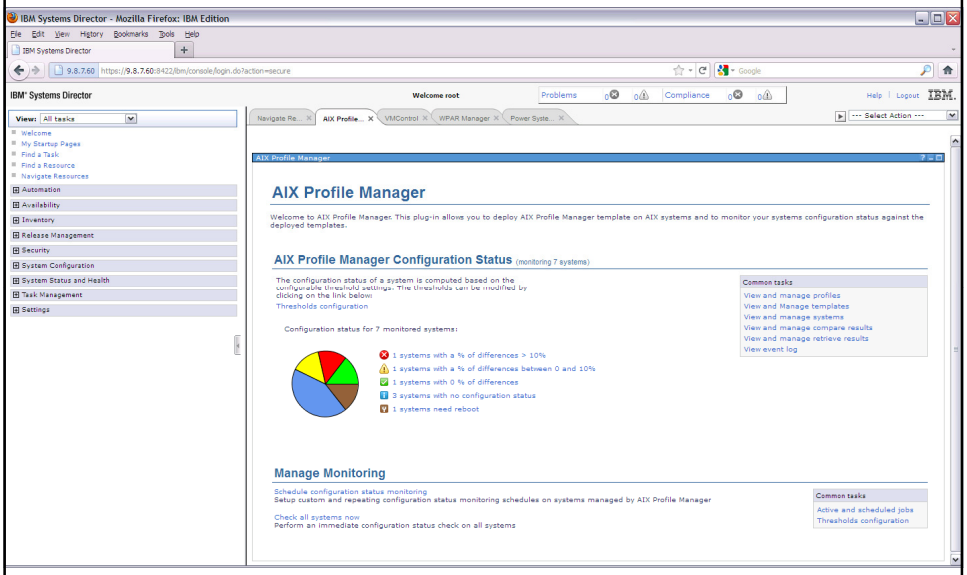
You can use these manually on each AIX (man-power intensive)

PowerSC & AIX Profile machine to Systems Director (ISD) allows

- Mass roll-out of a master set of profiles
- Via simple ISD user interface or command line
- Regular checking & reporting of mismatches from the master settings
- Updating master settings by set, update, capture

© 2012 IBM Corporation

Example of Systems Director AIX Profile Manager



© 2012 IBM Corporation

Reference Slide

Compliance Automation – PCI profile as an example

Payment Card Industry Data Security Standard v2.0

- Applies to any part of IT that processes, passes or stores credit card information. (https://www.**pci**securitystandards.org/)
- PCI-DSS requirements 70 pages document which describes 12 major security and security configuration sections.
  - Requirement 1: Build and Maintain a Secure Network
  - Requirement 2: Protect Cardholder Data
  - Requirement 3: Protect stored cardholder data
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks
  - Requirement 5: Use and regularly update anti-virus software or programs
  - Requirement 6: Develop and maintain secure systems and applications
  - Requirement 7: Restrict access to cardholder data by business need to know
  - Requirement 8: Assign a unique ID to each person with computer access.
  - Requirement 9: Restrict physical access to cardholder data
  - Requirement 10: Track and monitor all access to network resources and cardholder data.
  - Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security for employees and contractors

PowerSC PCI-DSS Coverage

- Approximately 126 XML rules to assist in the configuration in 7 of the 12 requirement areas.

IBM does not promise a profile will guarantee you are conformant – it is a very good start point & could save you man years of effort

© 2012 IBM Corporation

IBM

"But I've already written Scripts to check Security and Compliance"

A: Home Grown scripts are expensive to maintain and error prone:

- Who certifies to auditors that these scripts match security standards?
- Are scripts secure to modification or tampering?
- What is the cost of maintenance of scripts?
- Who monitors data security standards and ensures that the scripts are updated?
- Is there a standard set of scripts in the company or does every group roll their own?
- What happens when the author of the scripts leave the company?
- Do all administrators understand what the scripts do and what are the expected results?

- How fast do you detect some one "fiddling"? 1 day, 1 month, next years audit?

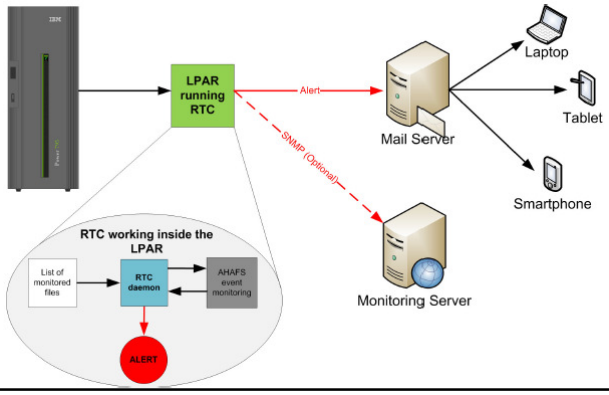
- **If you don't have two+ people working full-time on security then the hackers will overwhelm you as they are 100% full-time. So get the IBM security team fighting for you by using their tools.**

© 2012 IBM Corporation

IBM

Real-Time Compliance (RTC)

Built in to the AIX Kernel so no polling or cron scripts
As the resource is changed the AIX kernel immediately takes action
Actions are Email or SNMP trap
Built around a AIX Autonomic Health Advisor File System (AHAFS1)



© 2012 IBM Corporation

IBM

Real-Time Compliance (RTC)

Pre-req: AIX 6 TL7+ and AIX 7 TL1+
Install PowerSC Express
- powerscExp.rtc & powerscExp.license

Configure with: smitty RTC
- To set a email server and address

It is an AIX subsystem:
- lssrc -s rtcd
- stopsrc -s rtcd
- startsrc -s rtcd

Config file of pre-defined monitoring is in /etc/security/rtc/rtcd_policy.conf
- Edit this and start stop or use the chsec command

Problems also go in to the syslogd (if you have it switched on)

© 2012 IBM Corporation

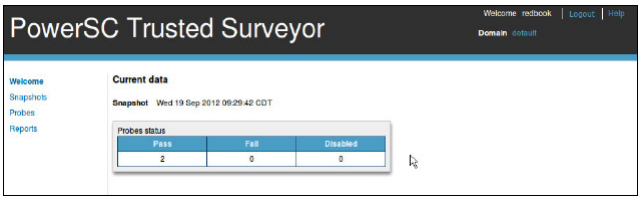
IBM

Trusted Surveyor

Separate LPP and cost
- You get different media & look for package: powersc.ts

Installed on AIX via installp
- Then you create a users and roles

It runs a web server
- All access is then via a web browser: Firefox 14+ IE8+



© 2012 IBM Corporation

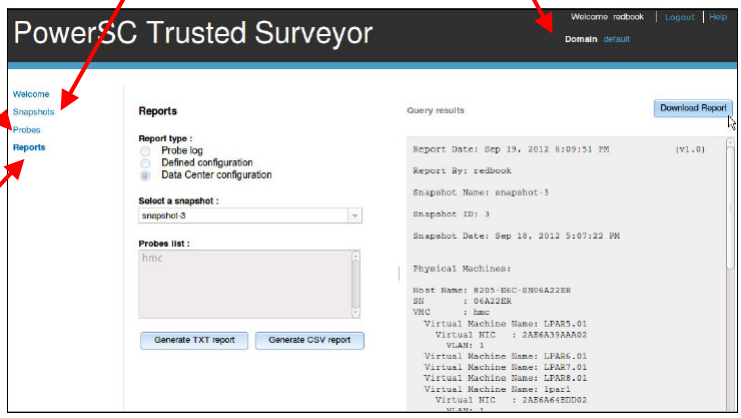
IBM

Trusted Surveyor

Domains to group machines

Snapshots to get the data

Probes to get information from HMC, IVM, … etc.



Reports of VM & VLANS in text or CSV

IBM

PowerSC Reduces the Cost and Complexity
Trusted Boot and Trusted Execution

	Before		After								
OpEx	(25min	-	< 2 min)	x	12	=	276 min	X	500	=	96 days
	Time per VM with manual scan		Time per VM with PowerSC virtual security		Manual scans run once/month		Time savings per VM		VMs per Datacenter		Total Datacenter Time per Year
						=	$166	X	500	=	$83,000
							Cost per VM		VMs per Datacenter		Total Datacenter Savings per Year

Assumptions:
•Before: Maintain a hash list of all trusted executables list 8 hours per year. Includes 25 min to login, compare trusted hash list to system install list, monitor results and remediate a percentage of the systems.
•After: Run Attestation from central console on anyone particular system or all systems

Pocket the savings while you enjoy these additional PowerSC Advantages:
- Improved Systems performance compared with "Known Bad" model scans like Symantec antivirus that slow your systems to a crawl.
- Reduced business risk with real time trusted execution compliance checks

PowerSC™

© 2012 IBM Corporation

IBM

PowerSC Reduces Cost and Complexity
Trusted Network Connect

OpEx

Before

20 min	x	52	x	500	=	520,000 min
Time per VM to manually confirm SW level and install patch		Weekly scans		VMs per Datacenter		Total Time

After

480 min	519,520	361	$ 311,712
Automatic monitoring with minor policy maintenance	Total Time Savings (mins)	Total Time Savings days	Total Datacenter Savings per Year

Pocket the savings while you enjoy these additional PowerSC Advantages:
- Actively detect compliance vulnerabilities
- Reduce your business risk from VMs that were paused or shutdown during a maintenance update and then restarted and joined the network with unpatched vulnerabilities.

PowerSC™

© 2012 IBM Corporation

IBM

PowerSC Reduces Cost and Complexity
Security Compliance Automation

OpEx

Before		After								
(150 min	-	10 min)	x	12	=	1,680 min	X	500	=	583 days
Time per VM to review 70-200 Security Settings		Time per VM with PowerSC virtual security		Monthly Scans		Time savings per VM		VMs per Datacenter		Total Datacenter Time per Year
					=	$1,008	X	500	=	$504,000
						Cost savings per VM		VMs per Datacenter		Total Datacenter Savings per Year

Assumptions:
•Before: manual process of setting or monitoring dozens of compliance configuration settings or maintaining home grown scripts, error prone.
•After: completely automated showing exceptions

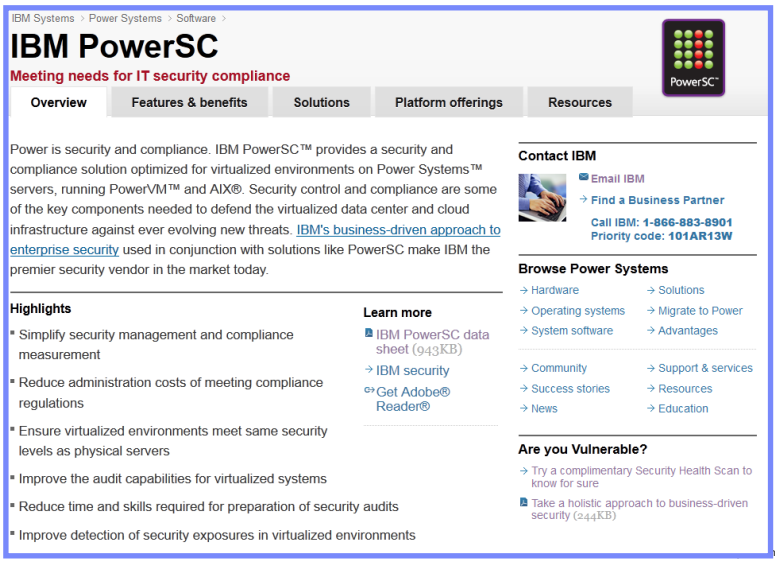
Pocket the savings while you enjoy these additional PowerSC Advantages:
- Smile when there's an audit! Count on PowerSC to produce your compliance report for *every image* in the AIX datacenter in under 10 mins.
- Use PowerSC templates to reduce errors in interpreting and applying complex regulatory standards like PCI, DoD STIG, and COBIT.

PowerSC™

© 2012 IBM Corporation

Learn more about PowerSC on the Web

http://www.ibm.com/systems/power/software/security/



IBM DeveloperWorks PowerSC Hands-On Wiki Page

https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Power%20Systems/page/PowerSC%20POWER%20Security%20and%20Compliance%20Toolset

- - or - -

http://tinyurl.com/newAIXwiki

and take the PowerSC link

http://youtube.com/user/nigelgriffiths

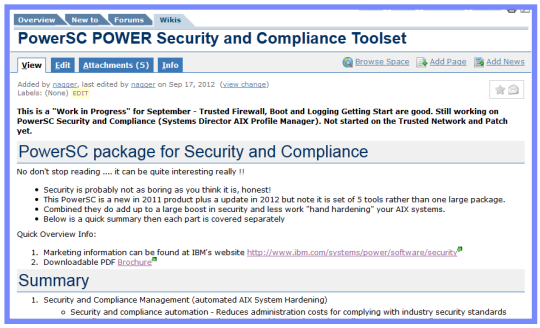
Videos on

Trusted Boot

Trusted Logging

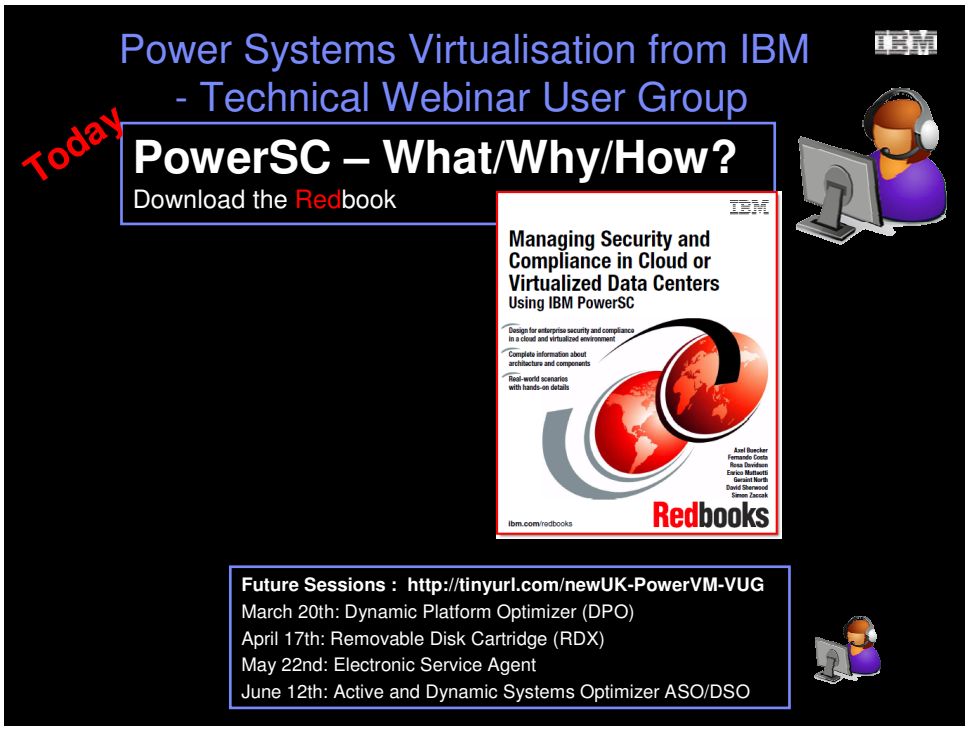
Trusted Firewall (short-cut)

for AIX aixpert and fpm



What more Information?

•PowerSC Redbook

© 2012 IBM Corporation

Selling IBM STG Systems Software to
Business Partners