

Stockholm, Sweden
POWER & AIX Workshop
Nov 2012



PowerSC Overview


Power Systems Security & Compliance



Nigel Griffiths
IBM Power Systems
Advanced Technology Support, Europe

Presentation Version 5



© 2012 IBM Corporation



PowerSC → **security** and **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



2

© 2012 IBM Corporation

Selling IBM STG Systems Software to Business Partners



PowerSC Editions

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


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

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

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

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

3
© 2012 IBM Corporation



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.

- 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 been certified for EAL4+ Common Criteria

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



4

† 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



AIX Security is already excellent - How can we raise it to brilliant!

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?



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

Just announced two more tools

6. **Real-time alerts** – no more periodic script running/polling

7. **Trusted Surveyor** – checks all LPARs on a VLAN + reports changes

Selling IBM STG Systems Software to Business Partners





PowerSC Moves to “Known Good Model”

Only Allow Known Trusted Software to Run


Security Vulnerability Detection tends to work on a **“Known Bad Model”** This reactive model blocks intrusions based on historical break-ins .

PowerSC Trusted Boot employs a more efficient **“Known Good Model”** which only allows trusted images to run.

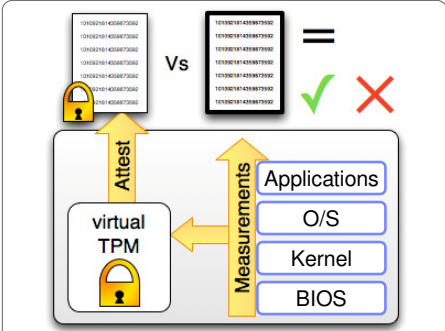
Power Systems are “hermetically sealed” with **tight interlocks** between the hardware, virtualization and software.

7
© 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.

8
© 2012 IBM Corporation

Selling IBM STG Systems Software to Business Partners

IBM

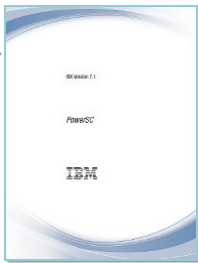
Trusted Boot Pre-Requisites

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



9

IBM

Trusted Boot Architecture

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

- Virtual Trusted Platform Module

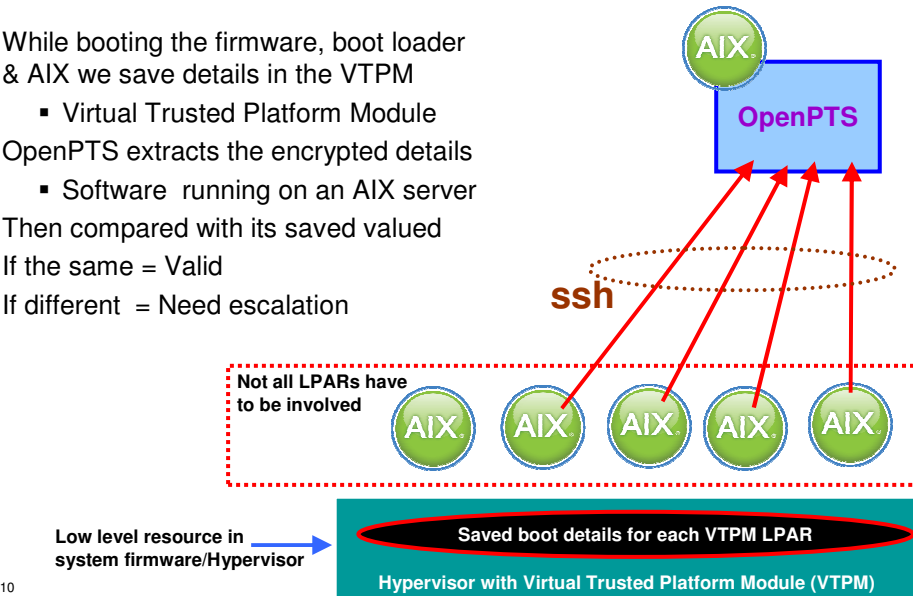
OpenPTS extracts the encrypted details

- Software running on an AIX server

Then compared with its saved values

If the same = Valid

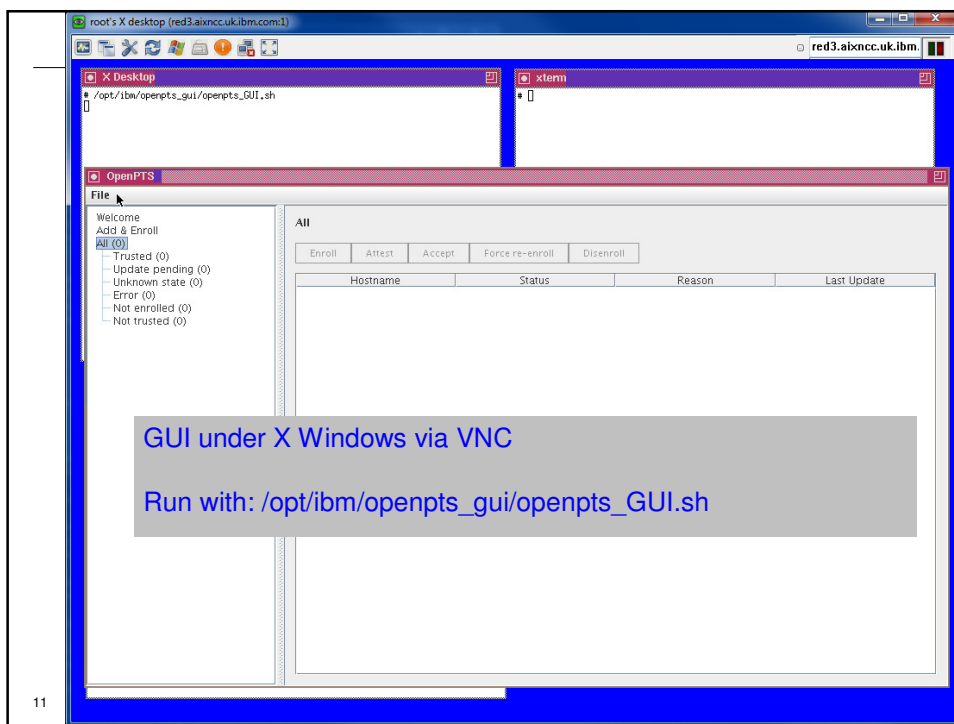
If different = Need escalation




The diagram illustrates the Trusted Boot Architecture. At the bottom, a teal box represents the 'Hypervisor with Virtual Trusted Platform Module (VTPM)', which contains 'Saved boot details for each VTPM LPAR'. An arrow labeled 'Low level resource in system firmware/Hypervisor' points to this box. Above the hypervisor, a red dashed box contains five green circles, each labeled 'AIX.'. A note states 'Not all LPARs have to be involved'. Red arrows labeled 'ssh' point from the AIX servers to a blue box labeled 'OpenPTS'. A green circle labeled 'AIX.' is positioned above the OpenPTS box.

10

Selling IBM STG Systems Software to Business Partners



11



Setup ssh and Enrol you AIX LPARs

“Enrol” captures current VTPM encrypted settings = Master

Welcome

Add & Enroll

All (2)

- Trusted (2)
- Update pending (0)
- Unknown state (0)
- Error (0)
- Not enrolled (0)
- Not trusted (0)

Trusted

Attest
Disenroll

Hostname	Last Update
indigo2	Thu Aug 09 14:41:02 BST 2012
indigo3	Thu Aug 09 14:40:44 BST 2012

List of Trusted hosts = Good

12

Selling IBM STG Systems Software to Business Partners

IBM

Modified a boot image → it is noticed

Ran bosboot on one LPAR – Can you tell which?

The image shows two screenshots of the OpenPTS console. The top screenshot, highlighted with a blue border, shows the 'Trusted' status for 'indigo2' with a 'Last Update' of 'Thu Aug 09 17:19:39 BST 2012'. The bottom screenshot, highlighted with a red border, shows the 'Update pending' status for 'indigo3' with a 'Last Update' of 'Thu Aug 09 17:20:21 BST 2012'. Both screenshots show a left-hand menu with options like 'Welcome', 'Add & Enroll', and 'All (2)'. The top screenshot also has 'Attest' and 'Disenroll' buttons, while the bottom one has 'Attest', 'Accept', and 'Disenroll' buttons.

13 © 2012 IBM Corporation

PowerSC Standard Edition IBM

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.

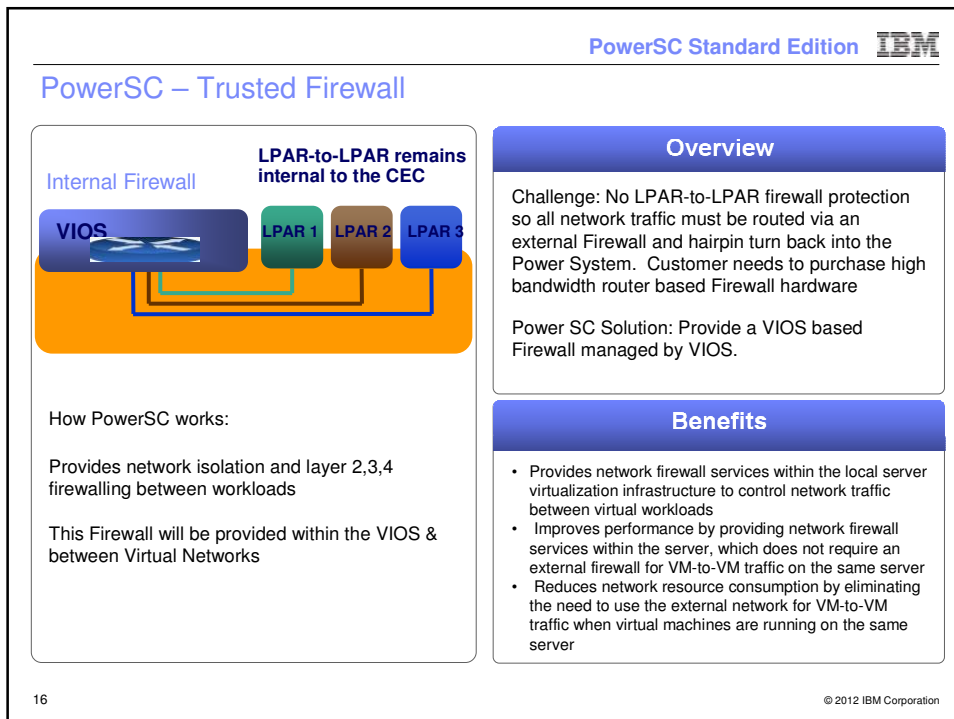
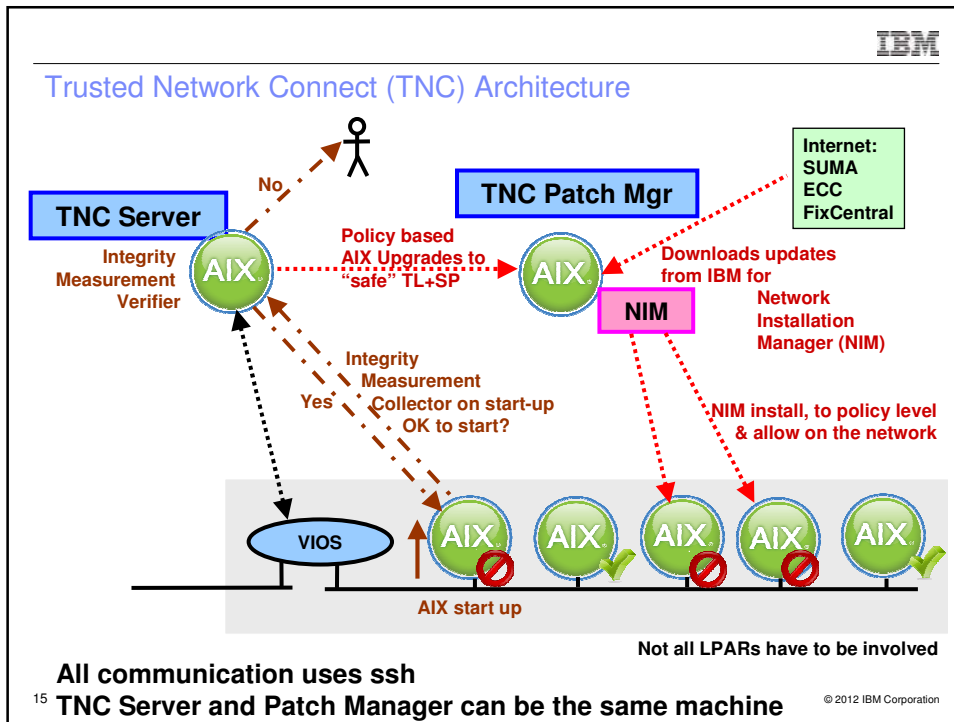
PowerSC Solution: Trusted Network Connect and Patch Management detects noncompliant virtual machines during activation and alerts administrators immediately. Offers automated updating of AIX (via NIM)

Benefits

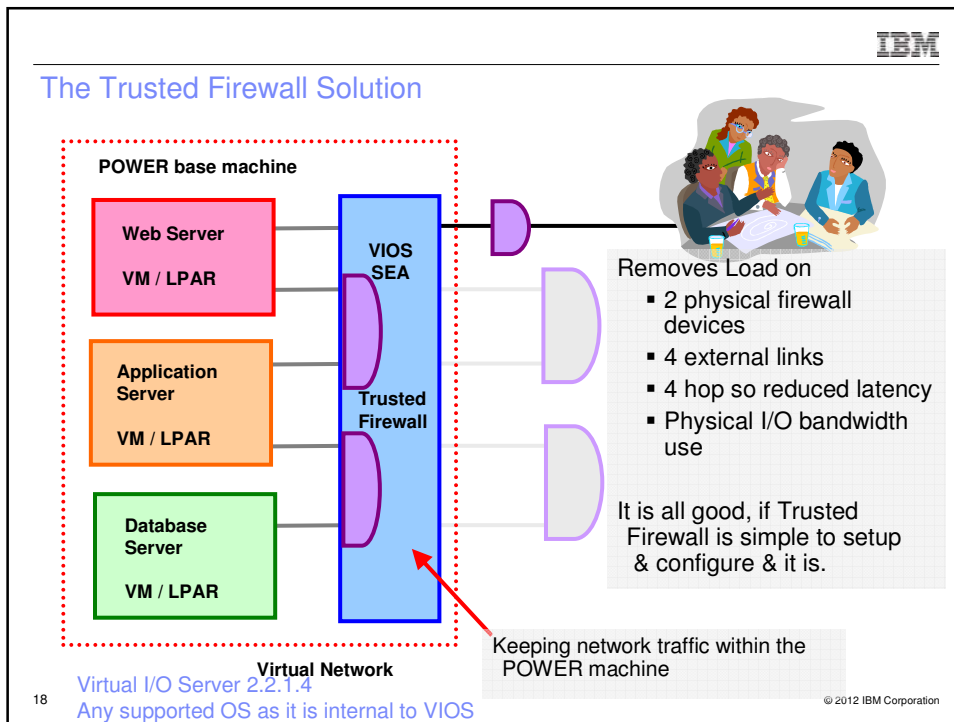
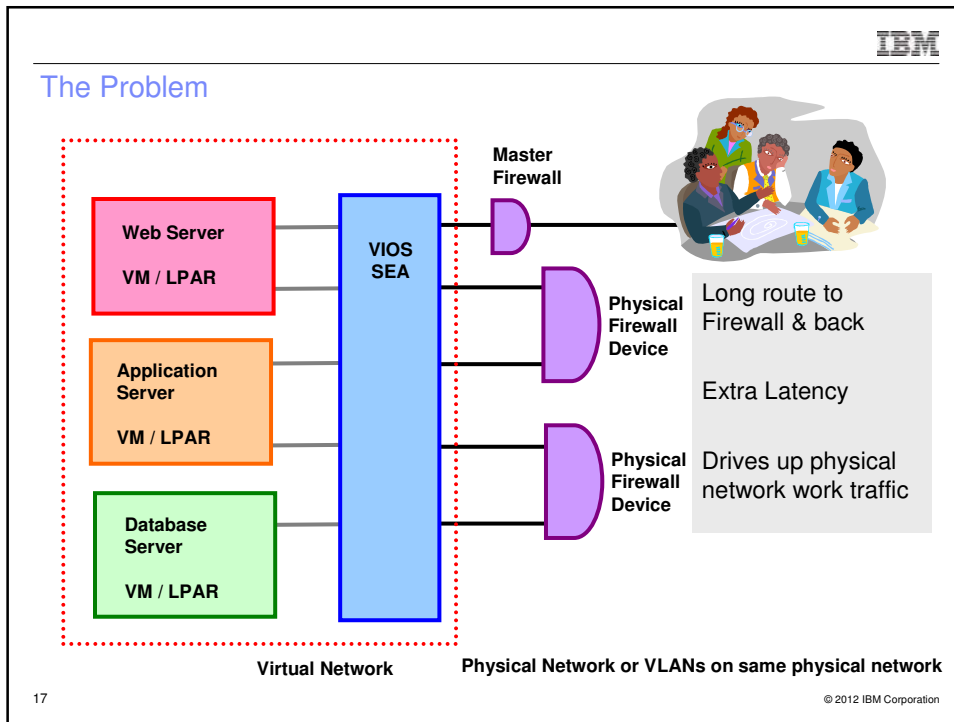
- Reduce business risk by active notification of down level systems via email and SMS.
- Lower admin costs by automatically spotting non compliant systems within the virtual data center and cloud environments
- Lower costs of demonstrating compliance. Monitoring at virtual machine activation proves compliance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

14 © 2012 IBM Corporation


Selling IBM STG Systems Software to Business Partners



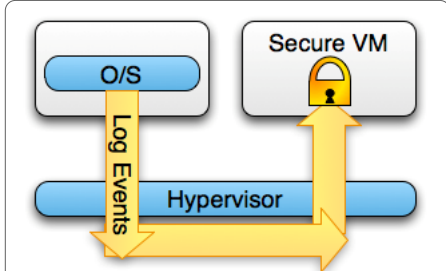
Selling IBM STG Systems Software to Business Partners



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.

21 © 2012 IBM Corporation



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>

22 © 2012 IBM Corporation

Selling IBM STG Systems Software to Business Partners

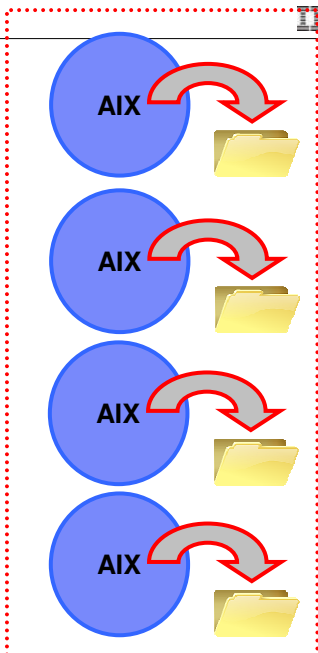
Logging Alternatives

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

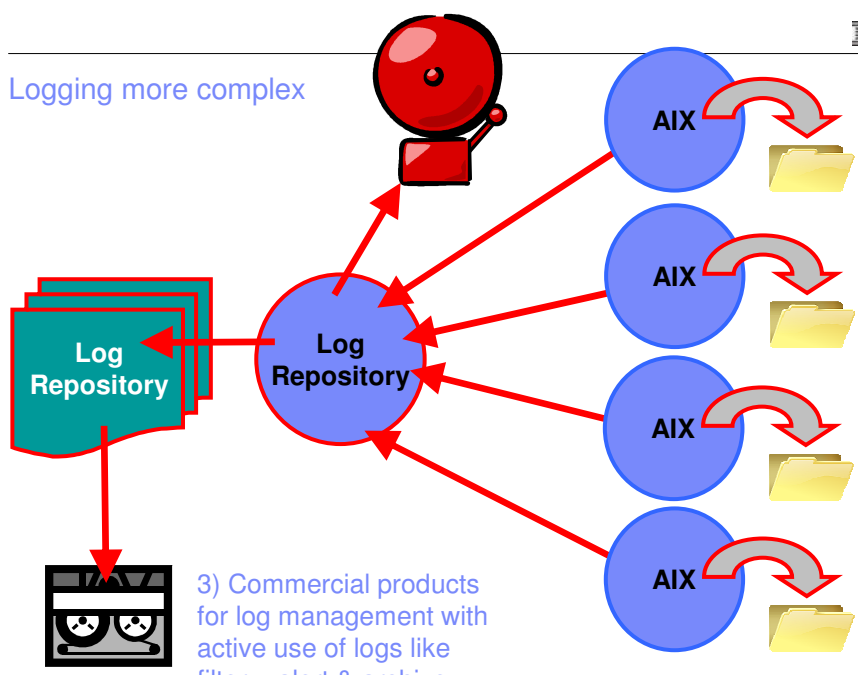


IBM

© 2012 IBM Corporation

23

Logging more complex



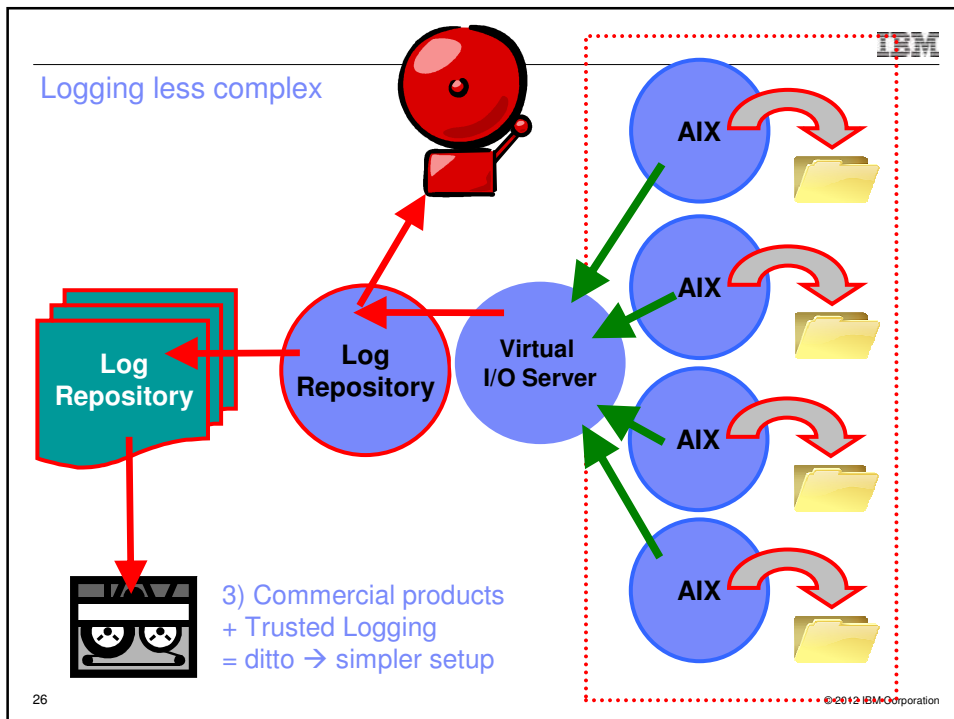
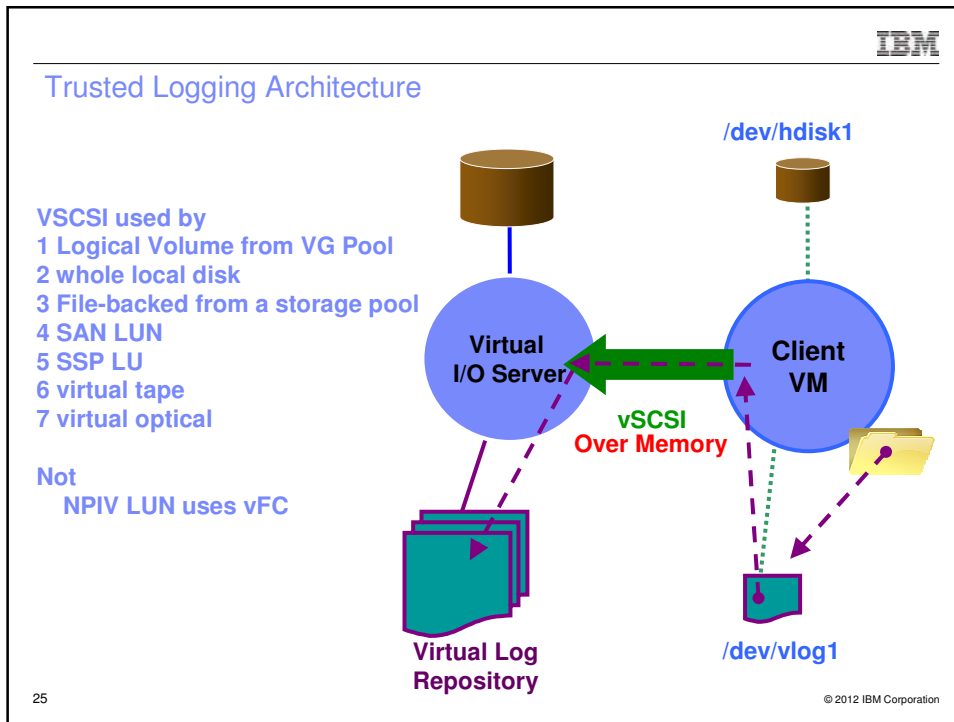
3) Commercial products for log management with active use of logs like filter + alert & archive

IBM


© 2012 IBM Corporation

24

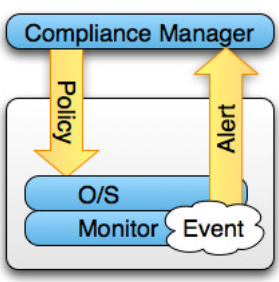
Selling IBM STG Systems Software to Business Partners



Selling IBM STG Systems Software to Business Partners

PowerSC Express & Standard Edition 

PowerSC – Security Compliance Automation



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

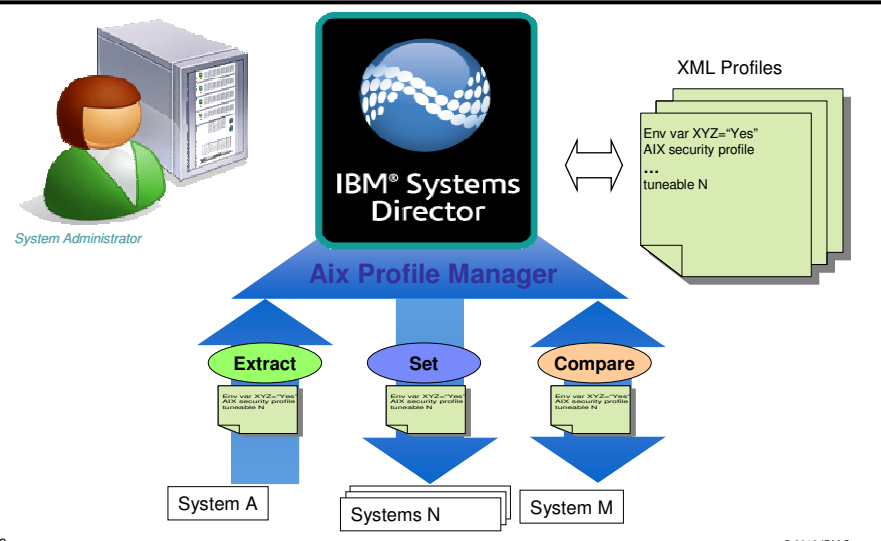
- Lower Administration costs by setting security configs in a repeatable manner
- Lower Admin costs by automating compliance reporting
- Automatic remediation of servers that are out of compliance

27 © 2012 IBM Corporation



AIX Profile Manager Architecture


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



The diagram illustrates the AIX Profile Manager architecture. At the top left, a **System Administrator** icon is shown. In the center is the **IBM® Systems Director** logo. Below it is the **Aix Profile Manager** component. To the right, **XML Profiles** are shown as a stack of documents with sample content: `Env var XYZ="Yes"`, `AIX security profile`, `...`, and `tuneable N`. Below the AIX Profile Manager are three main processes: **Extract**, **Set**, and **Compare**. **Extract** pulls data from **System A**. **Set** pushes data to **Systems N**. **Compare** pulls data from **System M**. Bidirectional arrows connect the AIX Profile Manager to the XML Profiles.

28 © 2012 IBM Corporation

Selling IBM STG Systems Software to Business Partners



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)

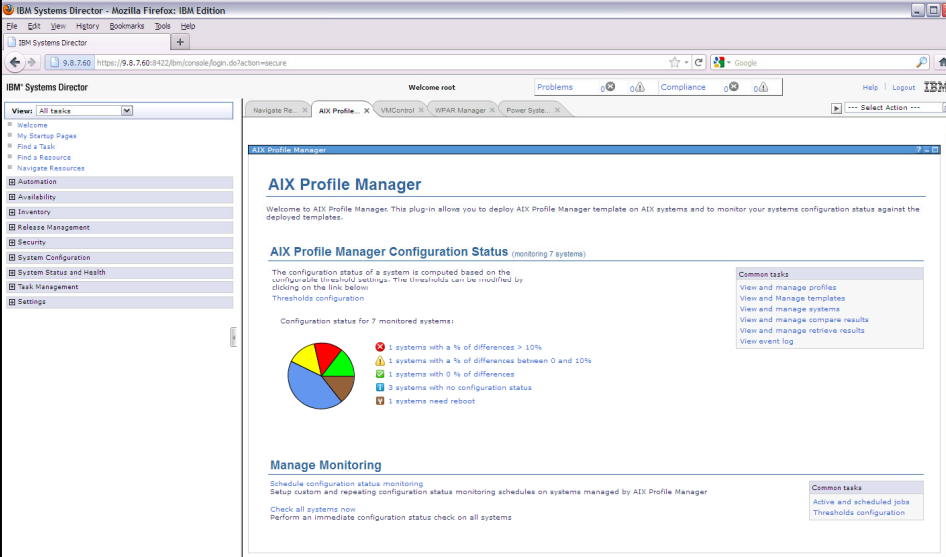
PowerSC & AIX Profile machine to Systems Director (ISD) allows

- 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

29 © 2012 IBM Corporation



Example of Systems Director AIX Profile Manager





The screenshot shows the IBM Systems Director AIX Profile Manager interface. The main content area displays the 'AIX Profile Manager Configuration Status' for 7 monitored systems. A pie chart shows the distribution of system configurations: 1 system with > 10% differences (red), 1 system with 4-10% differences (yellow), 1 system with 0% differences (green), 2 systems with no configuration status (blue), and 1 system needing a reboot (orange). The interface includes a left-hand navigation menu, a top navigation bar, and a right-hand 'Common tasks' panel.

30 © 2012 IBM Corporation

Selling IBM STG Systems Software to Business Partners

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.pcisecuritystandards.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 just a very good start point & could save you man years of effort**

31 © 2012 IBM Corporation




“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?



32 © 2012 IBM Corporation

Selling IBM STG Systems Software to Business Partners




PowerSC Reduces the Cost and Complexity Trusted Boot and Trusted Execution

OpEx	Before	After						
	(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



33 © 2012 IBM Corporation




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			
							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.



34 © 2012 IBM Corporation

Selling IBM STG Systems Software to Business Partners




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.




35
© 2012 IBM Corporation



Learn more about PowerSC on the Web

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

IBM Systems > Power Systems > Software >


IBM PowerSC

Meeting needs for IT security compliance

Overview
Features & benefits
Solutions
Platform offerings
Resources

Power is security and compliance. IBM PowerSC™ provides a security and compliance solution optimized for virtualized environments on Power Systems™ servers, running PowerVM™ and AIX®. Security control and compliance are some of the key components needed to defend the virtualized data center and cloud infrastructure against ever evolving new threats. [IBM's business-driven approach to enterprise security](#) used in conjunction with solutions like PowerSC make IBM the premier security vendor in the market today.

Highlights

- Simplify security management and compliance measurement
- Reduce administration costs of meeting compliance regulations
- Ensure virtualized environments meet same security levels as physical servers
- Improve the audit capabilities for virtualized systems
- Reduce time and skills required for preparation of security audits
- Improve detection of security exposures in virtualized environments

Learn more

- IBM PowerSC data sheet (943KB)
- IBM security
- Get Adobe® Reader®

Contact IBM

→ Email IBM

→ Find a Business Partner

Call IBM: 1-866-883-8901
Priority code: 101AR13W

Browse Power Systems

- Hardware
- Solutions
- Operating systems
- Migrate to Power
- System software
- Advantages
- Community
- Support & services
- Success stories
- Resources
- News
- Education

Are you Vulnerable?

- Try a complimentary Security Health Scan to know for sure
- Take a holistic approach to business-driven security (244KB)

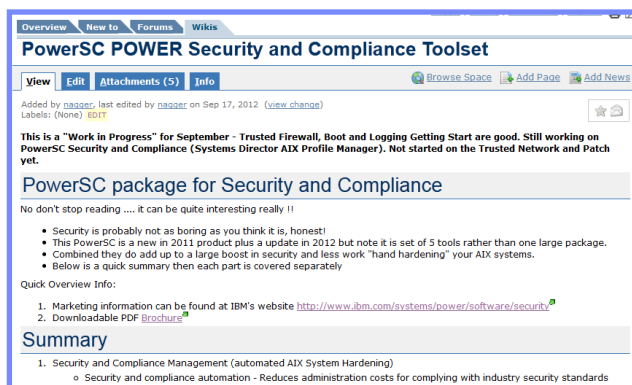
36

Selling IBM STG Systems Software to Business Partners



IBM DeveloperWorks PowerSC Hands-On Wiki Page

<https://tinyurl.com/PowerSC>



Social Media

- Nigel Griffiths on the [AIXpert blog](#) & follow on Twitter: [mr_nmon](#)
- Redbook
- IBM, BP & Customer Team working on the PowerSC [Redbook](#) Sept/Oct 2012