



# PowerSC Overview

## Power Systems Security & Compliance



**Nigel Griffiths**  
IBM Power Systems  
Advanced Technology Support, Europe

© 2013 IBM Corporation

### PowerSC has 7 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

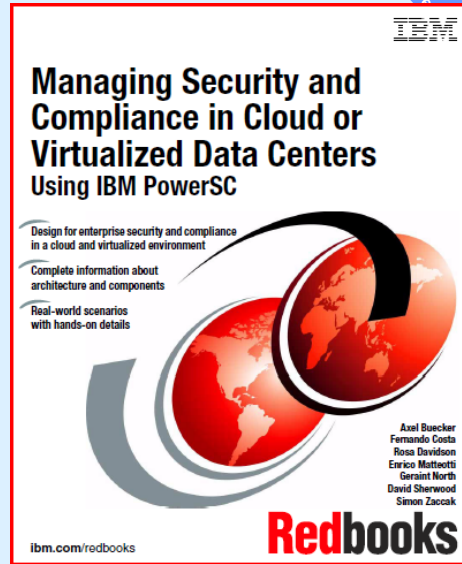
Announced late in 2012 two more tools

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

## 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



3 of 37

## PowerSC Packaging

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

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

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

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

**Top=1<sup>st</sup> Year License + 1 year SWMA**  
**Bottom=Subsequent years = SWMA**

4 of 37

## 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



† 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>

5 of 37

## 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**

6 of 37

AIX Security is already excellent



IBM  
© 2013 IBM  
PowerSC  
7

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

7 of 37

## 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



IBM  
© 2013 IBM  
PowerSC  
8

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

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

- [www.secnia.com](http://www.secnia.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.

8 of 37

## PowerSC and IBM i



IBM  
© 2013 IBM  
9

### 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
  - 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
  - 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
  - Password security
  - Authorizations to files/programs/
  - Manage users/system wide security settings
- ISV solutions for security & compliance provide additional advanced capabilities

~Trusted Logging

~Trusted Boot

~Trusted Security

### No equivalent IBM i functionality:

- Trusted Network Connect & Patch Management

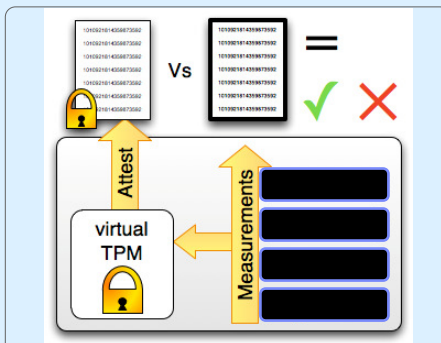
More info in the You and i blog entry - PowerSC and IBM i: Integration of Security:  
[http://ibmsystemsmag.blogs.com/you\\_and\\_i/2012/10/powersc-and-ibm-i-integration-of-security.html](http://ibmsystemsmag.blogs.com/you_and_i/2012/10/powersc-and-ibm-i-integration-of-security.html)

9 of 37

## PowerSC – Trusted Boot and Trusted Execution

PowerSC Standard Edition

IBM  
© 2013 IBM  
10  
PowerSC



### 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.

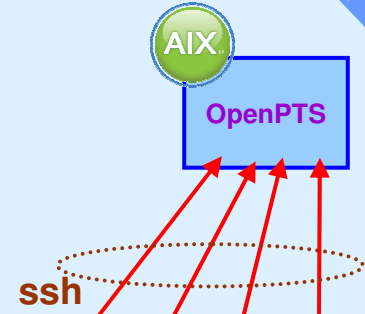
### Benefits

- 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.

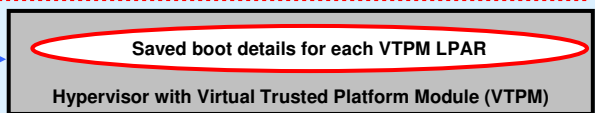
10 of 37

## Trusted Boot Architecture

- Pre-req:
- POWER7 C model (or later) for firmware 740-xxx
- AIX 6 TL7 or AIX 7 TL1 (and VIOS 2.2.1.4)
- 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



Low level resource in system firmware/Hypervisor

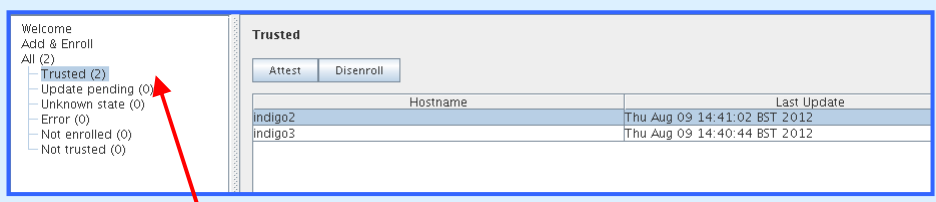


**GUI under X Windows via VNC**

**Run with: /opt/ibm/openpts\_gui/openpts\_GUI.sh**

## Setup ssh and Enrol you AIX LPARs

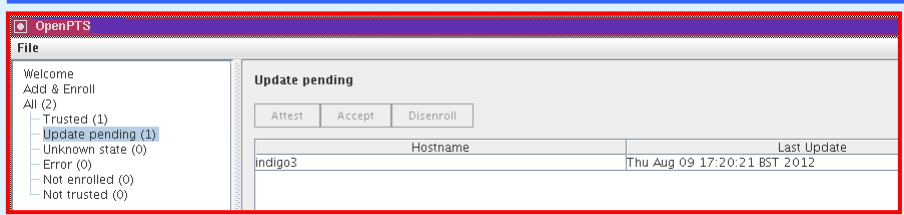
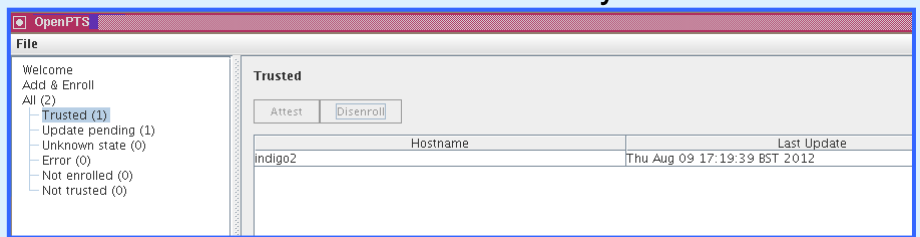
- “Enrol” captures current VTPM encrypted settings = Master



**List of Trusted hosts = Good**

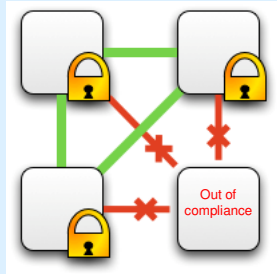
## Modified a boot image → it is noticed

- Ran bosboot on one LPAR – Can you tell which?



- Select the LPAR + Accept to move it back to Trusted

PowerSC Standard Edition  
**PowerSC – Trusted Network Connect and Patch Management**



- 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**

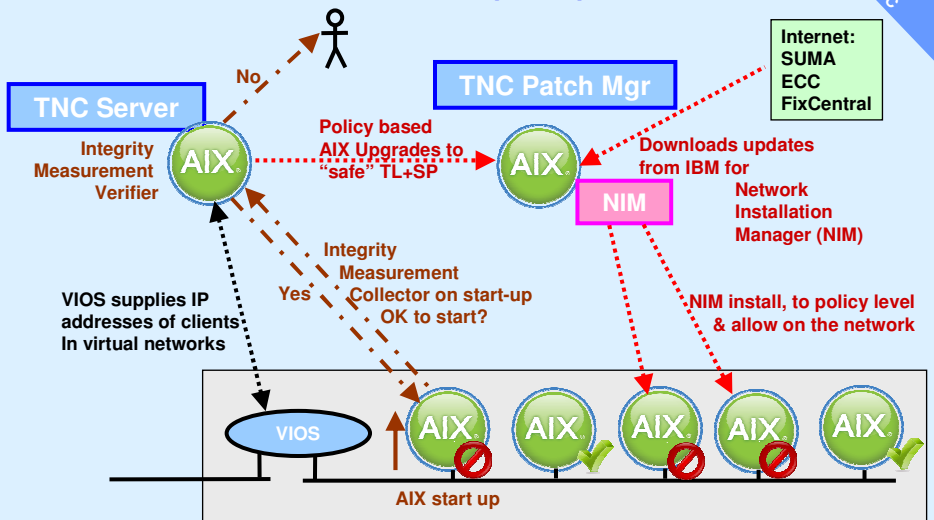
Challenge: Ensure that images are trusted and at the proper patch level when they connect to the network.

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

**Trusted Network Connect (TNC) Architecture**

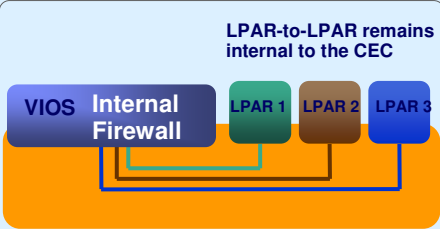


All communication uses ssh  
 TNC Server and Patch Manager can be the same machine



# PowerSC – Trusted Firewall

PowerSC Standard Edition



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

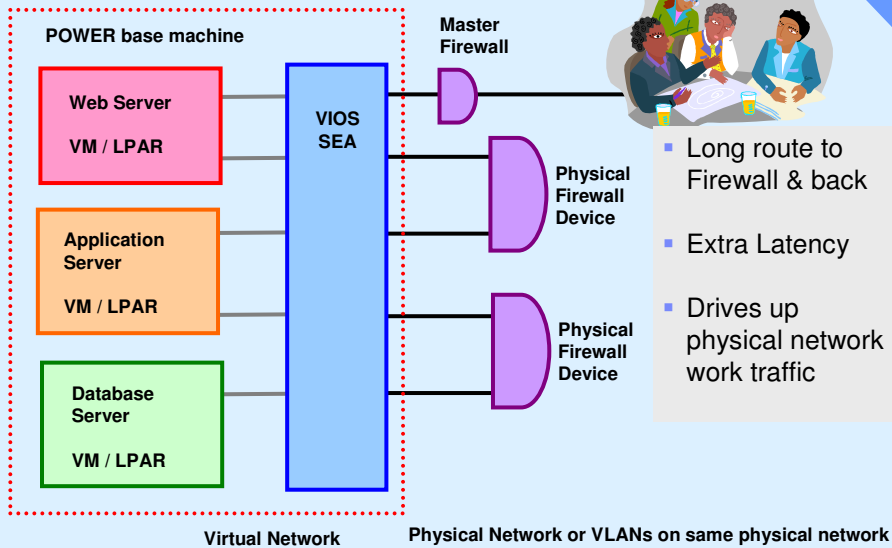
Challenge: No LPAR-to-LPAR firewall protection so all network traffic must be routed via an external Firewall and hairpin turn back into the Power System. Customer needs to purchase high bandwidth router based Firewall hardware

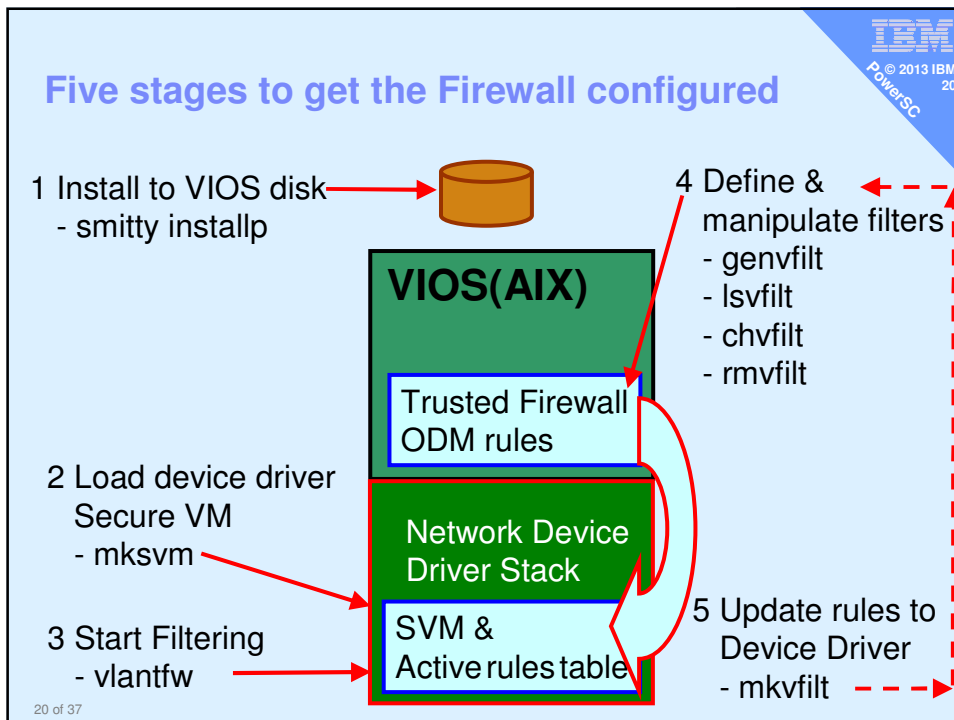
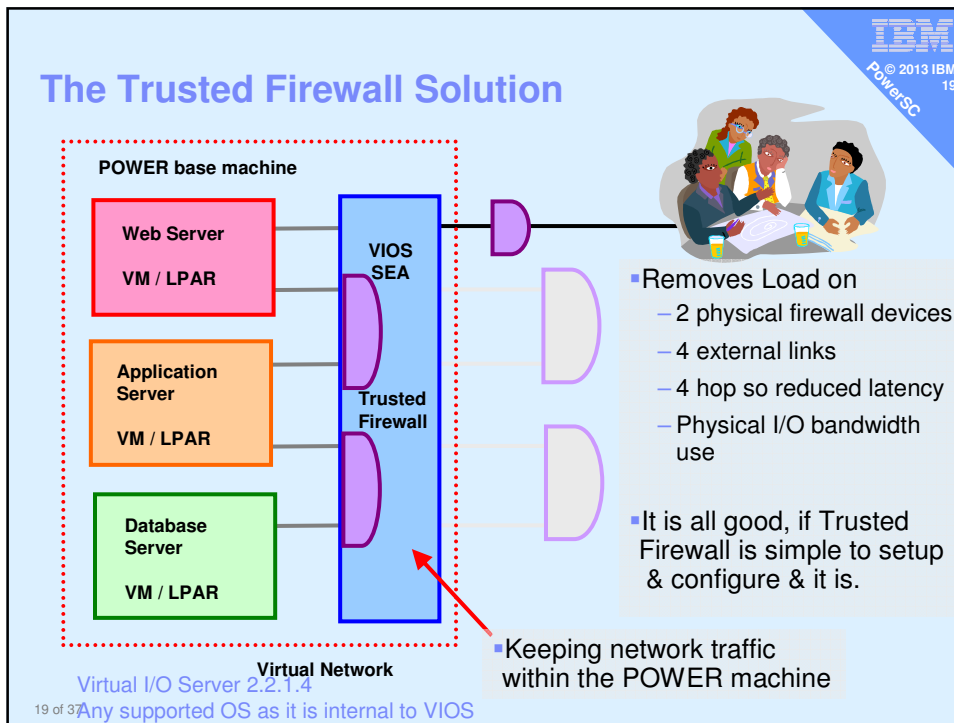
Power SC Solution: Provide a VIOS based Firewall managed by VIOS.

## 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

# The Problem







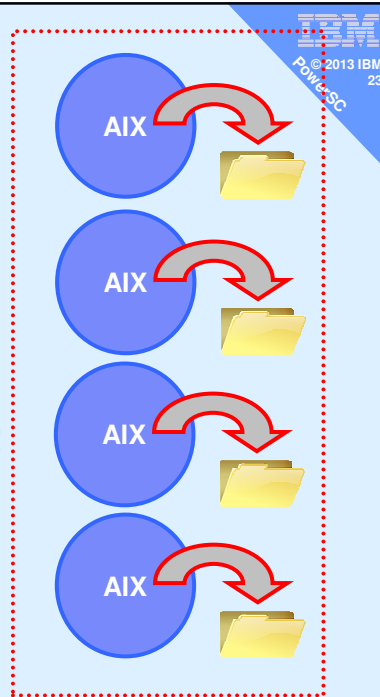
## Logging Alternatives

### 1) Local default AIX Logging

Risks: Your nasty hacker could

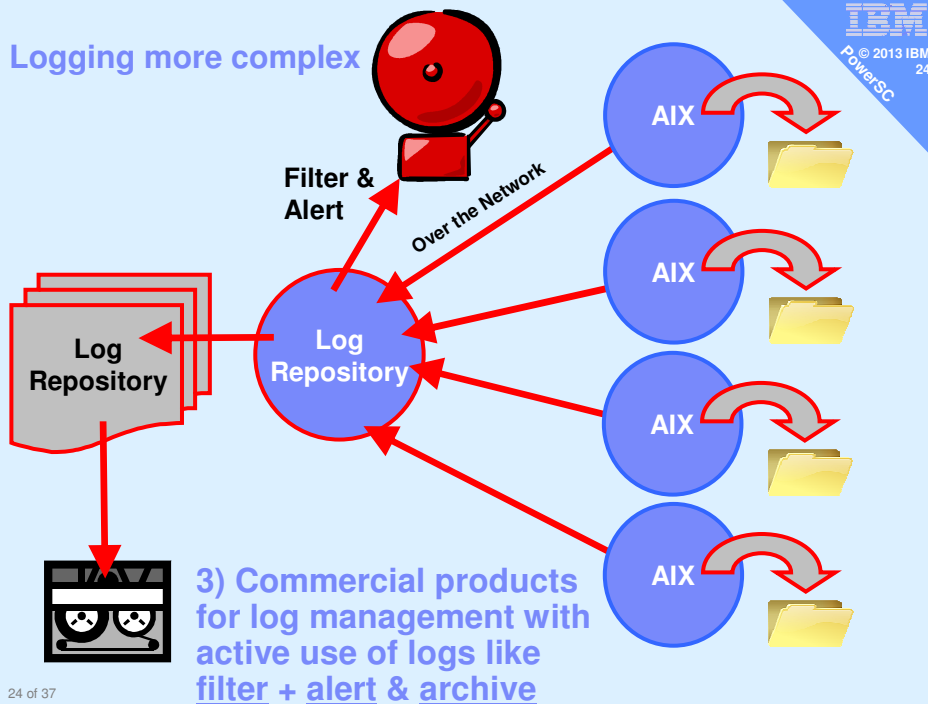
- shuts down logging
- removes log
- edits log
- destroys the LPAR and we will never work out how/why!

= No post-mortem analysis

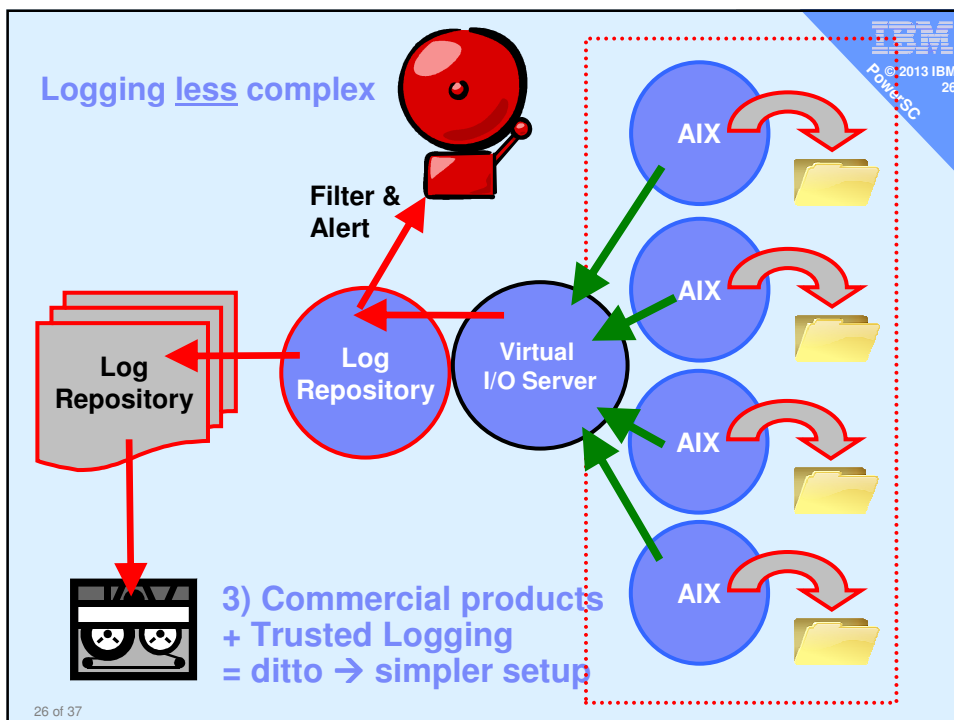
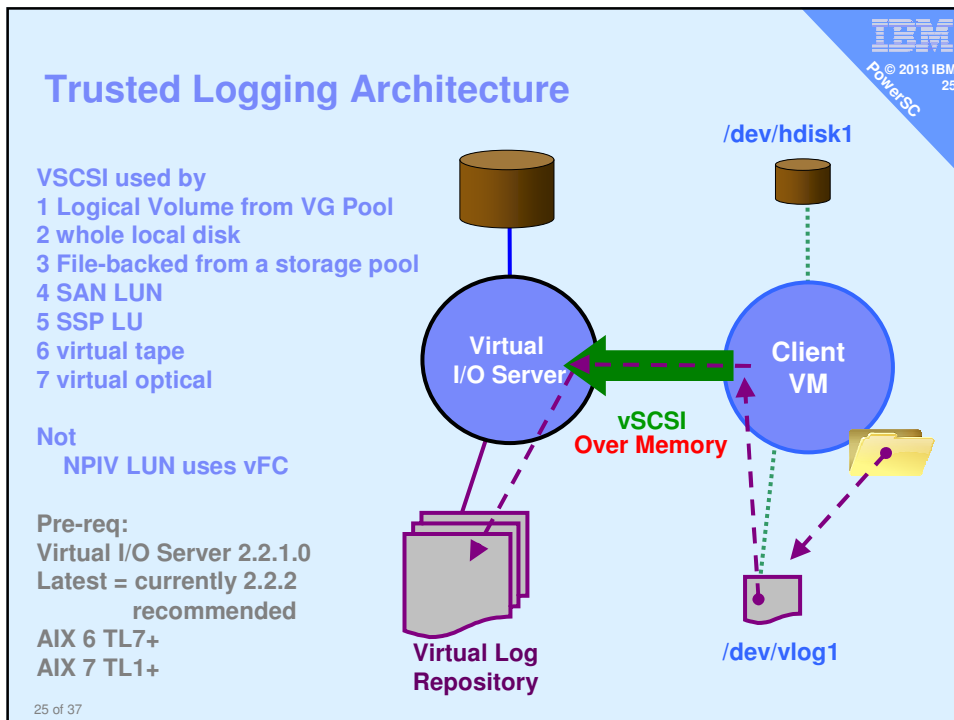


23 of 37

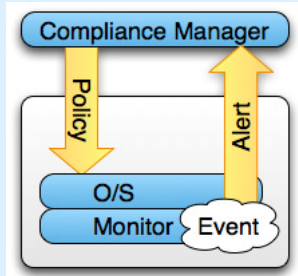
## Logging more complex



24 of 37



## 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.

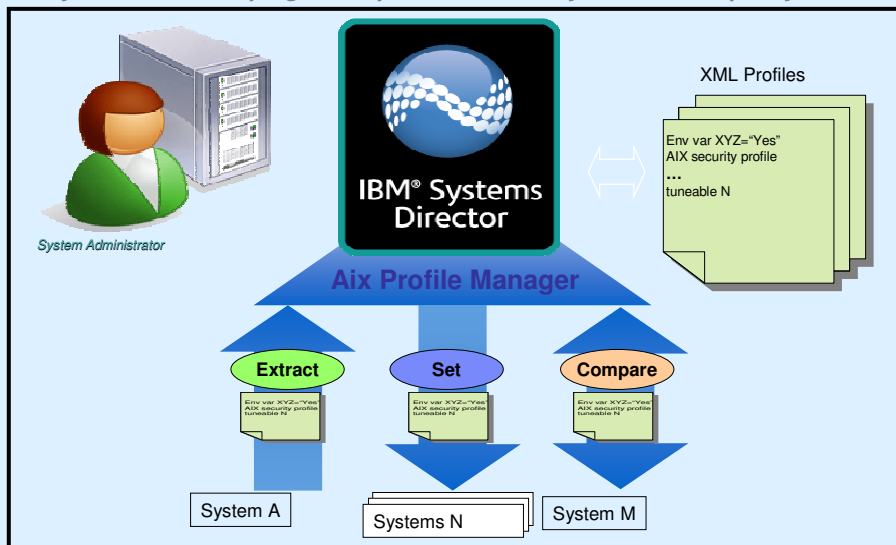
PowerSC solution: Compare settings across all of the systems in the datacenter against prebuilt profiles, e.g. Payment Card Industry (PCI), DoD STIG and COBIT.

### 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

## AIX Profile Manager Architecture

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



**IBM**  
© 2013 IBM  
Powersc 29

## Example of Systems Director AIX Profile Manager

IBM Systems Director - Mozilla Firefox: IBM Edition

IBM Systems Director

9.8.7.66 https://9.8.7.66:8422/ibm/console/login.do?action=secure

IBM Systems Director

Welcome root Problems Compliance Help Logout

AIX Profile Manager

### AIX Profile Manager

Welcome to AIX Profile Manager. This plug-in allows you to deploy AIX Profile Manager template on AIX systems and to monitor your systems configuration status against the deployed templates.

#### AIX Profile Manager Configuration Status (monitoring 7 systems)

The configuration status of a system is computed based on the configuration thresholds settings. The thresholds can be modified by clicking on the link below:

Thresholds configuration

Configuration status for 7 monitored systems:

- 1 system with a % of differences > 10%
- 1 system with 4 % of differences between 0 and 10%
- 1 system with 0 % of differences
- 3 systems with no configuration status
- 1 system need reboot

**Common tasks**

- View and manage profiles
- View and Manage templates
- View and manage systems
- View and manage compare results
- View and manage retrieve results
- View event log

#### Manage Monitoring

Schedule configuration status monitoring  
 Setup custom and repeating configuration status monitoring schedules on systems managed by AIX Profile Manager

Check all systems now  
 Perform an immediate configuration status check on all systems

**Common tasks**

- Active and scheduled jobs
- Thresholds configuration

29 of 37

**IBM**  
© 2013 IBM  
Powersc 30

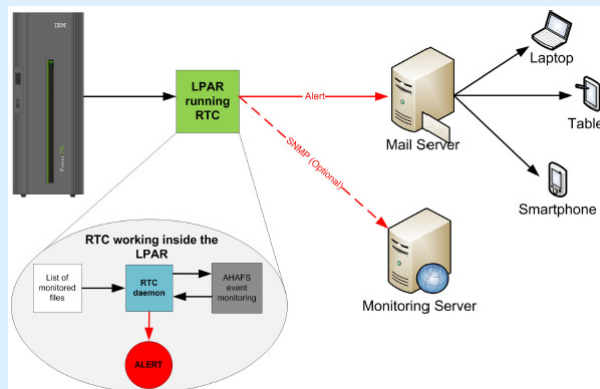
## “But I’ve already written Scripts to check Security and Compliance”

- 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.**

30 of 37

## 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)



31 of 37

## Real-Time Compliance (RTC)

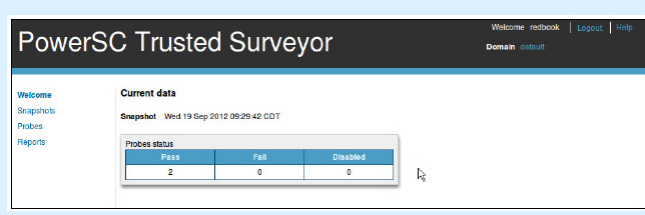
- Pre-req: AIX 6 TL7+ and AIX 7 TL1+
- Install PowerSC Express
  - powerscExp.rtc & powerscExp.license
- Configure with: smitty RTC
  - To set a email server and address
- It is an AIX subsystem:
  - lssrc -s rtcd
  - stopsrc -s rtcd
  - startsrc -s rtcd
- Config file of pre-defined monitoring is in /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)

32 of 37



## 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+ or IE8+



## Trusted Surveyor

- 1 Domains to group machines
- 2 Probes to get information from HMC, IVM, ... etc.
- 3 Snapshots to get the data

The screenshot shows the 'Reports' section of the PowerSC Trusted Surveyor web interface. Red arrows point to various elements with annotations:

- 1 Domains to group machines:** Points to the 'Domain default' text at the top right of the interface.
- 2 Probes to get information from HMC, IVM, ... etc.:** Points to the 'Probes' link in the left navigation menu.
- 3 Snapshots to get the data:** Points to the 'Select a snapshot' dropdown menu, which currently shows 'snapshot-3'.
- 4 Reports of VM & VLANS in text or CSV:** Points to the 'Generate TXT report' and 'Generate CSV report' buttons at the bottom of the 'Probes list' section.

The 'Query results' section on the right shows details for a report generated on Sep 19, 2012, including physical and virtual machine information.

**PowerSC – What more?**

Home website  
<http://www.ibm.com/systems/power/software/security>

<http://tinyurl.com/newAIXwiki>  
 and take the PowerSC link

<http://www.youtube.com/user/nigelargriffiths>  
 Videos on  
 Trusted Boot  
 Trusted Logging  
 Trusted Firewall (short-cut)  
 & for AIX aixpert and fpm

What more Information?  
 • PowerSC Redbook  
 • SG24-8082

The screenshot shows the IBM PowerSC website with the following elements:

- Navigation tabs: Overview, Features & benefits, Solutions, Platform offerings, Resources
- Text: "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"
- Learn more: "IBM PowerSC data"
- Contact IBM: "Email IBM", "Find a Business Partner", "Call IBM: 1-888-843-8801", "Priority code: 10248082"
- Browse Power Systems: "Hardware", "Solutions", "Operating systems", "Migrate to Power", "System software", "Advantages"
- PowerSC POWER Security and Compliance Toolset: "Updated today at 11:59 AM by magger | Tags: None | Add tags", "Edit", "Page Actions"
- Redbook: "Managing Security and Compliance in Cloud or Virtualized Data Centers Using IBM PowerSC", "Redbooks"
- Managing Security and Compliance in Cloud or Virtualized Data Centers Using IBM PowerSC:
  - Now available from <http://www.redbooks.ibm.com/redpieces/abstracts/sg248082.html>
  - 350 pages of good technical intro and hands-on examples
- YouTube Videos on PowerSC components:
  - Find this on this YouTube channel <http://youtube.com/user/nigelargriffiths> or directly to the video on these links
  - PowerSC Trusted Boot
  - PowerSC Trusted Logging
  - PowerSC Trusted Firewall (short-cut)
  - AIX security setting by profiles aixpert and File Permission Manager (fpm)

35 of 37

**PowerSC – What next?**

a) Download the PowerSC Redbook + quick look through it

Quick wins

b) Remove telnet and ftp from every AIX/VIOS  
 c) Move to aixpert for system hardening  
 d) Use ARTEX for consistent performance settings

PowerSC but what order?

1. Trusted Boot
2. Trusted Network Connect
3. Trusted Firewall
4. Trusted Logging
5. Compliance Automation
6. Real-time alerts
7. Trusted Surveyor

36 of 37

## PowerSC – What next?

- a) Download the PowerSC Redbook + quick look through it

### Quick wins

- b) Remove telnet and ftp from every AIX/VIOS
- c) Move to aixpert for system hardening
- d) Use ARTEX for consistent performance settings

### PowerSC but what order?

1. Trusted Boot
2. Trusted Network Connect
3. Trusted Firewall
4. Trusted Logging
5. Compliance Automation
6. Real-time alerts
7. Trusted Surveyor

"Low hanging fruit" IMHO

- ← 1) performance boost
- ← 2) if not remote logging
- ← 4) if 100's of LPARs
- ← 3) simple to setup