POWER & AIX User Group Meeting - Switzerland

PowerSC Overview

Power Systems Security & Compliance

Nigel Griffiths
IBM Power Systems
Advanced Technology Support, Europe

PowerSC has 7 Components

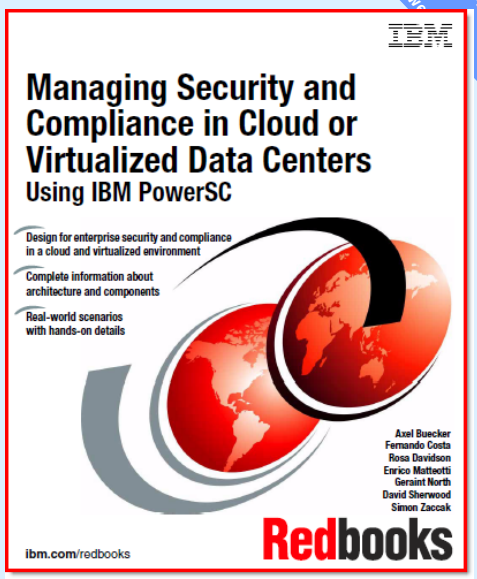
1. **Trusted Boot**
   Be sure that boot media & AIX has booted in a known-trusted state
2. **Trusted Network Connect**
   When an LPAR attempts to join a VLAN, ensure a minimum AIX level
3. **Trusted Firewall**
   Pass packets securely between LPARs without an external firewall
4. **Trusted Logging**
   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:



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
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

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

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

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

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

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**

AIX Security is already excellent

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

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.

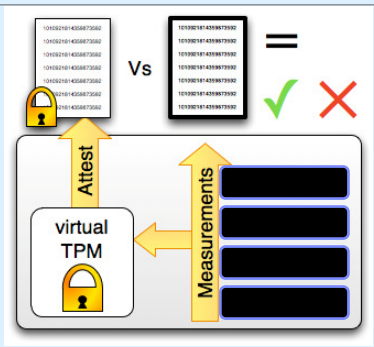
PowerSC and IBM i

- **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

PowerSC Standard Edition

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

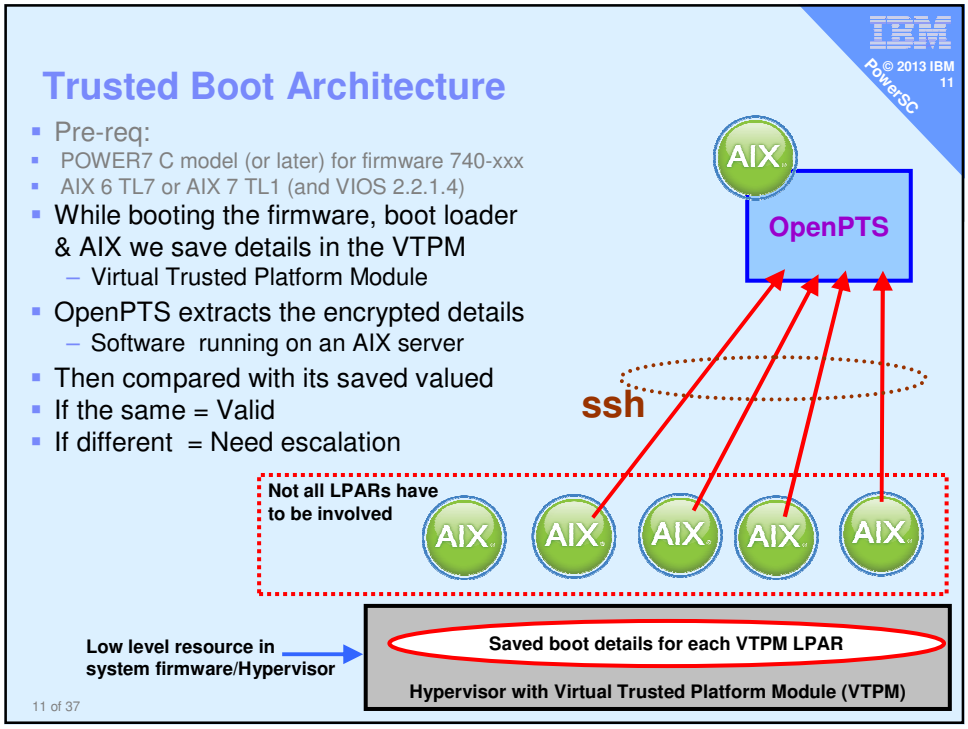
Overview

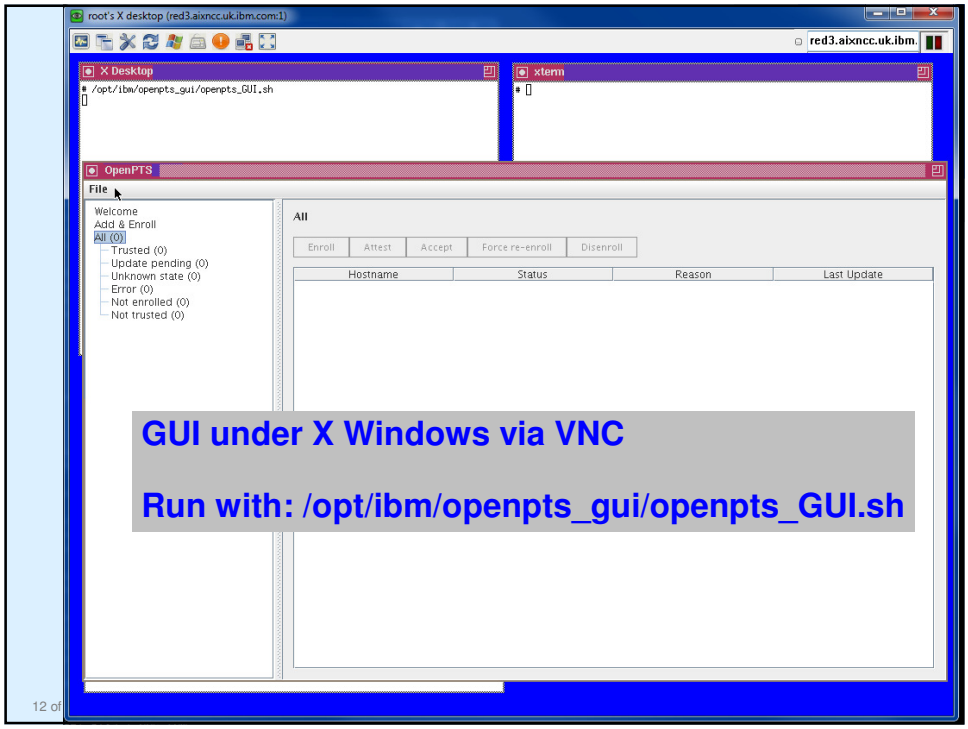
Challenge: Ensure that every virtual machine image in your datacenter hasn't been altered either by accident or maliciously (commonly called a RootKit attack).

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

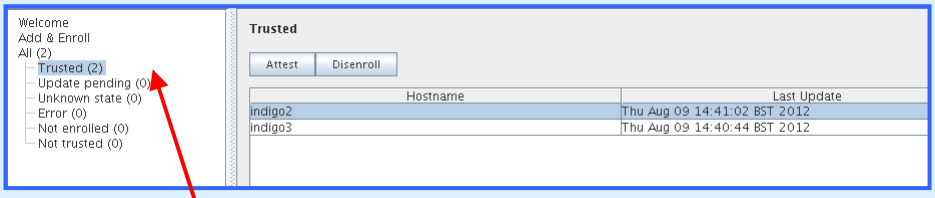
- PowerSC offers the only solution on the market to form a chain of trust for VMs all the way from boot to OS!
- Improve QoS by reducing the risk of accidental or malicious image tampering
- Reduce the time it takes to ensure that every VM in your datacenter is running authorized and trusted software.





Setup ssh and Enrol you AIX LPARs

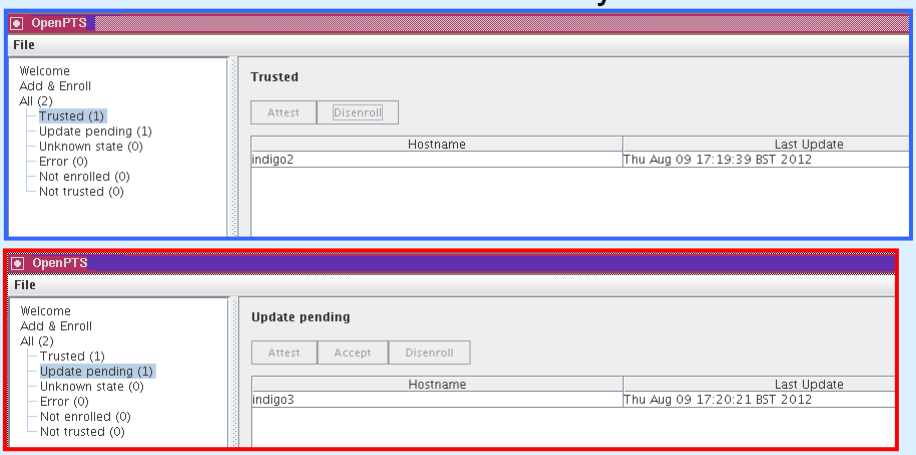
- "Enrol" captures current VTPM encrypted settings = Master



List of Trusted hosts = Good

Modified a boot image → it is noticed

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

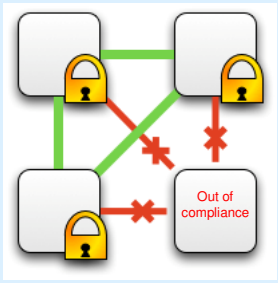


- Select the LPAR + Accept to move it back to Trusted

PowerSC Standard Edition

PowerSC – Trusted Network Connect and Patch

15



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.

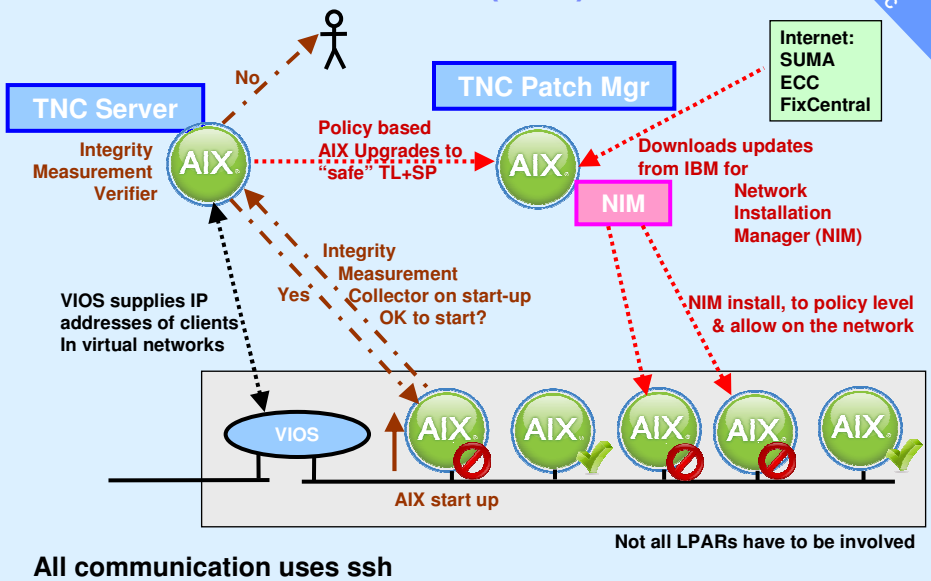
PowerSC Solution: Trusted Network Connect and Patch Management detects noncompliant virtual machines during activation and alerts administrators immediately. Offers automated updating of AIX (via NIM)

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

16

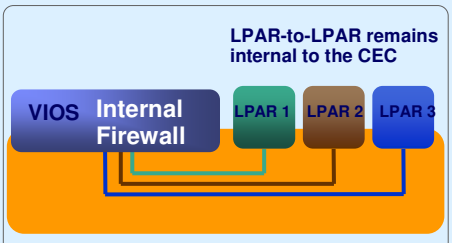


All communication uses ssh

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

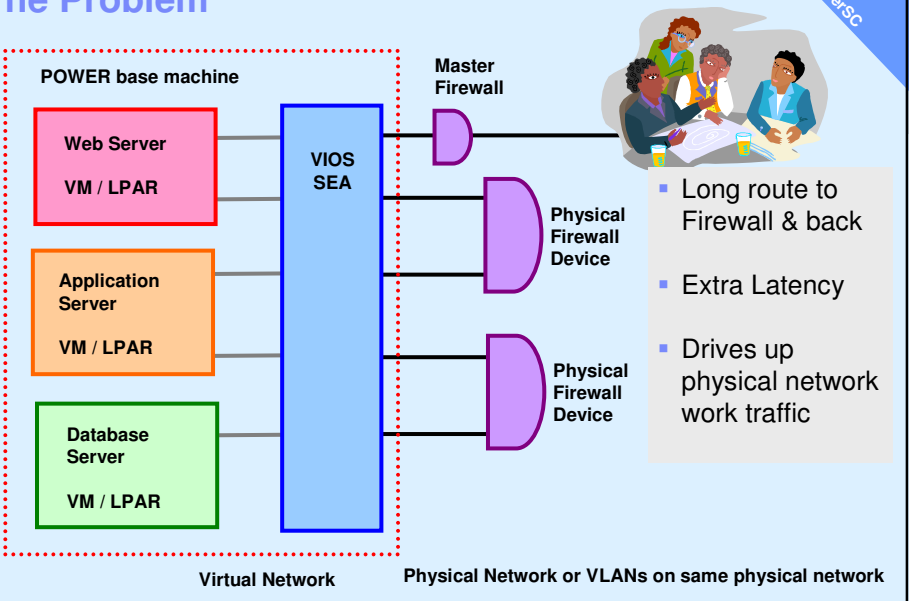
Challenge: No LPAR-to-LPAR firewall protection so all network traffic must be routed via an external Firewall and hairpin turn back into the Power System. Customer needs to purchase high bandwidth router based Firewall hardware

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

Benefits

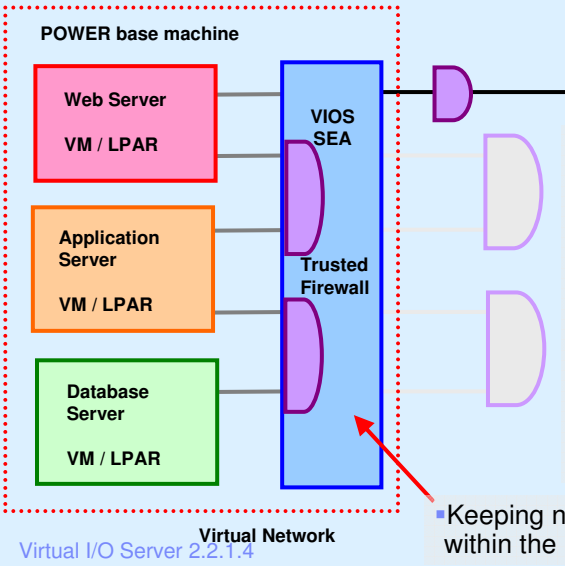
- Provides network firewall services within the local server virtualization infrastructure to control network traffic between virtual workloads
- Improves performance by providing network firewall services within the server, which does not require an external firewall for VM-to-VM traffic on the same 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



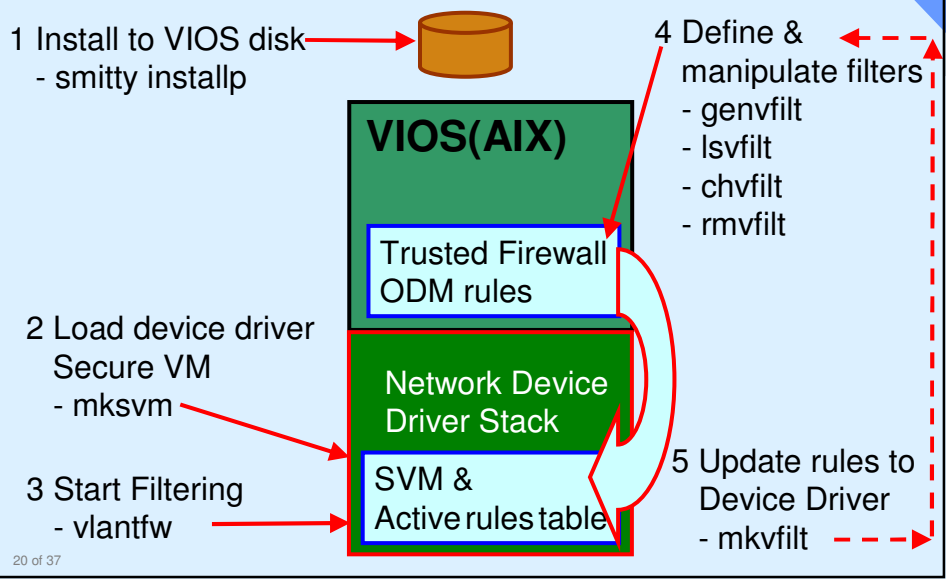
- Long route to Firewall & back
- Extra Latency
- Drives up physical network work traffic

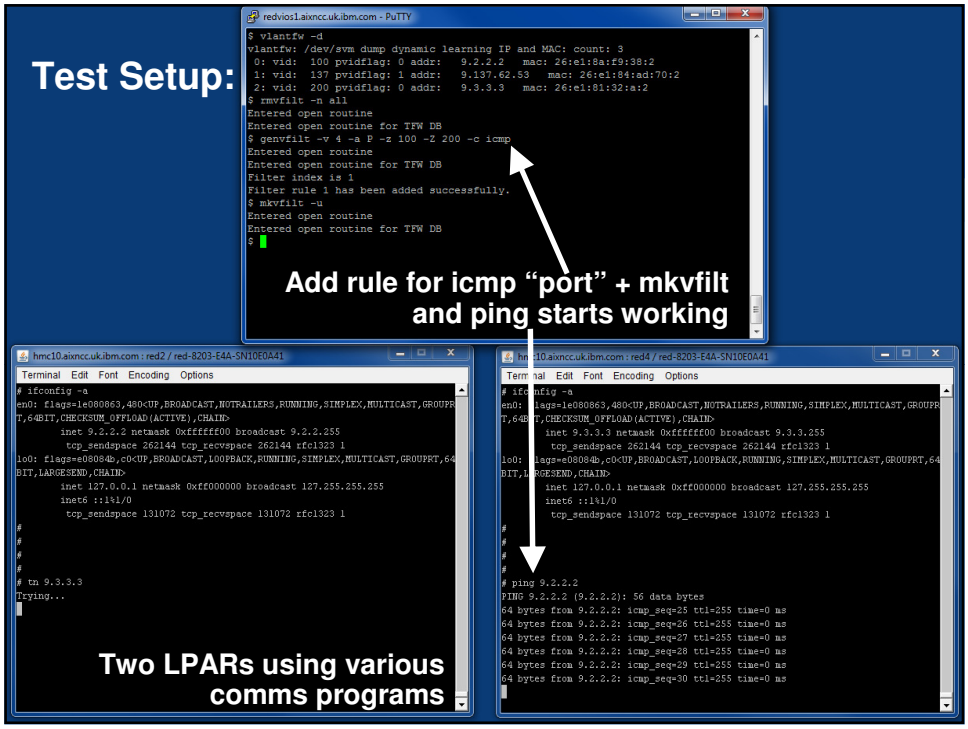
The Trusted Firewall Solution

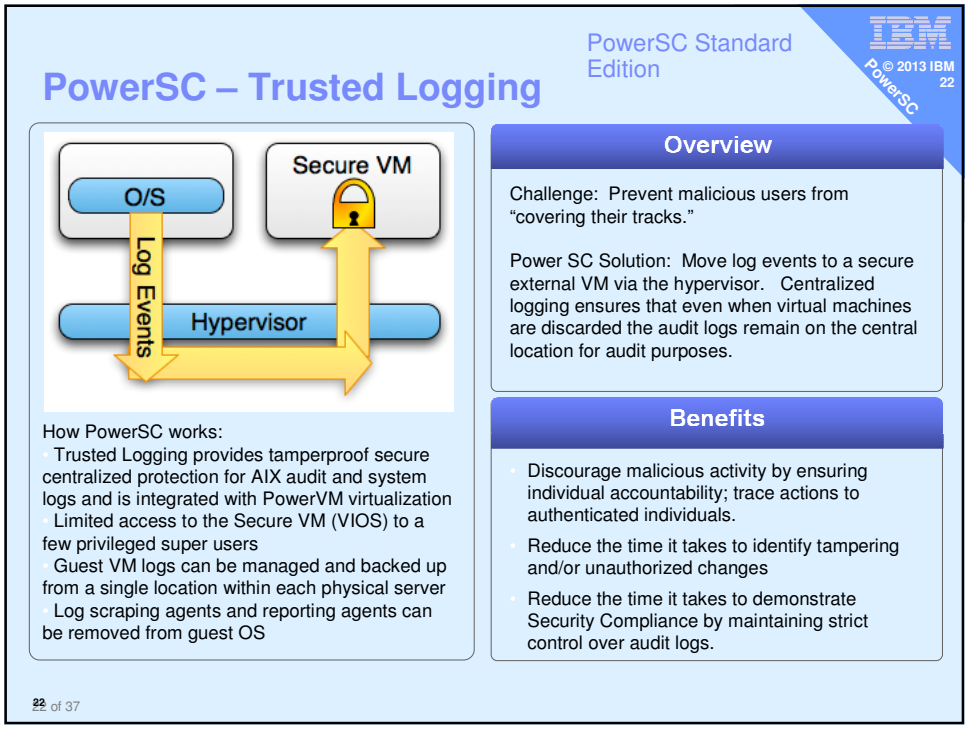


- Removes Load on
  - 2 physical firewall devices
  - 4 external links
  - 4 hop so reduced latency
  - Physical I/O bandwidth use
- It is all good, if Trusted Firewall is simple to setup & configure & it is.
- Keeping network traffic within the POWER machine

Five stages to get the Firewall configured





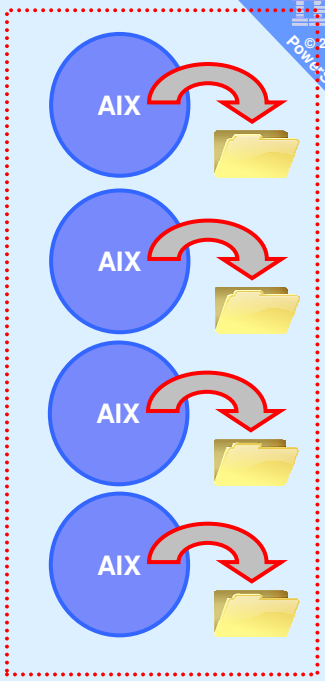


Logging Alternatives

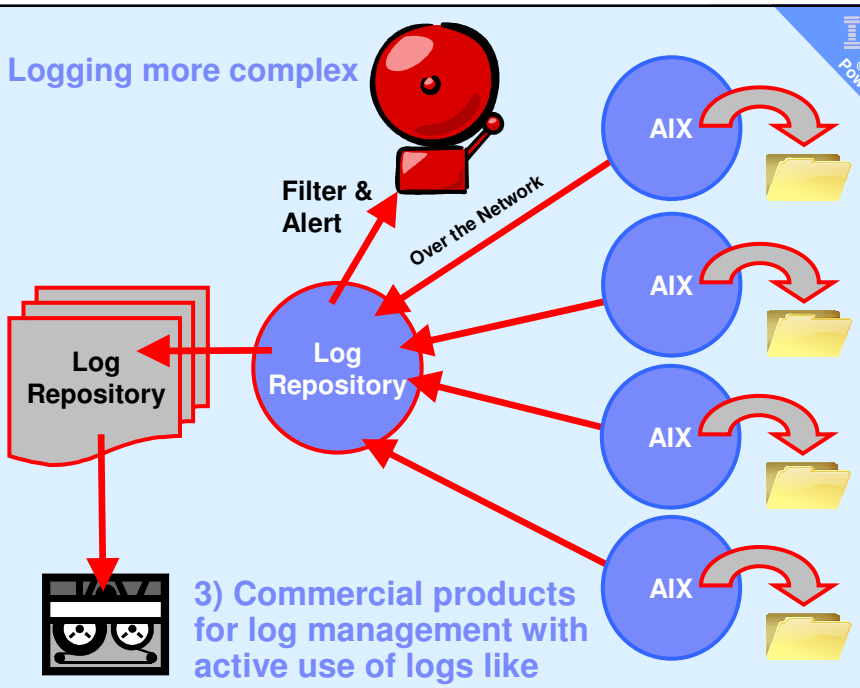
1) Local default AIX Logging

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



Logging more complex



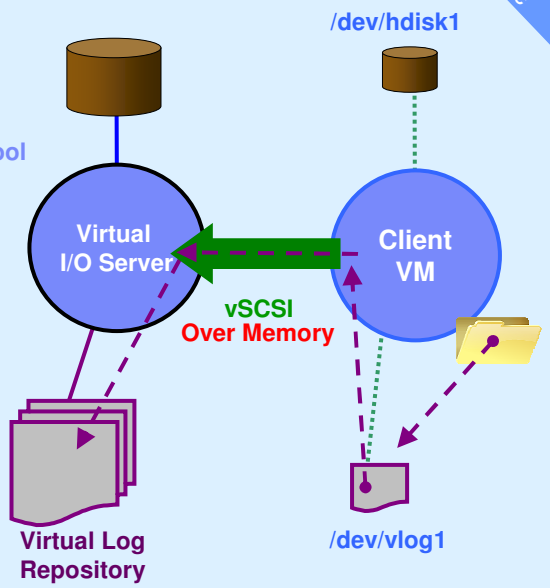
3) Commercial products for log management with active use of logs like filter + alert & archive

Trusted Logging Architecture

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

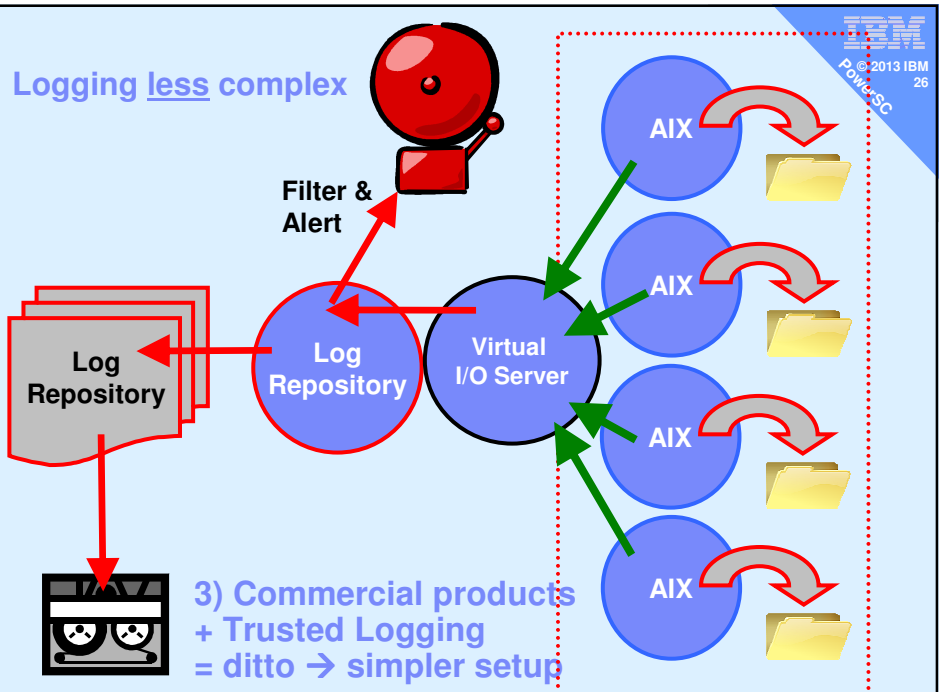
Not
NPIV LUN uses vFC

Pre-req:
Virtual I/O Server 2.2.1.0
Latest = currently 2.2.2
recommended
AIX 6 TL7+
AIX 7 TL1+



25 of 37

Logging less complex

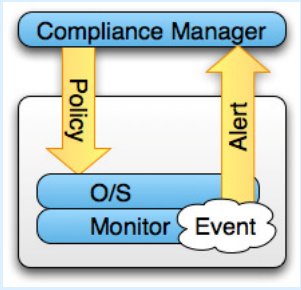


3) Commercial products
+ Trusted Logging
= ditto → simpler setup

26 of 37

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.

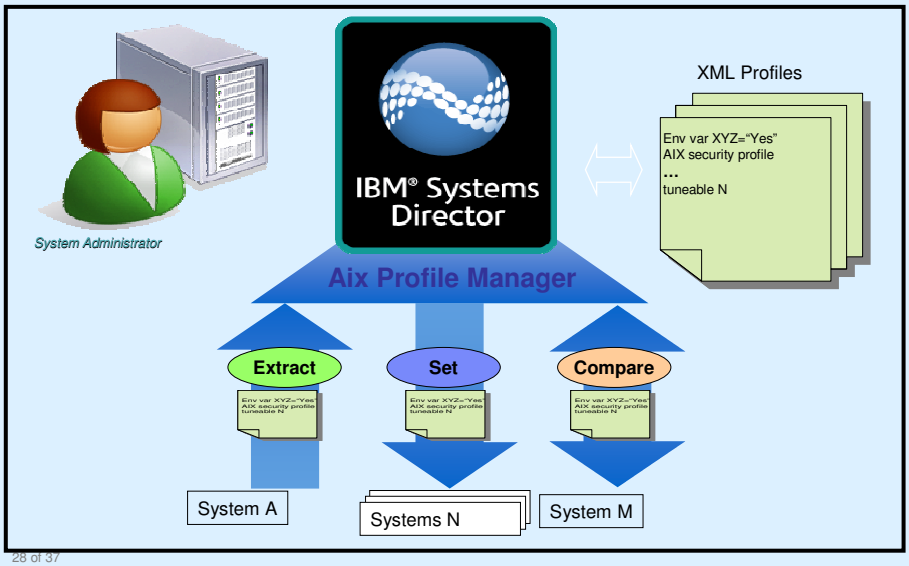
PowerSC solution: Compare settings across all of the systems in the datacenter against prebuilt profiles, e.g. Payment Card Industry (PCI), DoD STIG and COBIT.

Benefits

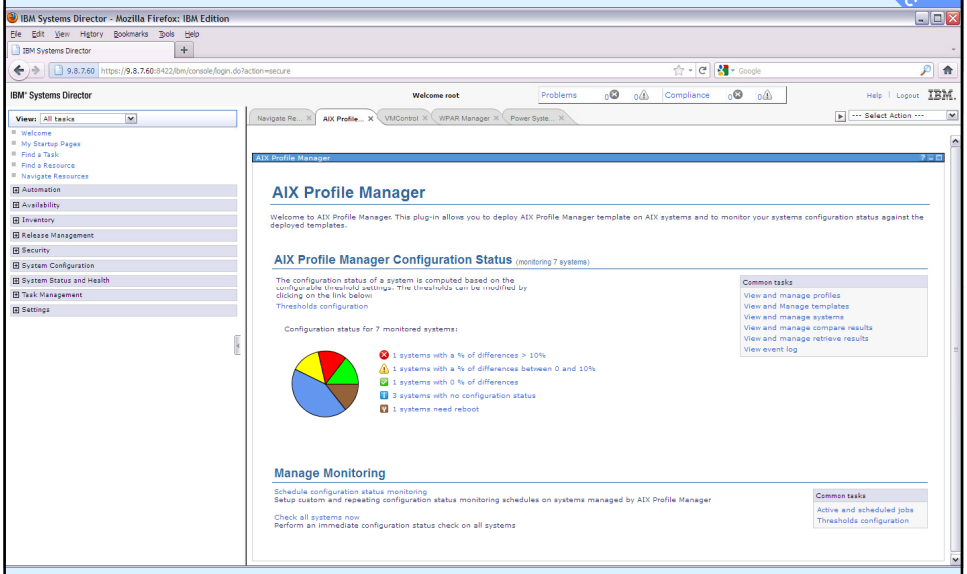
- Lower Administration costs by setting security configs in a repeatable manner
- Lower Admin costs by automating compliance reporting
- Automatic remediation of servers that are out of compliance

AIX Profile Manager Architecture

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



Example of Systems Director AIX Profile Manager

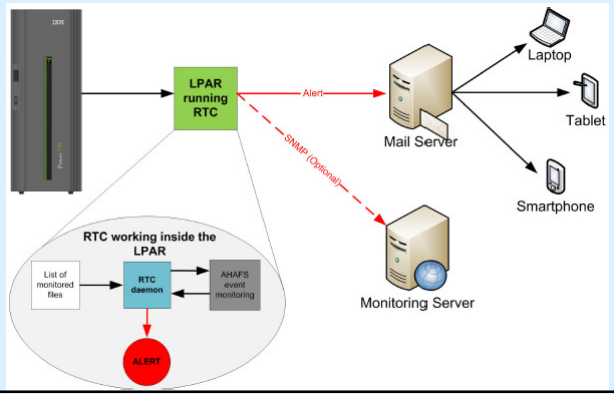


"But I've already written Scripts to check Security and Compliance"

- 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.**

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)



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

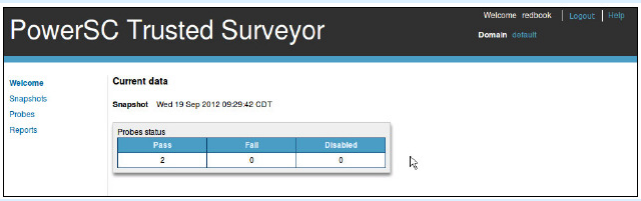
-It is an AIX subsystem:
  - lssrc -s rtcd
  - stopsrc -s rtcd
  - startsrc -s rtcd

-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)

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+



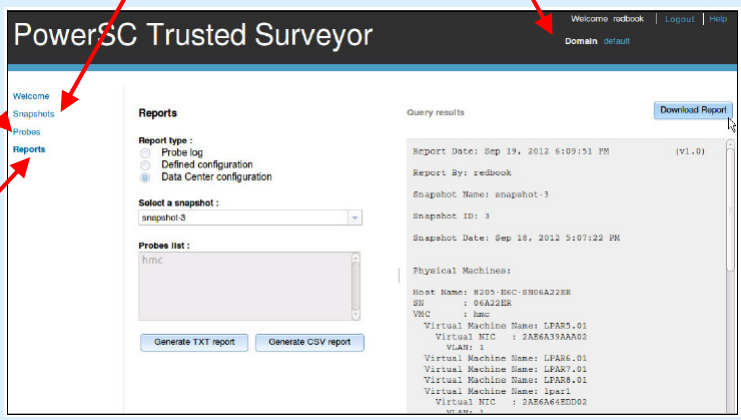
Trusted Surveyor

1 Domains to group machines

3 Snapshots to get the data

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

4 Reports of VM & VLANS in text or CSV



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

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

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?	”Low hanging fruit” IMHO
1. Trusted Boot	
2. Trusted Network Connect	
3. Trusted Firewall	← 1) performance boost
4. Trusted Logging	← 2) if not remote logging
5. Compliance Automation	← 4) if 100’s of LPARs
6. Real-time alerts	← 3) simple to setup
7. Trusted Surveyor	