IBM Power Systems
April 2012

PowerSC

Security and Compliance for Power Systems

Overview

Security Related News

Annual Threat Assessment of the
US Intelligence Community
for the Senate Select Committee on Intelligence

Dennis C. Blair
Director of National Intelligence

February 2, 2010

- US Intelligence Annual Threat Assessment - 2010
- Number 1: ***"Far-Reaching Impact of the Cyber Threat"***

Cyber Crime $100 Billion

- U.S. Department of Justice estimates financial losses from cyber crime at $100 Billion.

Bloomberg

- Carbon Thieves Force European Union to Improve Security, Close Spot Market

Cost of Being non-compliant is ~$9.3M Dollars annually.

Ponemon Institute

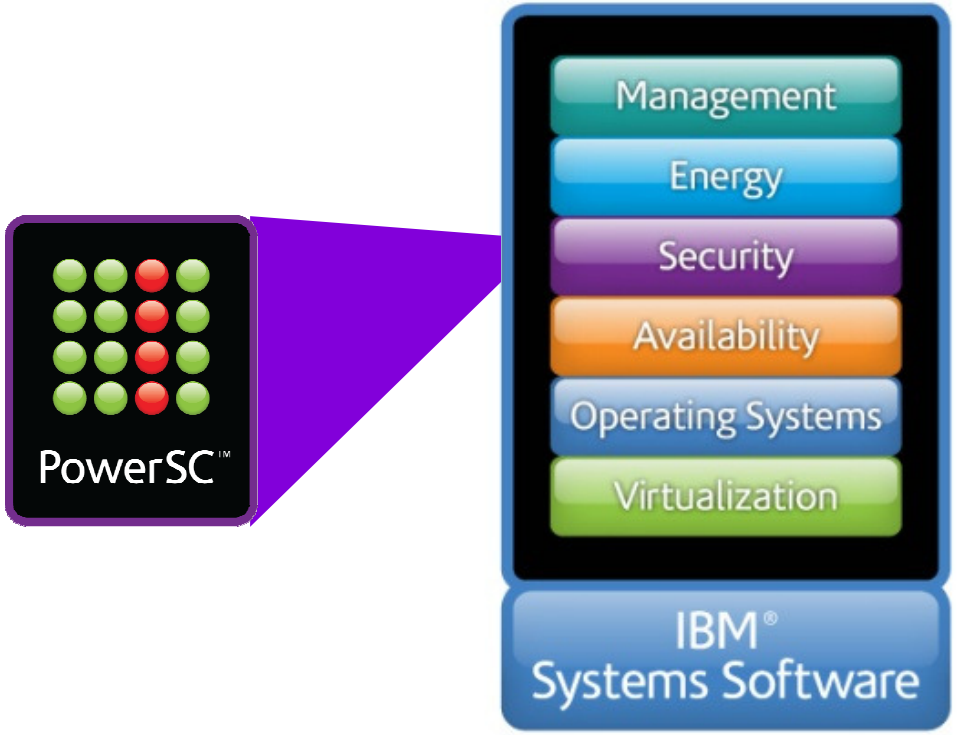
Power Systems Software

PowerSC

- PowerSC provides a **security** and **compliance** solution designed to protect data centers virtualized with PowerVM **enabling** Higher Quality Services.

Client Benefits

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



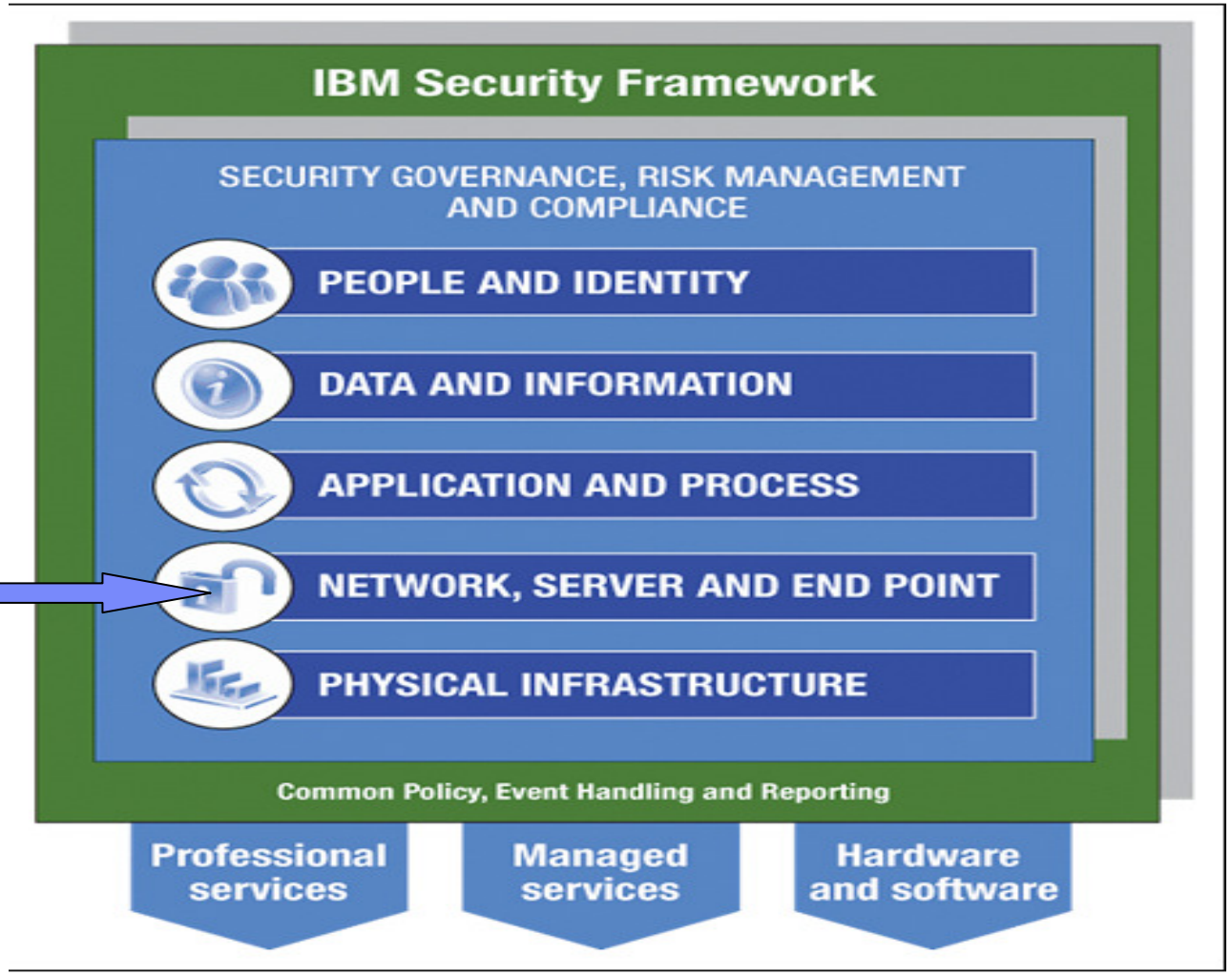
PowerSC Builds on IBM's unmatched global and local expertise in security

3,000+ security and risk management patents

Where Does PowerSC Fit within the IBM Security Framework?

PowerSC

- provides additional Security and Compliance Specifically for Virtualized Power Systems
- focused on the AIX Operating System and Hypervisor



PowerSC provides a security and compliance solution to protect data centers virtualized with PowerVM enabling higher quality services

Technology	***Client Benefits***
▪ ***Compliance Automation*** *managed with Director or single AIX/VIOS command.*	***Simplifies management,*** *by automating security and compliance configuration, auditing and monitoring; all systems are configured securely and consistently which simplifies compliance audits.*
▪ ***Trusted Logging*** *captures and protects logging in real-time in the virtualization layer*	***Tamperproof Logs*** *are centrally stored on the VIOS, simplifies log backup management, and eliminates the need for log-scraping agents running on the OS.*
▪ ***Trusted Network Connect and Patch Management*** *centrally manages installs, updates and patching.*	***Automatically Detects*** *any AIX system which boots, resumes or moves by live mobility into the virtual environment and ensures it is at the prescribed install and security patch level.*
▪ ***Trusted Boot*** *provides industry leading virtual Trusted Platform Module technology.*	***A Central Remote Console*** *can attest to the security and trust of the boot image, OS and all running applications; even if a malicious root is running on the system.*
▪ ***Trusted Firewall*** *ensures that every virtual machine has appropriate network isolation with the best possible performance.*	***Improves performance*** *by providing network firewall services within the server not requiring an external firewall for VM to VM traffic on the same CEC*

PowerSC – Security Compliance Automation

Actively Detect Compliance Issues

Business challenge:

Regulatory compliance requires setting security on systems in a uniform manner so they comply to various industry standards. Understanding and applying a particular standard is tedious, time consuming and error prone.

Solution:

Security Compliance Automation provides pre-built profiles that are certified to comply with industry standards like the Payment Card Industry Data Security Standard(PCI) v2, Department of Defense Security Technical Implementation Guide for Unix(DOD STIG) and the Control Objectives for Information and related Technology(COBIT)

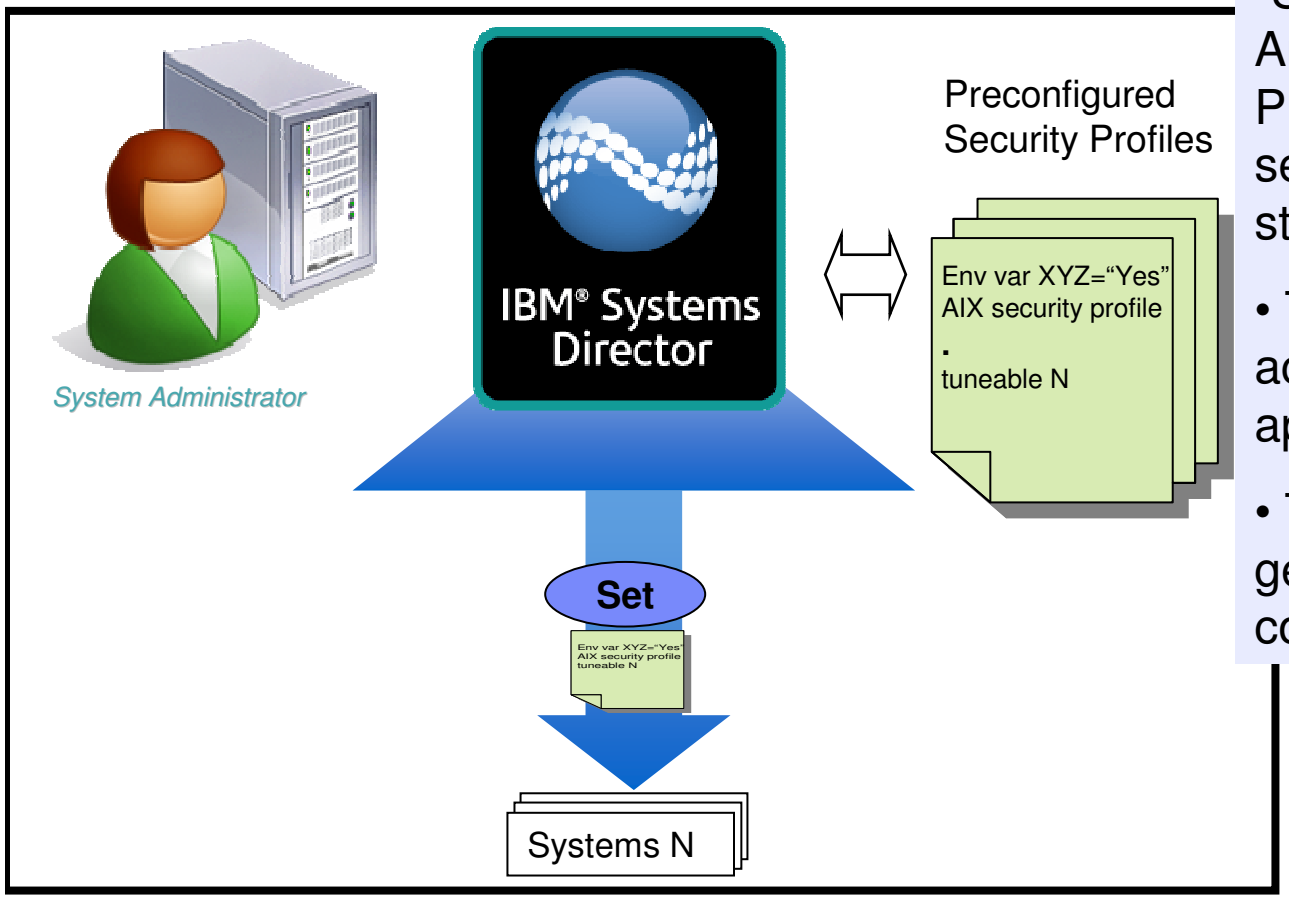
Benefits:

- Ability to **set security settings** more many AIX systems in a **repeatable** manner which **reduces** cost for administration
- **Reduces the labor cost** to continue to research changes in the various standards supported by IBM Security Compliance Automation
- Provides **centralized reporting** on an ongoing basis to **demonstrate compliance** to standards for auditing purposes

Security Compliance Automation – How does it work?

AIX Profile Manager is a Systems Director plug-in that is designed to simplify consistent AIX configuration across multiple systems

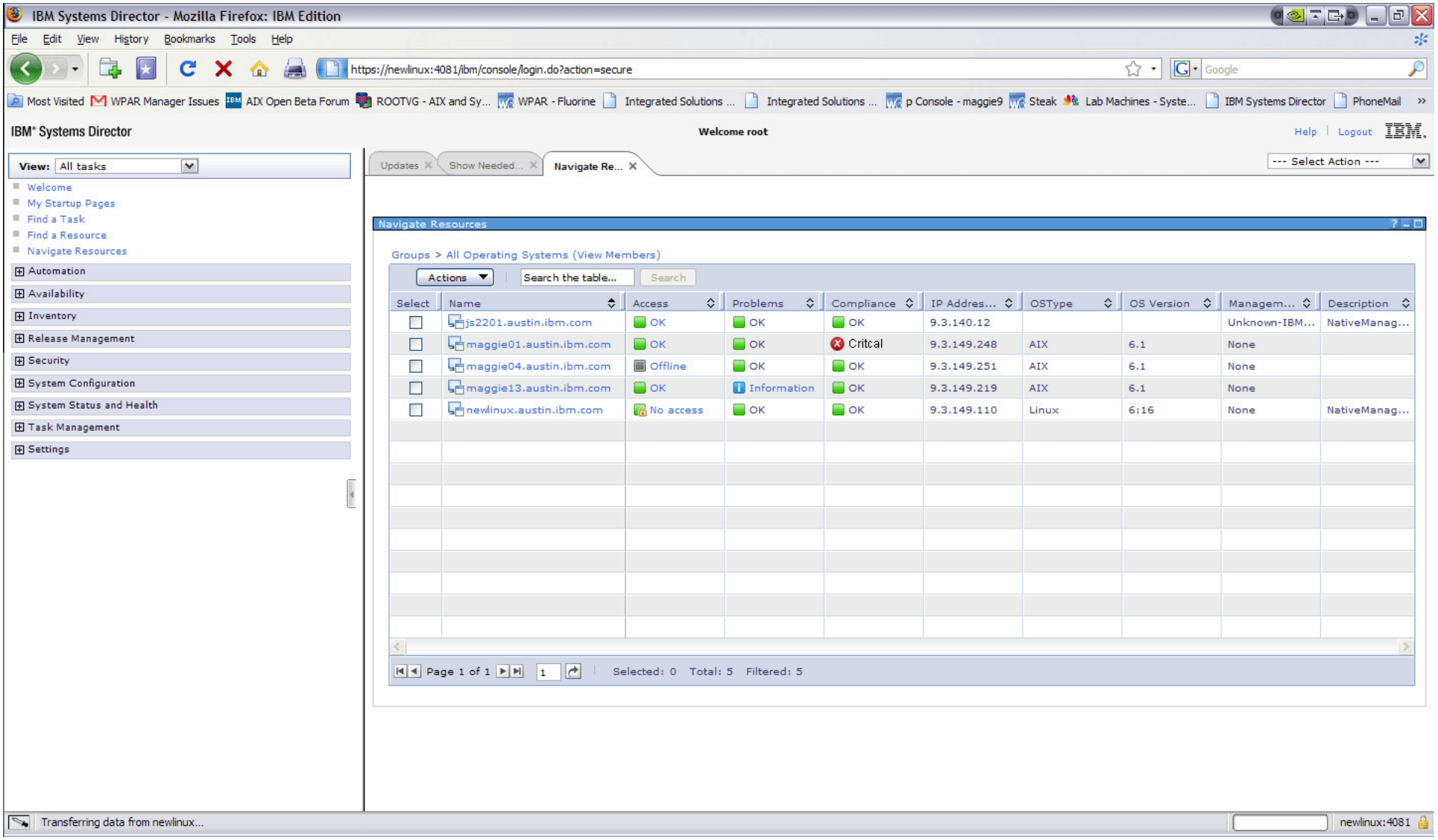
Simplified configuration using the AIX Profile Manager



- Security Compliance Automation provides AIX Profiles that set system settings to match supported standards
- The AIX Profile Manager activates these profiles applying the settings
- The AIX Profile Manager can generate reports to show any compliance exceptions

Security Compliance Automation

No extensive logs to read, no guess work.
Simply a clear view of system out of compliance.



PowerSC – Trusted Logging

Protecting, centralizing logs for Virtual Machines

Business challenge:

Security Compliance mandates strict control over system audit logs. Virtualized and Cloud workloads complicate this mandate.

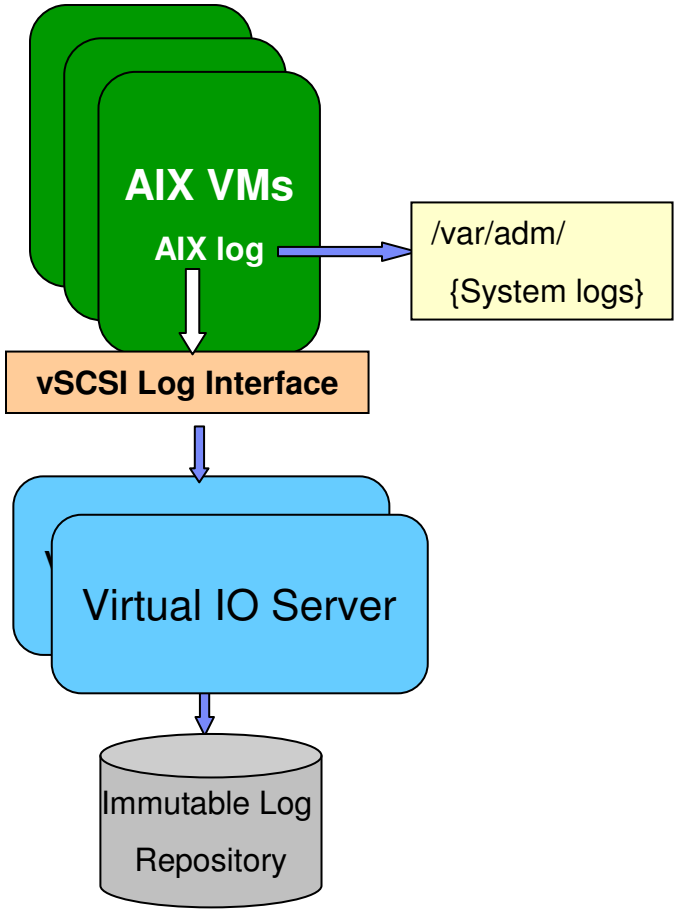
Solution:

Trusted Logging provides **secure centralized protection** for AIX audit and system logs and is integrated with PowerVM virtualization.

Benefits:

- Auditors are assured that Administrators for an AIX VM cannot delete audit trails
- Easy manageability: Centralized audit logs are easier to backup, archive and manage
- Centralized logging ensures that even when virtual machines are discarded the audit logs remain on the central location for audit purposes.

PowerSC Trusted Logging – How does it work?



- AIX Logs use a Special Log Virtual SCSI Device
- Log Virtual SCSI device is created and managed by VIOS
- Logging data is written to an Immutable Repository or storage connected to the VIOS Server
- As the data is stored the AIX VM cannot alter or remove logs owned by VIO Server
- Normal AIX Logs in the VM are still available as well

PowerSC – Trusted Boot
Validate Trust for a System

Business challenge:

Ensuring that system virtual boot images haven't be altered either by accident or maliciously

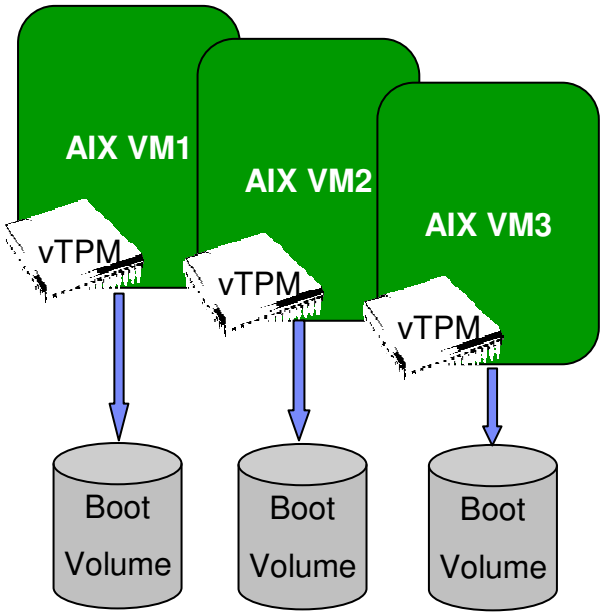
Solution:

Trusted Boot provides a **Virtual Trusted Platform Module(vTPM)** for each Virtual Machine. The vTPM is used to hold the boot measurement data to validate the Trust of a system.

Benefits:

- **Trust Visibility:** Gives ability to display trust of a system
- Allows security **compliance to be demonstrated**
- Provides additional **control and assurance** for Virtual Workloads

PowerSC Trusted Boot – How does it work?

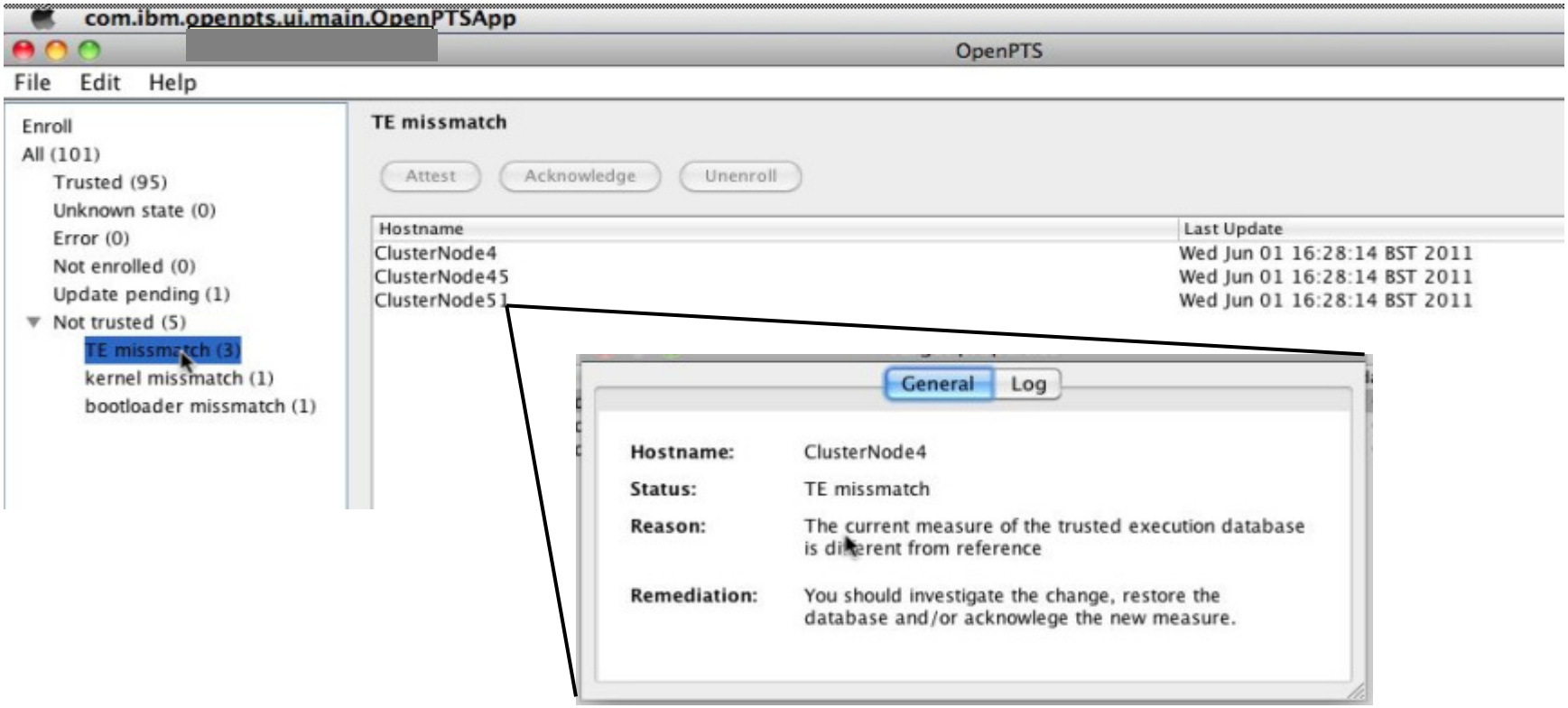


This feature requires Firmware 7.4 or above

- Each Virtual Machine has its own vTPM Configured using HMC/SDMC
- During the AIX Boot process Measurements are taken and Compared to vTPM contents
- PowerVM Hypervisor and PowerSC work together to metric the boot process and store the metrics in the vTPM
- Trusted Status is available for “Attestation” using OpenPTS Monitor

How to Monitor Trusted System Status?

Trusted Monitor OpenPTS GUI



- **A easy read list of not trusted systems**
- **A change in kernel extension, user command or application**
- **AIX TE will pin point the file that changed.**

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 is the way intrusions have been blocked based on historical break-ins

- With features like PowerSC Trusted Boot, this model is being switched to a "**Known Good Model**" which only allows trusted systems to run. This can only be done with a **tight interlock** between the hardware, virtualization and software.

PowerSC – Trusted Network Connect and Patch Management

Actively Detect Compliance Issues

Business challenge:

Maintaining virtual machines and ensuring that site specified patch levels are adhered to is challenging when many systems and virtual machines are deployed.

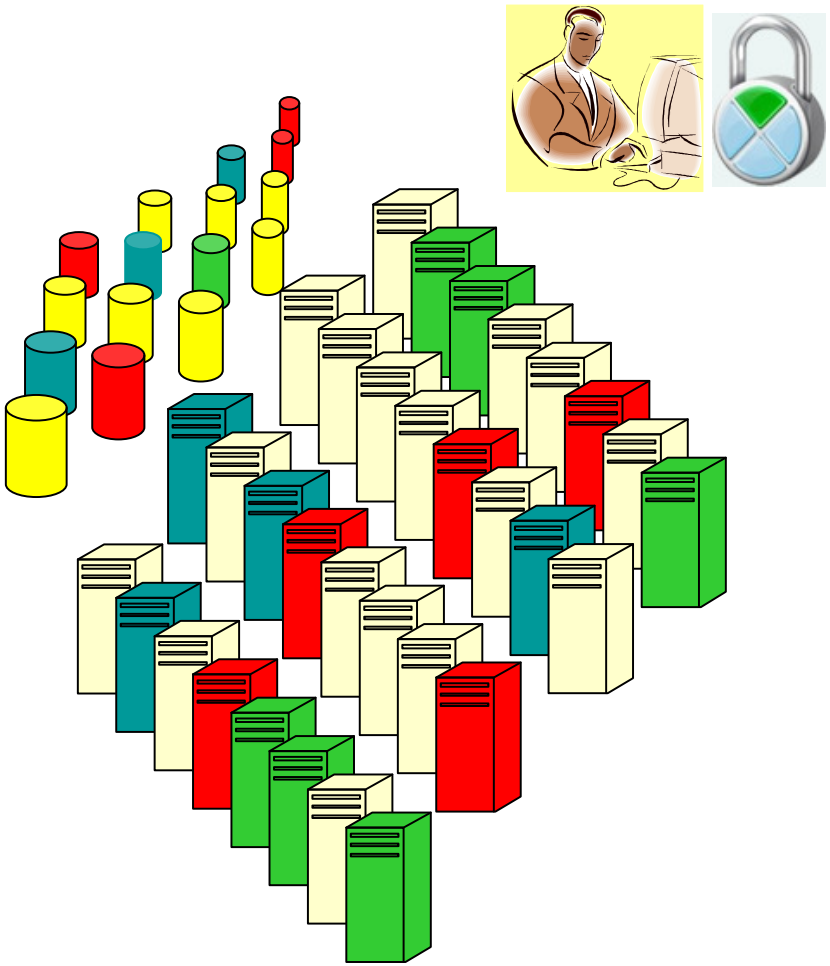
Solution:

Trusted Network Connect and Patch Management detects noncompliant virtual machines during activation and alerts administrators immediately.

Benefits:

- **Active notification** of down level systems via email and SMS
- **Simplifies audits** since active monitoring at virtual machine activation proves compliance to patch policy
- **Raises visibility** of non compliance within the virtual data center and cloud environments

PowerSC Trusted Network Connect and Patch Management – How does it work?



- Trusted Network Connect(TNC) is integrated with the Service Update Manager Assistant(SUMA) and the Network Installation Manager(NIM)
- During the Boot process TNC in the LPAR communicates to TNC server in VIOS
- TNC Server is notified of patch levels
- TNC Server Sends Alert if not at correct patch level

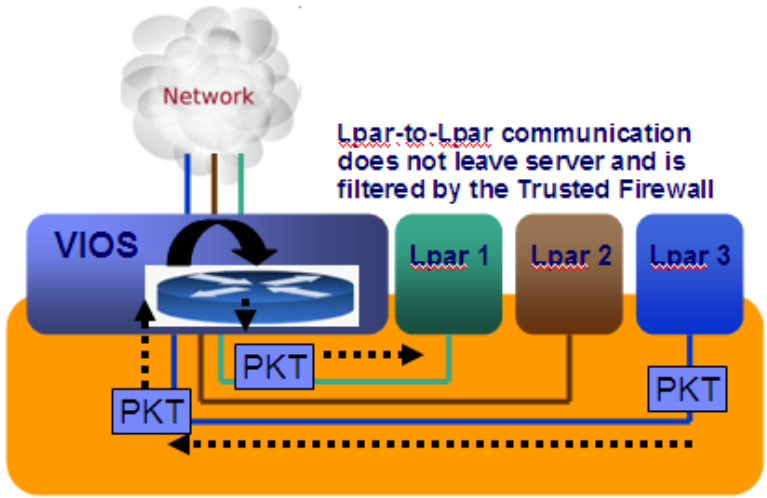
Sony Attack – Reality of IT Issue and Scenario to Benefits of TNC Patch Management

- A known vulnerability affects 77 million users and 10 million credit cards.

"Sony Says It Was Hacked Through a Known Vulnerability" …

"…its IT staff 'was not aware of this specific vulnerability.'"

PowerSC – Trusted Firewall



How PowerSC works:

1.When network traffic flows from one VM to another on the same CEC, the Trusted Firewall which is running in the VIO server provides network isolation and firewall services between VMs.

2. Trusted Firewall is managed just like any firewall with either BLADEHarmony Manager or Tivoli Netcool or via the command line.

Overview

Challenge: Ensure that every virtual machine has appropriate network isolation with the best possible performance.

PowerSC Solution: *Trusted Firewall* provides network isolation for VMs and layer 2,3,4 firewalling between virtual workloads within the server. Works with any VM type – AIX, IBM i or Linux

Benefits

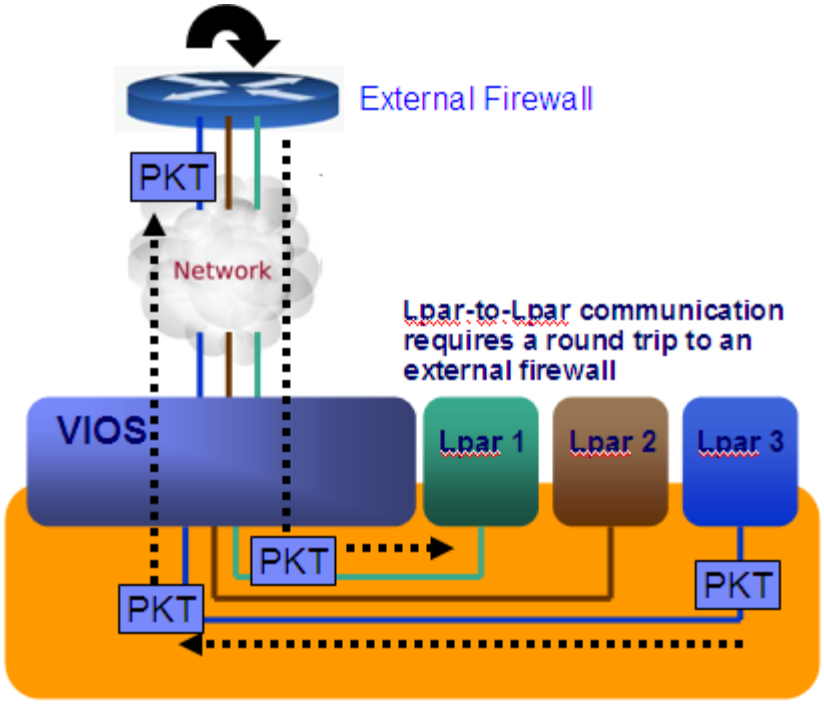
- Improves **performance** by providing network firewall services within the server not requiring an external firewall for VM to VM traffic on the same CEC.
- **Reduces network resource consumption** by not using network resources for VM to VM network traffic when VMs are running on the same CEC.

PowerSC “Trusted Firewall”

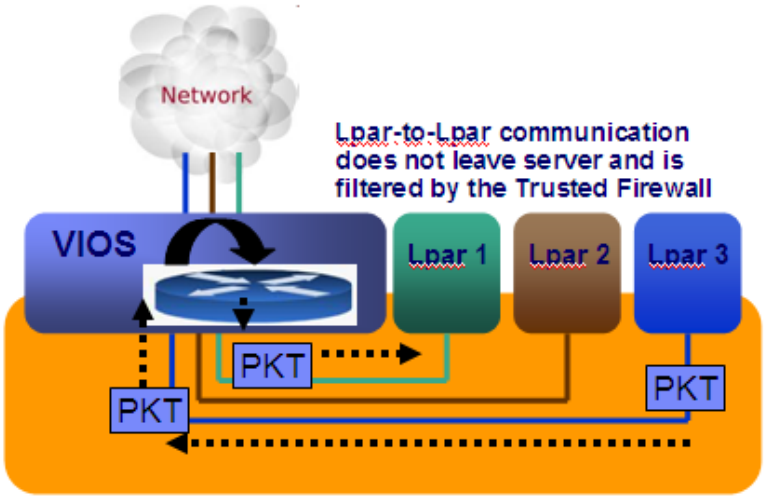
Trusted Firewall Benefits

Improves **Performance** and **Reduces** network **resource consumption** by providing firewall services within the local server virtualization infrastructure.

Without Trusted Firewall



Trusted Firewall



PowerSC Editions
Security and Compliance Options

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

PowerSC Editions	Express	Standard
Security and Compliance Automation	✓	✓
Trusted Logging		✓
Trusted Boot**		✓
Trusted Network Connect and Patch Management		✓
Trusted Firewall		✓

** Requires POWER7 System with eFW7.4

How is PowerSC Packaged?

- PowerSC Express
  - AIX PowerSC Express software package
- PowerSC Standard Edition is a combination of following
  - Includes PowerSC Express Edition + “Trusted Features”
  - PowerSC Software running on the AIX Operating System
  - Extensions to the Virtualization Firmware and VIOS
- PowerSC Standard Edition Installation Requires
  - AIX PowerSC Standard software Package
  - AIX Version 6 TL7 or higher or AIX 7 TL1 or higher
  - VIOS level v2.2.1 and above
  - Firmware(eFW7.4) and above for the “Trusted Boot” Feature

PowerSC Usage Example

Automating Security Compliance

Business challenge

A large financial institution wanted to reduce the time to setup a new system in their secure virtualized environment. They needed a streamlined process of hardening and monitoring their AIX systems for security compliance.

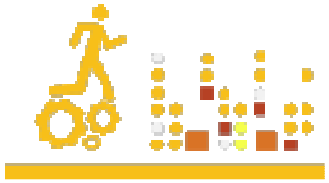
Solution

The solution used PowerSC Express compliance automation to set the AIX system security settings in a uniform manner across the systems that were created. The supplied profiles were tailored specifically to meet the specific needs of the business. Now they can apply or check the security settings with a single command locally or through a console.

Benefits

- **Accelerated** secure AIX system **provisioning**
- Provided **repeatable secure process** to maintain compliance
- **Reduced Cost** by Automating error prone Manual Steps
- Easy to **prove compliance** to auditors

Power is performance redefined



Deliver new services faster

– Compliance Automation accelerates secure system creation and compliance.

Deliver higher quality services

– PowerSC hardens the Cloud and Virtual Infrastructure avoiding security related events providing higher quality systems.

Deliver services with superior economics

– PowerSC automation and Trusted features reduce labor costs to maintain secure systems

IBM Systems Lab Services and Training: AIX Security Services Leverage the Experts

- **AIX Security Assessment** – a good starting point for security services. This service provides feedback and recommendations on improving your AIX security implementation. Feedback and recommendations are primarily derived from analyzing the security implementation of one of your operational AIX installations.
- **Centralized User Management Integration with MSAD and AIX -** LDAP directory services can save a great amount of time, effort, and energy by simplifying the task of supporting users as a business grows. Centralized user management with MSAD allows you to remove the need of syncing passwords and accounts for users on AIX systems.
- **AIX 6.1 Role Based Access Control (RBAC) Integration -** Privileged Users can create security problems by allowing unrestricted access to any file on the system. The most sophisticated and secure solution for providing privileges on AIX is the use of Enhanced RBAC in AIX 6.1.

PowerSC Services Offerings

- PowerSC Express Edition Integration
- PowerSC implementation assistance
- **AIX Auditing Integration**
- **General Security Consulting**
- **AIX 6.1 Encrypted File System (EFS) Integration -** AIX 6.1's EFS, Encrypted File System, introduces the ability to encrypt files on a per file basis without the need or expense of third-party tools.

www.ibm.com/systems/services/labservices stgls@us.ibm.com

Reference Links

- IBM Systems Magazine: PowerSC Cover Story
- http://www.ibmsystemsmagpowersystemsdigital.com/nxtbooks/ibmsystemsmag/ibmsystems_power_201111/index.php#/22%29

PowerSC hardens security and

simplifies compliance for AIX

virtual workloads

Security

in a Virtual World

Learn more about PowerSC on the Web

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

Power is performance redefined

Smarter Computing:
Power is Performance Redefined.

Power is Security and Compliance

Special notices

This document was developed for IBM offerings in the United States as of the date of publication. IBM may not make these offerings available in other countries, and the information is subject to change without notice. Consult your local IBM business contact for information on the IBM offerings available in your area.

Information in this document concerning non-IBM products was obtained from the suppliers of these products or other public sources. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. Send license inquires, in writing, to IBM Director of Licensing, IBM Corporation, New Castle Drive, Armonk, NY 10504-1785 USA.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The information contained in this document has not been submitted to any formal IBM test and is provided "AS IS" with no warranties or guarantees either expressed or implied.

All examples cited or described in this document are presented as illustrations of the manner in which some IBM products can be used and the results that may be achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions.

IBM Global Financing offerings are provided through IBM Credit Corporation in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government clients. Rates are based on a client's credit rating, financing terms, offering type, equipment type and options, and may vary by country. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice.

IBM is not responsible for printing errors in this document that result in pricing or information inaccuracies.

All prices shown are IBM's United States suggested list prices and are subject to change without notice; reseller prices may vary.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

Any performance data contained in this document was determined in a controlled environment. Actual results may vary significantly and are dependent on many factors including system hardware configuration and software design and configuration. Some measurements quoted in this document may have been made on development-level systems. There is no guarantee these measurements will be the same on generally-available systems. Some measurements quoted in this document may have been estimated through extrapolation. Users of this document should verify the applicable data for their specific environment.

Revised September 26, 2006

Special notices (cont.)

IBM, the IBM logo, ibm.com AIX, AIX (logo), AIX 5L, AIX 6 (logo), AS/400, BladeCenter, Blue Gene, ClusterProven, DB2, ESCON, i5/OS, i5/OS (logo), IBM Business Partner (logo), IntelliStation, LoadLeveler, Lotus, Lotus Notes, Notes, Operating System/400, OS/400, PartnerLink, PartnerWorld, PowerPC, pSeries, Rational, RISC System/6000, RS/6000, THINK, Tivoli, Tivoli (logo), Tivoli Management Environment, WebSphere, xSeries, z/OS, zSeries, Active Memory, Balanced Warehouse, CacheFlow, Cool Blue, IBM Systems Director VMControl, pureScale, TurboCore, Chiphopper, Cloudscape, DB2 Universal Database, DS4000, DS6000, DS8000, EnergyScale, Enterprise Workload Manager, General Parallel File System, , GPFS, HACMP, HACMP/6000, HASM, IBM Systems Director Active Energy Manager, iSeries, Micro-Partitioning, POWER, PowerExecutive, PowerVM, PowerVM (logo), PowerHA, Power Architecture, Power Everywhere, Power Family, POWER Hypervisor, Power Systems, Power Systems (logo), Power Systems Software, Power Systems Software (logo), POWER2, POWER3, POWER4, POWER4+, POWER5, POWER5+, POWER6, POWER6+, POWER7, System i, System p, System p5, System Storage, System z, TME 10, Workload Partitions Manager and X-Architecture are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries.

A full list of U.S. trademarks owned by IBM may be found at: http://www.**ibm.com**/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
AltiVec is a trademark of Freescale Semiconductor, Inc.
AMD Opteron is a trademark of Advanced Micro Devices, Inc.
InfiniBand, InfiniBand Trade Association and the InfiniBand design marks are trademarks and/or service marks of the InfiniBand Trade Association.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.
Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries or both.
Microsoft, Windows and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries or both.
NetBench is a registered trademark of Ziff Davis Media in the United States, other countries or both.
SPECint, SPECfp, SPECjbb, SPECweb, SPECjAppServer, SPEC OMP, SPECviewperf, SPECapc, SPEChpc, SPECjvm, SPECmail, SPECimap and SPECsfs are trademarks of the Standard Performance Evaluation Corp (SPEC).
The Power Architecture and Power.org wordmarks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org.
TPC-C and TPC-H are trademarks of the Transaction Performance Processing Council (TPPC).
UNIX is a registered trademark of The Open Group in the United States, other countries or both.

Other company, product and service names may be trademarks or service marks of others.

Revised December 2, 2010