IBM Power sistemler'de Güvenlik: PowerSC

Security and compliance for Power Systems

Kadri Aksoy, İş Geliştirme Yöneticisi CEE

Entegre Servis Yönetimi ve Güvenlik Çözümleri

30 Mayıs 2012, Çarşamba

Grand Hyatt İstanbul

PowerSC™

20 Years of IBM RISC Technology Leadership

Commercial & Technical Workloads

Virtualization Technologies

Enhanced SMT Support

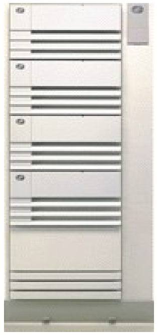
POWER7

POWER6

POWER5

POWER4

RS64
POWER3



PowerPC

RISC
POWER1

Performance Leadership

Reliability / Availability / Serviceability

1990 2010

Power Family supports all Power System servers...

Select from the broadest system portfolio in the industry

- The highest performance, most scalable UNIX system ever
- Modular footprints enable seamless growth
- The best selection of Entry servers and Blades for Linux

Power 795

Power 780

Power 770

Power 750

Power 720/740

Power 710/730

Power 7R2 Linux box

PS Blades

HMC & SDMC

Power 755

Power 775

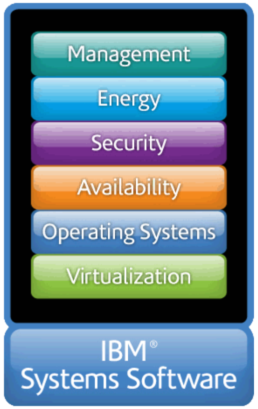
Where to find more information on Power Servers:

[illegible]/LinuxP/Performance+FAQs#PerformanceFAQs-WheredoIfindreferenceinformationonthePOWER7systems

Power your planet.

Workload-Optimizing Systems

+



AIX - The Future of UNIX

Total Integration with i

Scalable Linux ready for x86 Consolidation

Virtualization without Limits

- ✓ Drive over 90% utilization
- ✓ Dynamically scale per demand

Dynamic Energy Optimization

- ✓ 70-90% energy cost reduction
- ✓ EnergyScale™ technologies

Resiliency without Downtime

- ✓ Roadmap to continuous availability
- ✓ High availability systems & scaling

Management with Automation

- ✓ VMControl to manage virtualization
- ✓ Automation to reduce task time

IBM’s history of virtualization leadership

A 40-year tradition culminates with PowerVM

1967	1973	1987	1999	2004	2007	2008
IBM develops **hypervisor** that would become VM on the mainframe	IBM announces first machines to do **physical partitioning**	IBM announces **LPAR on the mainframe**	IBM announces **LPAR** on POWER™	IBM intro’s POWER Hypervisor ™ for System p and System i	IBM announces POWER6™, **the first UNIX servers with Live Partition Mobility**	**IBM announces PowerVM**

2011 Security Market - $50.7Billion

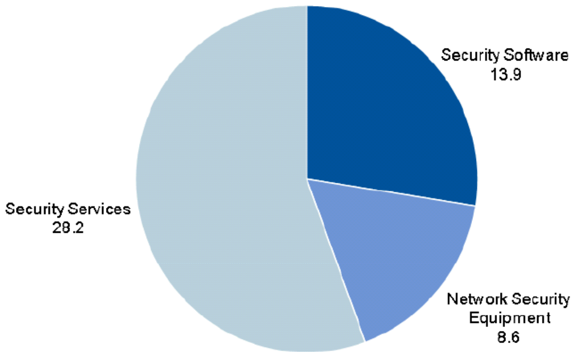
Compliance $29.9Billion

- AMR - North American Companies expected to spend $29.9B on regulatory compliance and will spend $8.8B on technology solutions to solve their compliance requirements.
- Forrester Research Approximately 6% to 11% of a company's overall IT spending will go to security.

Cyber Crime $100 Billion

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

Figure 1. Enterprise Security Infrastructure Market by Segment, Worldwide, 2011 (Billions of U.S. Dollars)



Source: Gartner (January 2011)

Annual Threat Assessment of the

US Intelligence Community

for the Senate Select Committee on Intelligence

Dennis C. Blair

Director of National Intelligence

February 2,

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

Bloomberg

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

What are the Key Customer Pains?

3. Maintain and demonstrate compliance

- Managing varied and dynamic regulatory requirements requires accurate, reliable visibility and comprehensive reporting – in order to stay ahead of both the threat and the auditor. In addition to enabling new innovation and maintaining the security, privacy and availability of critical business assets, IT organizations still need to prove it. IBM allows you to put security processes in place (people, technology) to meet and report on compliance guidelines outlined by legal and industry requirements.

Security Standards Help Target Customers

To Whom Does Payment Card Industry(PCI) Data Security Standard Apply?

All merchants & service providers that **store, process, use,** or **transmit *cardholder data***

- **Retail** (e commerce & brick & mortar)
- **Hospitality** (restaurants, hotel chains, etc.)
- **Convenience Stores** (gas stations, fast food)
- **Transportation** (i.e. airlines, car rental, etc.)
- **Financial Services** (credit processors, banks, insurance)
- **Healthcare/Education** (hospitals, universities)
- **Government** (where payment cards are accepted)

To Whom Does the following standards apply to?

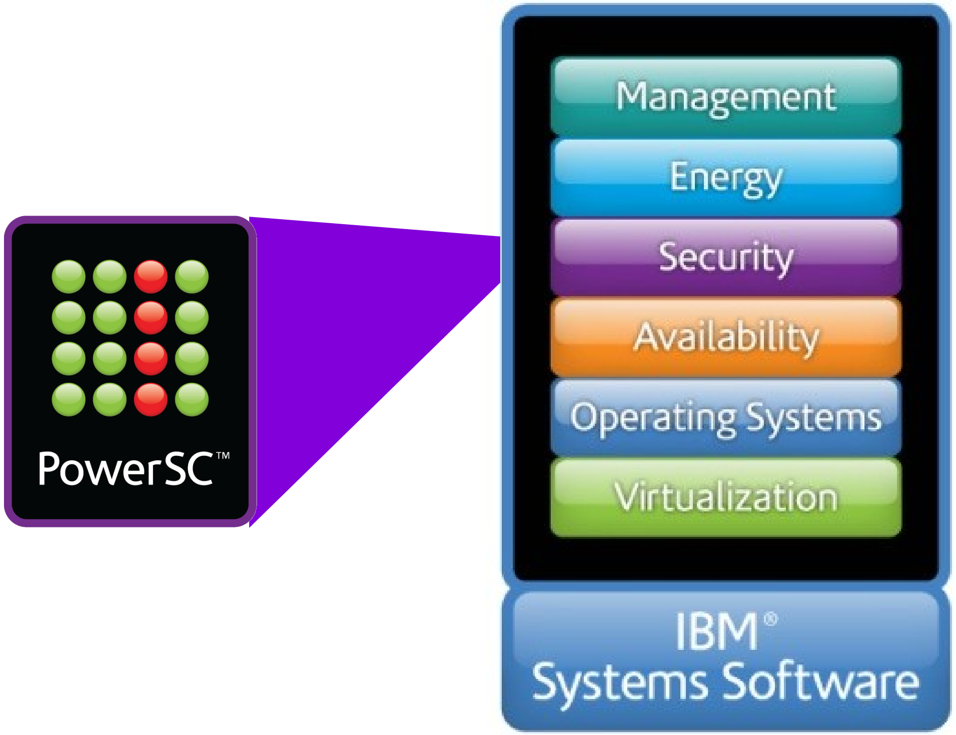
- DOD STIG – US Department of Defense
- Sarbanes Oxley (usually implemented using COBIT best practices) – All public companies that have registered securities with US Securities and Exchange

PowerSC

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

Client Benefits

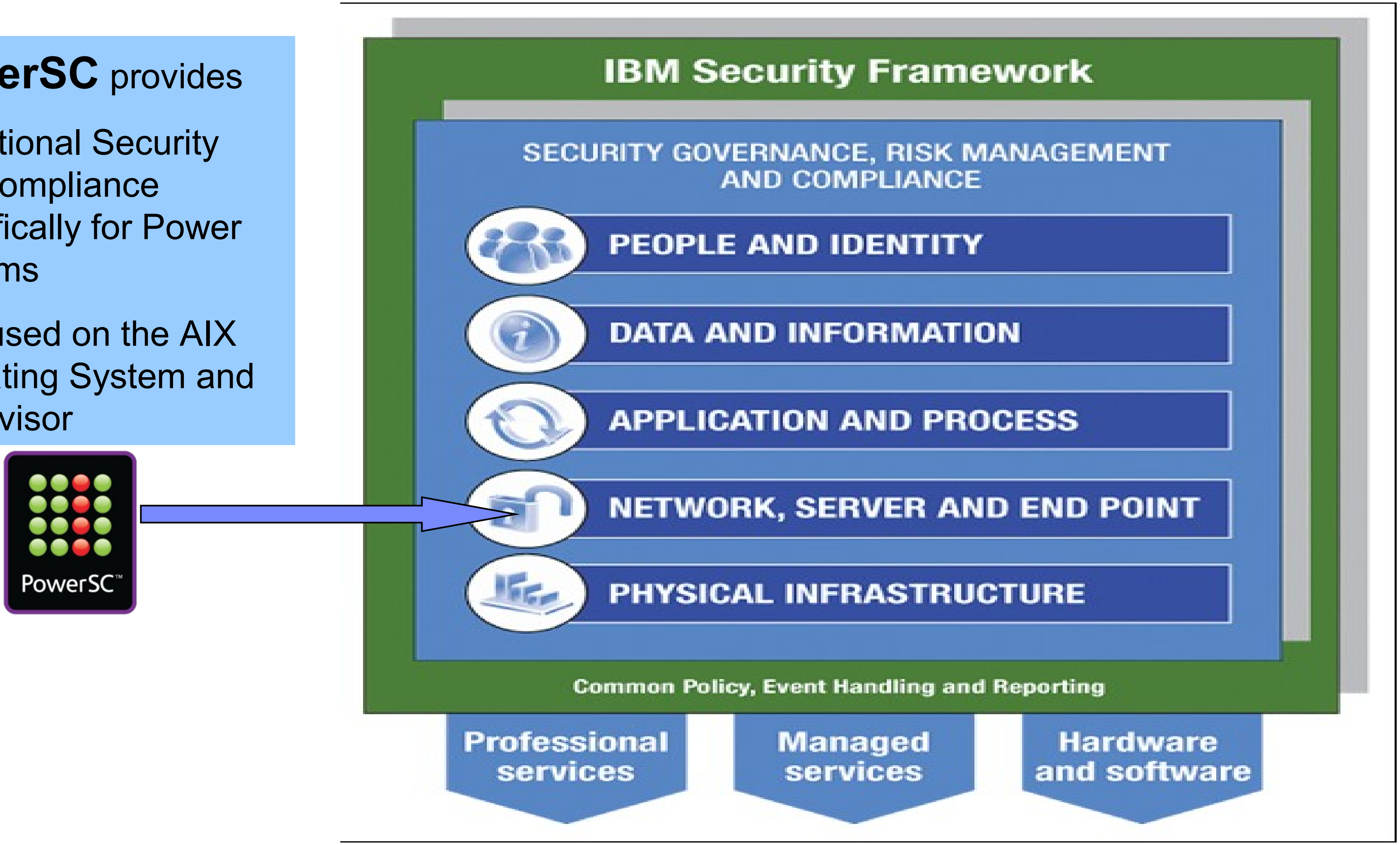
- ***Simplifies management*** *and measurement of security & compliance*
- ***Reduces cost*** *of security & compliance*
- ***Improves detection*** *and reporting of security exposures*
- ***Improves*** *the* ***audit capability*** *to satisfy reporting requirements*
- *Provides* ***"virtualization aware"***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



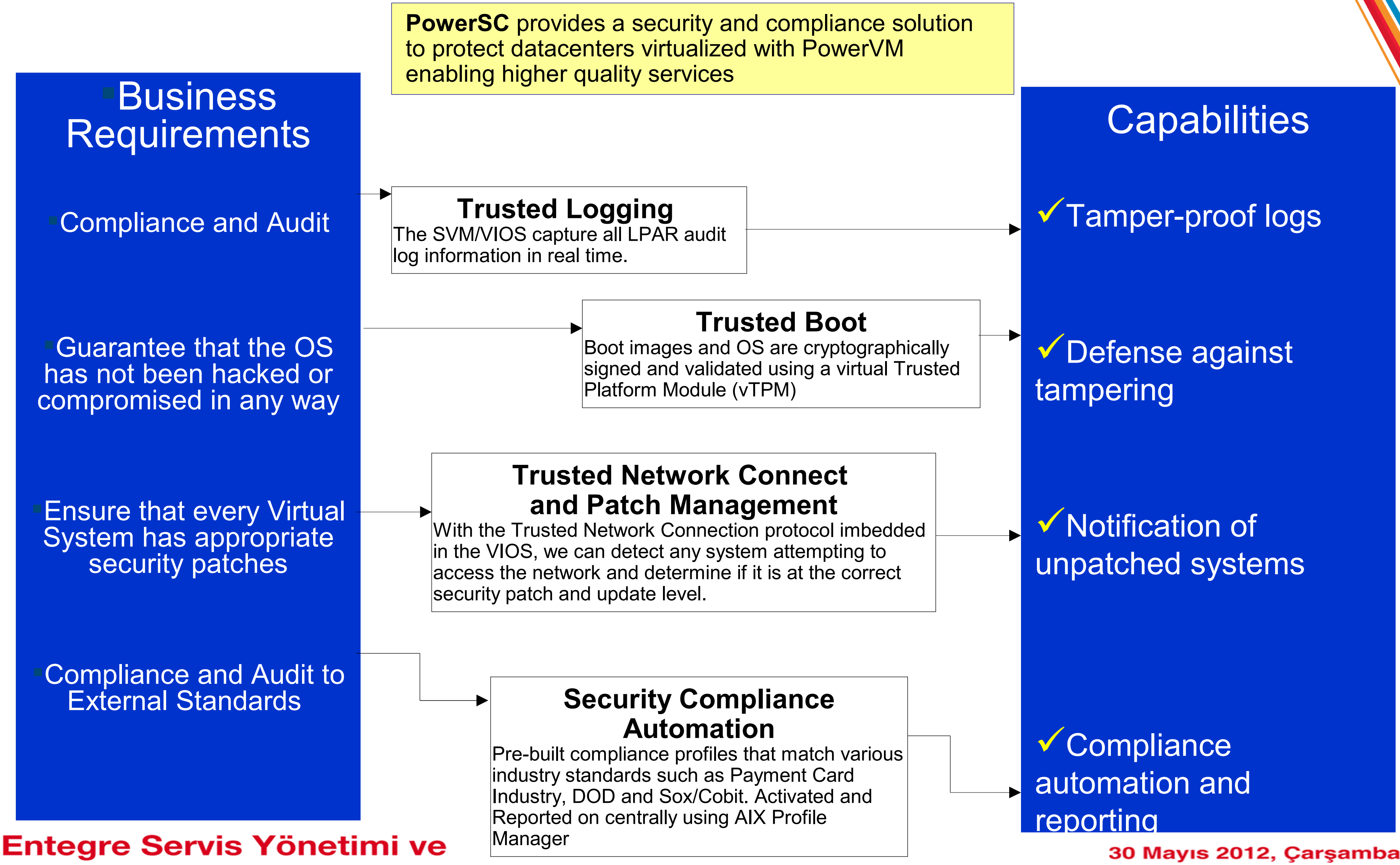
Where Does PowerSC Fit within the IBM Security Framework?

PowerSC provides

- Additional Security and Compliance Specifically for Power Systems
- Focused on the AIX Operating System and Hypervisor



PowerSC Features



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

Business Requirements

- Compliance and Audit
- Guarantee that the OS has not been hacked or compromised in any way
- Ensure that every Virtual System has appropriate security patches
- Compliance and Audit to External Standards

Trusted Logging

The SVM/VIOS capture all LPAR audit log information in real time.

Trusted Boot

Boot images and OS are cryptographically signed and validated using a virtual Trusted Platform Module (vTPM)

Trusted Network Connect and Patch Management

With the Trusted Network Connection protocol imbedded in the VIOS, we can detect any system attempting to access the network and determine if it is at the correct security patch and update level.

Security Compliance Automation

Pre-built compliance profiles that match various industry standards such as Payment Card Industry, DOD and Sox/Cobit. Activated and Reported on centrally using AIX Profile Manager

Capabilities

- ✓Tamper-proof logs
- ✓Defense against tampering
- ✓Notification of unpatched systems
- ✓Compliance automation and reporting

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.

IBM Power Sistemlerde Güvenlik : PowerSC

Security and Compliance for Power Systems

Zuhal AKSÜT
Power Sistemler Teknik Satış Uzmanı

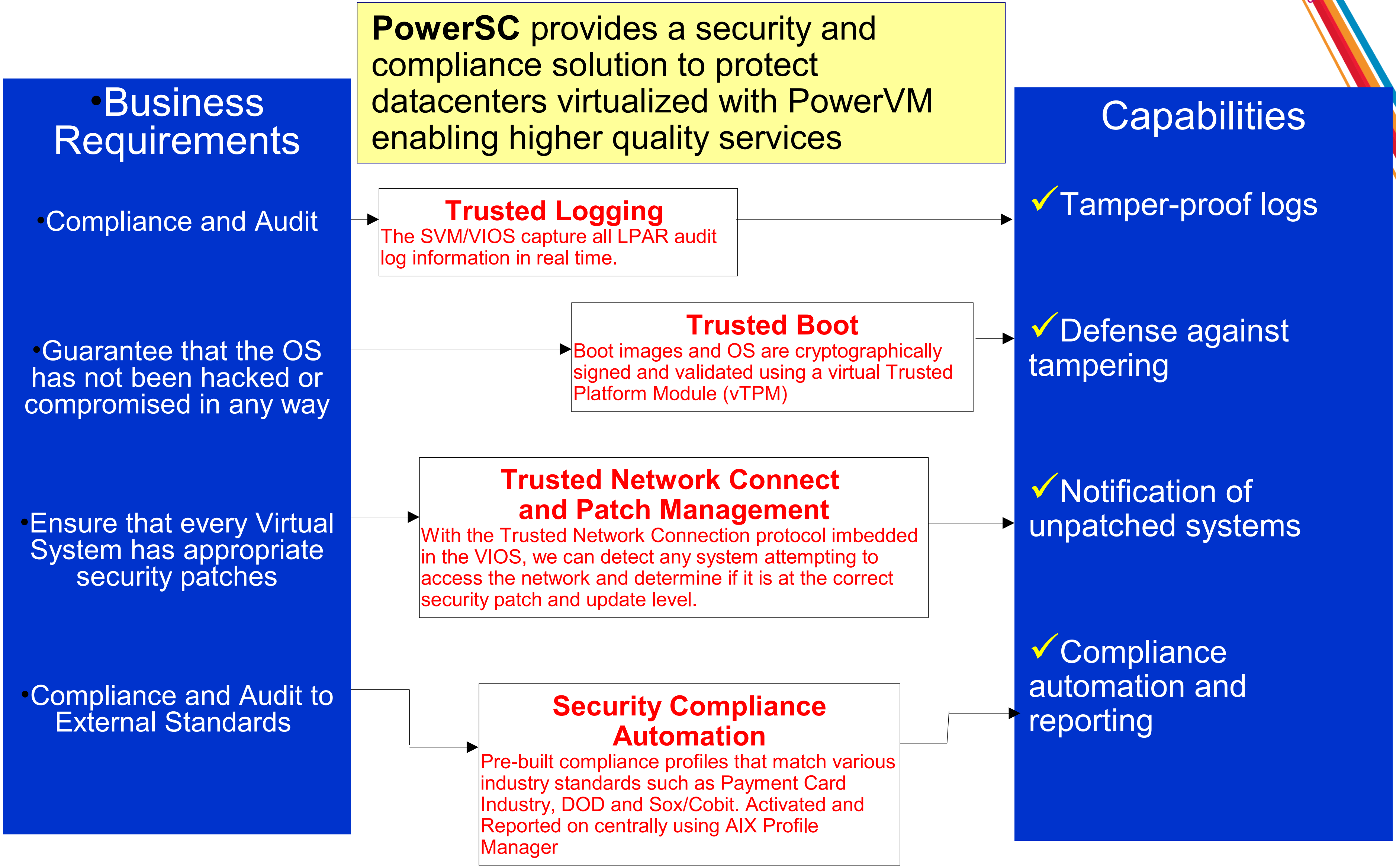
Entegre Servis Yönetimi ve Güvenlik Çözümleri

30 Mayıs 2012, Çarşamba

Grand Hyatt İstanbul

PowerSC™

PowerSC Features



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

•Business Requirements

- •Compliance and Audit
- •Guarantee that the OS has not been hacked or compromised in any way
- •Ensure that every Virtual System has appropriate security patches
- •Compliance and Audit to External Standards

Trusted Logging
The SVM/VIOS capture all LPAR audit log information in real time.

Trusted Boot
Boot images and OS are cryptographically signed and validated using a virtual Trusted Platform Module (vTPM)

Trusted Network Connect and Patch Management
With the Trusted Network Connection protocol imbedded in the VIOS, we can detect any system attempting to access the network and determine if it is at the correct security patch and update level.

Security Compliance Automation
Pre-built compliance profiles that match various industry standards such as Payment Card Industry, DOD and Sox/Cobit. Activated and Reported on centrally using AIX Profile Manager

Capabilities

- ✓Tamper-proof logs
- ✓Defense against tampering
- ✓Notification of unpatched systems
- ✓Compliance automation and reporting

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

Compliance Automation - Standards

DoD Security Technical Implementation Guide

- Automation of configuration and monitoring for AIX and VIOS in compliance with DoD Unix STIG v5r1 for UNIX http://iase.disa.mil/stigs/stig/unix-stig-v5r1.pdf
- 158 pages
- Currently, PowerSC can automate the configuration and monitoring of 90% of all settings required by DoD.

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

Compliance Automation

Payment Card Industry Data Security Standard v2.0

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

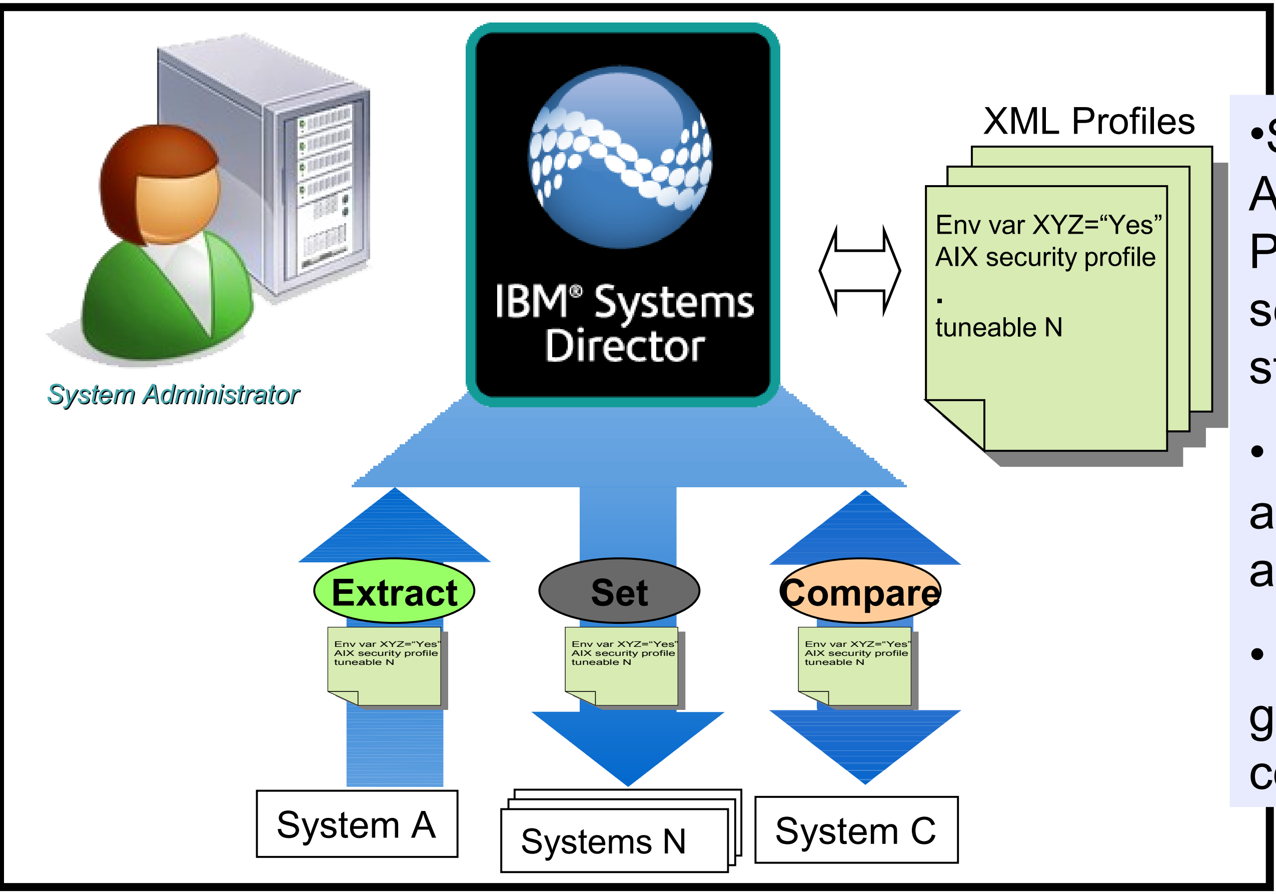
PowerSC PCI-DSS Coverage

- Approximately 150 xml rules to assist in the configuration in 7 of the 12 requirement areas.

Security Compliance Automation

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

What are the Key Customer Pains?

1. Control cost, increase operational efficiency and innovate

- Organizations are keen to take advantage of cost savings opportunities, including new computing architectures such as the cloud, virtualization, etc. However, these new models can increase risk substantially without the proper controls and visibility in place. With years of proven innovation, IBM allows you to enable new business initiatives and opportunities where trust risk converge.

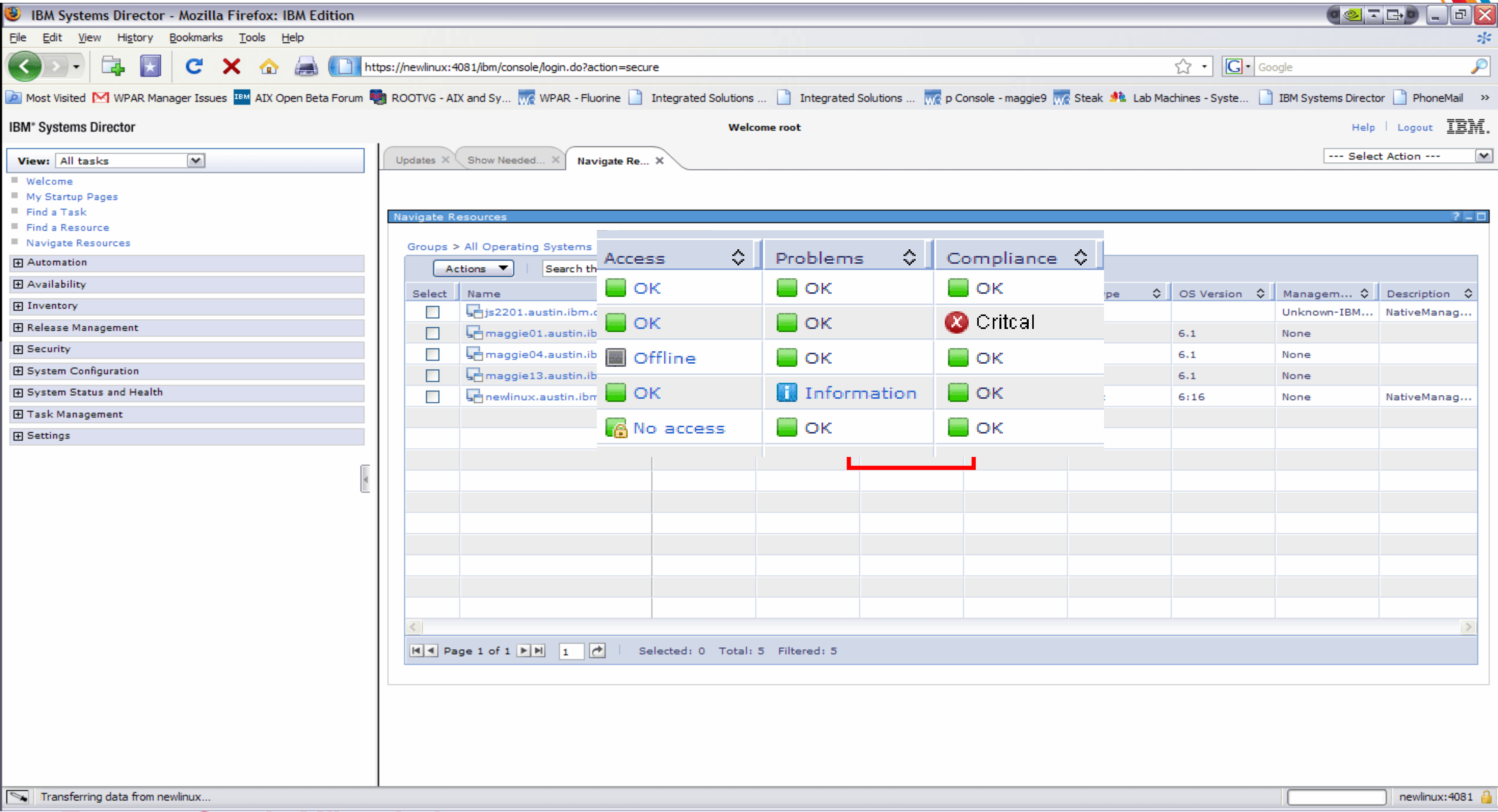
2. Keep IT infrastructure and information safe from threats

- At the most basic level, IT teams need to "keep the lights on" and a key aspect of this is maintaining the security, privacy, and availability of business assets. The more easily organizations can "operationalize" security throughout the entire lifecycle of their data, applications, systems, networks, processes and personnel, the better their overall security posture will be. IBM allows you to increase the resiliency of the data, systems, applications, networks, and devices that enable your business to operate.

And, don't forget...

Security Compliance Automation

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



Select	Name	...pe	OS Version	Managem...	Description
□	js2201.austin.ibm.c			Unknown-IBM...	NativeManag...
□	maggie01.austin.ib		6.1	None	
□	maggie04.austin.ib		6.1	None	
□	maggie13.austin.ib		6.1	None	
□	newlinux.austin.ibm		6:16	None	NativeManag...

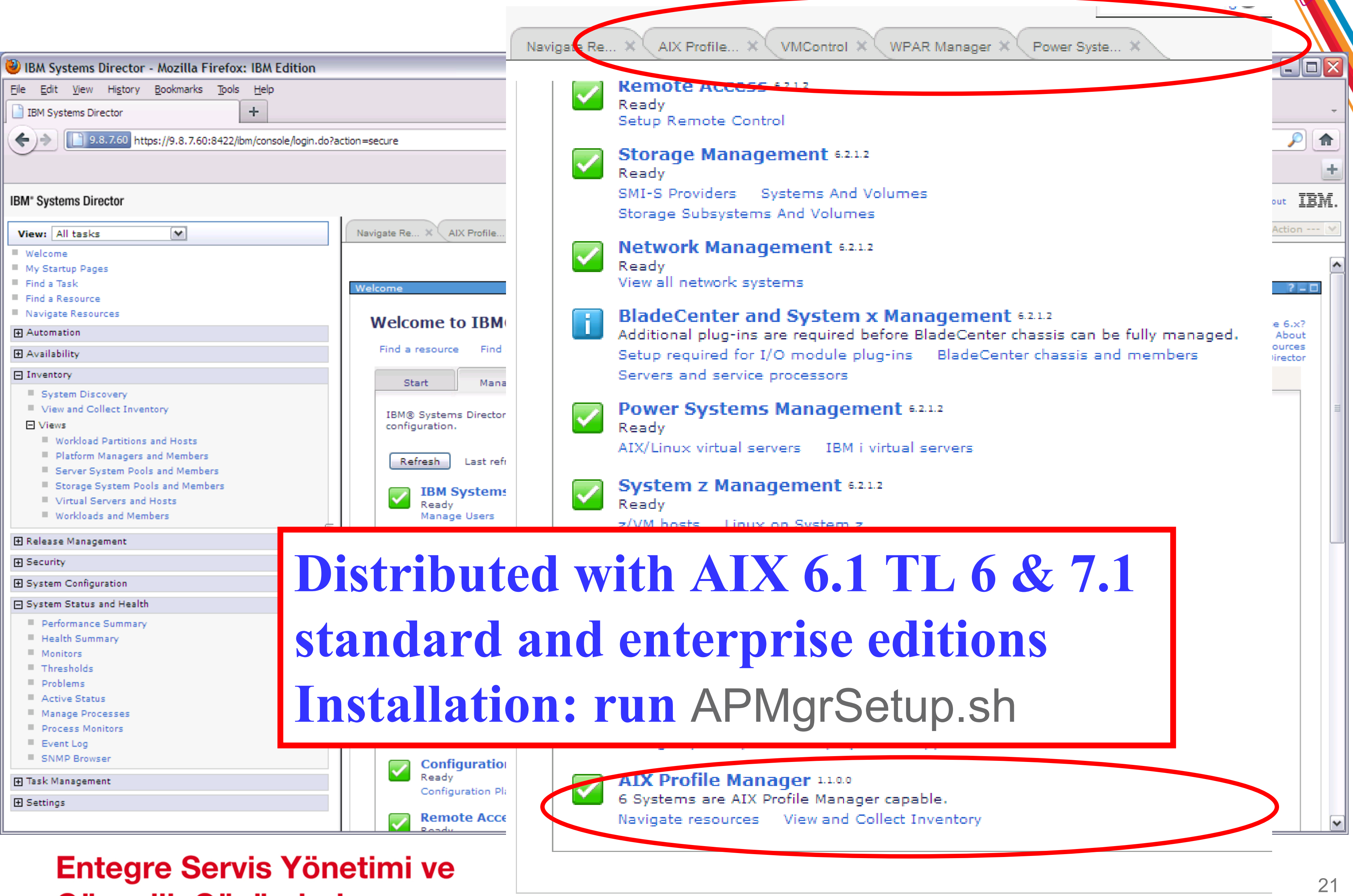
Access	Problems	Compliance
🟩 OK	🟩 OK	🟩 OK
🟩 OK	🟩 OK	☒ Critcal
▨ Offline	🟩 OK	🟩 OK
🟩 OK	ℹ Information	🟩 OK
🔒 No access	🟩 OK	🟩 OK

Page 1 of 1 | 1 | Selected: 0 Total: 5 Filtered: 5

Transferring data from newlinux...

newlinux:4081

IBM Systems Director welcome page



IBM Systems Director - Mozilla Firefox: IBM Edition

File Edit View History Bookmarks Tools Help

IBM Systems Director

9.8.7.60 https://9.8.7.60:8422/ibm/console/login.do?action=secure

IBM® Systems Director

View: All tasks

- Welcome
- My Startup Pages
- Find a Task
- Find a Resource
- Navigate Resources

⊞ Automation

⊞ Availability

⊟ Inventory

- System Discovery
- View and Collect Inventory
- ⊟ Views
  - Workload Partitions and Hosts
  - Platform Managers and Members
  - Server System Pools and Members
  - Storage System Pools and Members
  - Virtual Servers and Hosts
  - Workloads and Members

⊞ Release Management

⊞ Security

⊞ System Configuration

⊟ System Status and Health

- Performance Summary
- Health Summary
- Monitors
- Thresholds
- Problems
- Active Status
- Manage Processes
- Process Monitors
- Event Log
- SNMP Browser

⊞ Task Management

⊞ Settings

Navigate Re... ✕ AIX Profile...

Welcome

Welcome to IBM

Find a resource Find

Start Mana

IBM® Systems Director configuration.

Refresh Last refr

✓ IBM Systems
Ready
Manage Users

✓ Configuratio
Ready
Configuration Pl

✓ Remote Acce

Navigate Re... ✕ AIX Profile... ✕ VMControl ✕ WPAR Manager ✕ Power Syste... ✕

✓ Remote Access 6.2.1.2
Ready
Setup Remote Control

✓ Storage Management 6.2.1.2
Ready
SMI-S Providers Systems And Volumes
Storage Subsystems And Volumes

✓ Network Management 6.2.1.2
Ready
View all network systems

ℹ BladeCenter and System x Management 6.2.1.2
Additional plug-ins are required before BladeCenter chassis can be fully managed.
Setup required for I/O module plug-ins BladeCenter chassis and members
Servers and service processors

✓ Power Systems Management 6.2.1.2
Ready
AIX/Linux virtual servers IBM i virtual servers

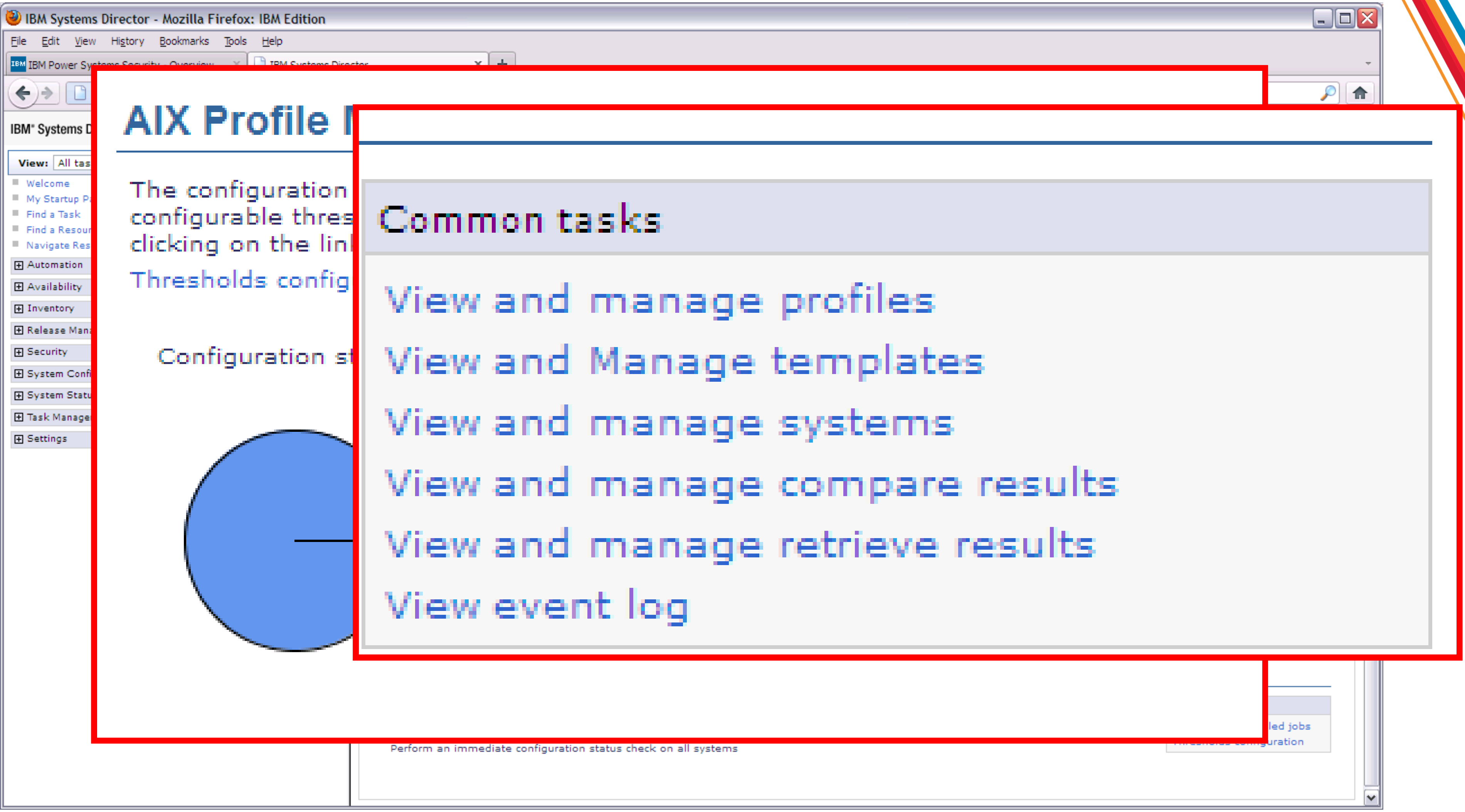
✓ System z Management 6.2.1.2
Ready
z/VM hosts Linux on System z

✓ AIX Profile Manager 1.1.0.0
6 Systems are AIX Profile Manager capable.
Navigate resources View and Collect Inventory

Distributed with AIX 6.1 TL 6 & 7.1 standard and enterprise editions

Installation: run APMgrSetup.sh

AIX Pofile Manager



AIX Profile M

The configuration
configurable thres
clicking on the lin

Thresholds config

Configuration st

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

Perform an immediate configuration status check on all systems

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:

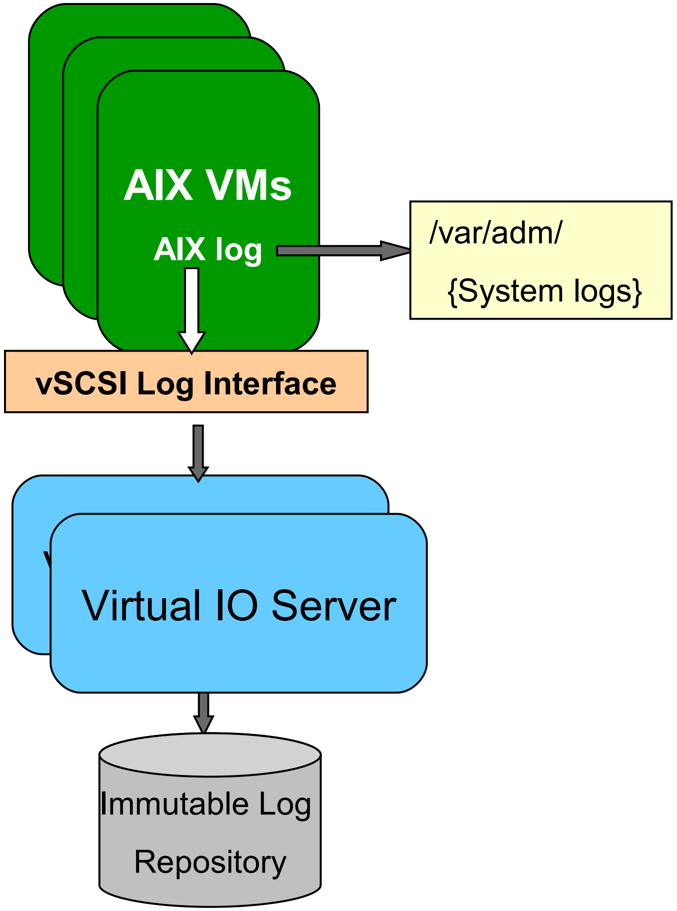
Trusted Logging provides **secure centralized protection** for AIX audit and system logs and is integrated with PowerVM virtualization.

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

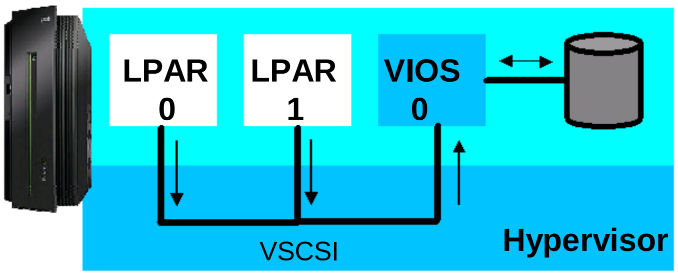
How does it work?



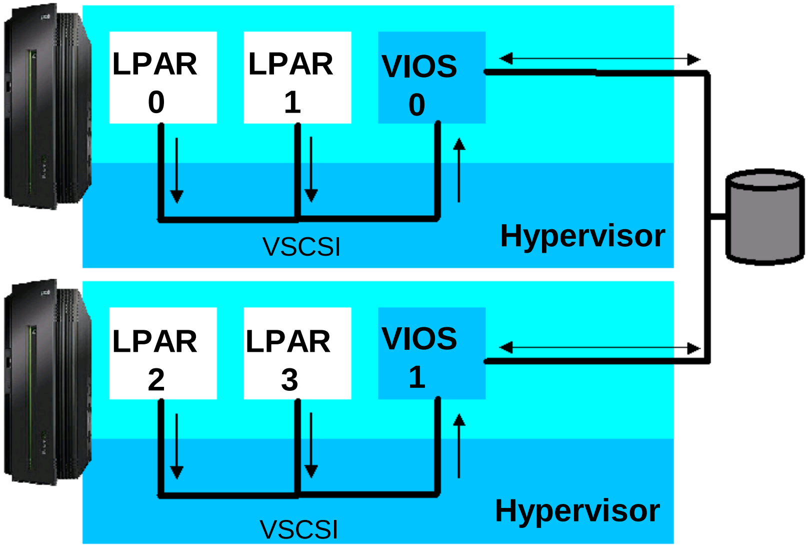
- AIX Logs use a Special Log Virtual SCSI Device
- Log Virtual SCSI device is created and managed by VIOS
- Logging data is written to an Immutable Repository or storage connected to the VIOS Server
- As the data is stored the AIX VM cannot alter or remove logs owned by VIO Server
- Normal AIX Logs in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

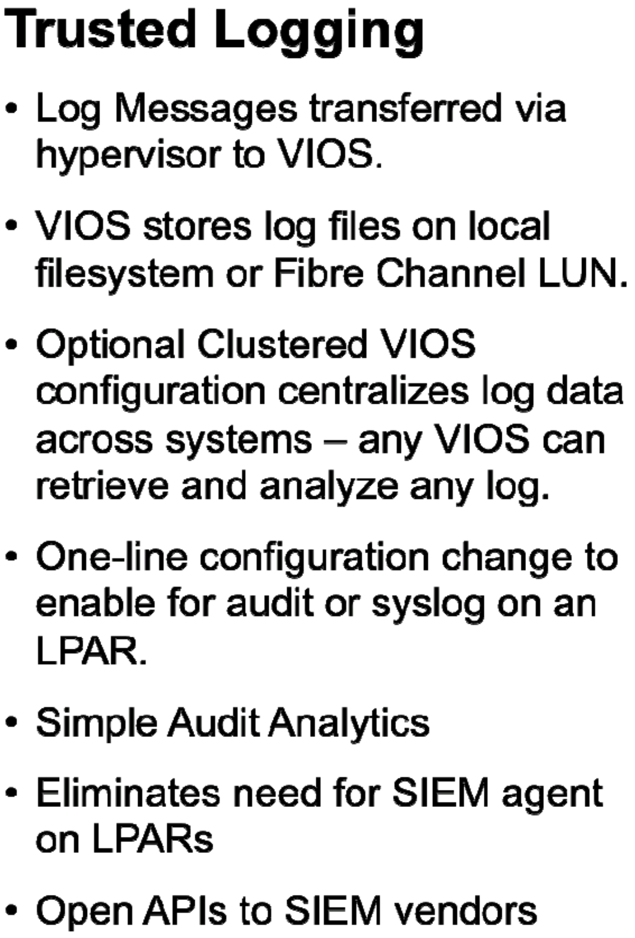
PowerSC Trusted Logging

Basic configuration:



Clustered VIOS configuration:





Trusted Logging

- Log Messages transferred via hypervisor to VIOS.
- VIOS stores log files on local filesystem or Fibre Channel LUN.
- Optional Clustered VIOS configuration centralizes log data across systems – any VIOS can retrieve and analyze any log.
- One-line configuration change to enable for audit or syslog on an LPAR.
- Simple Audit Analytics
- Eliminates need for SIEM agent on LPARs
- Open APIs to SIEM vendors

Power is performance redefined

VSCSI

Hypervisor

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:

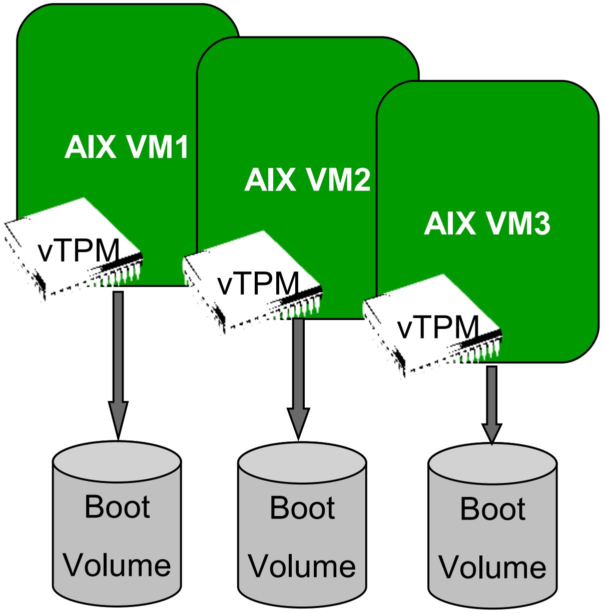
Trusted Boot provides a **Virtual Trusted Platform Module(vTPM)** for each Virtual Machine. The vTPM is used to hold the boot measurement data to validate the Trust of a system.

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

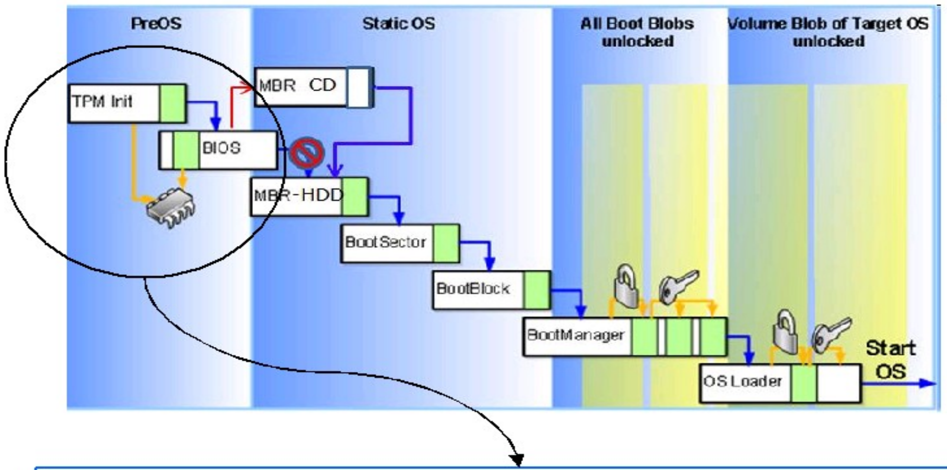
How does it work?



This feature requires Firmware 7.4 or above

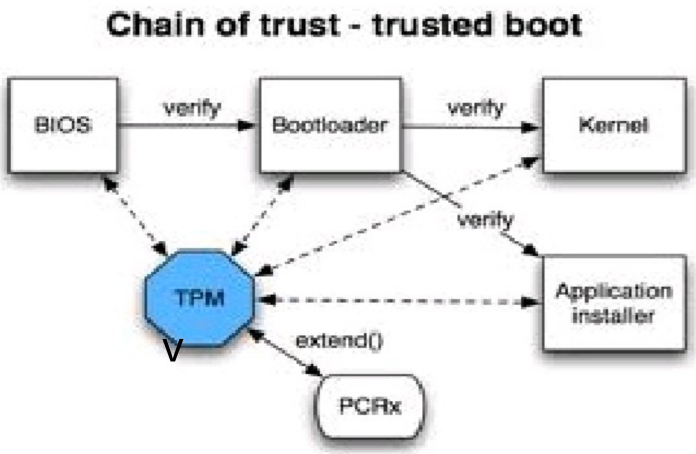
- Each Virtual Machine has its own vTPM Configured using HMC/SDMC
- During the AIX Boot process Measurements are taken and Compared to vTPM contents
- PowerVM Hypervisor and PowerSC work together to metric the boot process and store the metrics in the vTPM
- Trusted Status is available for “Attestation”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

Trusted Boot Technology Overview



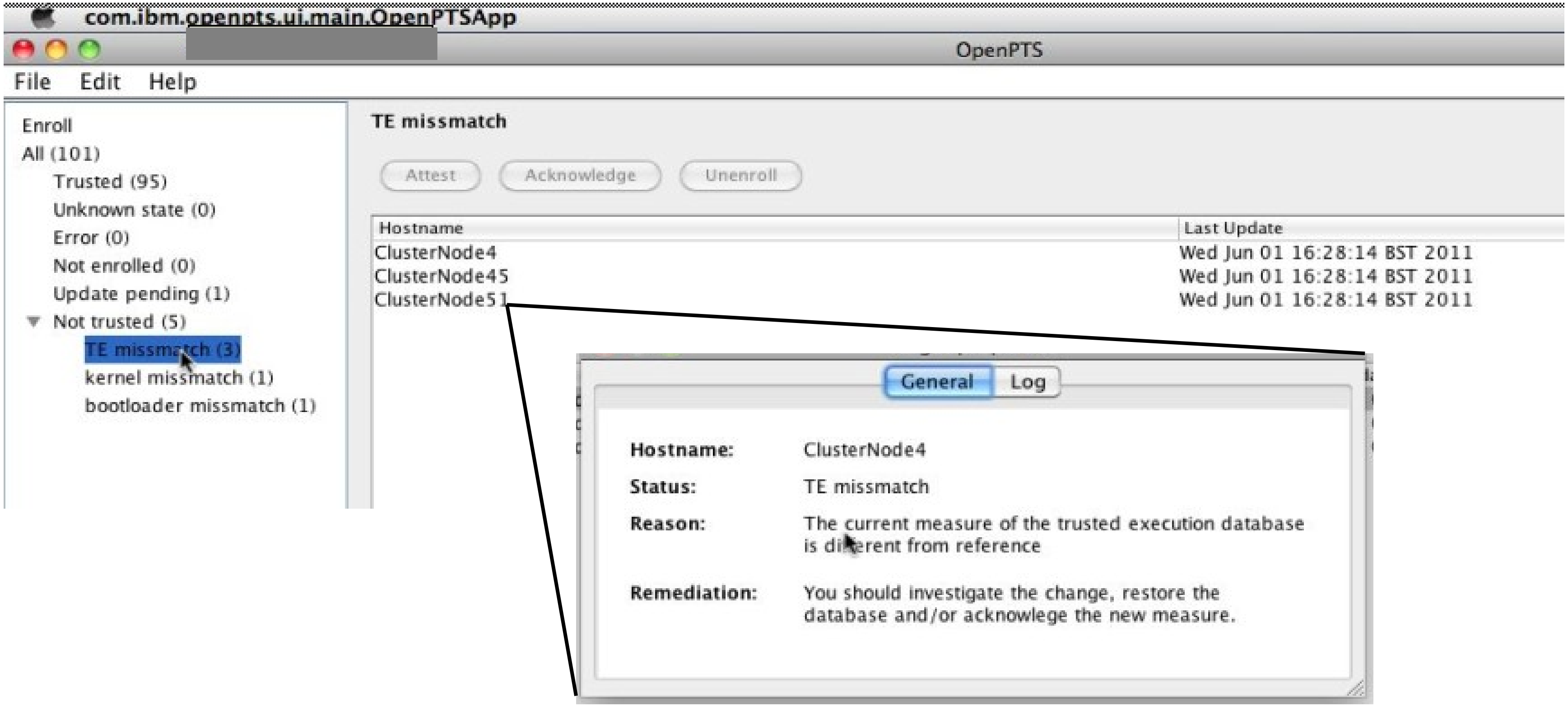
- vTPM virtual TPM
- Protected within the Power Hypervisor and with the pHyp's perfect security record
- Measure boot image
- Measure kernel extensions
- Measure AIX Trusted Execution (TE) Kernext
- TE to verify OS, and Applications.

TRUSTED COMPUTING GROUP™



How to Monitor Trusted System Status?

Trusted Monitor OpenPTS GUI



Hostname	Last Update
ClusterNode4	Wed Jun 01 16:28:14 BST 2011
ClusterNode45	Wed Jun 01 16:28:14 BST 2011
ClusterNode51	Wed Jun 01 16:28:14 BST 2011

Hostname: ClusterNode4

Status: TE missmatch

Reason: The current measure of the trusted execution database is different from reference

Remediation: You should investigate the change, restore the database and/or acknowlege the new measure.

- 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 – 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:

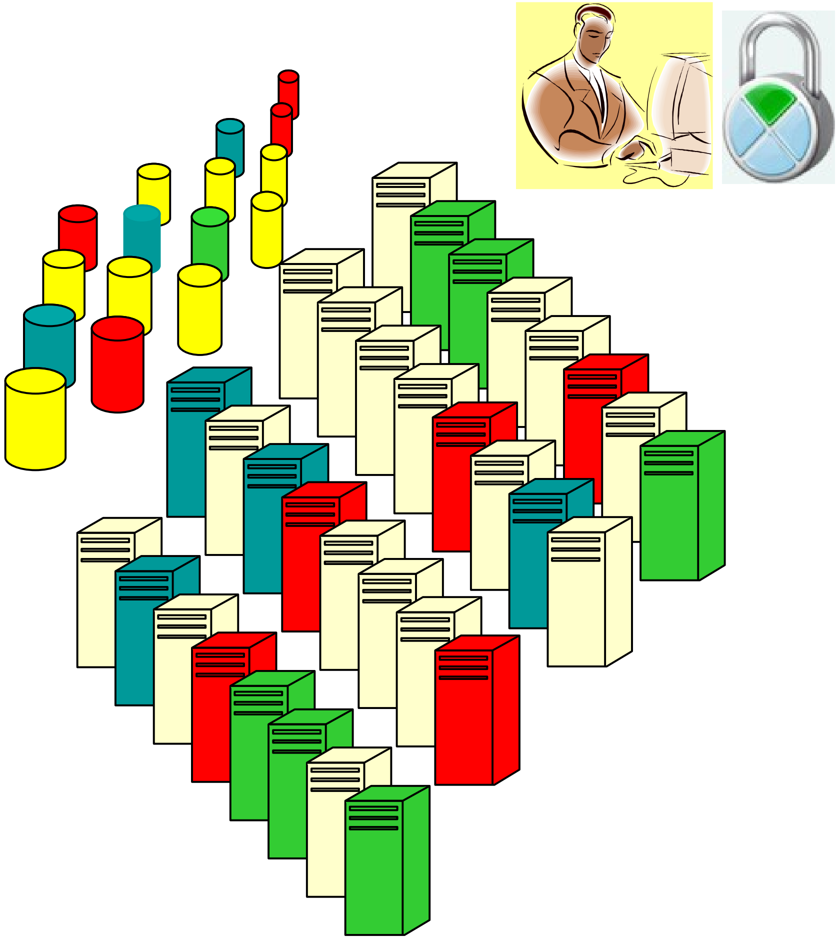
Trusted Network Connect and Patch Management detects noncompliant virtual machines during activation and alerts administrators immediately.

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

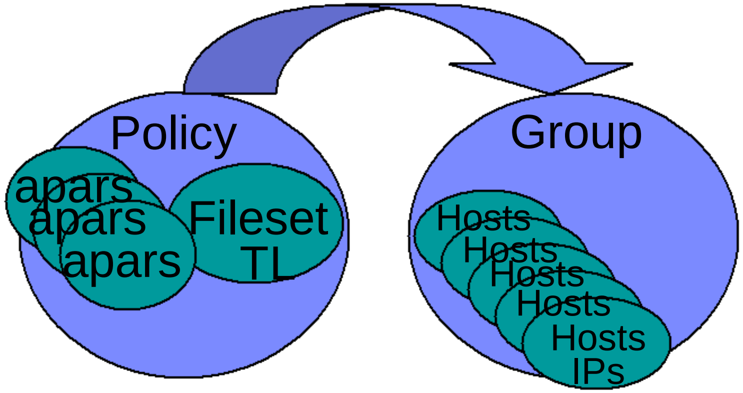
How does it work?



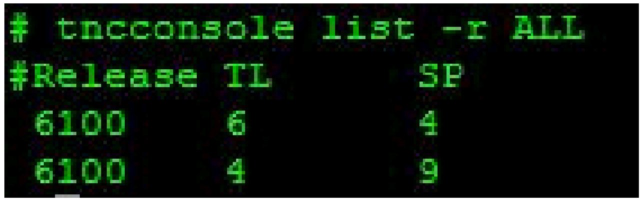
- Trusted Network Connect (TNC) is integrated with the Service Update Manager Assistant (SUMA) and the Network Installation Manager (NIM)
- During the Boot process TNC in the LPAR communicates to TNC server in VIOS
- TNC Server is notified of patch levels
- TNC Server Sends Alert if not at correct patch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

TNC Server

Process Flow

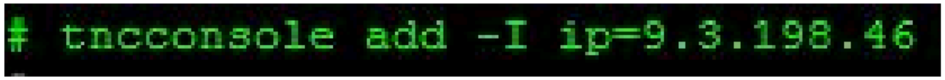


- View verification Technology Levels



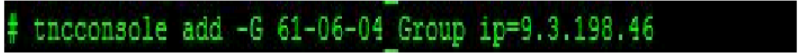
```
# tncconsole list -r ALL
#Release TL       SP
 6100     6       4
 6100     4       9
```

- Add a TNC Client to TNC Server

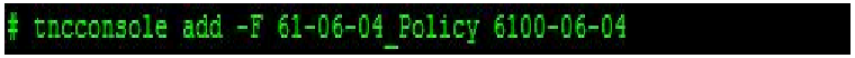


```
# tncconsole add -I ip=9.3.198.46
```

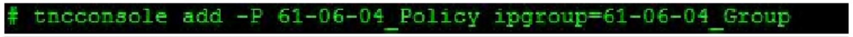
- Create a Policy and Policy Group



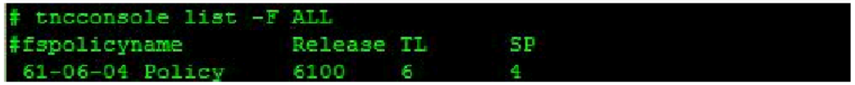
```
# tncconsole add -G 61-06-04_Group ip=9.3.198.46
```



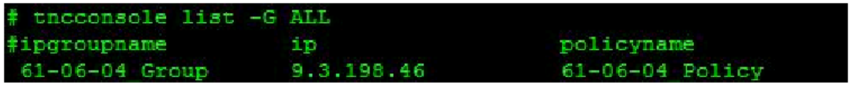
```
# tncconsole add -F 61-06-04_Policy 6100-06-04
```



```
# tncconsole add -P 61-06-04_Policy ipgroup=61-06-04_Group
```



```
# tncconsole list -F ALL
#fspolicyname          Release TL      SP
 61-06-04_Policy       6100    6       4
```



```
# tncconsole list -G ALL
#ipgroupname           ip                  policyname
 61-06-04_Group        9.3.198.46          61-06-04_Policy
```

Power is performance redefined

TNC with integrated Patch Management

- Automatic Notification of Security Patches
- Identification of down level systems
- Centralized management through NIM to patch systems.
- Automatic Notification if new, down level virtualized system boot, migrates, resumes into datacenter

Security Patch Announced

Alert. Unpatched system activated in Data Center.

Power is performance redefined

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		✓

** 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

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

Power is performance redefined

AIX®

i for Business

Linux®

POWER7 BUILT ON Power™

IBM® Systems Director

PowerSC™

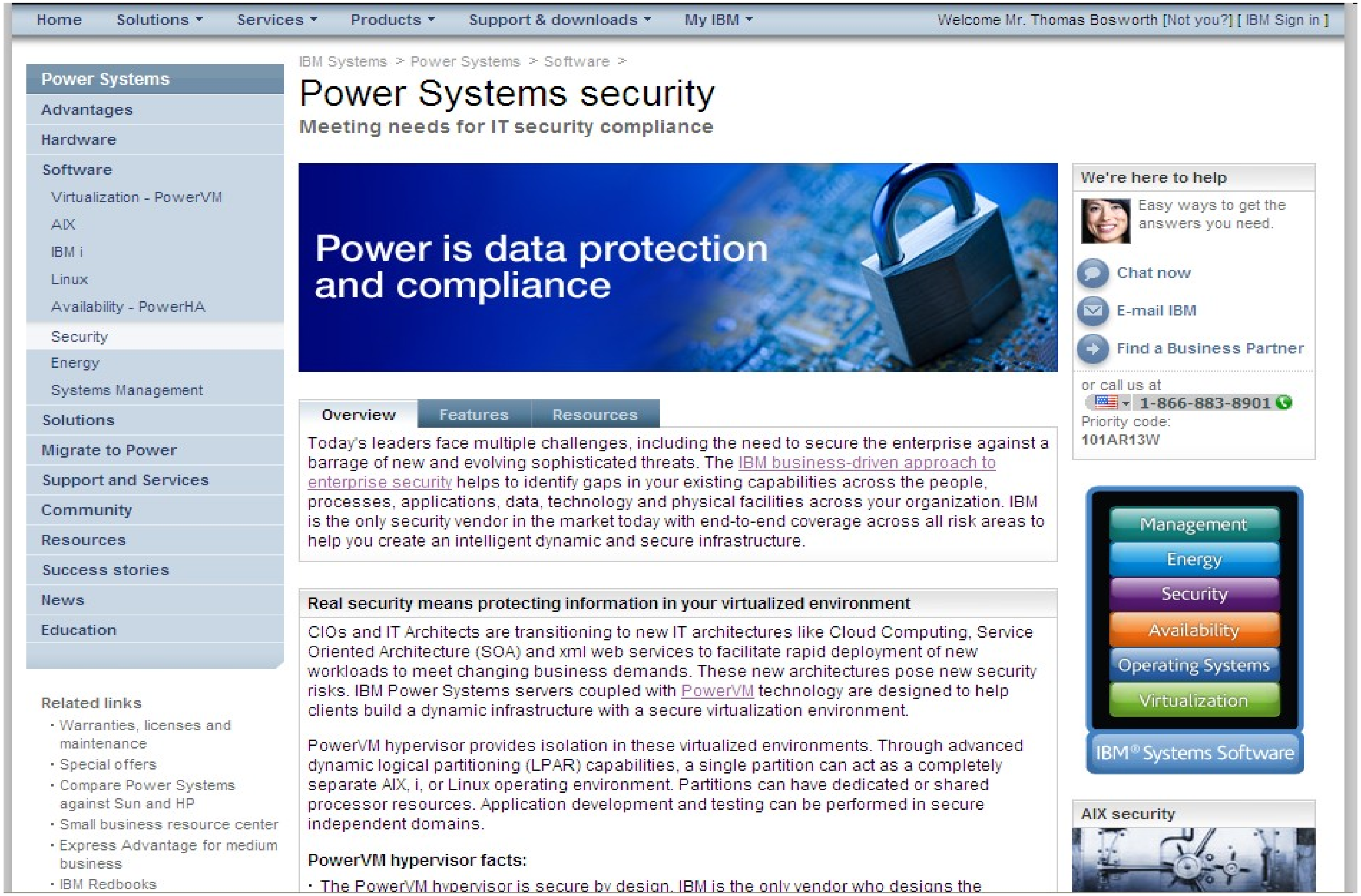
PowerHA™

PowerVM™

Power is Security and Compliance

Learn more about PowerSC on the Web

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



Related links

- Warranties, licenses and maintenance
- Special offers
- Compare Power Systems against Sun and HP
- Small business resource center
- Express Advantage for medium business
- IBM Redbooks

Power Systems security

Meeting needs for IT security compliance

Today's leaders face multiple challenges, including the need to secure the enterprise against a barrage of new and evolving sophisticated threats. The IBM business-driven approach to enterprise security helps to identify gaps in your existing capabilities across the people, processes, applications, data, technology and physical facilities across your organization. IBM is the only security vendor in the market today with end-to-end coverage across all risk areas to help you create an intelligent dynamic and secure infrastructure.

Real security means protecting information in your virtualized environment

CIOs and IT Architects are transitioning to new IT architectures like Cloud Computing, Service Oriented Architecture (SOA) and xml web services to facilitate rapid deployment of new workloads to meet changing business demands. These new architectures pose new security risks. IBM Power Systems servers coupled with PowerVM technology are designed to help clients build a dynamic infrastructure with a secure virtualization environment.

PowerVM hypervisor provides isolation in these virtualized environments. Through advanced dynamic logical partitioning (LPAR) capabilities, a single partition can act as a completely separate AIX, i, or Linux operating environment. Partitions can have dedicated or shared processor resources. Application development and testing can be performed in secure independent domains.

PowerVM hypervisor facts:

- The PowerVM hypervisor is secure by design. IBM is the only vendor who designs the

We're here to help

Easy ways to get the answers you need.

or call us at

1-866-883-8901

Priority code:

101AR13W

Resources

- PowerSC 7.1 (pdf)
  - http://www-03.ibm.com/systems/power/software/security/index.html
- IBM Systems Director 6.2.x Information Center
  - http://publib.boulder.ibm.com/infocenter/director/v6r2x/index.jsp
- AIX Profile Manager V1.1.1 for IBM Systems Director
  - http://publib.boulder.ibm.com/infocenter/aix/v6r1/topic/com.ibm.aix.apmgr/apmgr_pdf.pdf
- IBM AIX Version 7.1 Differences Guide, *SG24-7910-00*
  - http://www.redbooks.ibm.com/abstracts/sg247910.html?Open
- Beat the AIX Security Expert gotchas, developerWorks
  - http://www.ibm.com/developerworks/aix/library/au-aixsecexpert/index.html
- The clever way to catch new stuff (or catch up):
  - AIX movies (system hardening with aixpert, pConsole and much, much more)

TEŞEKKÜRLER ...