Getting Started
PowerSC Real-Time Compliance

Release 1.1.2 from Nov 2012

Alice Keating-Withers
IBM Power Systems
Client Technical Specialist

Nigel Griffiths
IBM Power Systems
Advanced Technology Support, Europe

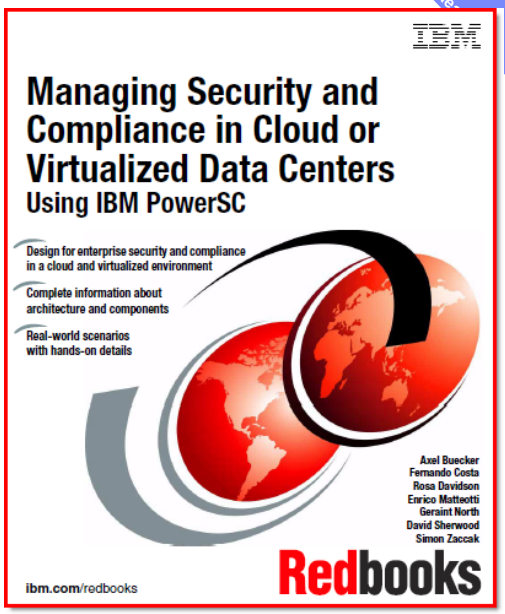
Presentation Version 2

Why Real-Time Alerts?

- Don't wait for the yearly audit
- Don't wait for that daily, weekly, monthly script to run and report your security

- Get alerted of a security mistake or hacker, the same second it happens so you can react, immediately.

Released in 2013
PowerSC Redbook
See Chapter 4, ~20 pages



PowerSC Editions

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

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

Trusted Surveyor ##

Separate LPP & price

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

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

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

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

PowerSC Real-Time

PowerSC Editions

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

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

PowerSC Real-Time

Real-Time Compliance Pre-Requisites

- AIX 6 TL7+ or AIX 7 TL1+ with all service packs please
- Purchase PowerSC Express Edition
  - With Media
- Downloaded from PowerSC from ESS website as normal
  - Entitled Software Support - http://www.ibm.com/servers/eserver/ess/index.wss
- Alert Reporting is via email and/or SNMP trap
- It is assume you have email working from the AIX machine running RTC
  - If not, have fun with sendmail!
- Of course, email includes tablets & smart phones can be alerted as well as your service desk or operators
- Alternatively, have an SNMP server ready

PowerSC Real-Time

Real-Time Compliance Pre-Requisites

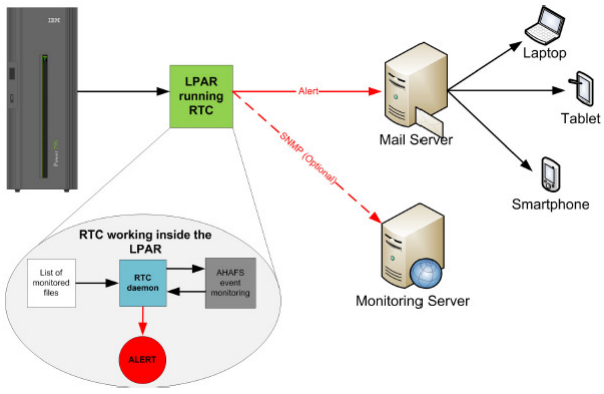
PowerSC Standard Edition files

- ESD_-_PowerSC_Standard_Edition_V1.1_112012.tar.gz
- openpts.verifier
  - 1.0.0.0 Open Platform Trust Services - verifier
- powerscExp.ice
  - 1.1.2.0 ICE Express Security Extension
- powerscExp.license
  - 6.1.6.15 PowerSC Express Edition
- **powerscExp.rtc**
  - **1.1.2.0 Real-Time Compliance**
- powerscStd.license
  - 6.1.8.0 PowerSC Standard Edition
- powerscStd.svm
  - 1.1.2.0 Secure Virtual Machine
- powerscStd.tnc_pm
  - 1.1.2.0 Trusted Network Connect for Patch Management
- powerscStd.vlog
  - 1.1.2.0 Virtual Log Device Software
- powerscStd.vtpm
  - 1.1.2.0 Virtual Trusted Platform Module

PowerSC Real-Time

Real-Time Compliance (RTC)

- Built around a AIX Autonomic Health Advisor File System (AHAFS1)
- As the resource is changed the AIX kernel immediately takes action
- No polling or cron scripts



Real-Time Compliance (RTC)

- Configure with:
  - smitty RTC → set the email user(s), detail level, etc.
  - Or edit **/etc/security/rtc/rtcd.conf**
  - Then: **startsrc -s rtcd**

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

Real-Time Compliance (RTC)

Information Levels:

- Infolevel:1
  - timestamp
  - sequence number
  - event producer return code
  - process info
  - program name
- Infolevel:2 above plus
  - message of the event producer, if applicable
- Infolevel:3 above plus
  - stack of the event, if applicable

Real-Time Compliance (RTC)

PowerSC Real-Time

Config file of pre-defined monitoring is in
/etc/security/rtc/rtcd_policy.conf

/etc/environment:
eventtype = modFile

Valid are modFile, modFileAttr or both

Edit this file then: **stopsrc -s rtcd; startsrc -s rtcd**

- Or use the **chsec** command
  Could be useful to remotely update lots of machines
  Also automatically restarts rtcd

Real-Time Compliance Summary

1. Simple to implement & understand
2. Simple to extend to your own local needs

3. Immediate warning of unusual security changes
4. Need an escalation process to deal with problems

Alice Keating-Withers
IBM Power Systems
Client Technical Specialist

Nigel Griffiths
IBM Power Systems
Advanced Technology Support, Europe