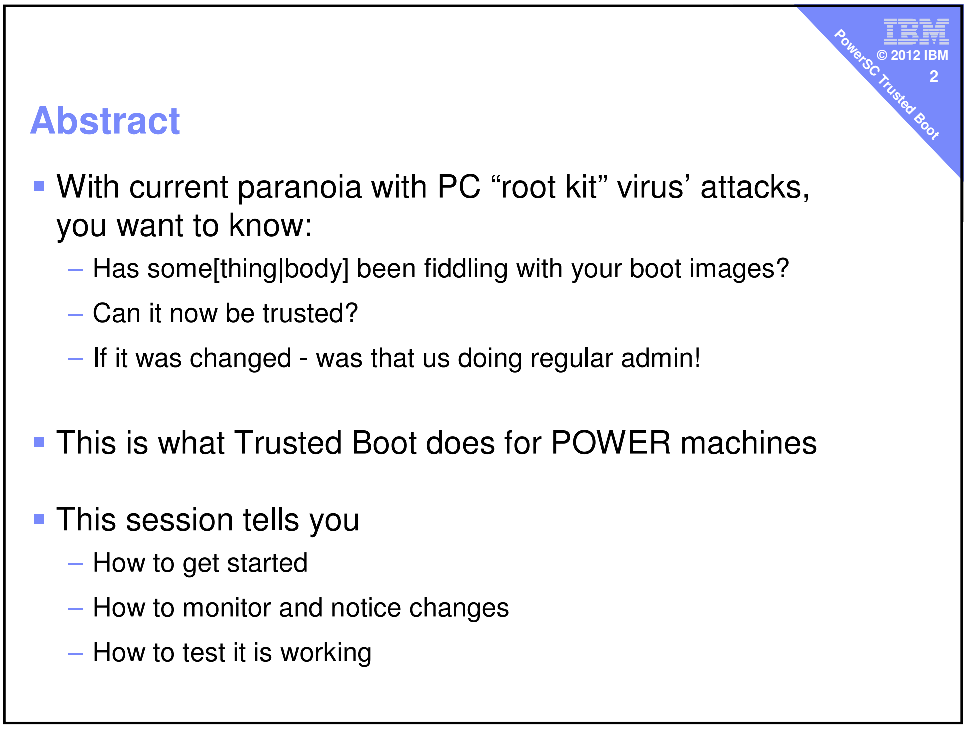
Getting Started PowerSC Trusted Boot

Release 1.1 Nov 2012

Nigel Griffiths
IBM Power Systems
Advanced Technology Support, Europe

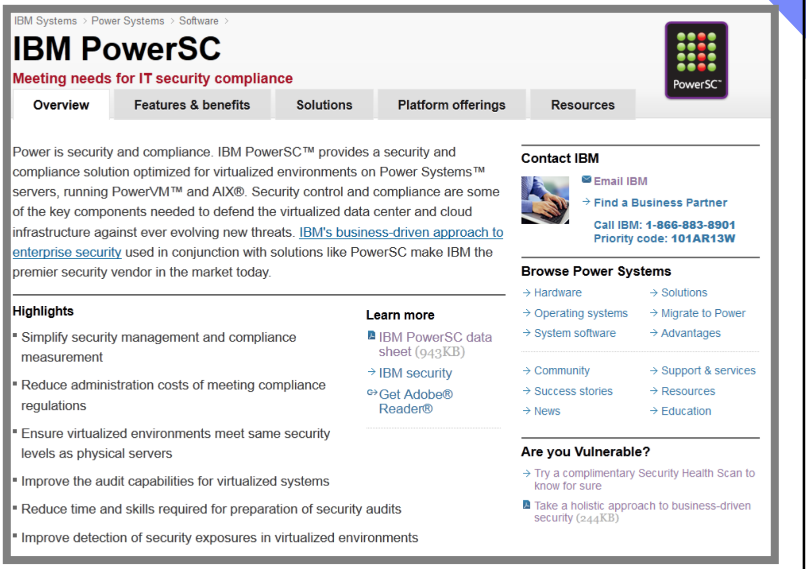
Presentation Version 6



Abstract

- With current paranoia with PC “root kit” virus’ attacks, you want to know:
  - Has some[thing|body] been fiddling with your boot images?
  - Can it now be trusted?
  - If it was changed - was that us doing regular admin!
- This is what Trusted Boot does for POWER machines
- This session tells you
  - How to get started
  - How to monitor and notice changes
  - How to test it is working

10,000 feet overview but no “How To” details
http://www.ibm.com/systems/power/software/security/



IBM Systems > Power Systems > Software >

IBM PowerSC

Meeting needs for IT security compliance

Overview | Features & benefits | Solutions | Platform offerings | Resources

PowerSC

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 measurement
- Reduce administration costs of meeting compliance regulations
- Ensure virtualized environments meet same security levels as physical servers
- Improve the audit capabilities for virtualized systems
- Reduce time and skills required for preparation of security audits
- Improve detection of security exposures in virtualized environments

Learn more

- IBM PowerSC data sheet (943KB)
- IBM security
- Get Adobe® Reader®

Contact IBM

Email IBM
Find a Business Partner
Call IBM: 1-866-883-8901
Priority code: 101AR13W

Browse Power Systems

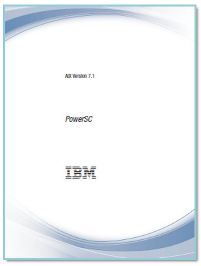
Hardware	Solutions
Operating systems	Migrate to Power
System software	Advantages
Community	Support & services
Success stories	Resources
News	Education

Are you Vulnerable?

- Try a complimentary Security Health Scan to know for sure
- Take a holistic approach to business-driven security (244KB)

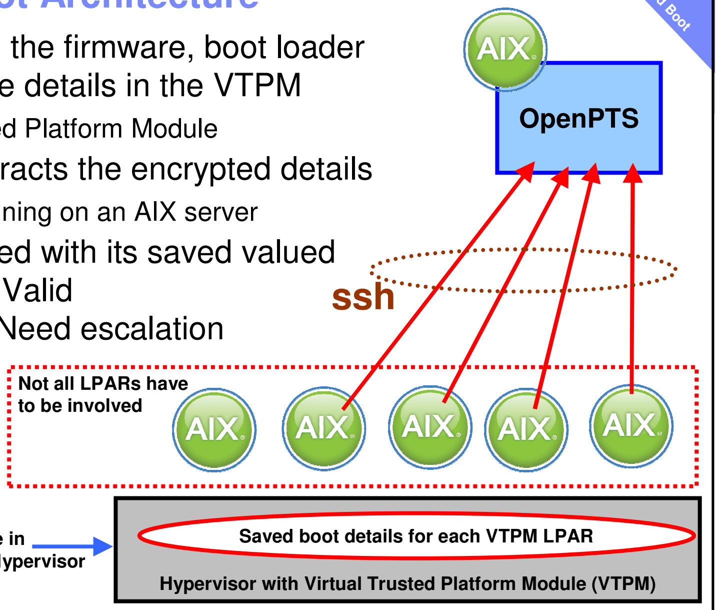
Trusted Boot Pre-Requisites

- POWER7 C model (or later) for firmware 740-xxx
- AIX 6 TL7 or AIX 7 TL1 (and VIOS 2.2.1.4)
  - Sorry: no Linux or IBM i
- PowerSC documentation page 11-16
- http://pic.dhe.ibm.com/infocenter/aix/v6r1/topic/com.ibm.aix.powersc/powersc_pdf.pdf



Trusted Boot Architecture

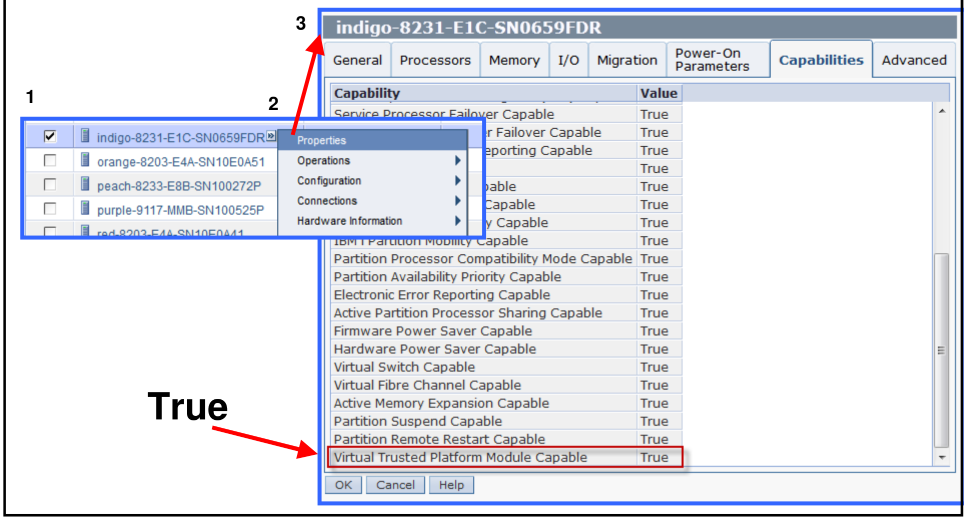
- While booting the firmware, boot loader & AIX we save details in the VTPM
  - Virtual Trusted Platform Module
- OpenPTS extracts the encrypted details
  - Software running on an AIX server
- Then compared with its saved valued
- If the same = Valid
- If different = Need escalation


AIX
OpenPTS
ssh
Not all LPARs have to be involved
AIX
AIX
AIX
AIX
AIX
Saved boot details for each VTPM LPAR
Hypervisor with Virtual Trusted Platform Module (VTPM)

Low level resource in system firmware/Hypervisor

Check you are capable?

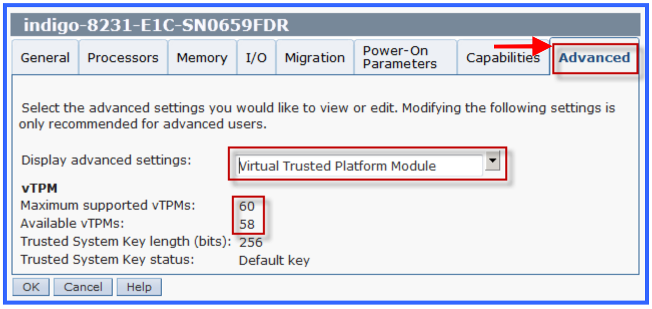
- On the HMC, select the machine then Properties



Capability	Value
Service Processor Failover Capable	True
r Failover Capable	True
eporting Capable	True
	True
able	True
Capable	True
y Capable	True
IBM i Partition Mobility Capable	True
Partition Processor Compatibility Mode Capable	True
Partition Availability Priority Capable	True
Electronic Error Reporting Capable	True
Active Partition Processor Sharing Capable	True
Firmware Power Saver Capable	True
Hardware Power Saver Capable	True
Virtual Switch Capable	True
Virtual Fibre Channel Capable	True
Active Memory Expansion Capable	True
Partition Suspend Capable	True
Partition Remote Restart Capable	True
Virtual Trusted Platform Module Capable	True

Check you are capable?

- Can also check Advanced panel



indigo-8231-E1C-SN0659FDR

Select the advanced settings you would like to view or edit. Modifying the following settings is only recommended for advanced users.

Display advanced settings: Virtual Trusted Platform Module

vTPM

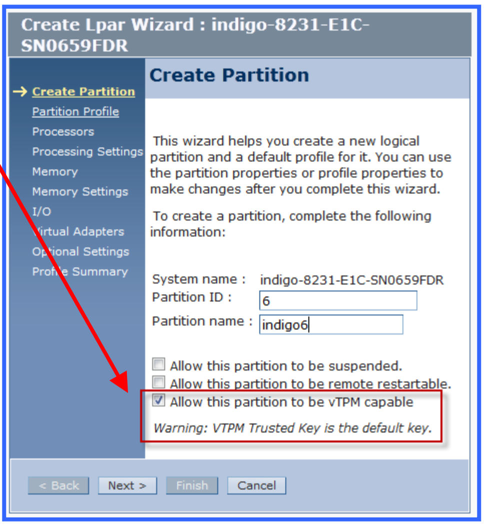
Maximum supported vTPMs:	60
Available vTPMs:	58
Trusted System Key length (bits):	256
Trusted System Key status:	Default key

- Note: Current maximum of 60 LPARs per machine

When creating a New LPARs

- Make sure you click this new option

- Allow this partition to be VTPM capable



Create Lpar Wizard : indigo-8231-E1C-SN0659FDR

Create Partition

This wizard helps you create a new logical partition and a default profile for it. You can use the partition properties or profile properties to make changes after you complete this wizard.

To create a partition, complete the following information:

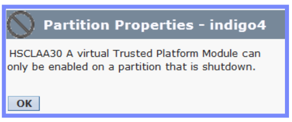
System name : indigo-8231-E1C-SN0659FDR
Partition ID : 6
Partition name : indigo6

□ Allow this partition to be suspended.
□ Allow this partition to be remote restartable.
☑ Allow this partition to be vTPM capable

Warning: VTPM Trusted Key is the default key.

Older LPAR need this attribute added

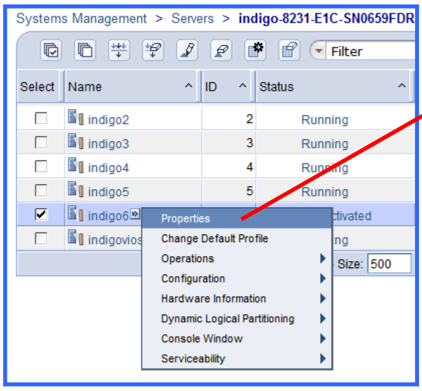
- Shutdown the LPAR or you get →



Partition Properties - indigo4

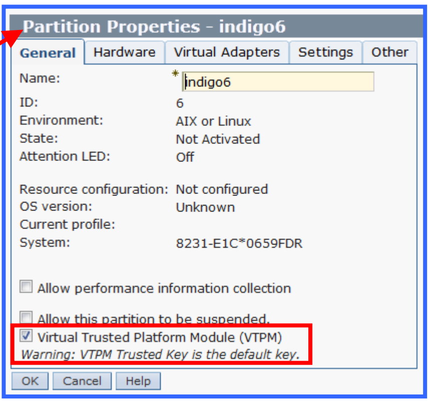
HSCLAA30 A virtual Trusted Platform Module can only be enabled on a partition that is shutdown.

- Then switch on VTPM



Systems Management > Servers > **indigo-8231-E1C-SN0659FDR**

Select	Name	ID	Status
□	indigo2	2	Running
□	indigo3	3	Running
□	indigo4	4	Running
□	indigo5	5	Running
☑	indigo6		ctivated
□	indigovios		ng



Partition Properties - indigo6

Name: * indigo6
ID: 6
Environment: AIX or Linux
State: Not Activated
Attention LED: Off

Resource configuration: Not configured
OS version: Unknown
Current profile:
System: 8231-E1C*0659FDR

□ Allow performance information collection

□ Allow this partition to be suspended.

☑ Virtual Trusted Platform Module (VTPM)

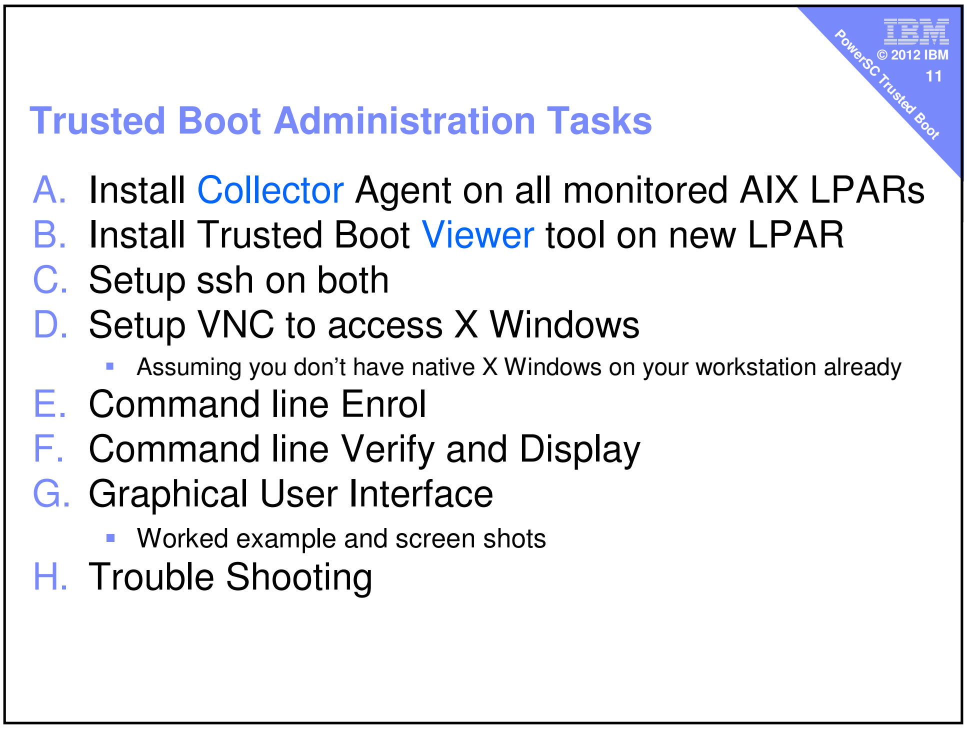
Warning: VTPM Trusted Key is the default key.

- and restart the LPAR

The VTPM monitoring software

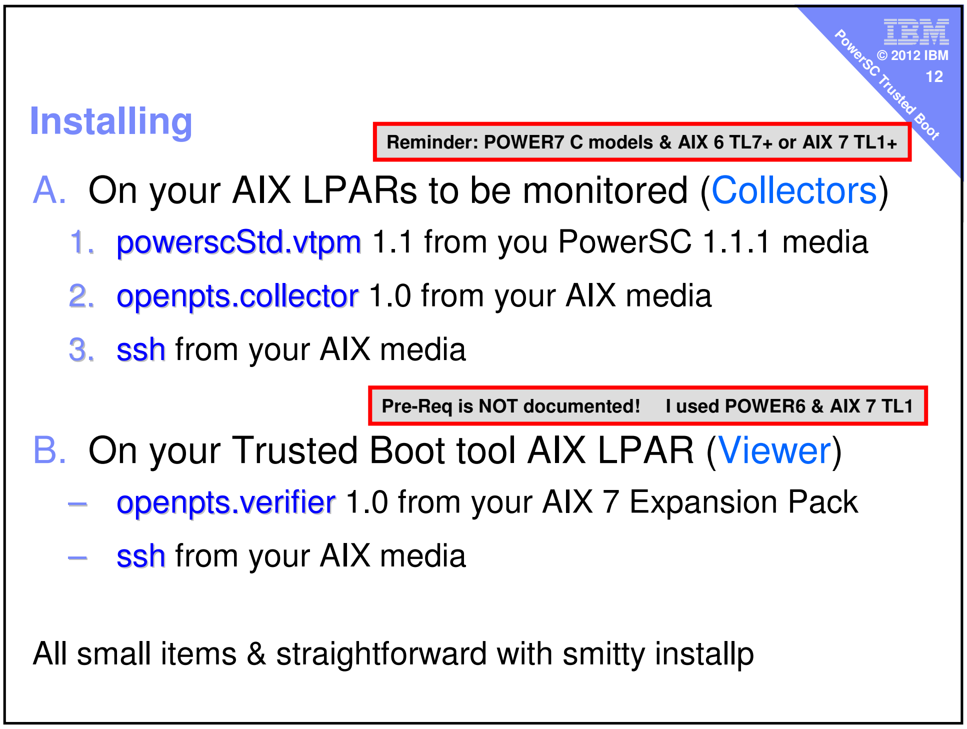
- Trusted Boot tool runs on an AIX LPAR
  - Used to test the boot status image remotely via ssh
  - Runs the OpenPTS software 😮
- OpenPTS briefly:
  - OpenPTS → Open Platform Trusted Services
  - Open Source package from SourceForge
  - Supplied/compiled by IBM for running on AIX
    - You could download and/or compile for another platform like Linux but no IBM support
  - Mostly the "openpts" command
  - Optional: Graphical user program via X Windows

[I recommended the GUI by using VNC]



Trusted Boot Administration Tasks

A. Install Collector Agent on all monitored AIX LPARs
B. Install Trusted Boot Viewer tool on new LPAR
C. Setup ssh on both
D. Setup VNC to access X Windows
   - Assuming you don't have native X Windows on your workstation already
E. Command line Enrol
F. Command line Verify and Display
G. Graphical User Interface
   - Worked example and screen shots
H. Trouble Shooting



Installing

Reminder: POWER7 C models & AIX 6 TL7+ or AIX 7 TL1+

A. On your AIX LPARs to be monitored (Collectors)
   1. powerscStd.vtpm 1.1 from you PowerSC 1.1.1 media
   2. openpts.collector 1.0 from your AIX media
   3. ssh from your AIX media

Pre-Req is NOT documented!   I used POWER6 & AIX 7 TL1

B. On your Trusted Boot tool AIX LPAR (Viewer)
   – openpts.verifier 1.0 from your AIX 7 Expansion Pack
   – ssh from your AIX media

All small items & straightforward with smitty installp

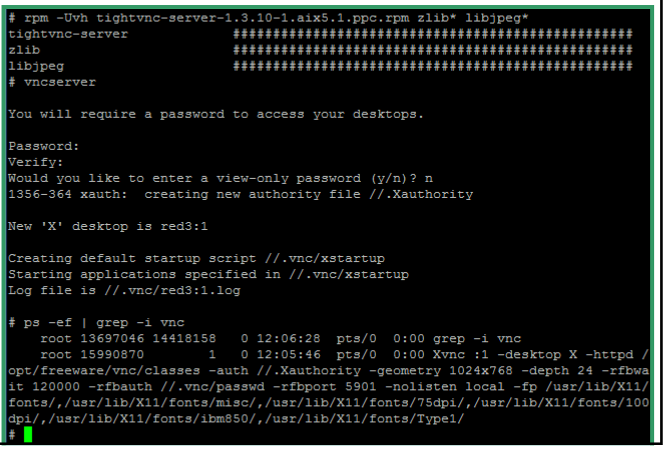
C) Setup of ssh – it is a security tool !

- OpenPTS needs to regularly fetch the saved boot images details, so lets make it easy with ssh
- On the Trusted Boot tool AIX LPAR (as root)
  - ssh-keygen # No passphrase
  - Then copy ~/.ssh/id_rsa.pub
  - To /tmp on each collector LPAR
- On all the monitored AIX LPARs (as root)
  - mkdir ~/.ssh → in case it does not exist
  - cat /tmp/id_rsa.pub >> ~/.ssh/authorized_keys

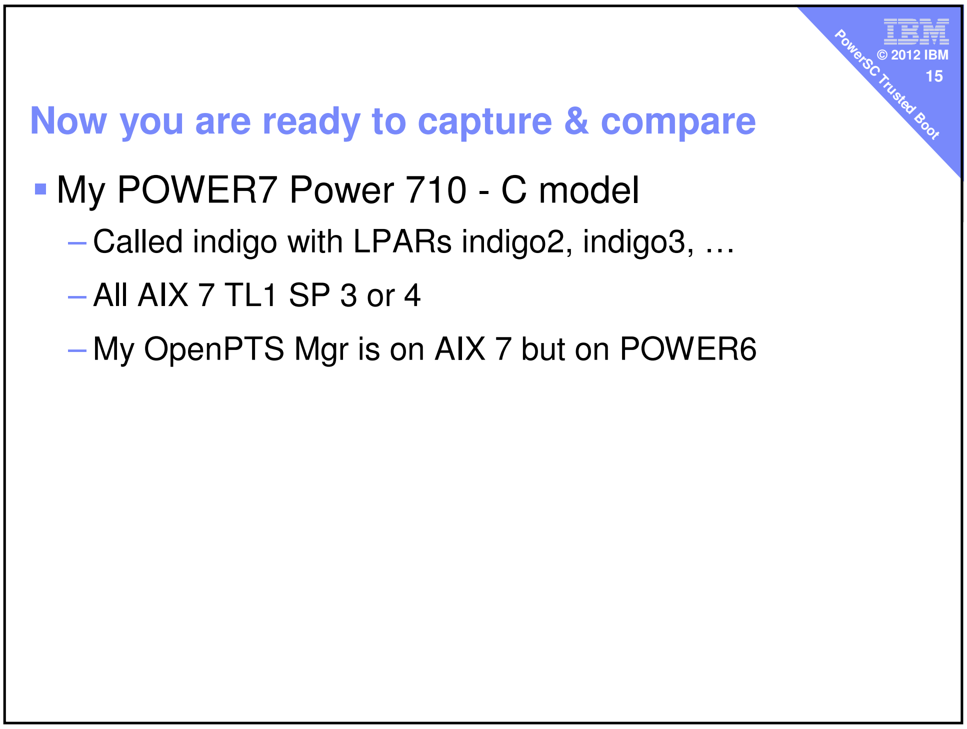
D) If you want the GUI you need X Windows

You will have to decide if/how to access X Windows

- I decided to install VNCserver from perzl.org + pre-reqs
- Then UltraVNC viewer on Windows 7

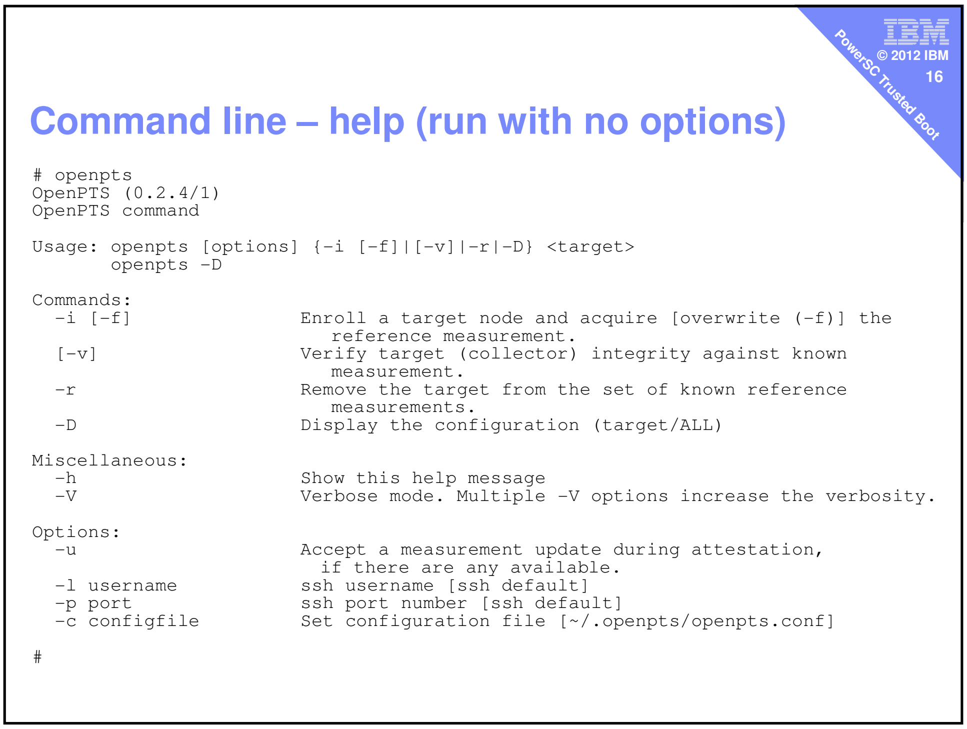


```
# rpm -Uvh tightvnc-server-1.3.10-1.aix5.1.ppc.rpm zlib* libjpeg*
tightvnc-server             ##################################################
zlib                        ##################################################
libjpeg                     ##################################################
# vncserver

You will require a password to access your desktops.

Password:
Verify:
Would you like to enter a view-only password (y/n)? n
1356-364 xauth:  creating new authority file //.Xauthority

New 'X' desktop is red3:1

Creating default startup script //.vnc/xstartup
Starting applications specified in //.vnc/xstartup
Log file is //.vnc/red3:1.log

# ps -ef | grep -i vnc
    root 13697046 14418158   0 12:06:28  pts/0  0:00 grep -i vnc
    root 15990870        1   0 12:05:46  pts/0  0:00 Xvnc :1 -desktop X -httpd /
opt/freeware/vnc/classes -auth //.Xauthority -geometry 1024x768 -depth 24 -rfbwa
it 120000 -rfbauth //.vnc/passwd -rfbport 5901 -nolisten local -fp /usr/lib/X11/
fonts/,/usr/lib/X11/fonts/misc/,/usr/lib/X11/fonts/75dpi/,/usr/lib/X11/fonts/100
dpi/,/usr/lib/X11/fonts/ibm850/,/usr/lib/X11/fonts/Type1/
# 
```



Now you are ready to capture & compare

- My POWER7 Power 710 - C model
  - Called indigo with LPARs indigo2, indigo3, …
  - All AIX 7 TL1 SP 3 or 4
  - My OpenPTS Mgr is on AIX 7 but on POWER6



Command line – help (run with no options)

```
# openpts
OpenPTS (0.2.4/1)
OpenPTS command

Usage: openpts [options] {-i [-f]|[-v]|-r|-D} <target>
       openpts -D

Commands:
  -i [-f]                  Enroll a target node and acquire [overwrite (-f)] the
                              reference measurement.
  [-v]                     Verify target (collector) integrity against known
                              measurement.
  -r                       Remove the target from the set of known reference
                              measurements.
  -D                       Display the configuration (target/ALL)

Miscellaneous:
  -h                       Show this help message
  -V                       Verbose mode. Multiple -V options increase the verbosity.

Options:
  -u                       Accept a measurement update during attestation,
                             if there are any available.
  -l username              ssh username [ssh default]
  -p port                  ssh port number [ssh default]
  -c configfile            Set configuration file [~/.openpts/openpts.conf]

#
```

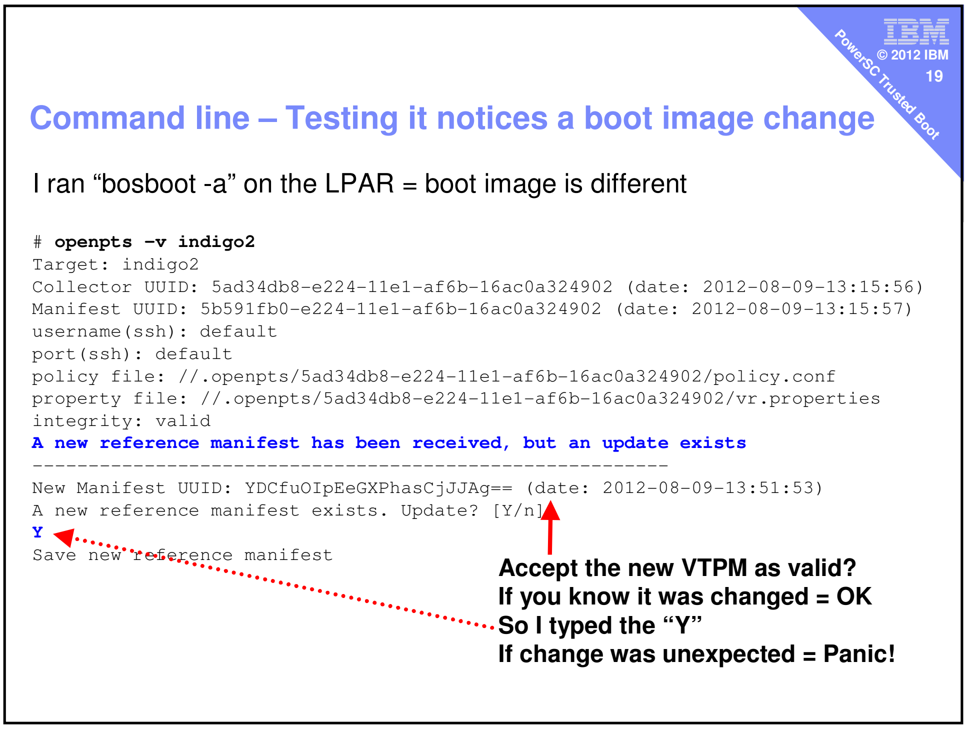
E) Command line – Enrol
Capture 1st VTPD - assumes currently safe

```
# openpts -i indigo2
# openpts -i indigo3
```

If ssh is not right,
it starts asking for passwords

F) Command line – Verify
= check current VTPD is the same as the saved one

```
# openpts -v indigo2
Target: indigo2
Collector UUID: 5ad34db8-e224-11e1-af6b-16ac0a324902 (date: 2012-08-09-13:15:56)
Manifest UUID: 5b591fb0-e224-11e1-af6b-16ac0a324902 (date: 2012-08-09-13:15:57)
username(ssh): default
port(ssh): default
policy file: //.openpts/5ad34db8-e224-11e1-af6b-16ac0a324902/policy.conf
property file: //.openpts/5ad34db8-e224-11e1-af6b-16ac0a324902/vr.properties
integrity: valid
--------------------------------------------------
```

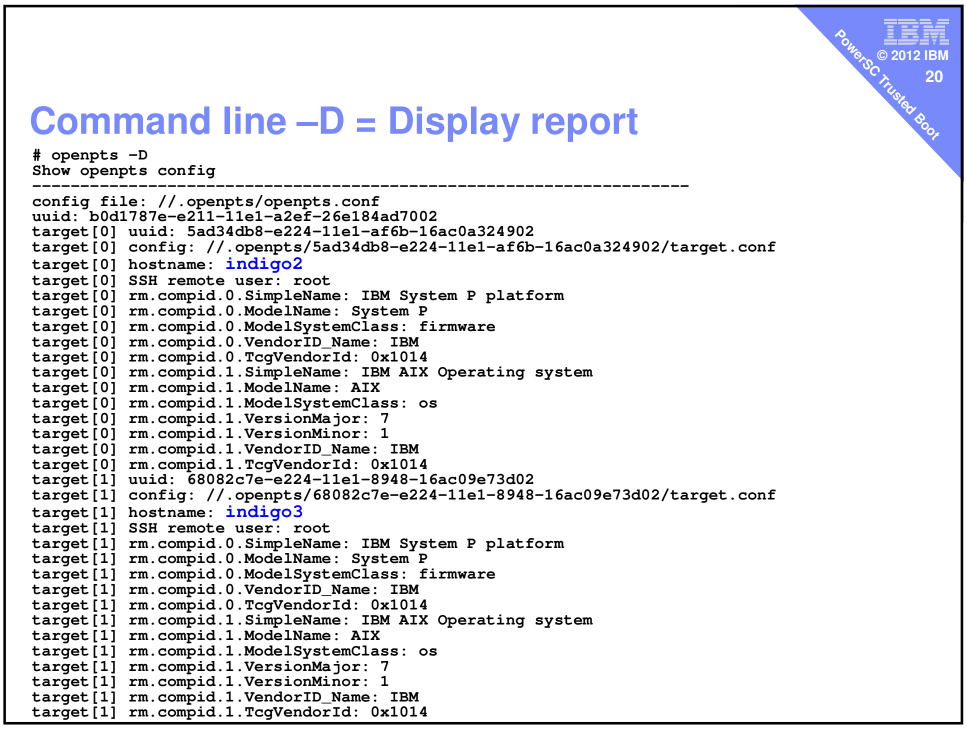


Command line – Testing it notices a boot image change

I ran “bosboot -a” on the LPAR = boot image is different

```
# openpts -v indigo2
Target: indigo2
Collector UUID: 5ad34db8-e224-11e1-af6b-16ac0a324902 (date: 2012-08-09-13:15:56)
Manifest UUID: 5b591fb0-e224-11e1-af6b-16ac0a324902 (date: 2012-08-09-13:15:57)
username(ssh): default
port(ssh): default
policy file: //.openpts/5ad34db8-e224-11e1-af6b-16ac0a324902/policy.conf
property file: //.openpts/5ad34db8-e224-11e1-af6b-16ac0a324902/vr.properties
integrity: valid
A new reference manifest has been received, but an update exists
---------------------------------------------------------------------
New Manifest UUID: YDCfuOIpEeGXPhasCjJJAg== (date: 2012-08-09-13:51:53)
A new reference manifest exists. Update? [Y/n]
Y
Save new reference manifest
```

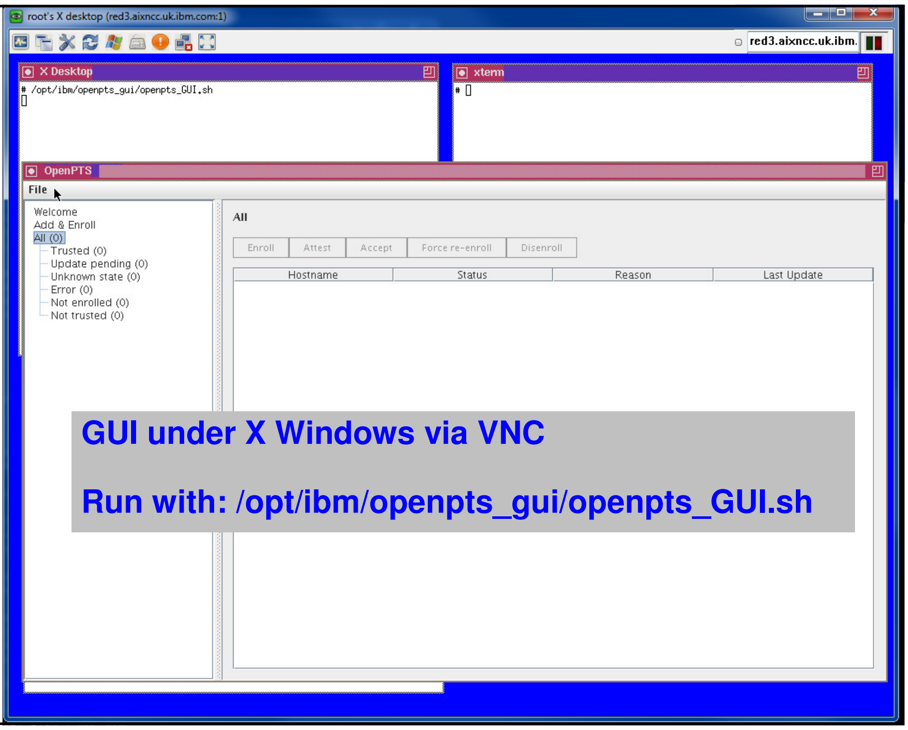
Accept the new VTPM as valid?
If you know it was changed = OK
So I typed the “Y”
If change was unexpected = Panic!



Command line –D = Display report

```
# openpts -D
Show openpts config
---------------------------------------------------------------------
config file: //.openpts/openpts.conf
uuid: b0d1787e-e211-11e1-a2ef-26e184ad7002
target[0] uuid: 5ad34db8-e224-11e1-af6b-16ac0a324902
target[0] config: //.openpts/5ad34db8-e224-11e1-af6b-16ac0a324902/target.conf
target[0] hostname: indigo2
target[0] SSH remote user: root
target[0] rm.compid.0.SimpleName: IBM System P platform
target[0] rm.compid.0.ModelName: System P
target[0] rm.compid.0.ModelSystemClass: firmware
target[0] rm.compid.0.VendorID_Name: IBM
target[0] rm.compid.0.TcgVendorId: 0x1014
target[0] rm.compid.1.SimpleName: IBM AIX Operating system
target[0] rm.compid.1.ModelName: AIX
target[0] rm.compid.1.ModelSystemClass: os
target[0] rm.compid.1.VersionMajor: 7
target[0] rm.compid.1.VersionMinor: 1
target[0] rm.compid.1.VendorID_Name: IBM
target[0] rm.compid.1.TcgVendorId: 0x1014
target[1] uuid: 68082c7e-e224-11e1-8948-16ac09e73d02
target[1] config: //.openpts/68082c7e-e224-11e1-8948-16ac09e73d02/target.conf
target[1] hostname: indigo3
target[1] SSH remote user: root
target[1] rm.compid.0.SimpleName: IBM System P platform
target[1] rm.compid.0.ModelName: System P
target[1] rm.compid.0.ModelSystemClass: firmware
target[1] rm.compid.0.VendorID_Name: IBM
target[1] rm.compid.0.TcgVendorId: 0x1014
target[1] rm.compid.1.SimpleName: IBM AIX Operating system
target[1] rm.compid.1.ModelName: AIX
target[1] rm.compid.1.ModelSystemClass: os
target[1] rm.compid.1.VersionMajor: 7
target[1] rm.compid.1.VersionMinor: 1
target[1] rm.compid.1.VendorID_Name: IBM
target[1] rm.compid.1.TcgVendorId: 0x1014
```

G) There is also a GUI which is easier to use



```
# /opt/ibm/openpts_gui/openpts_GUI.sh
```

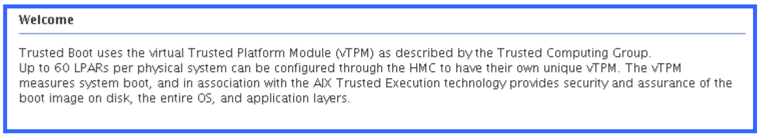
```
# 
```

GUI under X Windows via VNC

Run with: /opt/ibm/openpts_gui/openpts_GUI.sh

First Use …

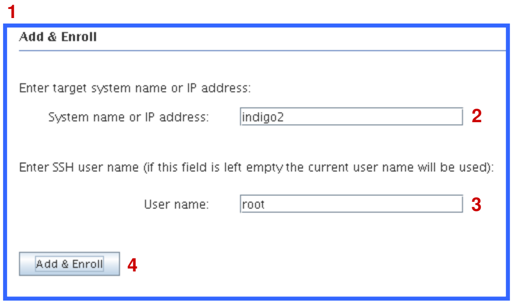
- Welcome information



Welcome

Trusted Boot uses the virtual Trusted Platform Module (vTPM) as described by the Trusted Computing Group. Up to 60 LPARs per physical system can be configured through the HMC to have their own unique vTPM. The vTPM measures system boot, and in association with the AIX Trusted Execution technology provides security and assurance of the boot image on disk, the entire OS, and application layers.

- Add & Enrol



1

Add & Enroll

Enter target system name or IP address:

System name or IP address: indigo2 2

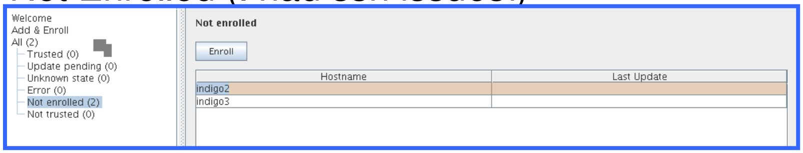
Enter SSH user name (if this field is left empty the current user name will be used):

User name: root 3

4

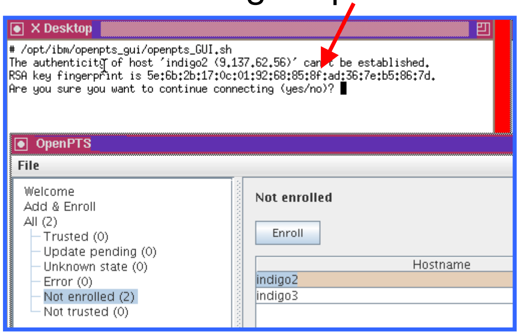
Added two hosts but not looking good

- List Not Enrolled (I had ssh issues!)



Hostname	Last Update
indigo2	
indigo3	

- And ssh was asking for passwords – Ugh!

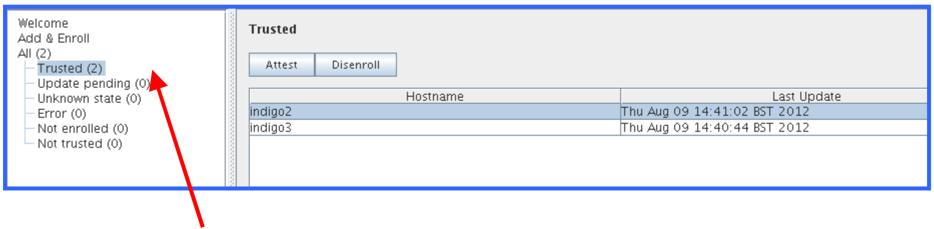


```
# /opt/ibm/openpts_gui/openpts_GUI.sh
The authenticity of host 'indigo2 (9.137.62.56)' can't be established.
RSA key fingerprint is 5e:6b:2b:17:0c:01:92:68:85:8f:ad:36:7e:b5:86:7d.
Are you sure you want to continue connecting (yes/no)?
```

Hostname
indigo2
indigo3

Fixed ssh – “much better”

- Once I fixed ssh and hit “Enrol” it looked better



Welcome
Add & Enroll
All (2)
Trusted (2)
Update pending (0)
Unknown state (0)
Error (0)
Not enrolled (0)
Not trusted (0)

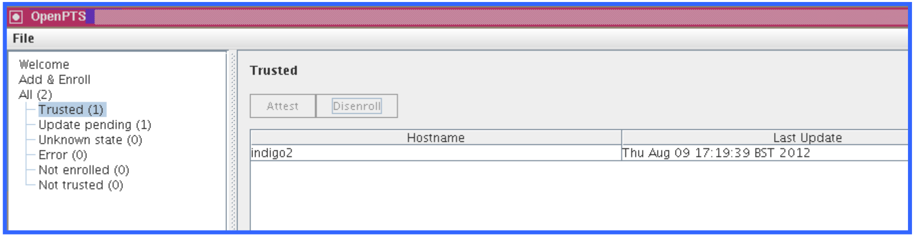
Trusted

Hostname	Last Update
indigo2	Thu Aug 09 14:41:02 BST 2012
indigo3	Thu Aug 09 14:40:44 BST 2012

List of Trusted hosts = Good

Modified a boot image → it is noticed

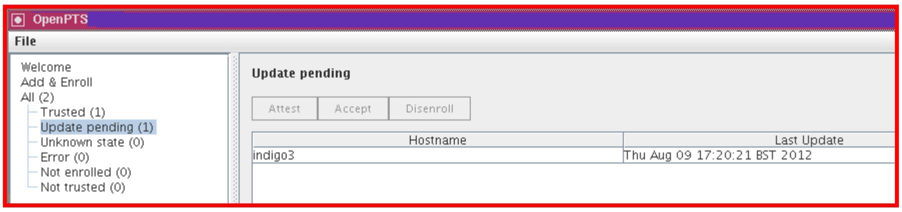
- Ran bosboot on one LPAR – Can you tell which?



Welcome
Add & Enroll
All (2)
Trusted (1)
Update pending (1)
Unknown state (0)
Error (0)
Not enrolled (0)
Not trusted (0)

Trusted

Hostname	Last Update
indigo2	Thu Aug 09 17:19:39 BST 2012



Welcome
Add & Enroll
All (2)
Trusted (1)
Update pending (1)
Unknown state (0)
Error (0)
Not enrolled (0)
Not trusted (0)

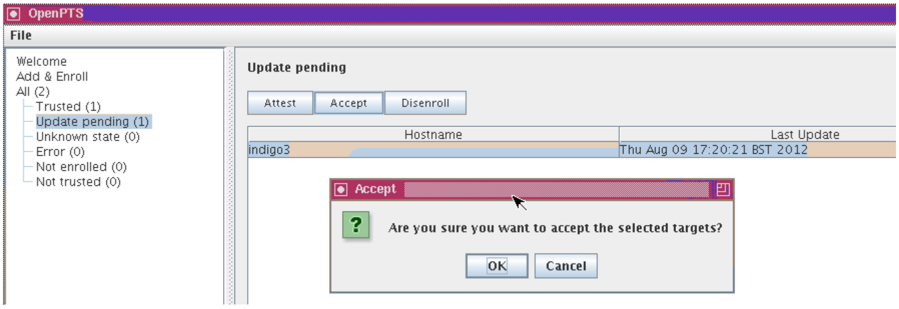
Update pending

Hostname	Last Update
indigo3	Thu Aug 09 17:20:21 BST 2012

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

Was the updated expected?

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

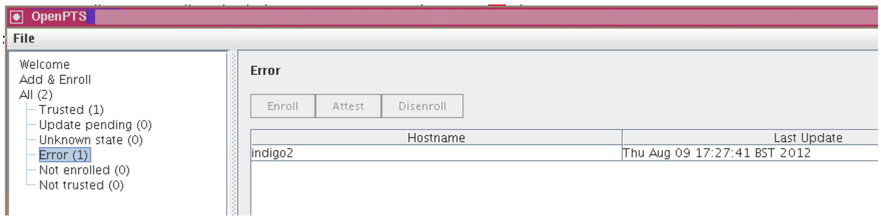


Hostname	Last Update
indigo3	Thu Aug 09 17:20:21 BST 2012

Are you sure you want to accept the selected targets?

What if we can’t reach the host?

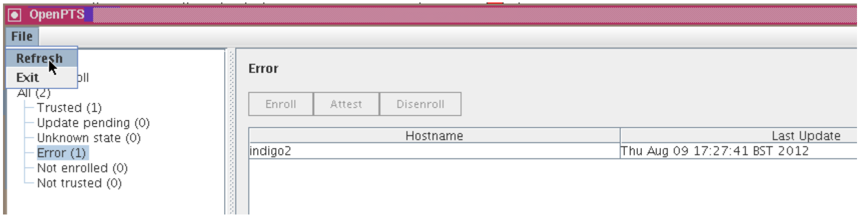
- One LPAR: ifconfig en0 down → off the network
- ssh fails after about a minute



Hostname	Last Update
indigo2	Thu Aug 09 17:27:41 BST 2012

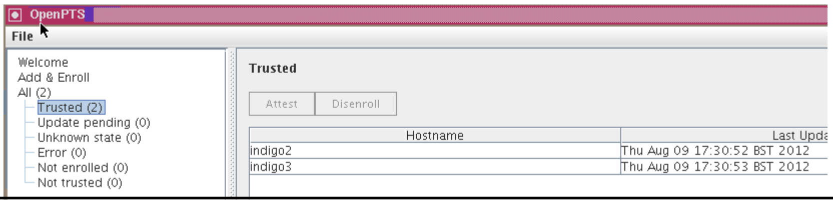
What if we fix the network?

- Same LPAR: ifconfig en0 up
- Then Refresh ← **GOOD OPTION**



Hostname	Last Update
indigo2	Thu Aug 09 17:27:41 BST 2012

- All OK again



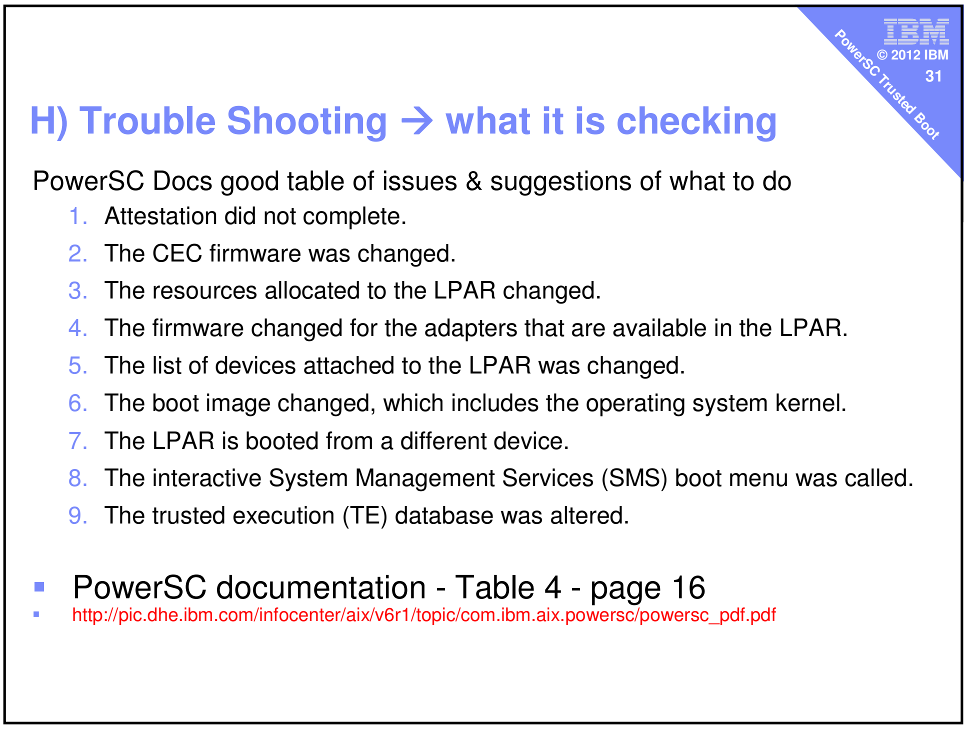
Hostname	Last Upda
indigo2	Thu Aug 09 17:30:52 BST 2012
indigo3	Thu Aug 09 17:30:53 BST 2012

Command line has no GUI Refresh function

- GUI Refresh runs openpts cmd for each host
- So a simple script could be used

```
for i in `openpts -D | grep hostname | awk '{print $3 }'`
do
  echo n | openpts -v $i | grep -v UUID | grep -v file: | grep -v ssh
done

Target: indigo2
integrity: valid
----------------------------------------------------------
Target: indigo3
integrity: valid
A new reference manifest has been received, but an update exists
----------------------------------------------------------
Keep current manifest
…
```

- "echo n" is used to answer the Yes/No question about accepting LPAR changes

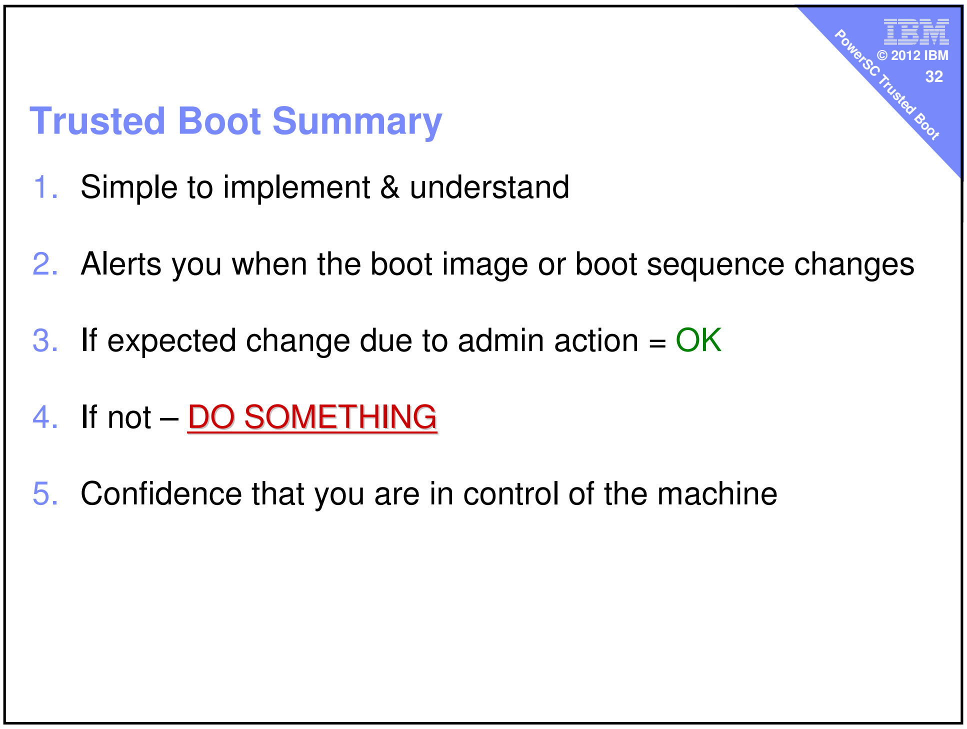


H) Trouble Shooting → what it is checking

PowerSC Docs good table of issues & suggestions of what to do

1. Attestation did not complete.
2. The CEC firmware was changed.
3. The resources allocated to the LPAR changed.
4. The firmware changed for the adapters that are available in the LPAR.
5. The list of devices attached to the LPAR was changed.
6. The boot image changed, which includes the operating system kernel.
7. The LPAR is booted from a different device.
8. The interactive System Management Services (SMS) boot menu was called.
9. The trusted execution (TE) database was altered.

- PowerSC documentation - Table 4 - page 16
- http://pic.dhe.ibm.com/infocenter/aix/v6r1/topic/com.ibm.aix.powersc/powersc_pdf.pdf



Trusted Boot Summary

1. Simple to implement & understand
2. Alerts you when the boot image or boot sequence changes
3. If expected change due to admin action = OK
4. If not – DO SOMETHING
5. Confidence that you are in control of the machine