MANEWS Issue Number 20

the Mainframe Audit News

This newsletter tells you stuff you need to know to audit IBM mainframe computers runinng with z/OS and the MVS operating system. This issue we show you how to understand important hardware linkages that affect your audit.

Table of Contents

1) How to Learn LPARs, Sysplexes, Shared DASD

To lay the foundation for any mainframe audit, you need to understand the various hardware pieces and how they fit together. This is part of "Get familiar with the environment" and a critical step to ensuring that your audit is complete. The connections between hardware pieces can provide pathways that weaken or bypass security altogether. You need to verify that this is not the case, or else address it in your audit.

Mainframe systems can be connected in ways that let information which is protected by one set of file access controls become exposed through a different set of file access controls (for example through a different security software database for RACF, ACF2, or TopSecret).

To take a quick example, imagine a data center with two CPUs, each running z/OS with MVS, one labeled PRODUCTION and the other labeled TEST. Suppose that you are auditing security over the datasets of an important production financial application. If you confine your audit to just the PRODUCTION CPU, you might miss the fact that disk drives containing sensitive datasets for the application are shared between the two CPUs, and that the programmers in the TEST environment are able to read and write production datasets on these disk drives. This can be possible if the PRODUCTION and TEST CPUs each have a different database of rules for RACF, ACF2, or TopSecret.

The way to address this in your audit is to understand the hardware pieces and how they are connected and shared. This task has become more complicated in recent years, but the tools to collect the information are available now.

To understand how this works with the current technology, you need to know about new connections, including LPARs and sysplexes. Here's a brief rundown of some terms you need to know for any mainframe audit:

CPU or **CPC** (Central Processing Unit or Central Processor Complex) the part of the hardware that does arithmetic, comparison, branching, and logic

LPAR (Logical Partition) a "virtual CPU" or the logical splitting of a CPU into two or more "pretend" CPUs, each of which can run its own copy of the MVS operating system. If you are familiar with VMware, you'll understand that VMware uses software to create virtual machines, while LPARs do the same in the hardware. It is common for a CPU to be split into a TEST LPAR and a PRODUCTION LPAR.

SYSPLEX a collection of CPUs connected by fiber optic cables, often with immense data storage boxes called coupling facilities between the CPUs. This hardware arrangement can be used to provide automatic mirroring of databases across CPUs.

DASD (Direct Access Storage Device) a fancy name for a disk drive, also called a disk pack, (like the hard drive on your laptop, but very much bigger)

Shared DASD a disk drive that is shared between two or more CPUs or LPARs, often between the TEST and PRODUCTION CPUs

All of these connections are defined in files or datasets called the **IODF**s (or Input Output Definition Files), and administered by a tool called the **HCD** (or Hardware Configuration Definition).

You can now see that a sensitive file could be stored on a DASD shared between the TEST and PRODUCTION CPUs. If each of these CPUs used a different security software database, you would not know everyone who could access the file unless you checked both security software databases.

A similar risk could occur if a financial database (perhaps DB2) is mirrored across a sysplex, with the hardware automatically reflecting changes in each copy of the database onto the other copy. If the two copies of the database lived on CPUs with different security software databases, you would have to look at both sets of security software rules to perform a complete audit.

So how do you learn about LPARs, Syplexes, Shared DASD, and related connections? There are three ways:

1. Ask the system programmers and assume that they are knowledgable and forth-coming.
2. Learn to read the IODF files, and then read them
3. Get a tool to map the hardware for you.

To make it easy, we have chosen the third option to show you, by means of the StepOne tool from New Era. Thanks to New Era for permission to show samples of the StepOne reports. (The folks at New Era are unusually technically competent and unusually willing to share their knowledge. You can learn more about them and StepOne at their website www.newera.com.)

On the next page is a sample report, showing you the CPCs in a data center and the number of LPARs in each. (Paul Robichaux of New Era has kindly added call-outs with white backgrounds as a guide.)

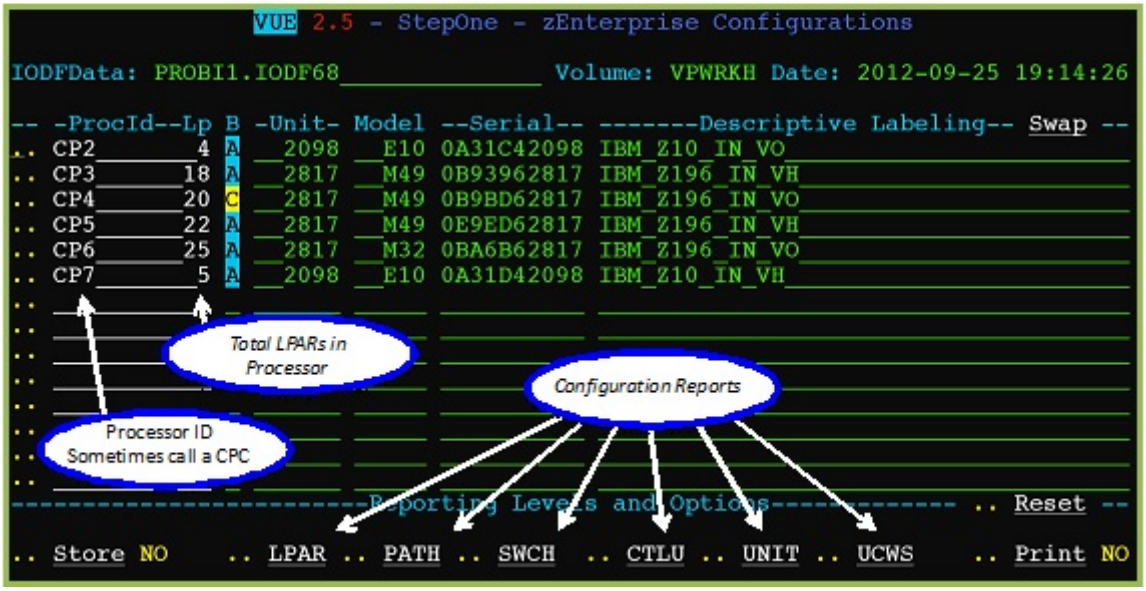
MANEWS Issue Number 20

the Mainframe Audit News

NewEra Software

z/OS Integrity and Compliance

zEnterprise Management – StepOne – Processor (CPC) Identification!



The call-out labeled “Processor ID” point you to the list of CPCs, while the call-out labeled “Total LPARS..” shows you how many LPARs are contained in each CPC.

The call-out labeled “Configuration Reports” points you to where you would click to obtain more detailed reports. The next page shows you one of these, listing for one CPC, the LPARs defined in it, and the connections to each. The **Chpids** (pointed to by the “Active Elements” call-out on the next page) are channel path identifiers, listing channel paths or connections between an LPAR and various devices.

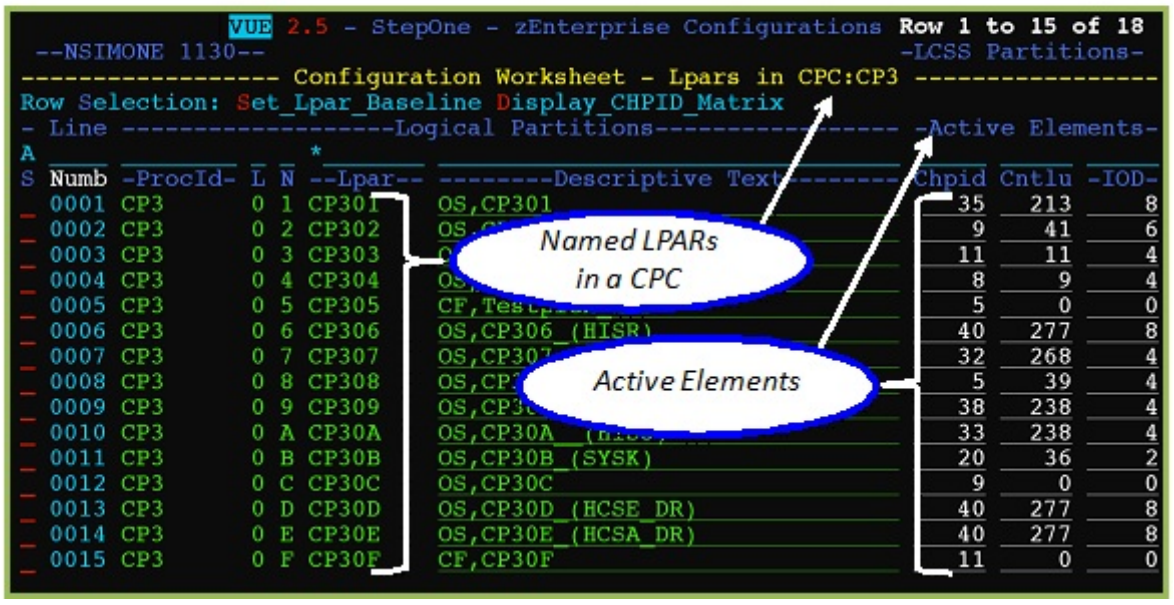
MANEWS Issue Number 20

the Mainframe Audit News

NewEra Software

z/OS Integrity and Compliance

zEnterprise Management – StepOne – Active Elements in a CPC

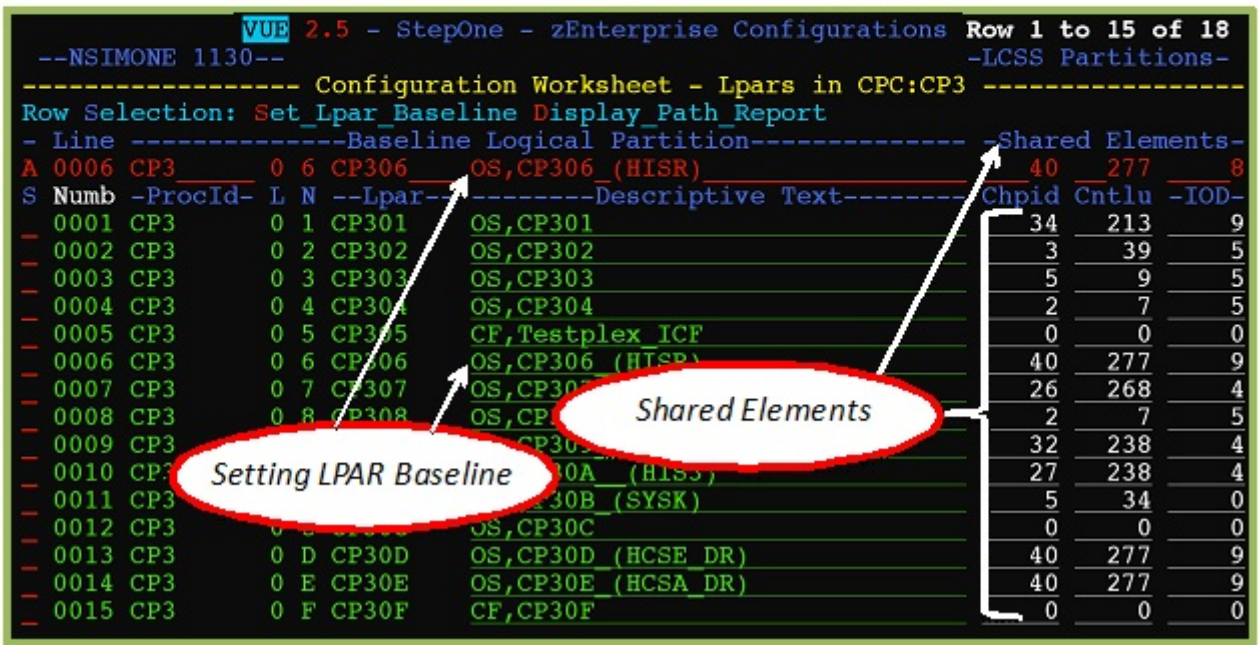


I bet you would like to see which Chpids are shared with other LPARs. The report on the next page shows you.

NewEra Software

z/OS Integrity and Compliance

zEnterprise Management – StepOne – Shared Elements with a CPC



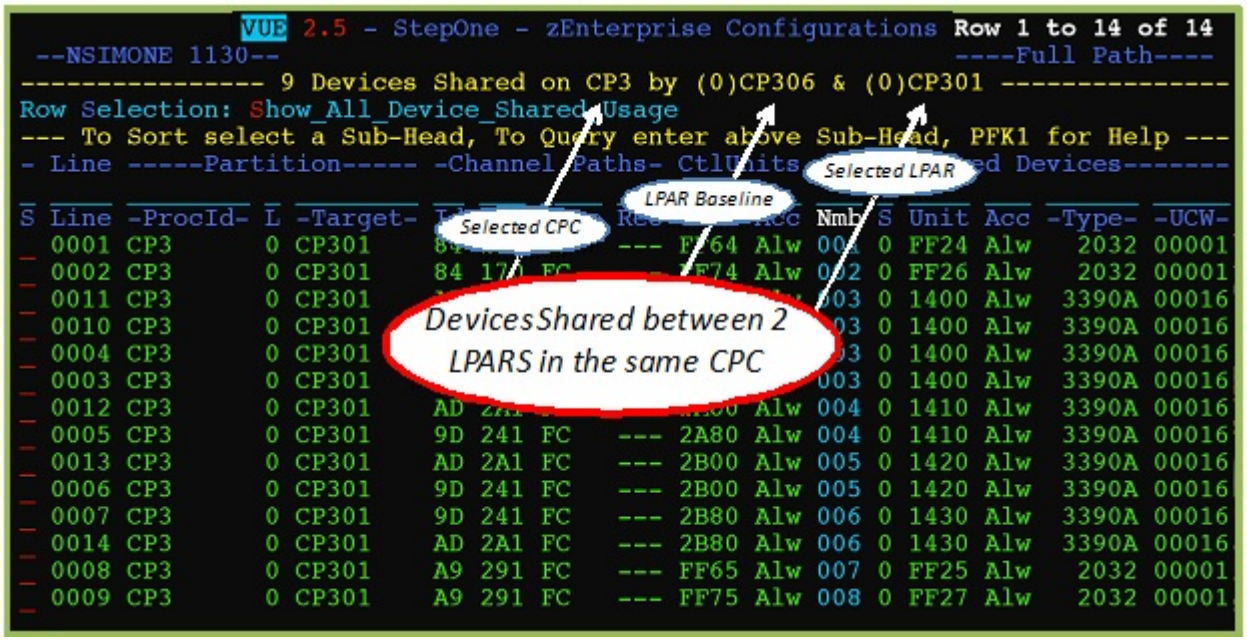
This report shows for one CPC named CP3, one line for each LPAR defined in it. Each line shows on the right the number of Shared Elements or Chpids connected to that LPAR. I bet you'd like to know what those shared elements are. See the next page to find out.

MANEWS Issue Number 20
the Mainframe Audit News

NewEra Software

z/OS Integrity and Compliance

zEnterprise Management – StepOne – Shared I/O Devices LPAR Vs. LPAR!



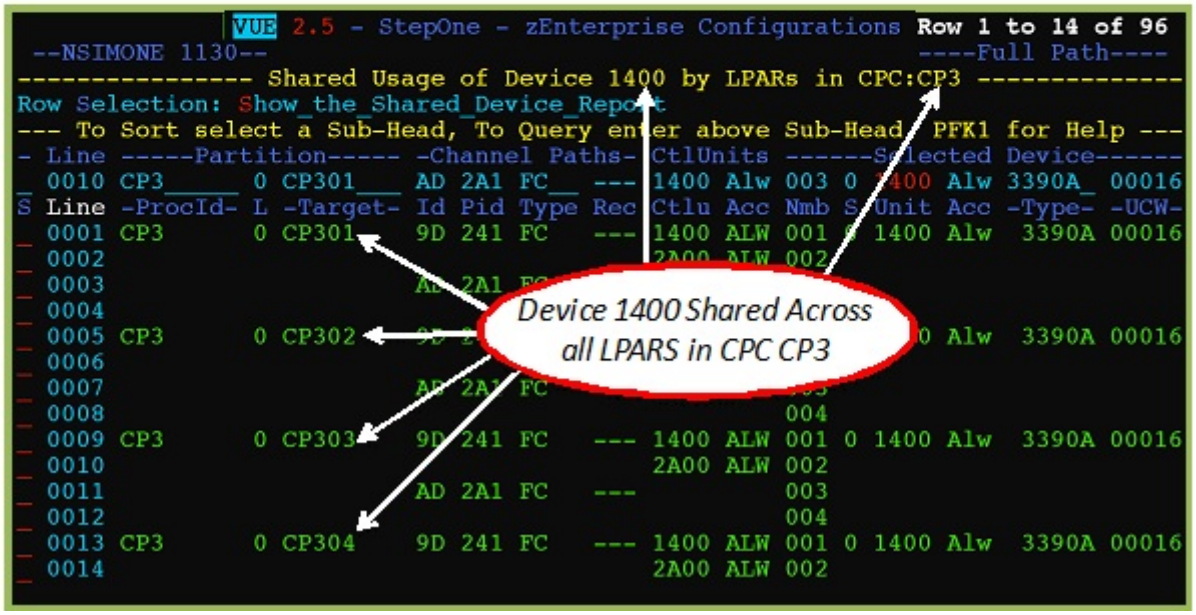
This report still shows us just one CPC named CP3. We have asked StepOne to tell us how many shared devices (such as disk drives) are connected between the LPAR named CP306 and the LPAR named CP301. Each line describes one such device. The next to right-most column tells the device type: 3390A is a model of disk drive. The 2032 is a fiber optic connector.

But perhaps you'd like to approach it from the other angle, and ask for a specified device, which LPARs in CP3 share it. See the next page.

NewEra Software

z/OS Integrity and Compliance

zEnterprise Management – StepOne – Shared I/O Devices across multiple CHPIDS!



This report is still looking just at the CPC named CP3. We have asked StepOne to list all the LPARs in CP3 which are sharing device 1400. It turns out that all of the LPARs in CP3 share this device. The next to right-most column (3390A) tells us that this device is a disk drive.

A good next audit step would be to find out whether all these LPARs share the same security software database or whether they have separate ones which will need to be reviewed.

Thanks to Paul Robichaux Jerry Seefeldt, and NewEra for sharing these reports. You can learn more by contacting them at www.newera.com. Or (408) 520-7101.

==========
==========

2) What About Printers?

So now that we've learned about Shared DASD, what about protecting printers? For example, imagine that you are auditing a major financial institution which has a printer connected to its mainframe. The printer does nothing but print checks on pre-signed check stock all day long, in a locked room. On the back end of the printer is a machine that slices the checks, stuffs them into window envelopes with postal permits, and seals the envelopes. Every once in a while someone comes into the room, turns on the lights, adds new check stock to the input bin, and hauls the sealed envelopes off to the post office. (We hope he turns off the lights and locks the door behind him.)

Do we need to control whether a rogue programmer could create a printout in the correct format and route it to this printer, causing unauthorized checks to be mailed to his brother-in-law? Yes, but we control this with the security software, not with hardware controls. With RACF, ACF2, or TopSecret, there is a resource class called WRITER which is used to control who can send printouts to which printers. You will want to review the rules in this class, as well as the procedures for keeping the room locked and the check stock protected.

==========
==========

3) New Blog for IS Audit

There is a new blog available with more practical suggestions to improve IS audits on all types of computer. You can see it at
http://www.stuhenderson.com/isauditblog/

==========
==========

4. RACF and PCI Audits

We heard from a friend who was being audited for PCI compliance in a mainframe datacenter using RACF for security software. The auditor claimed that the data center was not in compliance with PCI regulations, since RACF uses DES for encryption, and the auditor believed DES to be "easily crackable". (ACF2 and TopSecret can be implemented with either DES or AES encryption.)

It was finally noted that the auditor was missing the point. Yes, RACF uses DES to encrypt, but only to encrypt its passwords. RACF does not provide encryption support for anything other than the passwords in the RACF database. If you want to encrypt credit card information, RACF is not the tool to use. (Nor is ACF2 or TopSecret, for the same reasons. Encryption of data at rest or on the fly can be provided by hardware or by software, but not by the security software.

RACF passwords are considered sufficiently encrypted with DES. You can learn more about why by reading page four of this issue of the *"RACF User News".* http://www.stuhenderson.com/RUGNEW80.pdf

==========
==========

5. Learn How to Improve IS Audit Support of Financial Audits

Stu Henderson is conducting a study of what works and what doesn't work for integration of IS audits and financial. If you would like to take part in a ten to fifteen minute phone interview to share your thoughts and experiences, contact him at stu@stuhenderson.com. Indicate best times for him to call you, and the best phone number. Your name and organization will not appear in the final report unless you authorize it in writing. All participants will received a copy of the final report, which will have recommendations on how to improve this integration..

==========
==========

6) Seminar Information and Miscellanea

6A) >>>>Seminar Information

Henderson Group seminars are available for in-house as well as public sessions.

The Henderson Group offers these "How to Audit..." courses :

- How to Audit **z/OS with MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (**New**: March 25-28, 2012 in Chicago, and May 7-10, 2013 in Raleigh, NC)
- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (April 8-10, 2013 in Bethesda, MD), a logical follow-on to the previous course
- How to Audit **TCP/IP Security** (May 29, 2013 in Bethesda, MD) **(NEW)**
- How to Audit **UNIX and Windows Security** (September 9-12, 2013 in Bethesda, MD) **(NEW)**

To learn more about them, please go to

http://www.stuhenderson.com/XAUDTTXT.HTM

6B >>>>This Issue's Proverb of the Day

"*Tell me and I'll forget; show me and I may remember; involve me and I'll understand. - Chinese Proverb*"

6C) >>>>Useful Information

Here's a source of free, practical information on mainframe security and auditing, from a variety of sources. Topics include:

- Glossary of Mainframe Terms
- How to Get z/OS Basic Skills and IBM z/OS Manuals in pdf Format
- Integrity Statements from CA Technologies and IBM
- z/OS Configuration Info: Documents, Audit Guides from NewEra
- Back Issues of z/Journal Magazine and Mainframe Executive Magazine
- IBM Presentation Handouts on Security and RACF from SHARE and GSE
- Free Articles on Mainframe Security and Auditing

Here's the link: http://www.stuhenderson.com/XINFOTXT.HTM

6D) >>>>About the Mainframe Audit News; How to Subscribe/Unsubscribe

The MA News is a free, email, newsletter for auditors who need (or suspect that they will need) to be auditing IBM mainframe systems (primarily **MVS**, **z/OS**, and the system software associated with them). This software includes: **CICS**, **DB2**, **JES**, **VTAM**, **MQSeries**, **TSO**, **USS** (UNIX System Services), **TCP/IP**, and others. It also includes the **httpd daemon** software which connects a mainframe to the Internet. (Note, we expand each of these acronyms and explain how the software works in past and future issues.)

The MA News is meant for auditors who are new to IBM mainframes, as well as for experienced MVS auditors who want to keep up to date with the latest developments from IBM. We will not make the list of subscribers available to anyone else for any reason.

To Subscribe or Unsubscribe

Click on http://www.stuhenderson.com/subscribe.html
and follow the easy directions there.