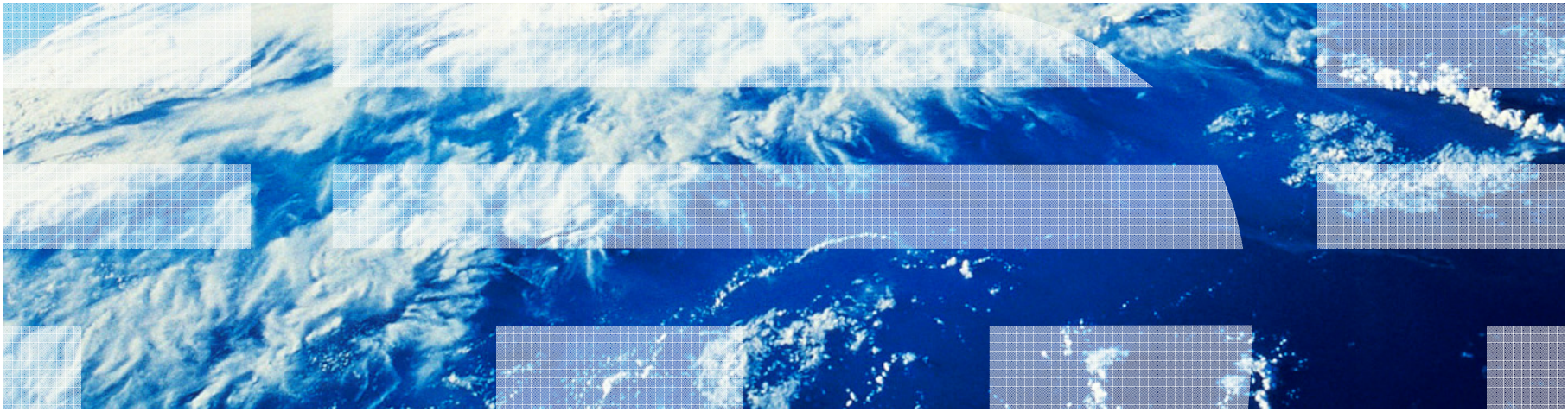
Jamie Pease, CISA, CISSP
IT Specialist, System z Security, IBM Software Group

IBM Tivoli zSecure Suite

What is new in zSecure 1.11



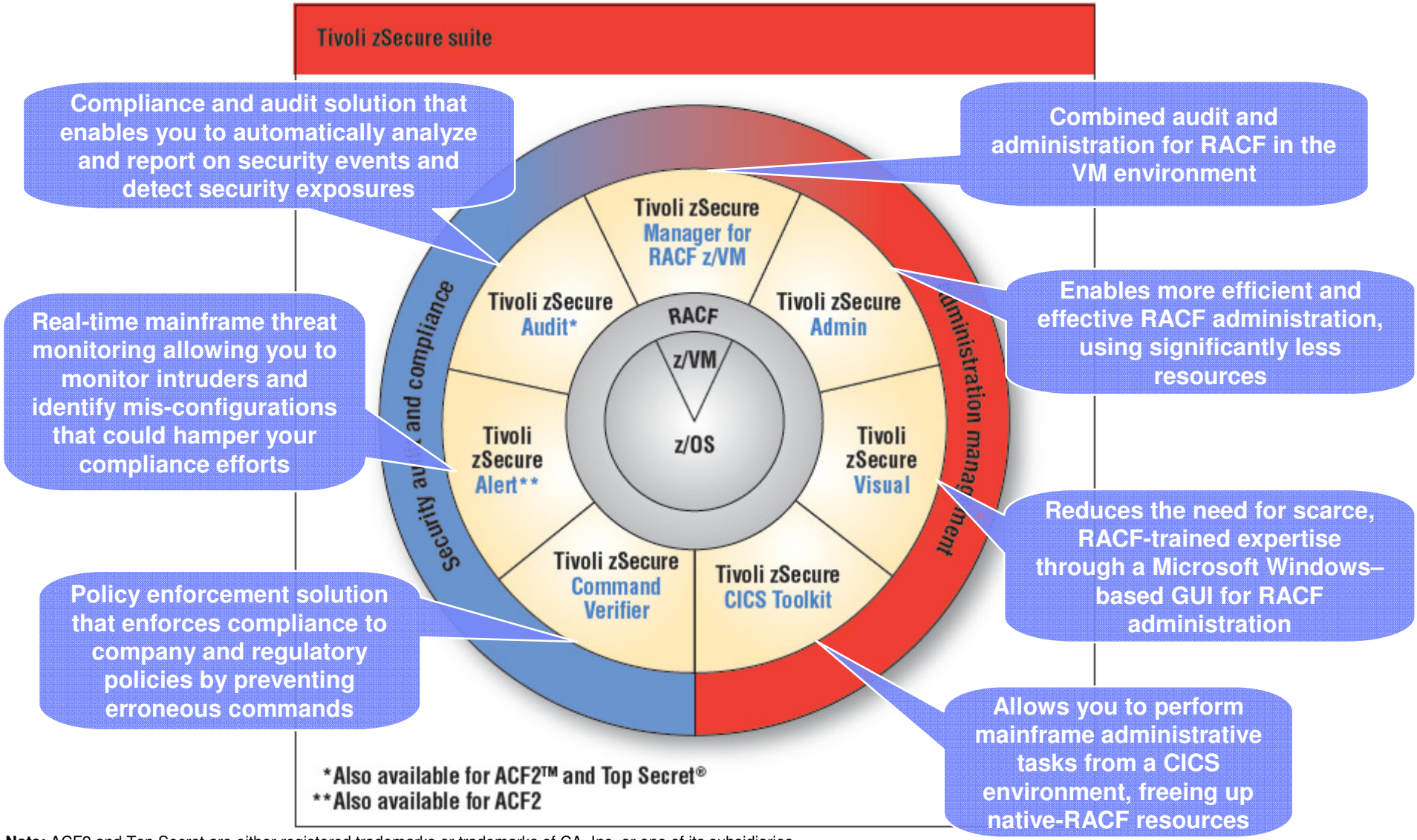
© 2010 IBM Corporation

Agenda

- Announcement November 3rd, 2009
  - z/OS, RACF, ACF2, TSS functions only
  - zSecure Manager for RACF/zVM still at 1.8.1 level
- New functions
- Availability and support
- Suggestions for enhancements
- Useful resources
- Education
- Q&A

© 2010 IBM Corporation

IBM Tivoli zSecure Suite



Note: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

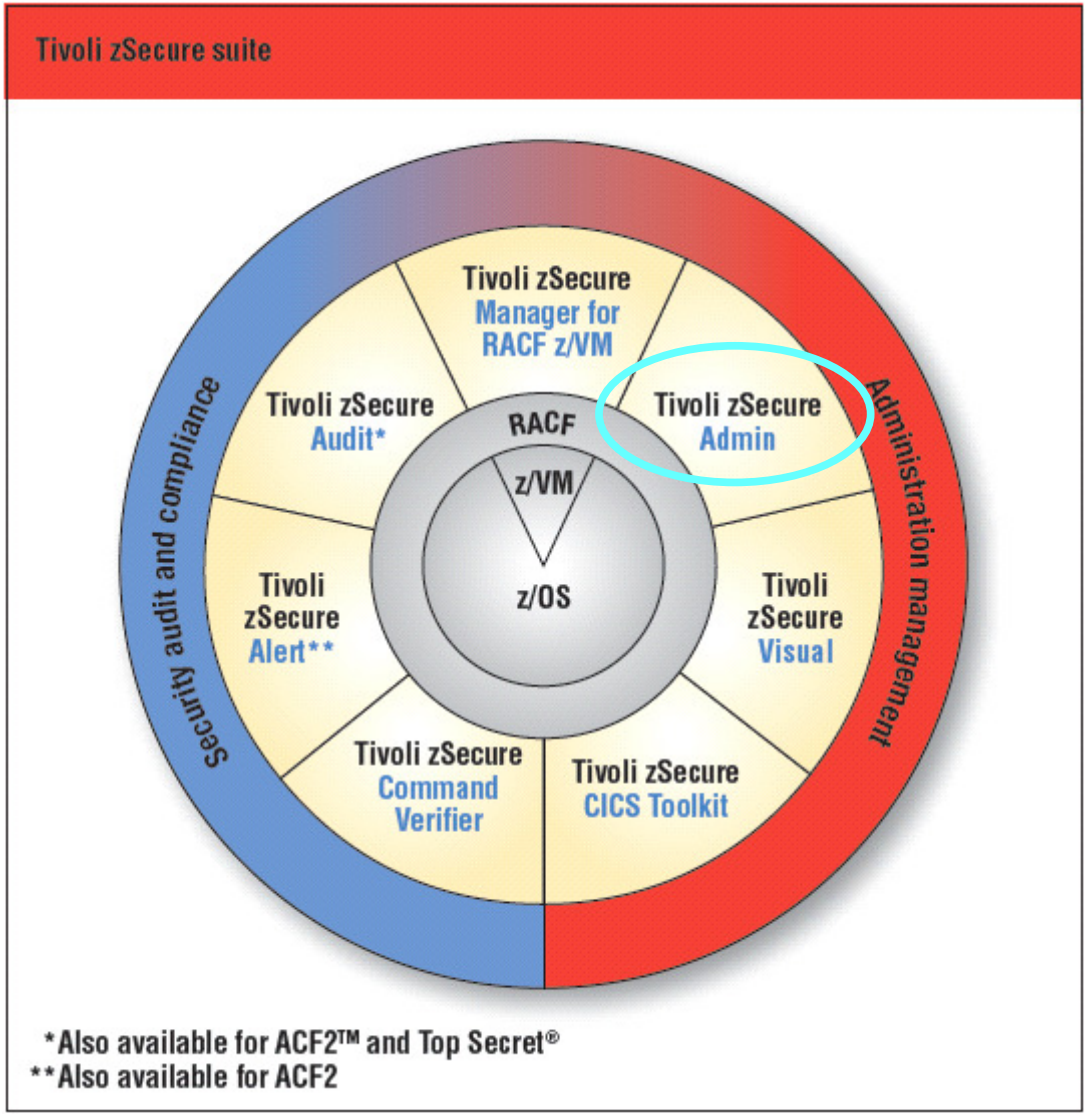
© 2010 IBM Corporation

zSecure 1.11 new functions and features

- New functions
  - Access Monitor for RACF
  - Finding RACF profiles with values in segment fields
  - TCPIP stack configuration
  - Support and Reporting of SMF records extended
  - Extended monitoring
  - z/OS and ACF2 currency
  - Globalization
  - and more

© 2010 IBM Corporation

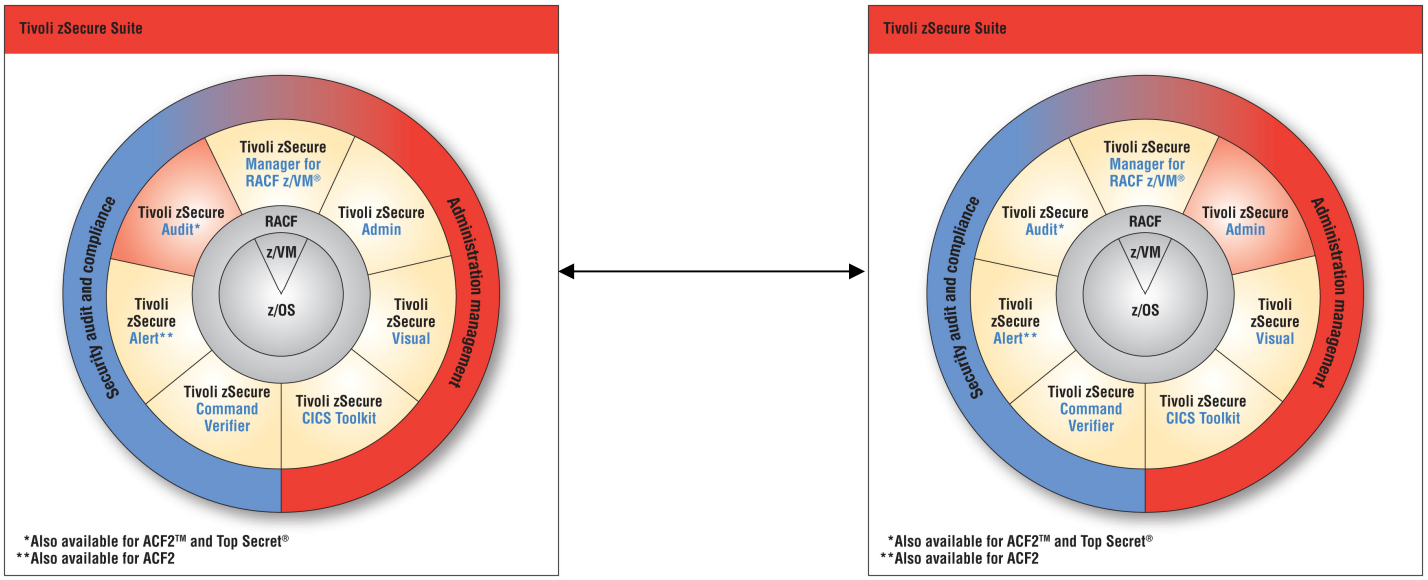
Access Monitor for RACF



© 2010 IBM Corporation

RACF database cleanup: Conventional methods

- SMF reporting of successful access
  - Typically **not** logged to SMF
  - Huge volume of data
  - How to correlate with RACF profiles?
- RACF profile analysis
  - How to see if a PERMIT is still used?
    - Access count works for discrete, but not generic profiles
  - Lastuse date for users
  - Obsolete permits (group or user no longer in RACF)



© 2010 IBM Corporation

zSecure Admin: Access Monitor for RACF

- New functionality in zSecure Admin version 1.11
  - Runs as started task C2PACMON
- Collects information about RACF decisions
  - Date, time, userid, class, resource, profile, intent, RACF decision, flags
  - Saved into an *Access Monitor* file
- Consolidates into daily, monthly, yearly summaries
  - One line per unique set of value
    - Same userid, class, resource, profile, etc
    - Date and time of most recent event, count of events
  - Size is manageable because of consolidation

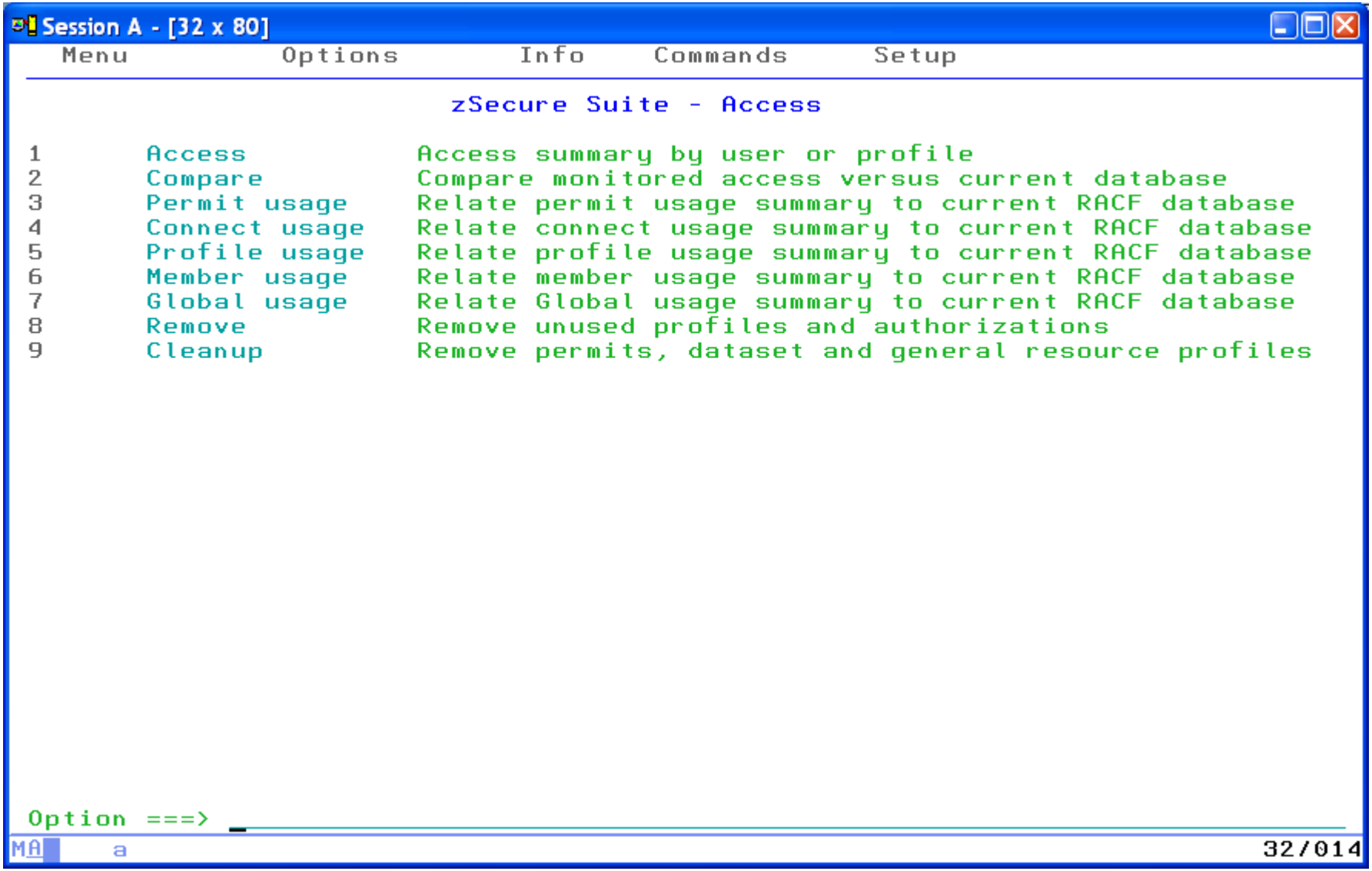
© 2010 IBM Corporation

Analysis of Access Monitor files

- New menu option in zSecure Admin
  - AM - Access Monitor
    - Analyzes Access Monitor file(s)
  - Which resources has a specific user accessed
    - In last month, in last year?
    - When was last access?
  - Who has accessed a given resource?

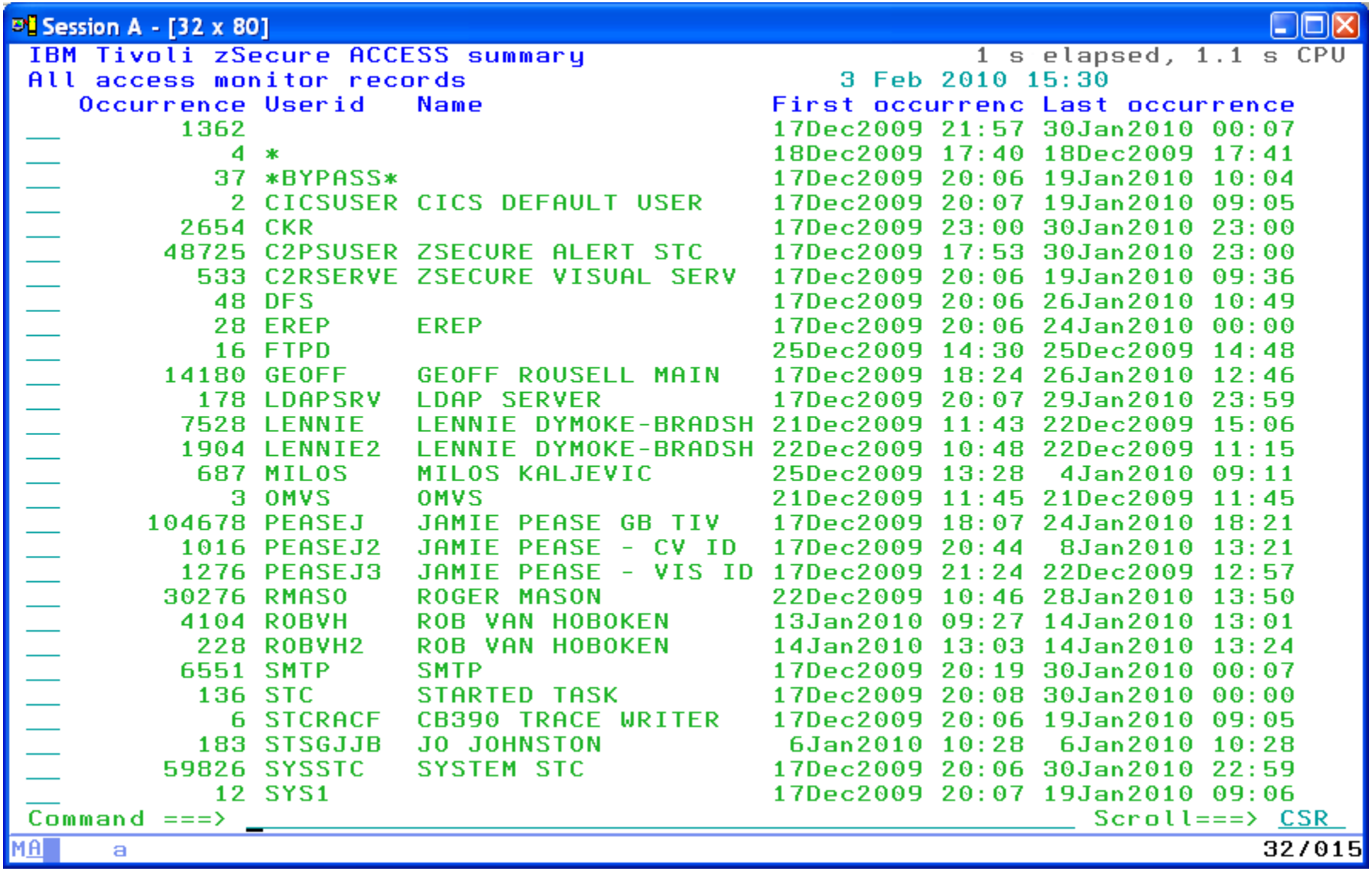
© 2010 IBM Corporation

Access Analysis menu



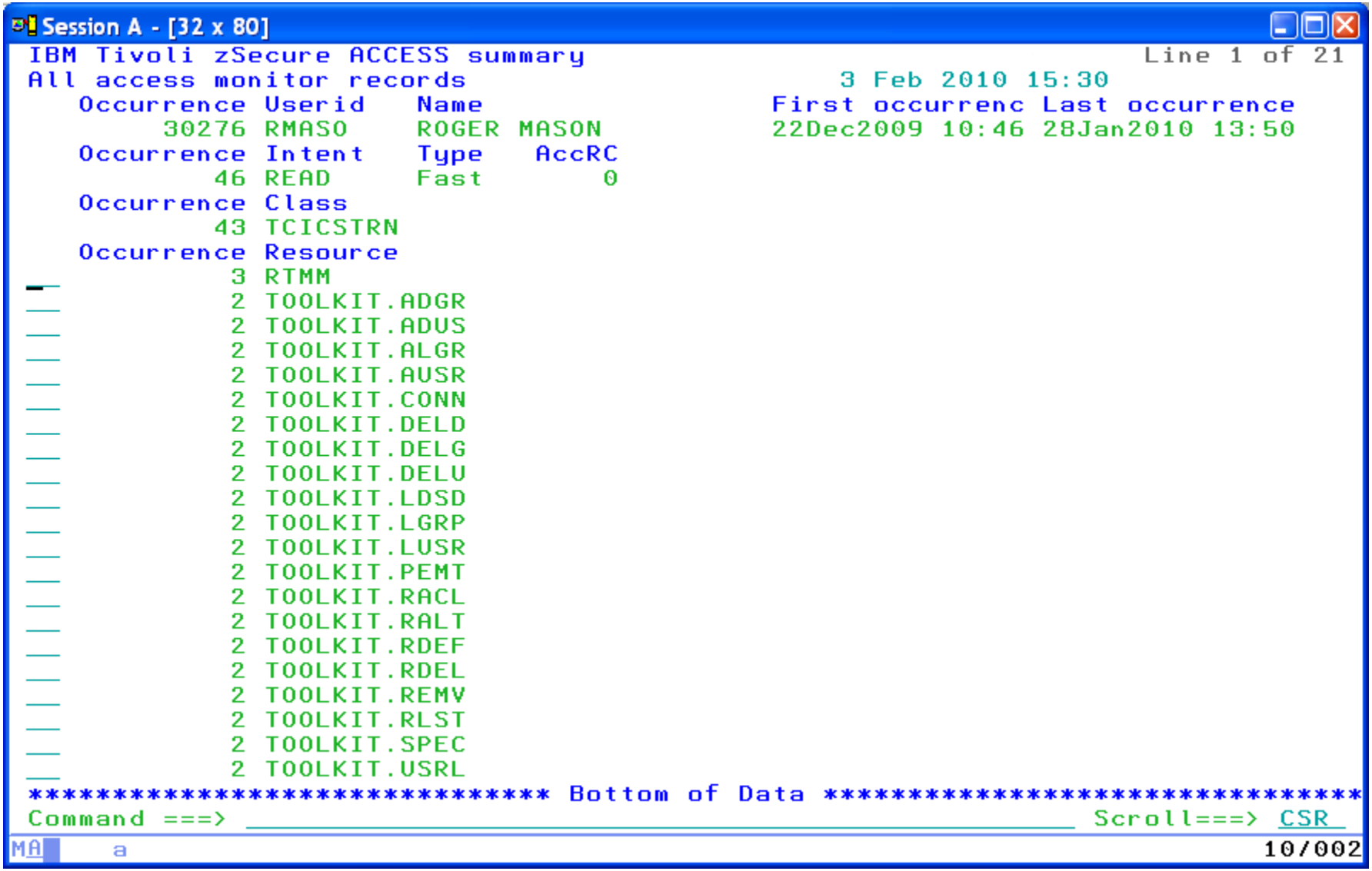
© 2010 IBM Corporation

Access summary by user



© 2010 IBM Corporation

Access summary for a user



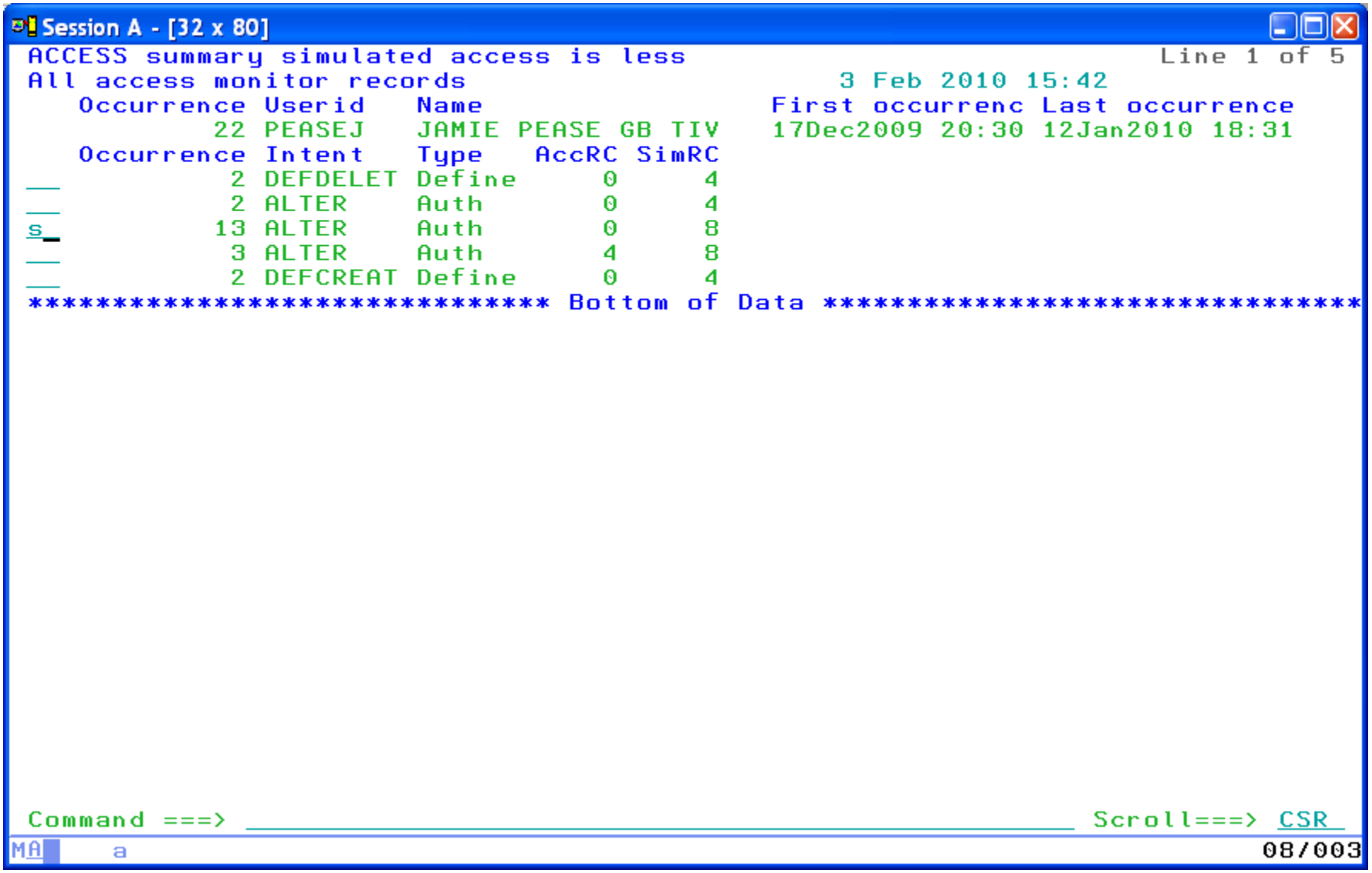
© 2010 IBM Corporation

Analysis of Access Monitor files

- Compare monitored access with RACF database
  - Monitored access is less than access in RACF
    - Identify candidate permits for removal
  - Monitored access is greater than access in RACF
    - Simulate if past access will fail after RACF cleanup

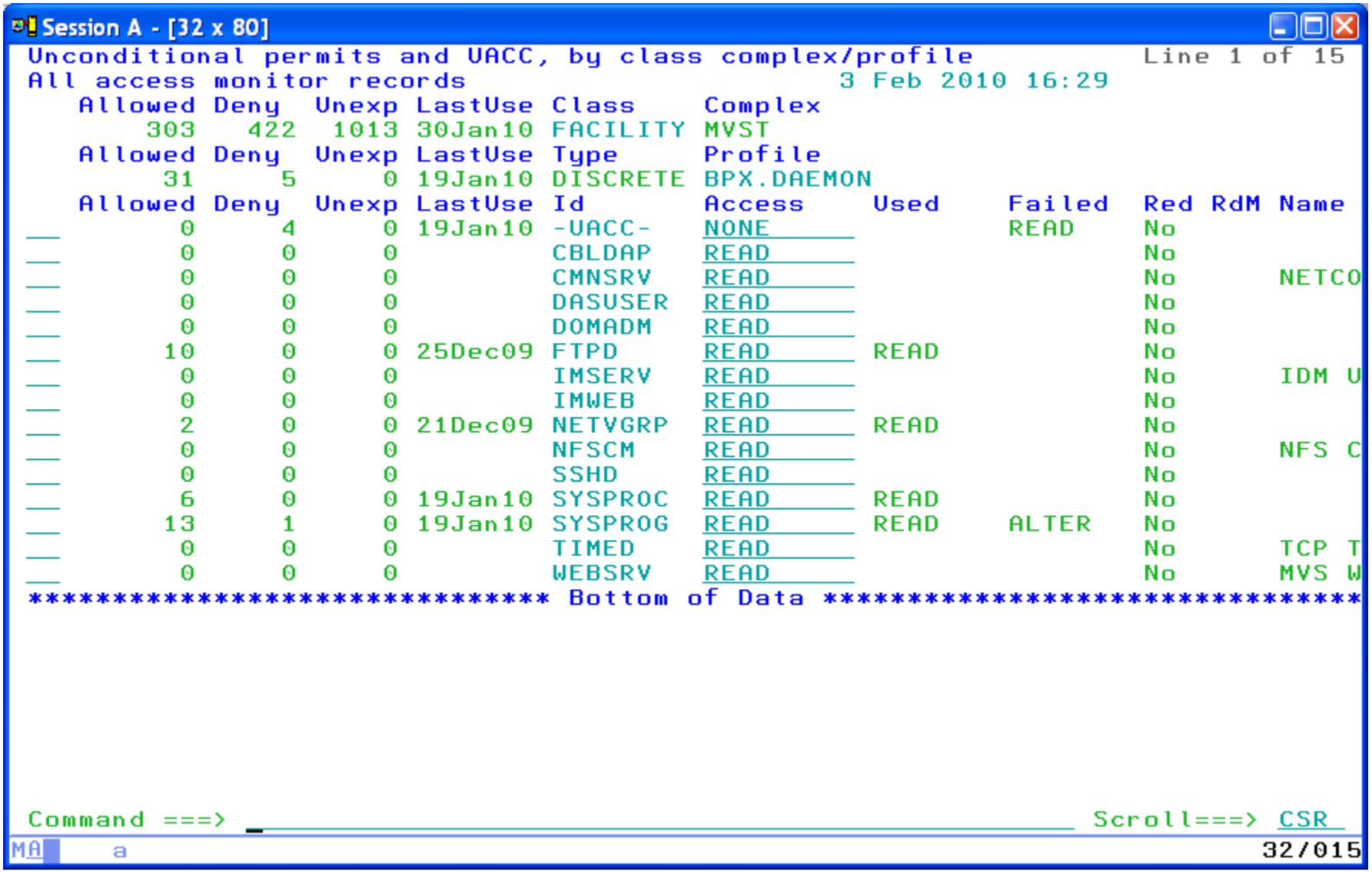
© 2010 IBM Corporation

Allowed in Access Monitor, now denied in RACF



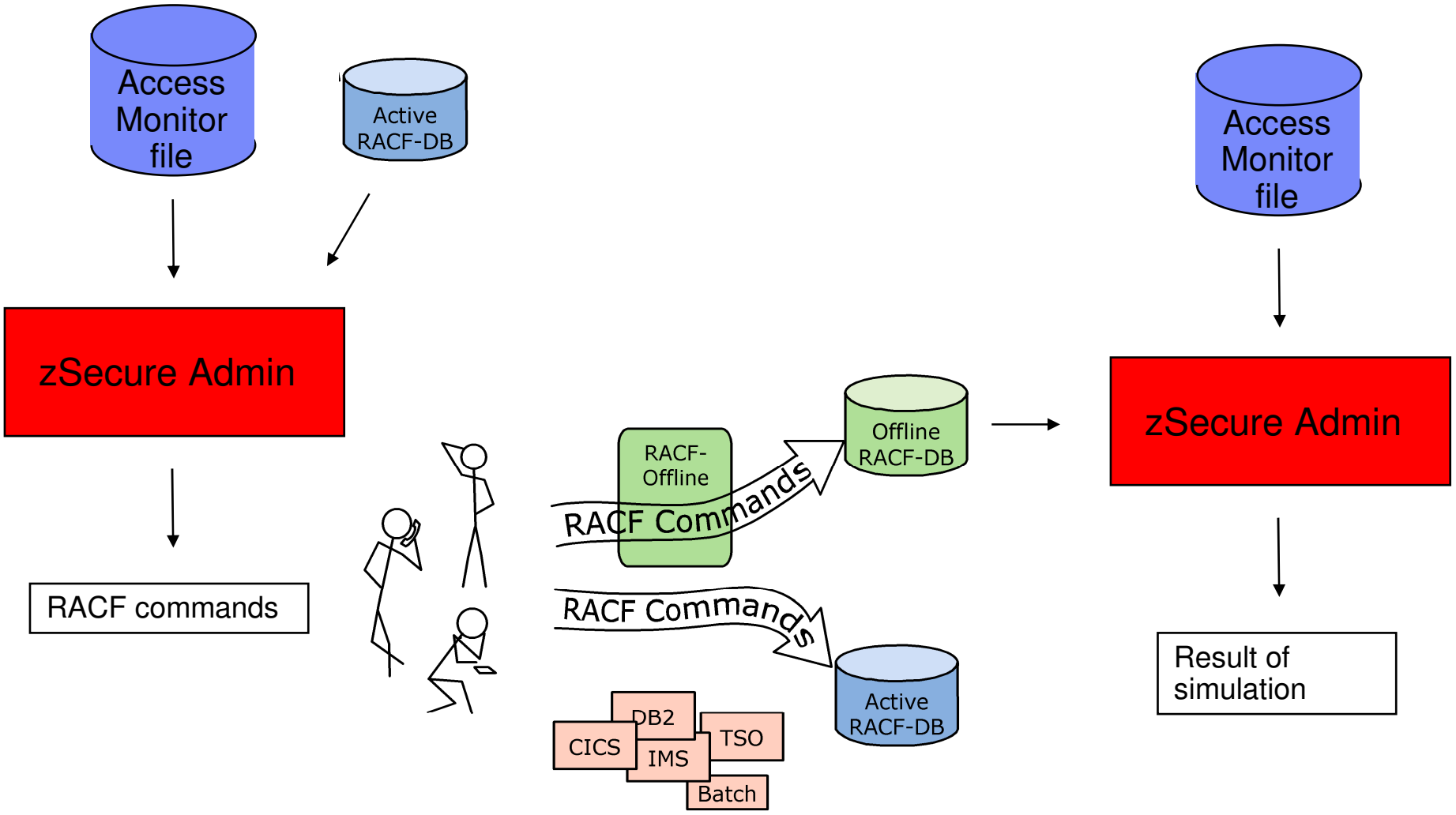
© 2010 IBM Corporation

Access list of a profile, with usage info



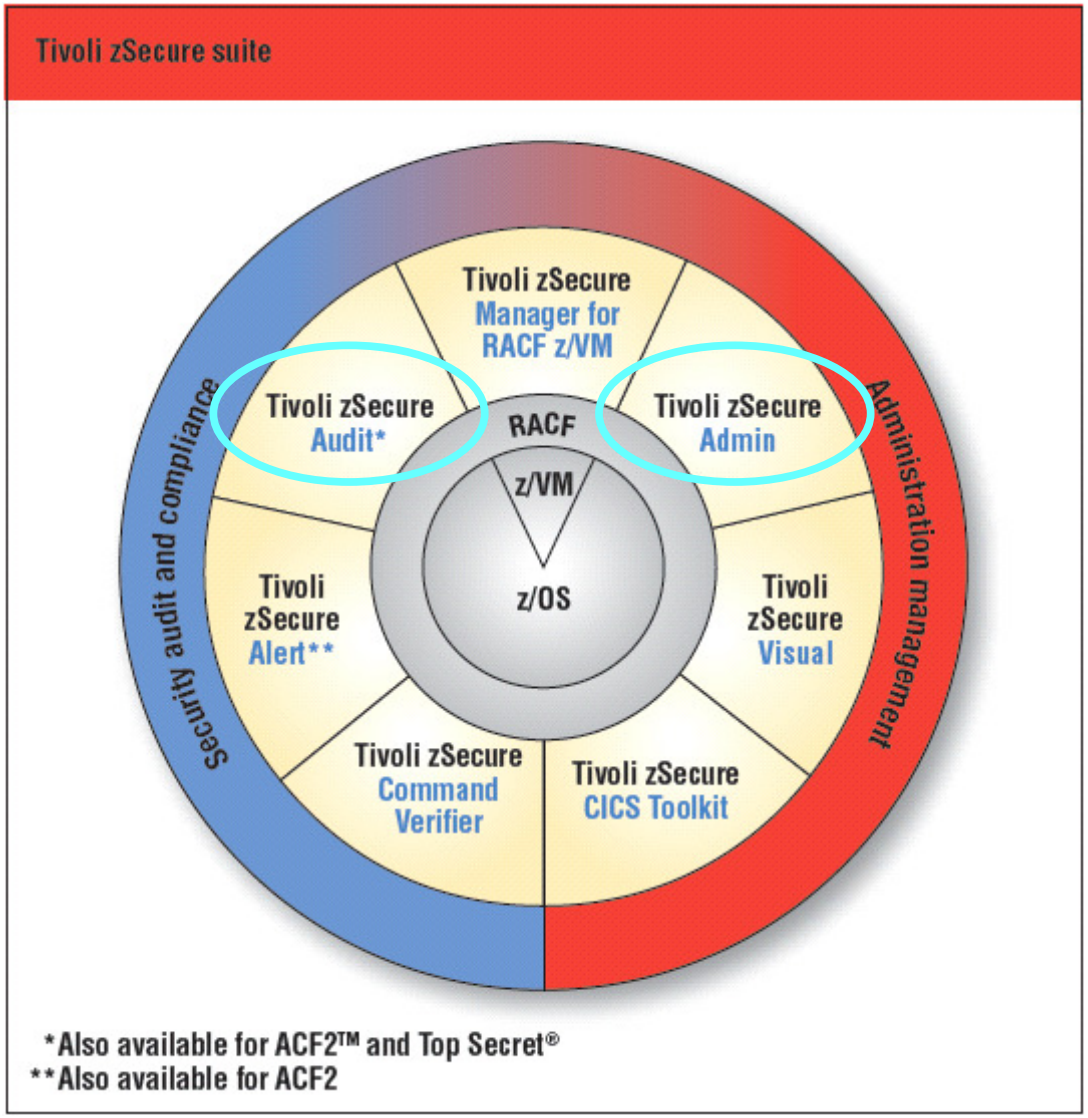
© 2010 IBM Corporation

RACF Offline environment to test cleanup



© 2010 IBM Corporation

Find field values in RACF application segments



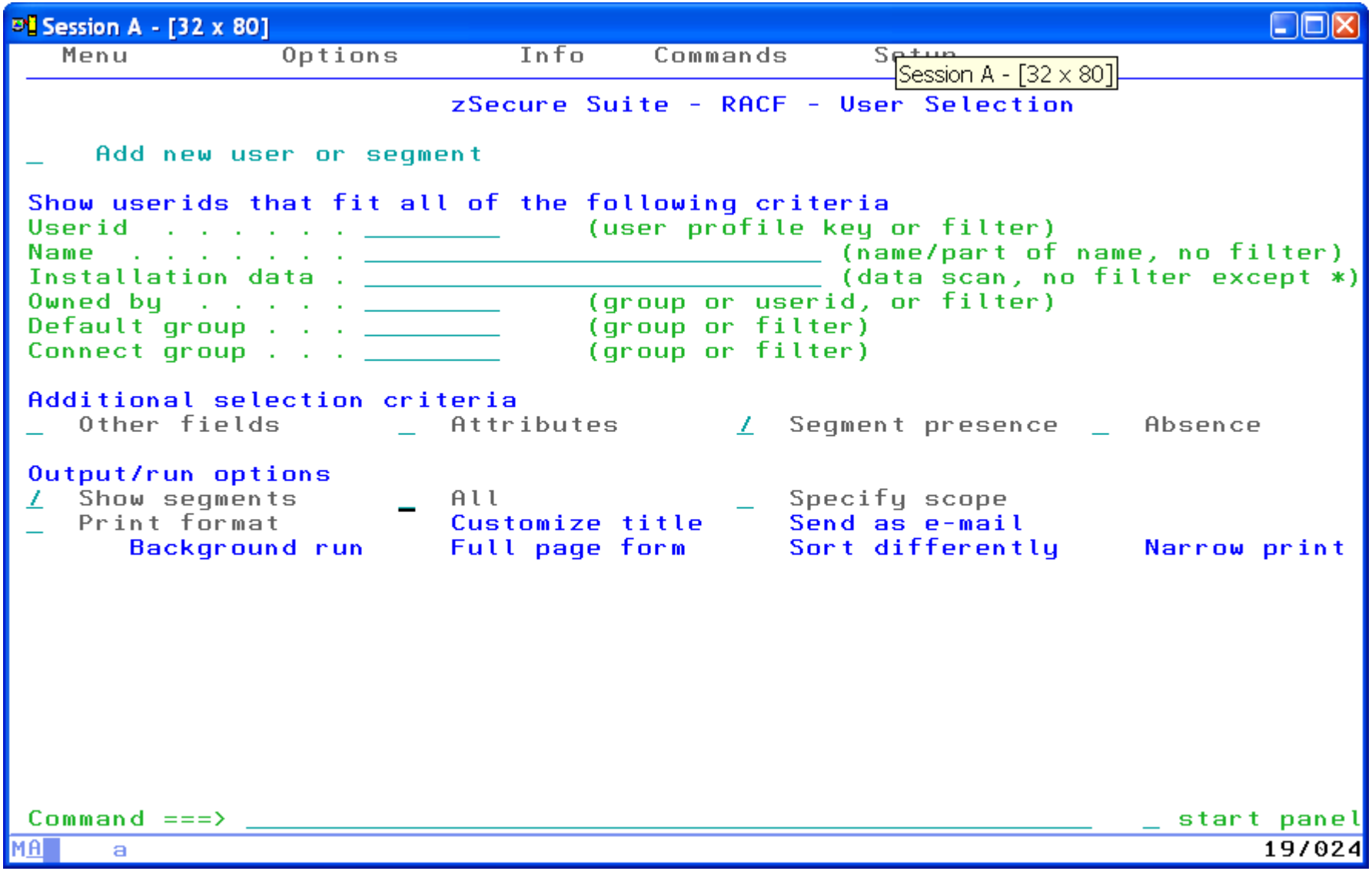
© 2010 IBM Corporation

Find field values in RACF application segments

- Until zSecure 1.10
  - Search on fields in *base* segment
  - Presence/absence of application segments
  - Application segment fields shown
  - Use SORT and FIND in display
- With zSecure 1.11
  - After *presence* and *absence* selections
  - Prompt for selection/exclude criteria in segments
  - Options RA.D, G, R and U

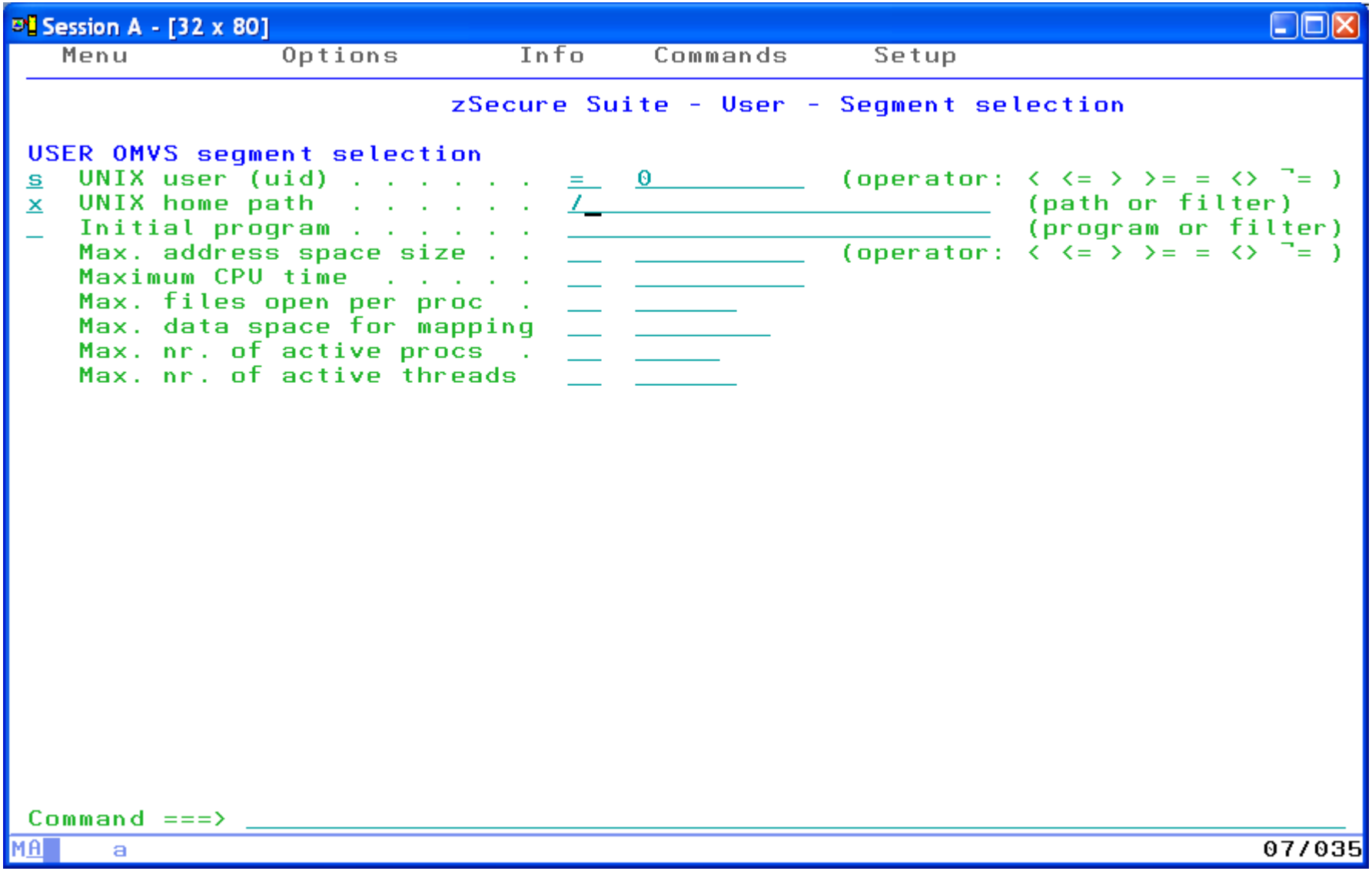
© 2010 IBM Corporation

Research UID(0) users...



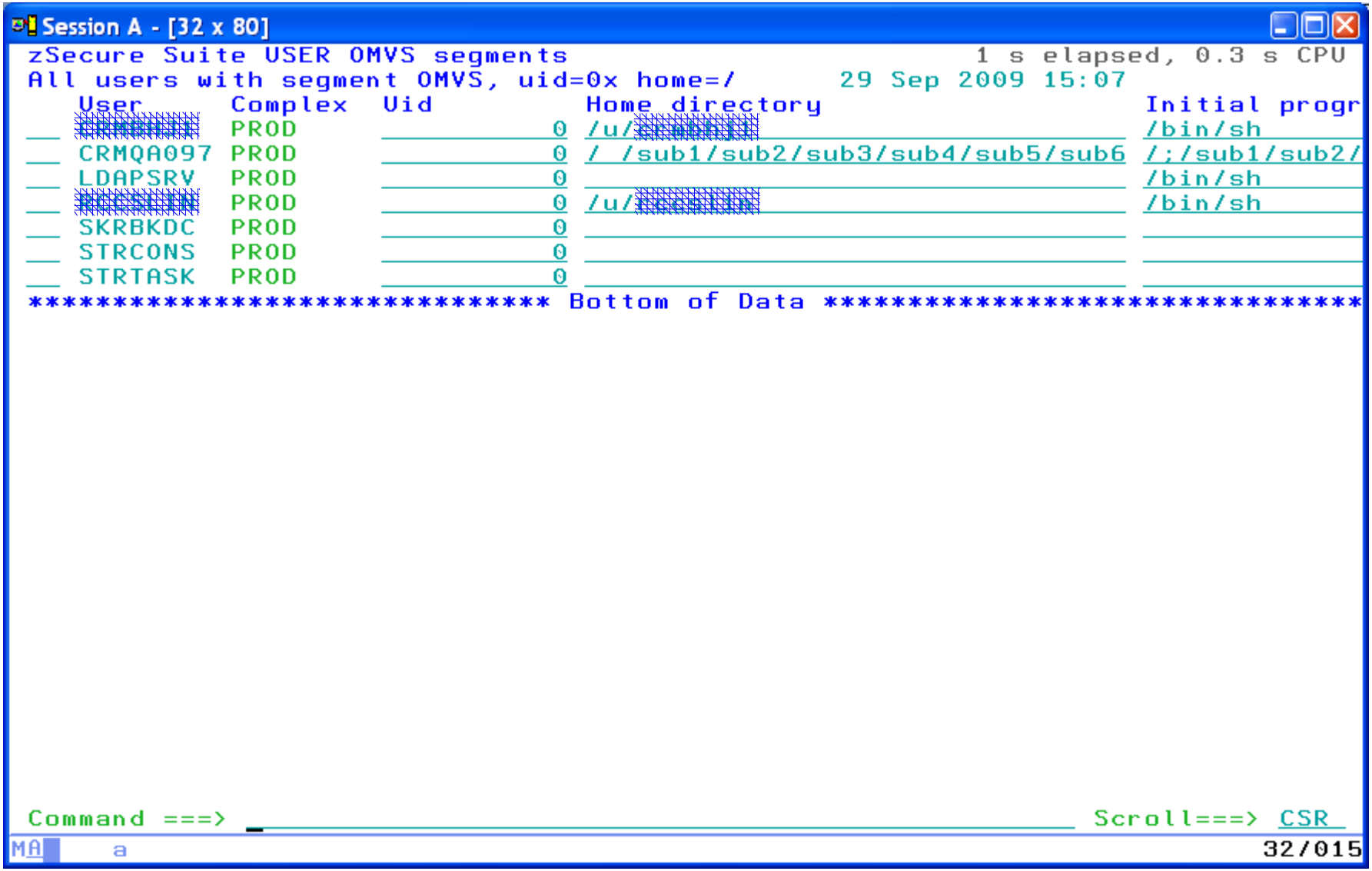
© 2010 IBM Corporation

UID(0) and exclude HOME('/')



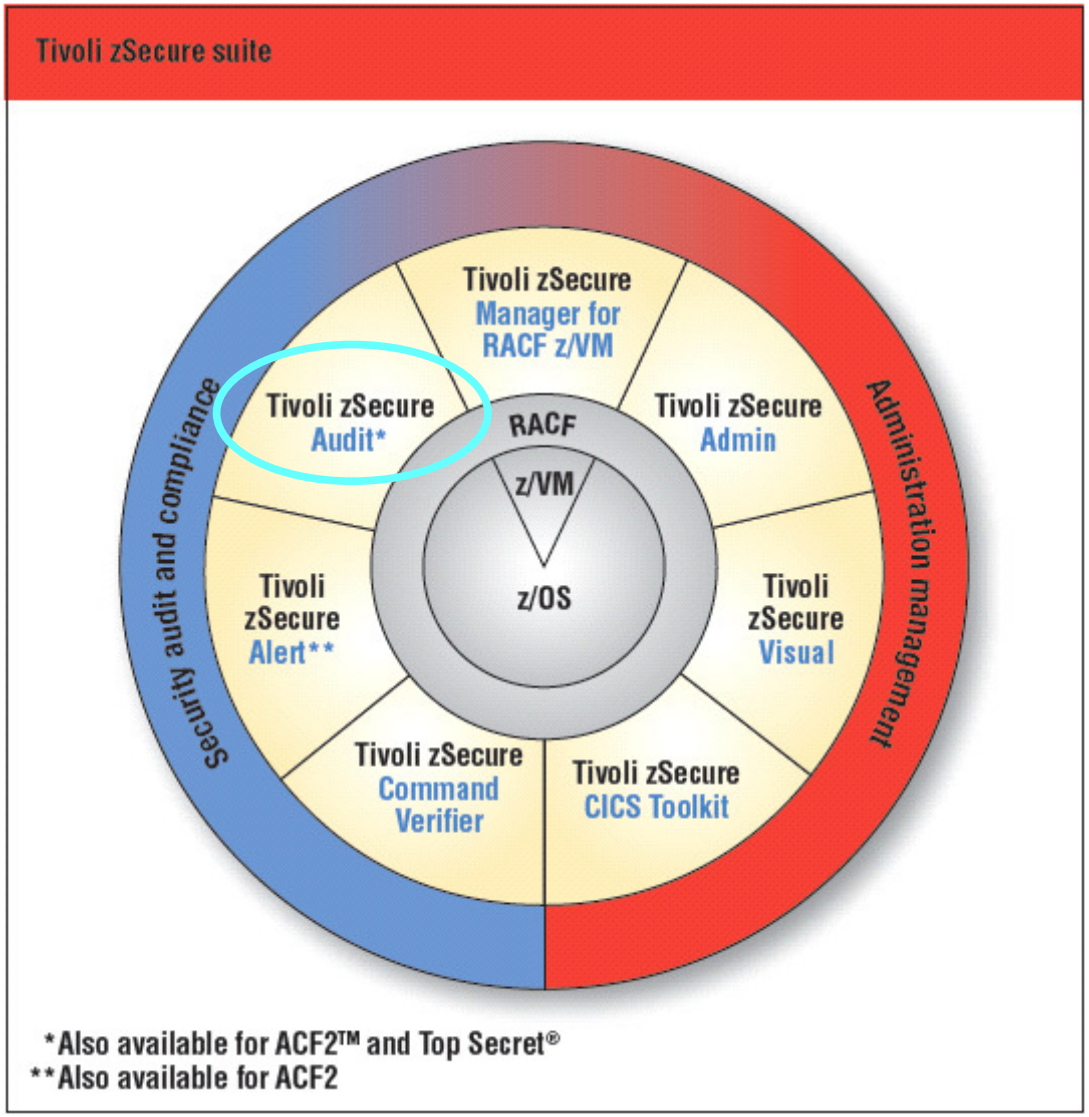
© 2010 IBM Corporation

Result: UID(0) and exclude HOME('/')



© 2010 IBM Corporation

TCPIP Stack Configuration reporting



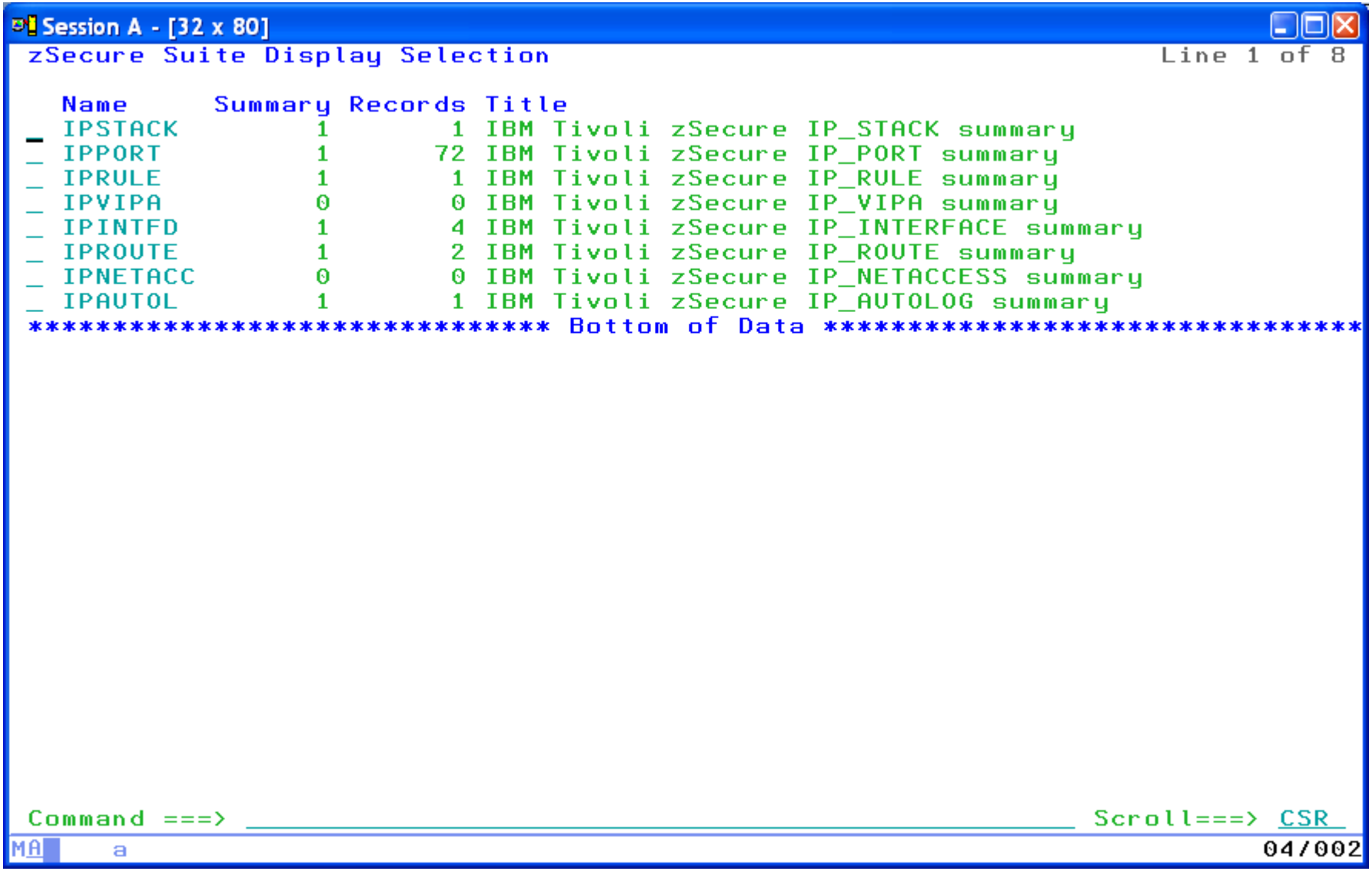
© 2010 IBM Corporation

TCPIP Stack Configuration

- NMI call in Communication Server: GetProfile
  - New service in z/OS 1.11
  - APF protected
  - zSecure Collect executes GetProfile
    - Stores result in CKFREEZE
  - Comm Serv also logs configuration in SMF record 119
- zSecure Audit analyzes
  - Option RE.I and AU.S for CKFREEZE
  - Option EV.I for SMF

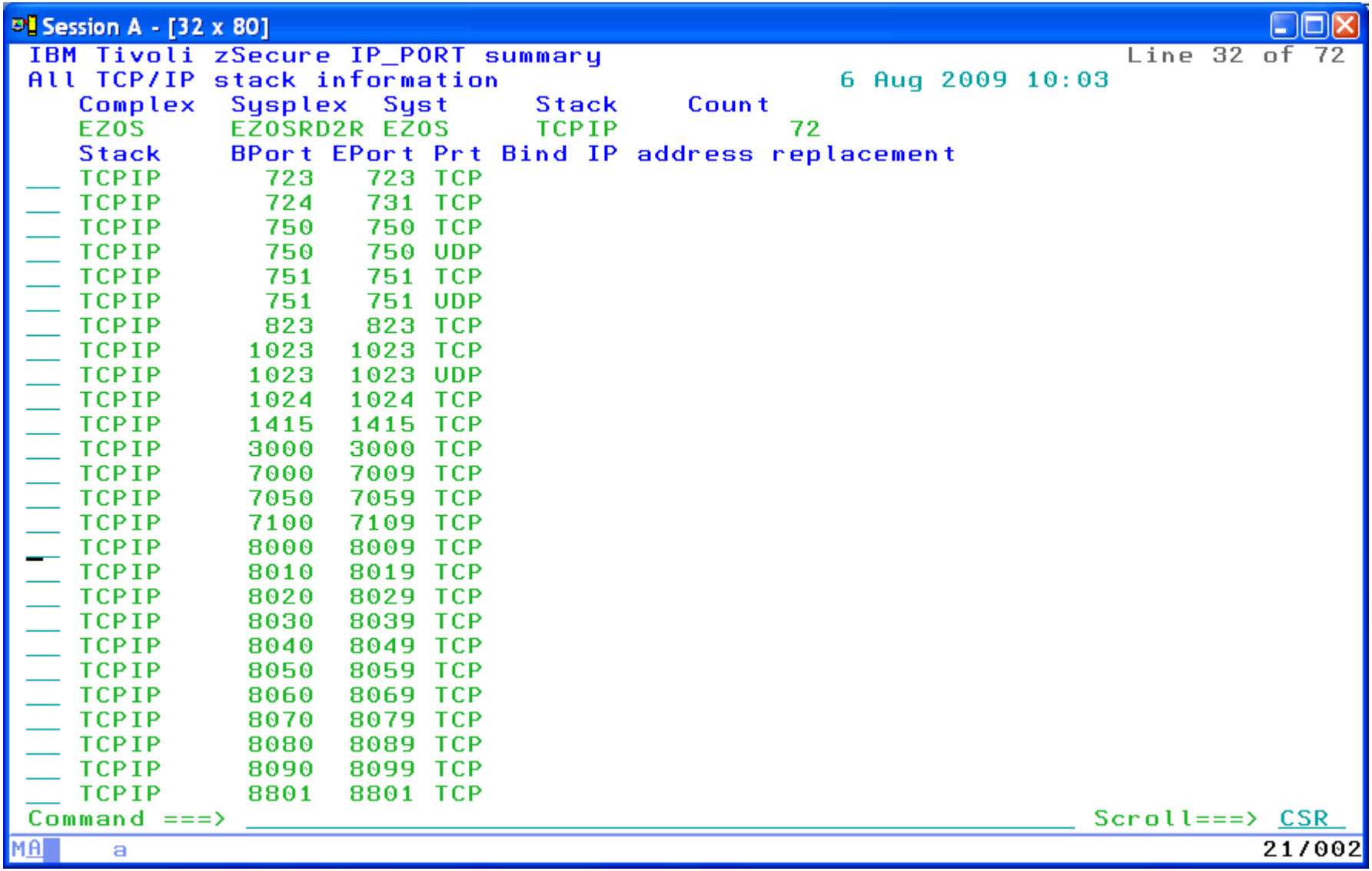
© 2010 IBM Corporation

TCPIP Stack Configuration



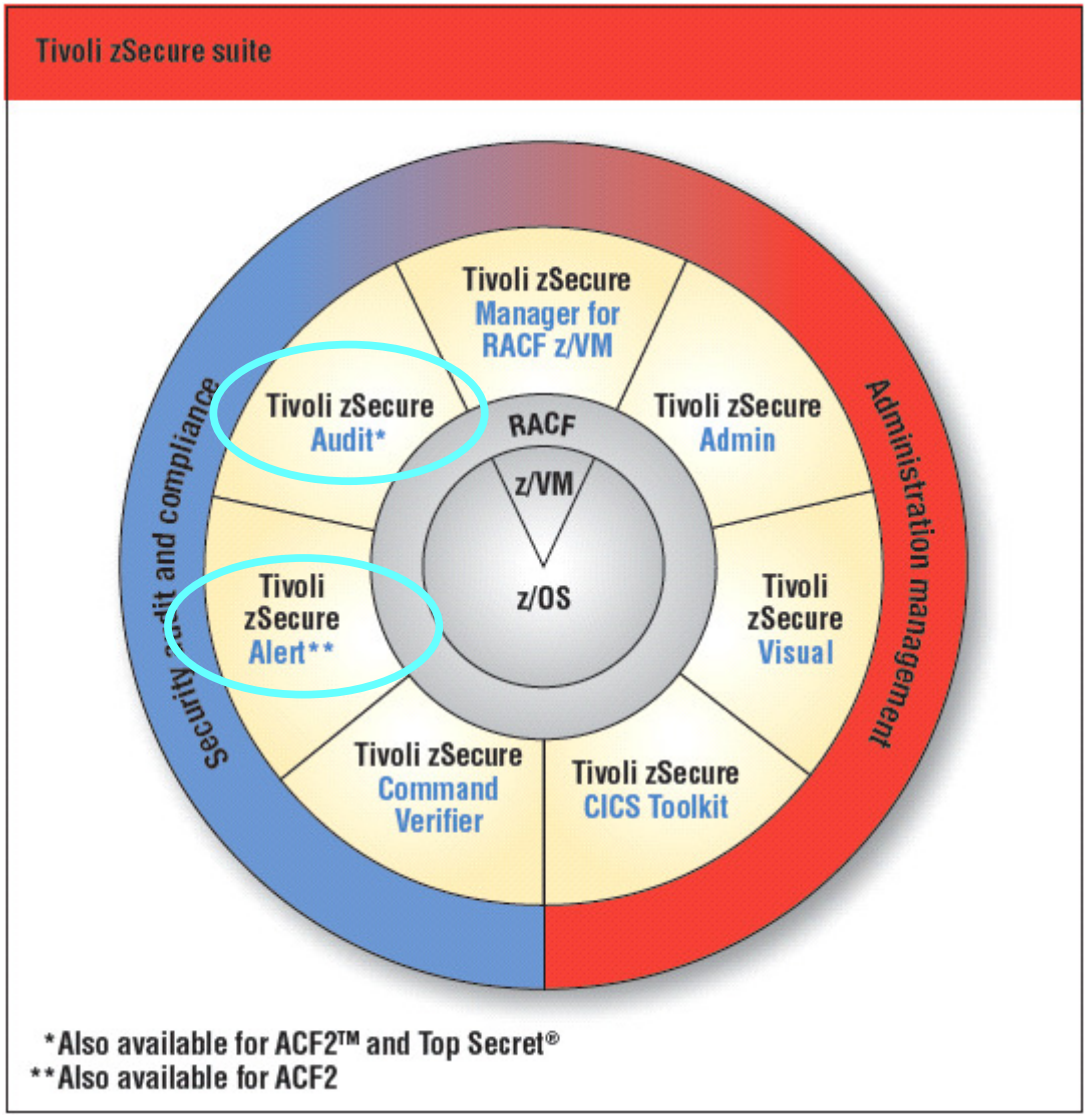
© 2010 IBM Corporation

TCPIP Stack Configuration



© 2010 IBM Corporation

SMF record support and reporting



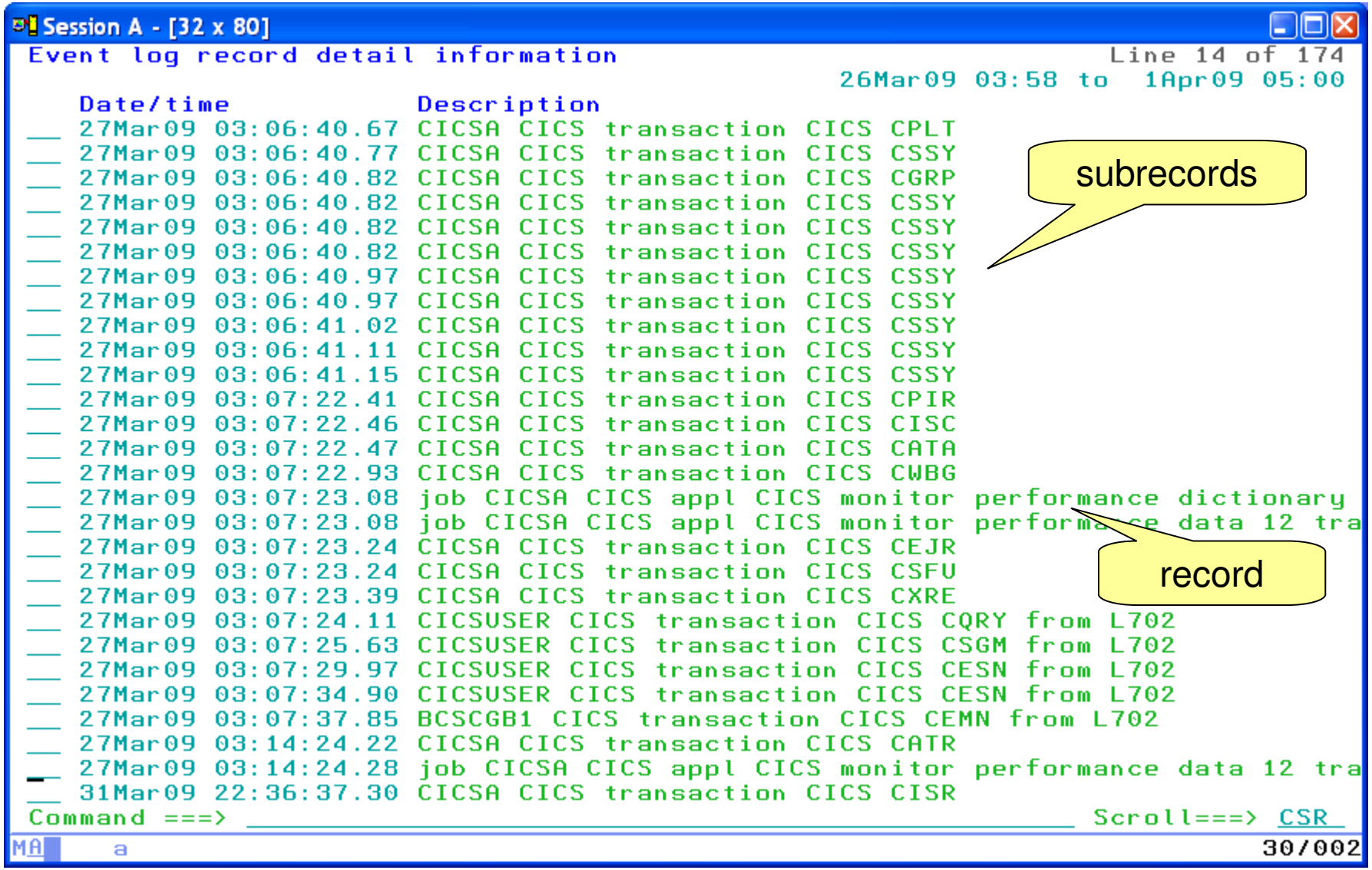
© 2010 IBM Corporation

Additional SMF record types and fields

- CICS (type 110)
- Communication Server, IP Stack Configuration, IPSEC (type 119)
- Member level changes (type 42)
- New RACF events (type 80)
- OAM (type 85)
- Omegamon (use SIMULATE SMF=nnn FORMAT=OMEG)
- R_auditx (type 83, subtype 2)
- TKLM (type 83, subtype 6)
- UNIX extended attribute change (type 92, subtype 15)
- Websphere Application Server (type 83, subtype 5)

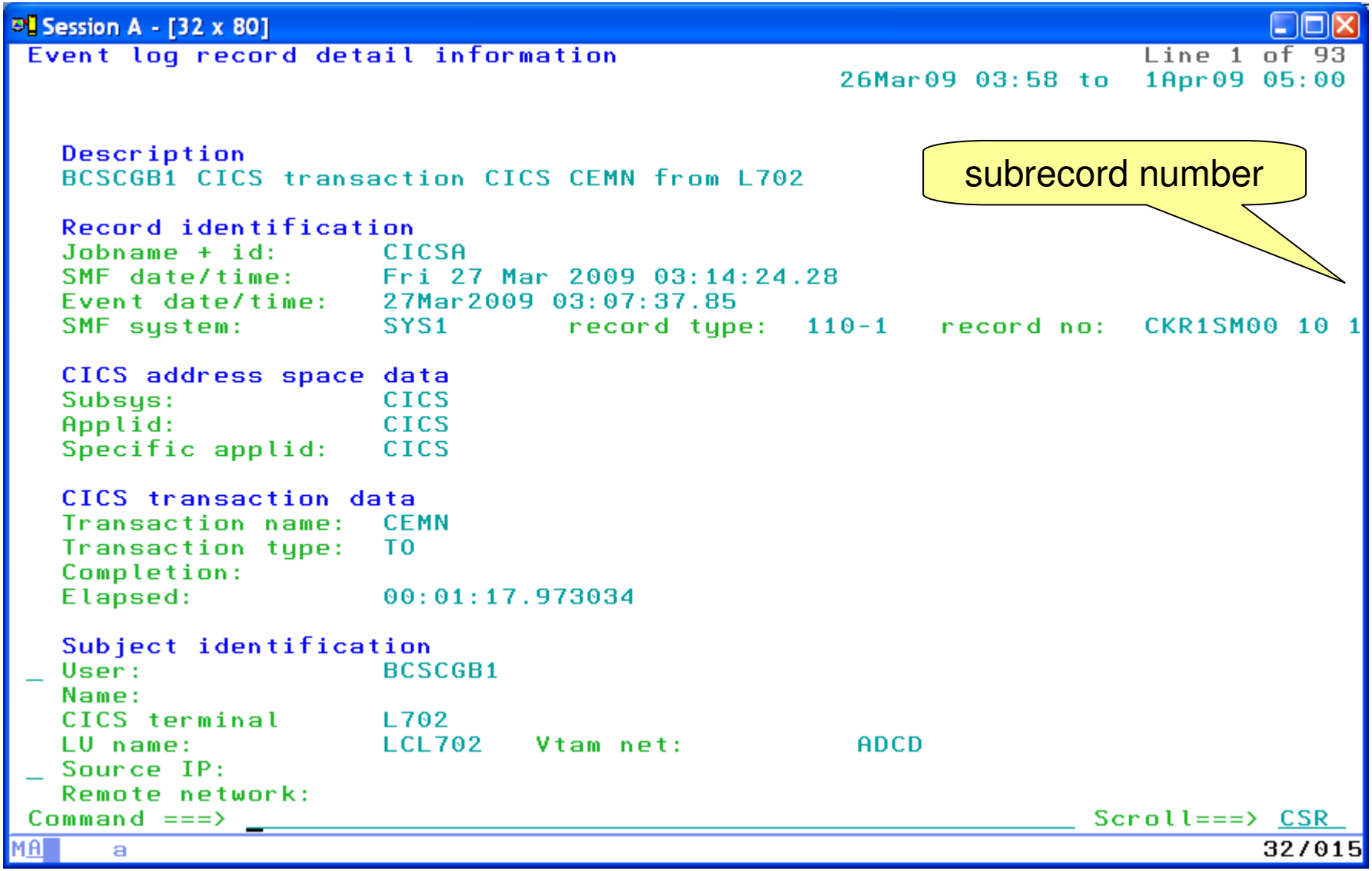
© 2010 IBM Corporation

CICS SMF records



© 2010 IBM Corporation

CICS SMF records



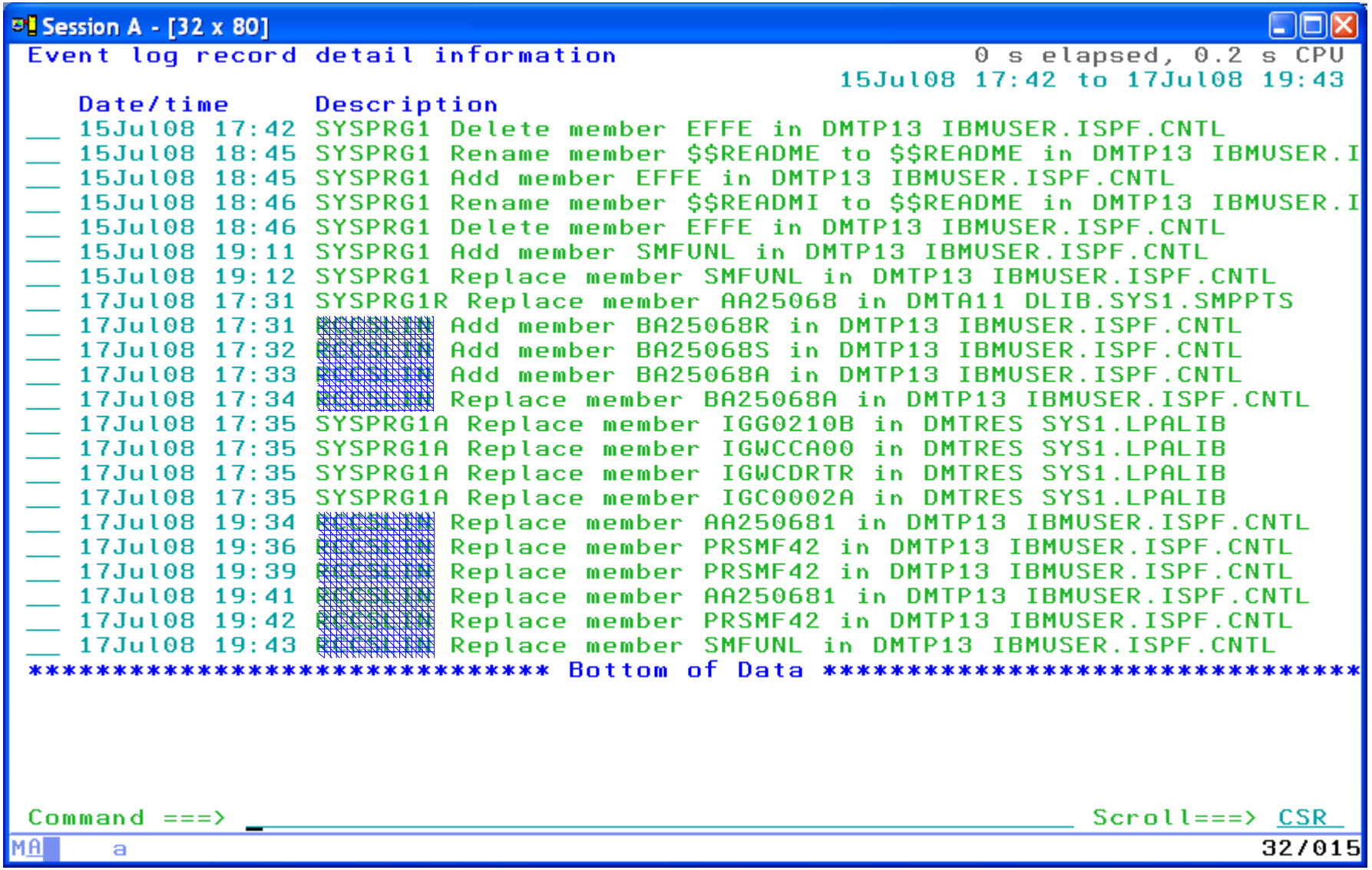
© 2010 IBM Corporation

Member level changes

- DFSMS logs changes to PDS and PDSE
  - Starting with z/OS 1.11, back level via PTF
    - RA10 PSY UA42647 UP08/09/16 P F809
    - R180 PSY UA42648 UP08/09/16 P F809
    - R190 PSY UA42649 UP08/09/16 P F809
  - SMF 42
    - INITIALIZE, DELETE, ADD, CHANGE, REPLACE, RENAME
- zSecure Audit and Alert recognize these records
  - Also from SMF 14 and 15
    - When *member* code in TSO ALLOC, DYNALLOC or JCL DD
  - Monitor updates to Trusted Computing Base
    - With date, time, userid, dsname and member name

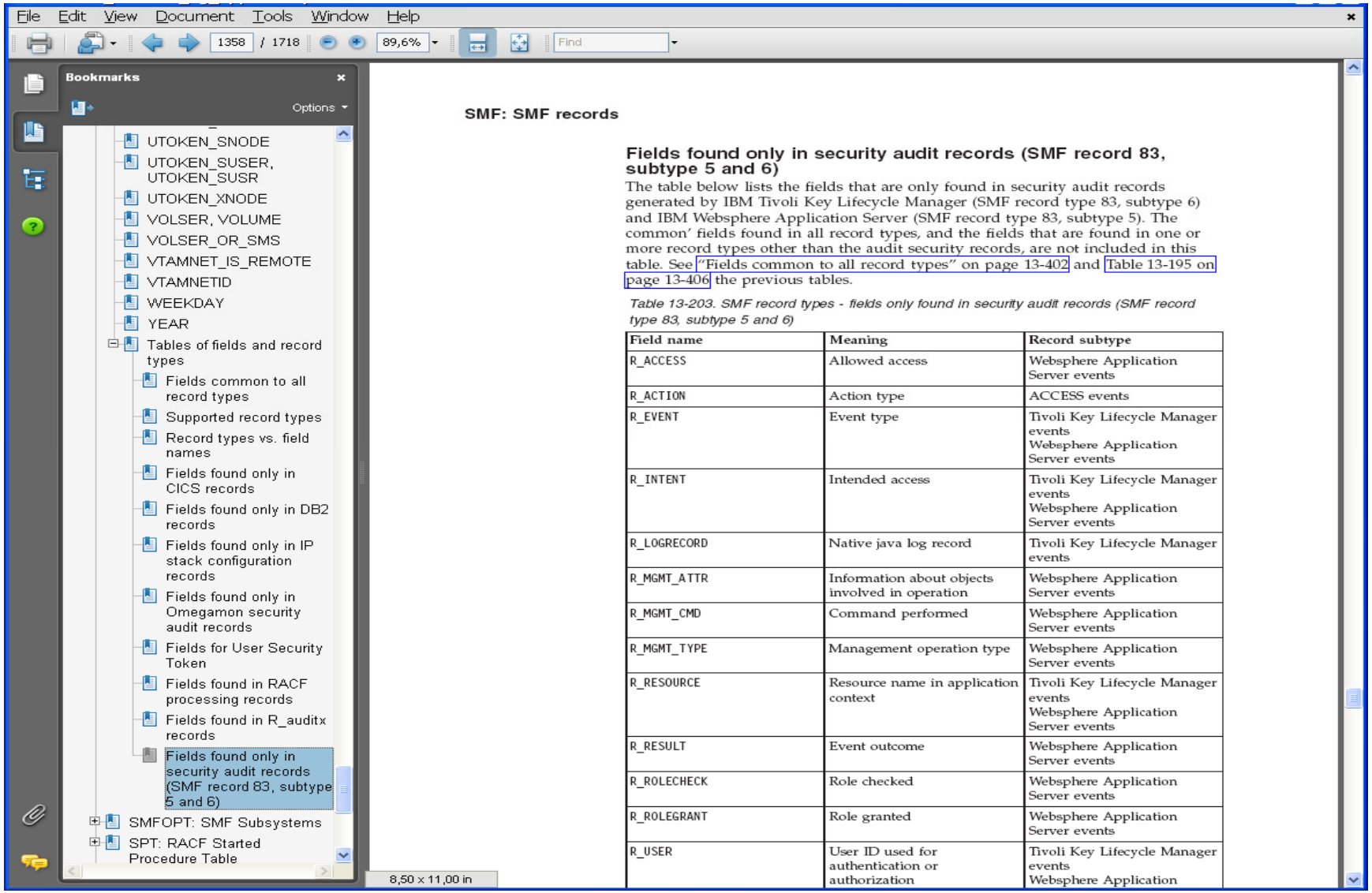
© 2010 IBM Corporation

Member level changes



© 2010 IBM Corporation

WAS and TKLM security audit event records



SMF: SMF records

Fields found only in security audit records (SMF record 83, subtype 5 and 6)

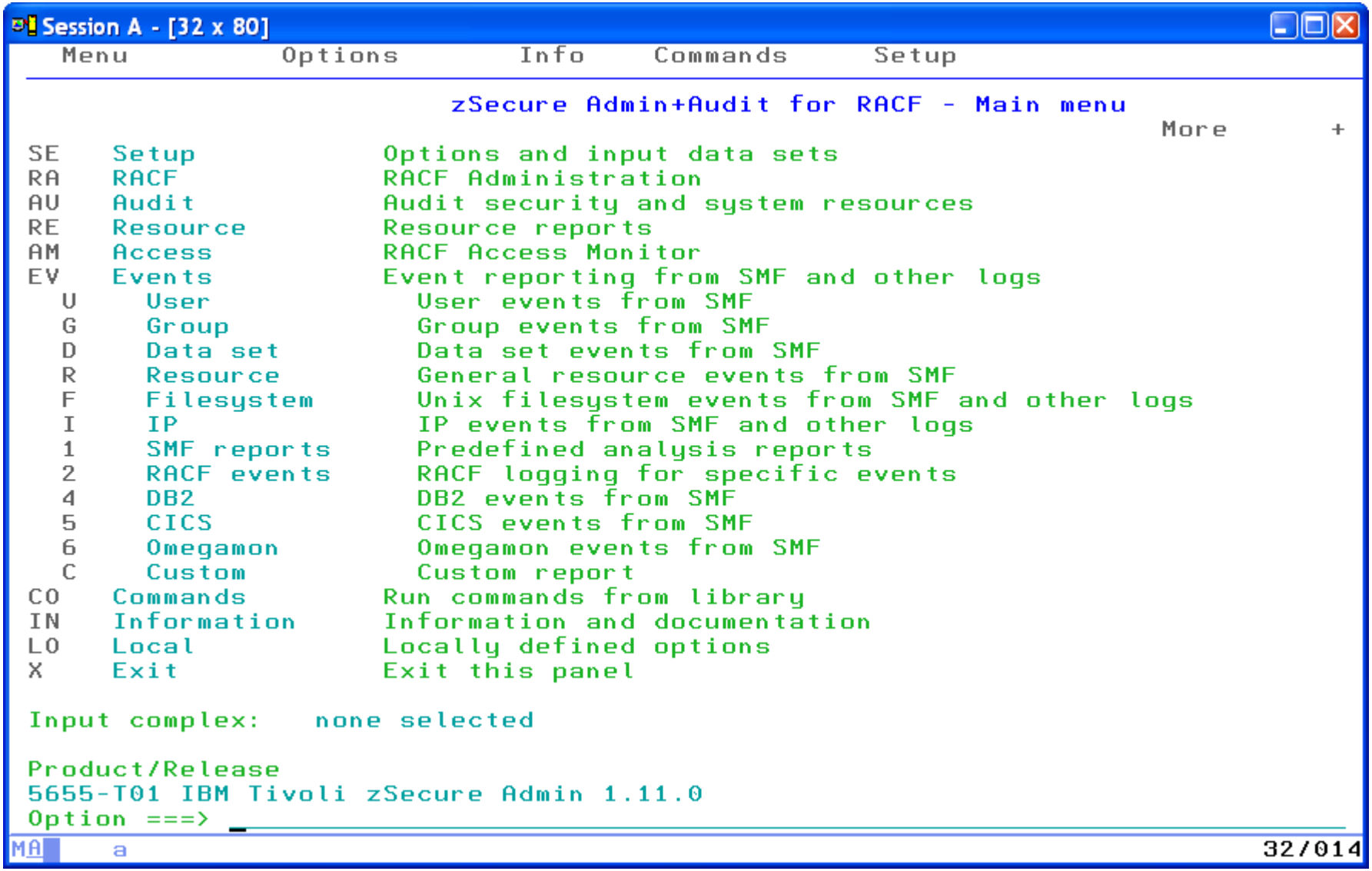
The table below lists the fields that are only found in security audit records generated by IBM Tivoli Key Lifecycle Manager (SMF record type 83, subtype 6) and IBM Websphere Application Server (SMF record type 83, subtype 5). The common' fields found in all record types, and the fields that are found in one or more record types other than the audit security records, are not included in this table. See "Fields common to all record types" on page 13-402 and Table 13-195 on page 13-406 the previous tables.

Table 13-203. SMF record types - fields only found in security audit records (SMF record type 83, subtype 5 and 6)

Field name	Meaning	Record subtype
R_ACCESS	Allowed access	Websphere Application Server events
R_ACTION	Action type	ACCESS events
R_EVENT	Event type	Tivoli Key Lifecycle Manager events Websphere Application Server events
R_INTENT	Intended access	Tivoli Key Lifecycle Manager events Websphere Application Server events
R_LOGRECORD	Native java log record	Tivoli Key Lifecycle Manager events
R_MGMT_ATTR	Information about objects involved in operation	Websphere Application Server events
R_MGMT_CMD	Command performed	Websphere Application Server events
R_MGMT_TYPE	Management operation type	Websphere Application Server events
R_RESOURCE	Resource name in application context	Tivoli Key Lifecycle Manager events Websphere Application Server events
R_RESULT	Event outcome	Websphere Application Server events
R_ROLECHECK	Role checked	Websphere Application Server events
R_ROLEGRANT	Role granted	Websphere Application Server events
R_USER	User ID used for authentication or authorization	Tivoli Key Lifecycle Manager events Websphere Application

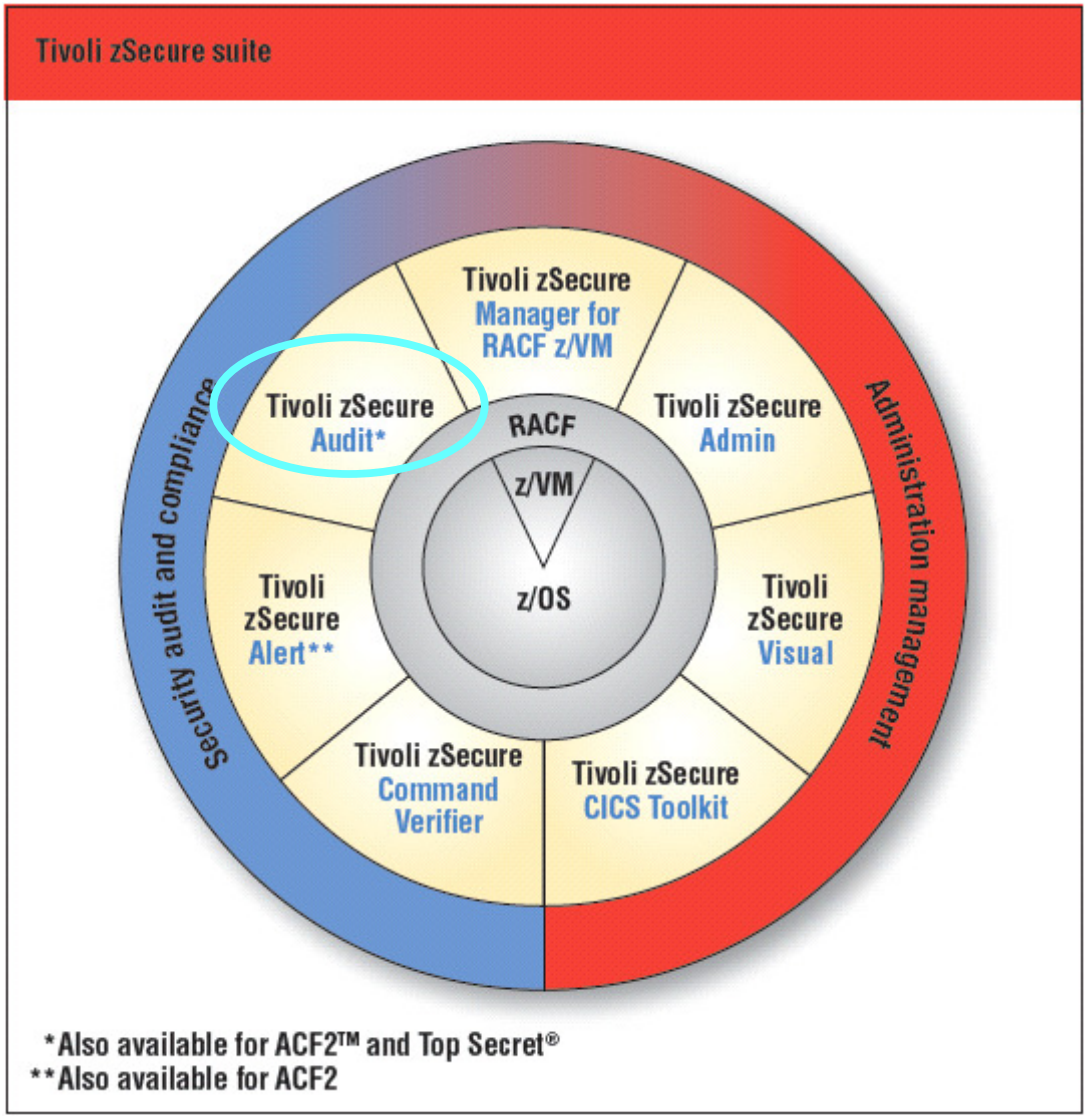
© 2010 IBM Corporation

New ISPF options for Event selection and reporting



© 2010 IBM Corporation

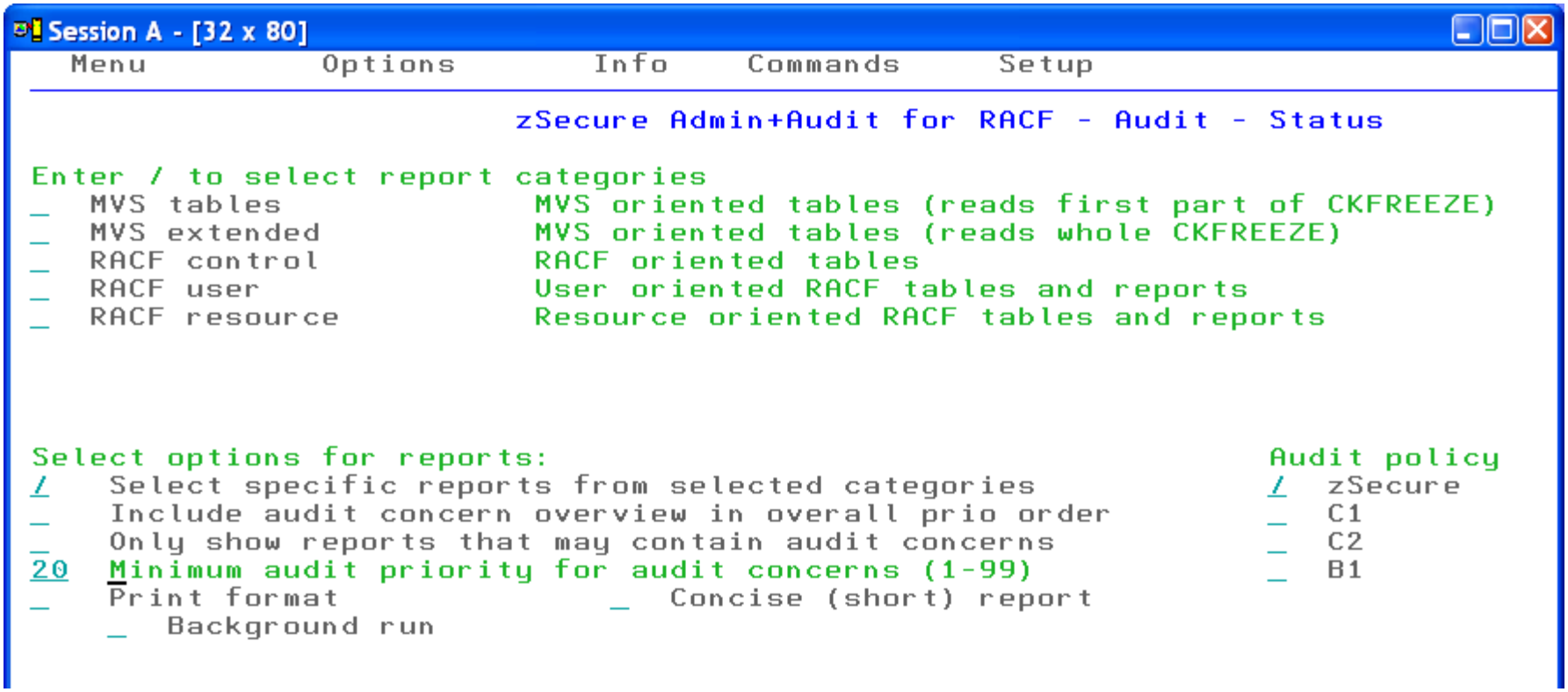
Other enhancements to Audit



© 2010 IBM Corporation

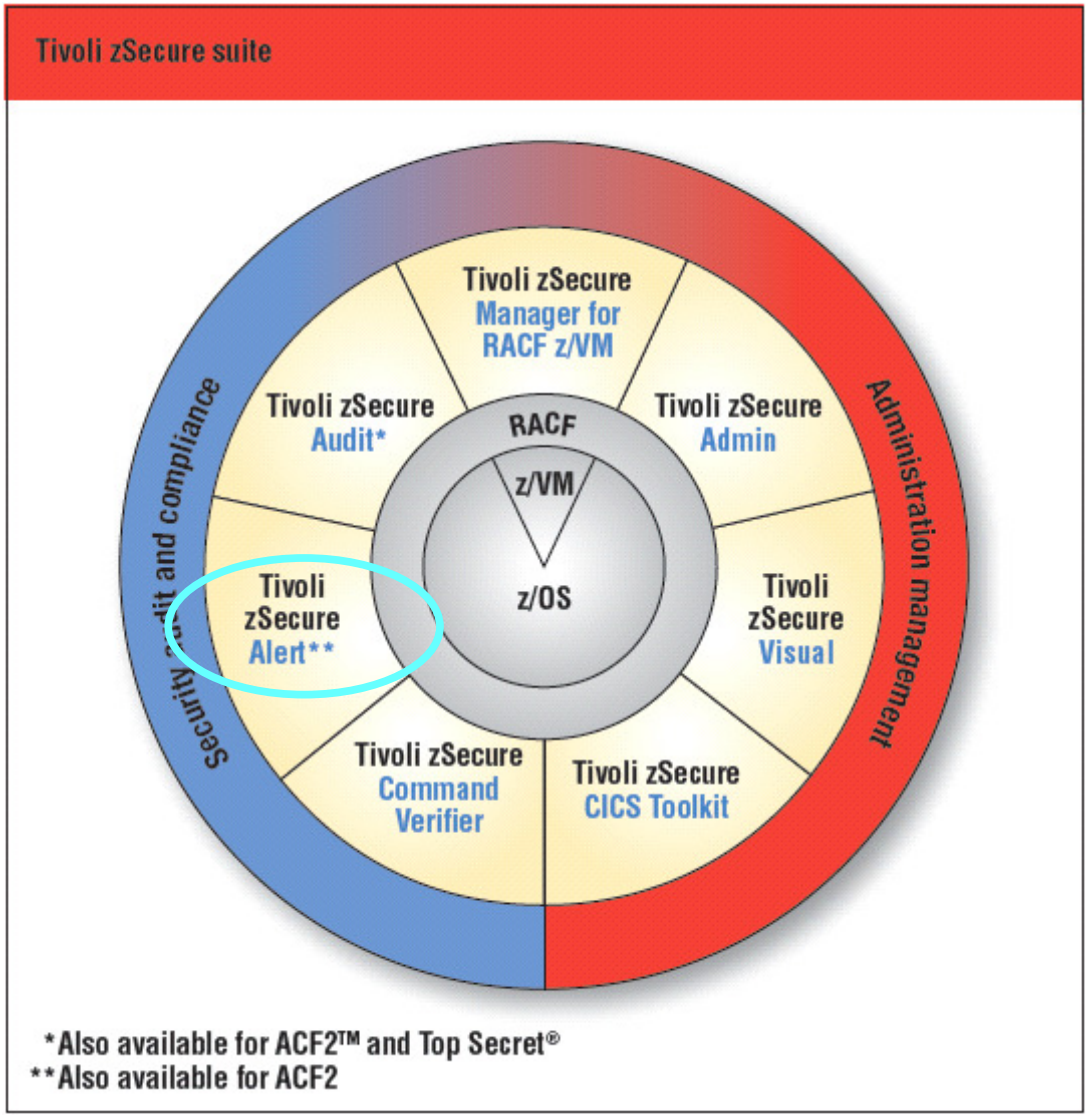
Other enhancements to Audit

- Minimum audit priority for reporting
  - e.g., suppress “housekeeping” issues



© 2010 IBM Corporation

Extended Monitoring



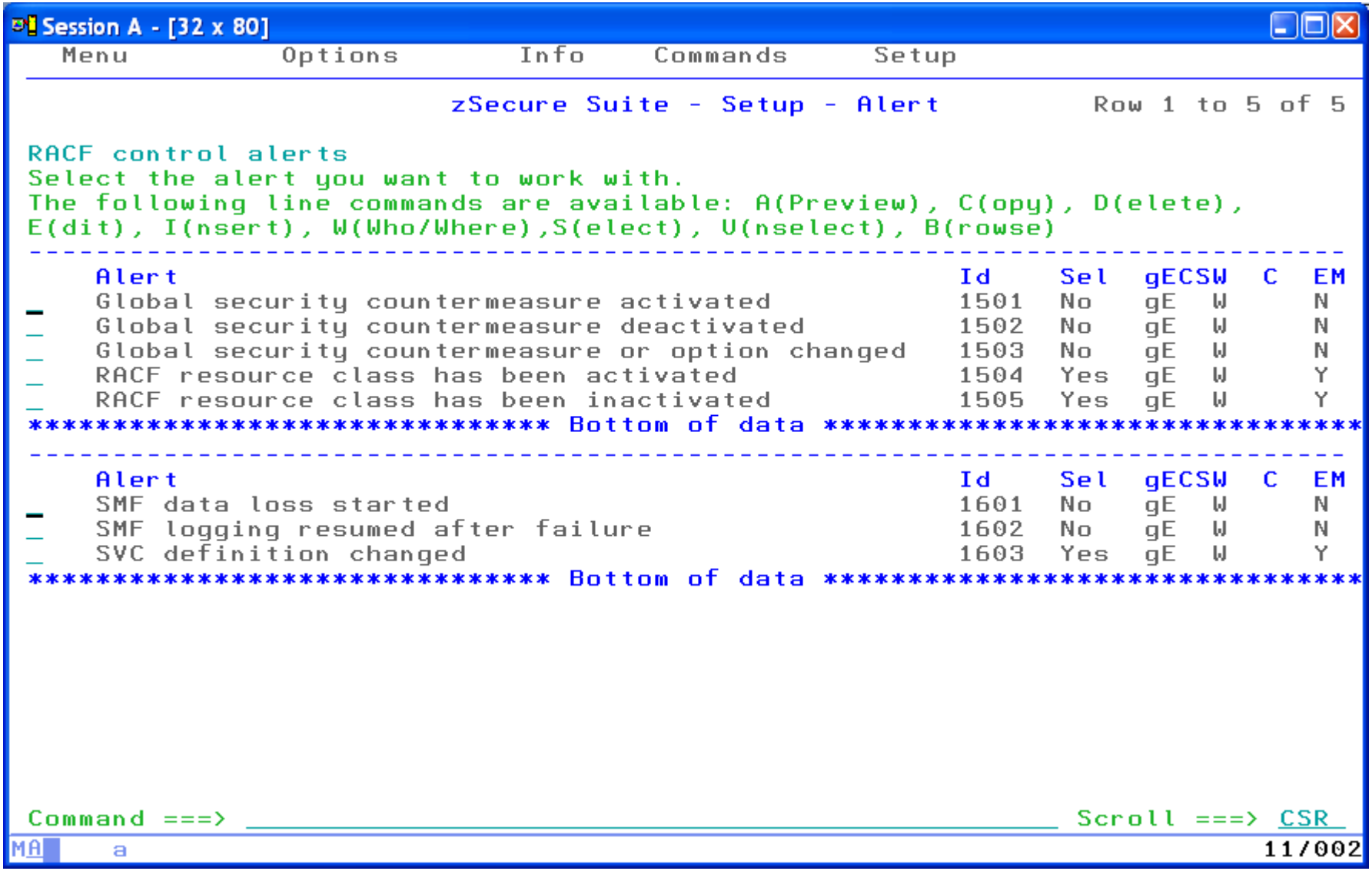
© 2010 IBM Corporation

Extended Monitoring

- Identify changes in the configuration
  - Even when there is no SMF record or syslog message
- zSecure Alert started task (C2POLICE)
  - Keeps 2 snapshot files
    - *Current* and *base*
    - Refresh at user-specified intervals
  - Compares *current* with *base*
    - Fields that must match to identify entry
    - Fields where changes matter
    - Examples: SETROPTS class options and SVC Table
  - Alert when change is found

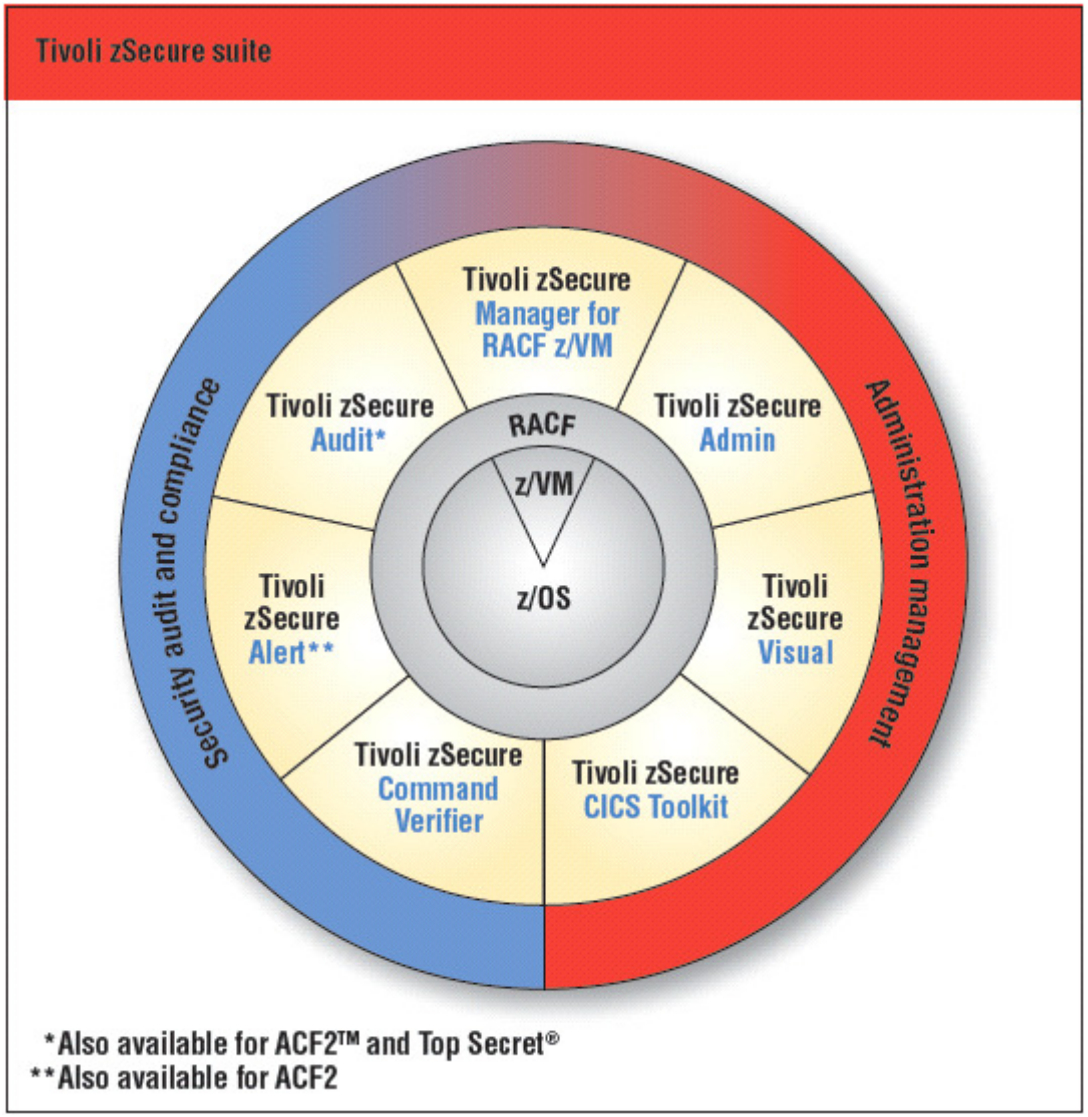
© 2010 IBM Corporation

Extended Monitoring: configuring



© 2010 IBM Corporation

z/OS currency



© 2010 IBM Corporation

z/OS currency support

- Load module signature verification
- Extended member statistics in audit reports (1.10)
- Identity propagation
- RACF fields and classes for ICSF
- Password phrase exploitation (1.8)
- TCPIP configuration (NMI & SMF, record type 119)

© 2010 IBM Corporation

z/OS currency support

- PDS(E) member level auditing - SMF 42
- New RACF events - SMF 80
  - Event 86: Load Module Signature Verification
  - event 87: IDID mapping
  - event 88+89: AUTOPROF and QRECOVER
- WAS SMF - 83(5)
- TKLM SMF - 83(6)
- OAM SMF - 85
- UNIX extended attribute change - SMF 92(15)
- IPSEC - SMF 119 (1.10)

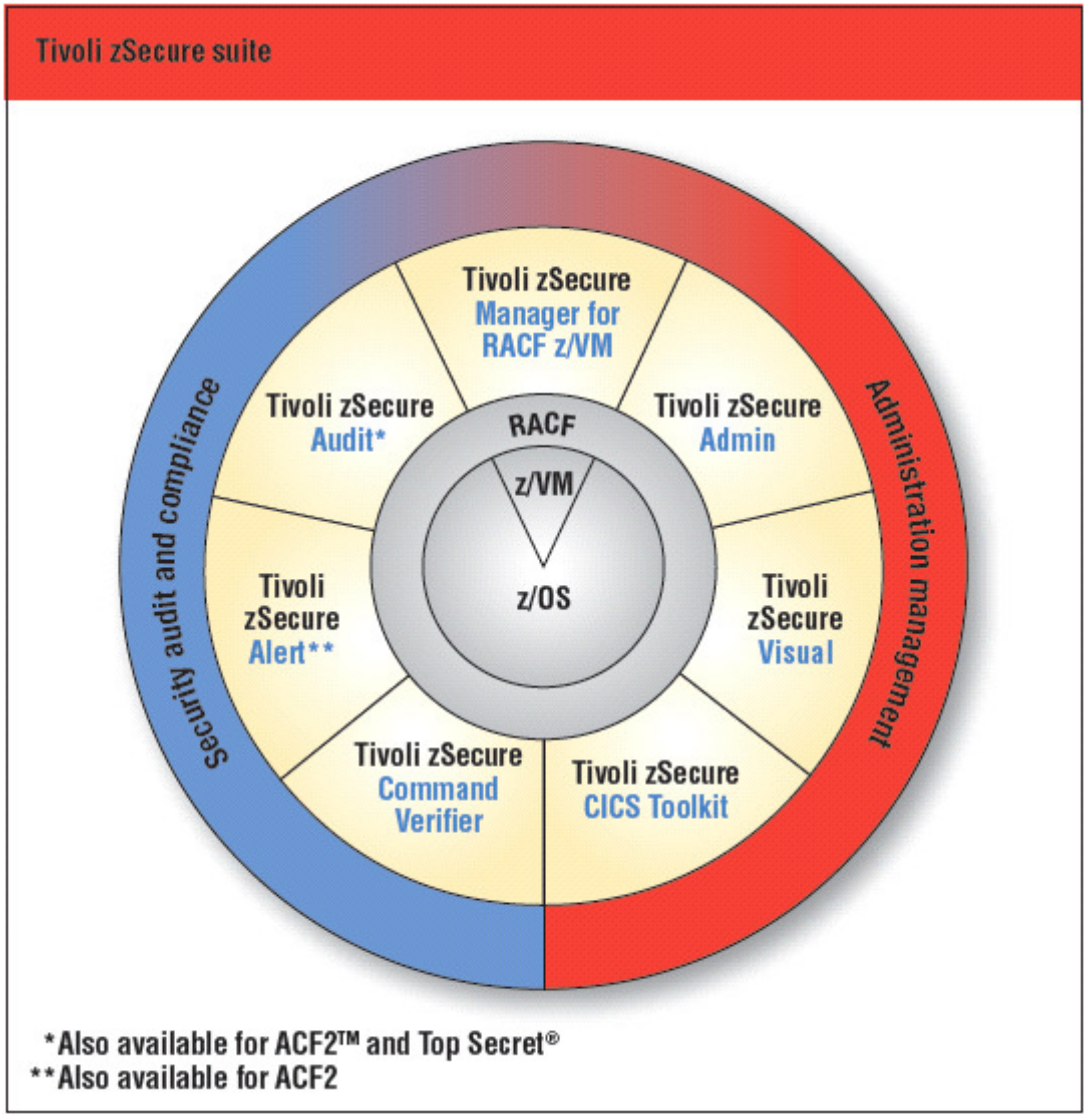
© 2010 IBM Corporation

z/OS currency support

- Dynamic exits (RMM)
- OAM exit (CBRUXSA)
- IPLPARM (AXR, ZIIPZAAP)
- >64 CPUs per LPAR
- Extended address volumes
- Dynamic TIOT size change

© 2010 IBM Corporation

ACF2 currency



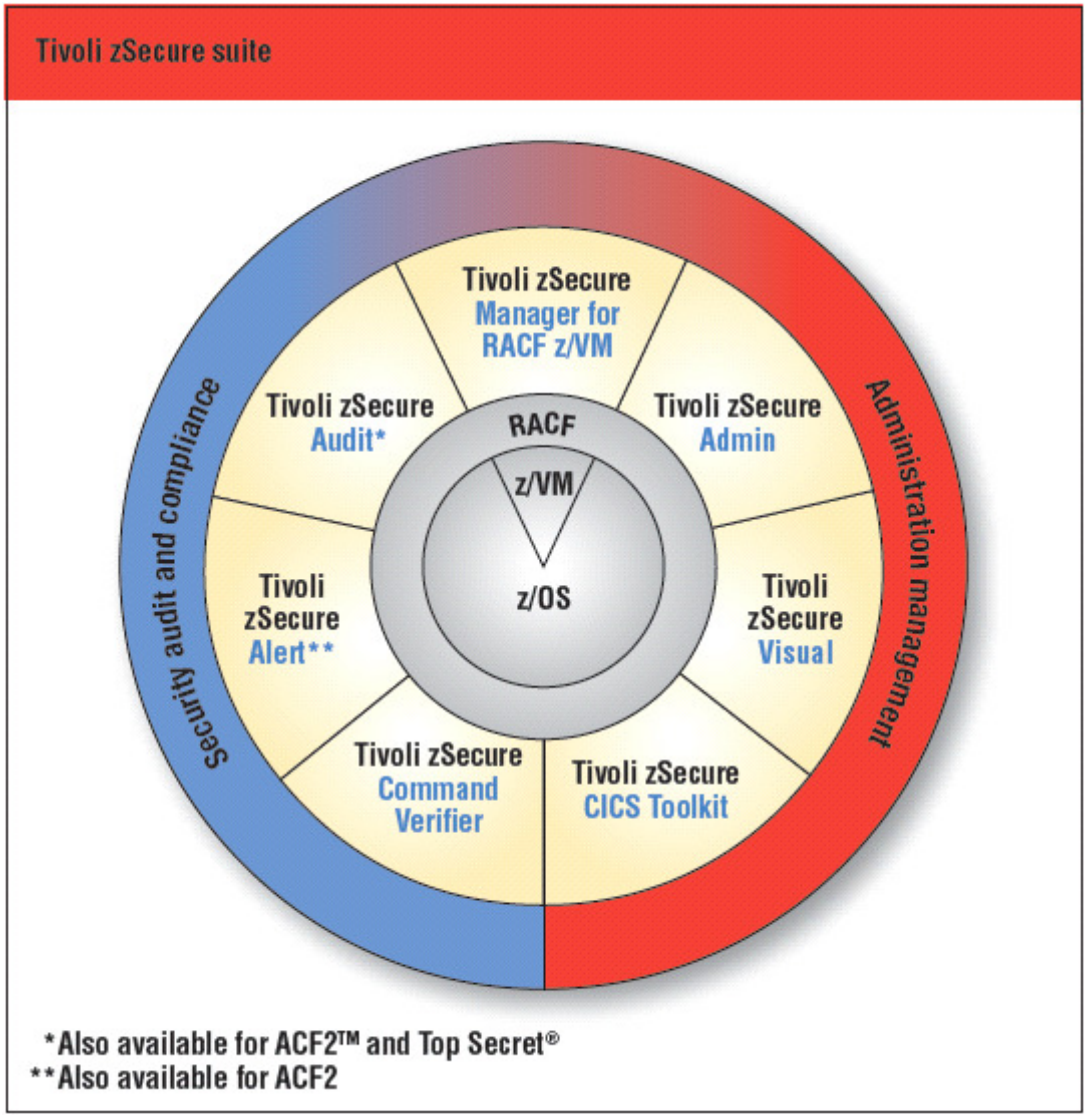
© 2010 IBM Corporation

ACF2 currency support

- ACF2 R12
  - Password phrases
  - Restricted access userids
  - New fields in Global System Options
  - New SMF fields and events
  - Record changes (LID, GSO)

© 2010 IBM Corporation

Globalization



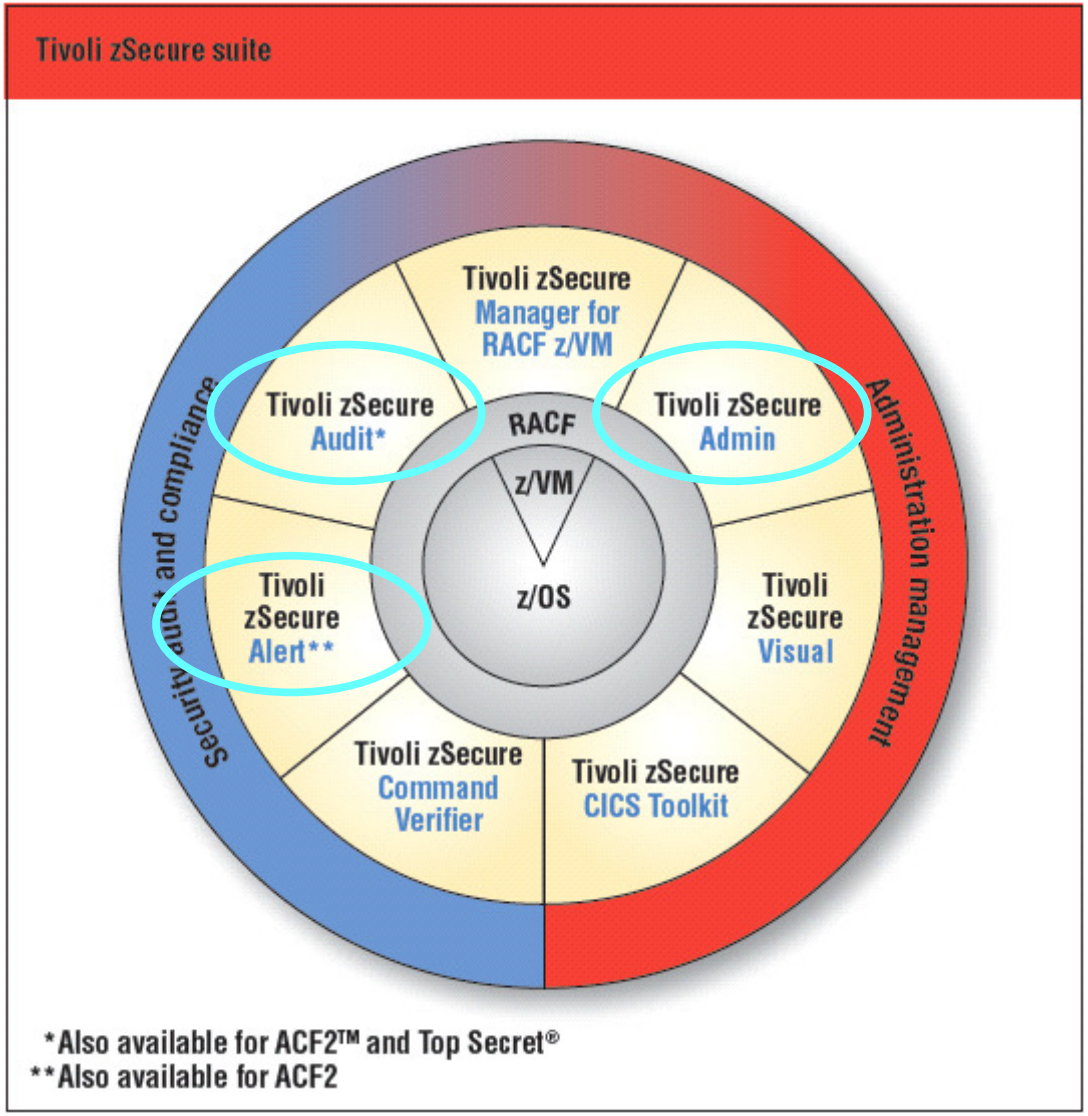
© 2010 IBM Corporation

DBCS support

- FIND command supports partial DBCS strings
- Support DBCS in quoted strings
- WRAP modifier wraps DBCS
  - Overtyping DBCS data is not allowed with WRAP or WORDWRAP
- Reliable switch between SBCS and DBCS
  - SO/SI inserted when fields are wrapped/truncated
- Reports with audit concerns in Japanese
- No mix of English and Japanese in panels
- WORDWRAP understands Japanese hyphenation
  - Kinsoku shori rules
  - Only when column is wide enough

© 2010 IBM Corporation

CARLa update



© 2010 IBM Corporation

Newlist type=SMF fields

- TYPE=42
  - MEMBER (also 14,15), MEMBER_OLDNAME, MEMBER_ALIAS
  - ACTION (INITIALIZE, DELETE, ADD, CHANGE, REPLACE, RENAME, etc)
- TYPE=83
  - Fields from UNIX, long field length
- TYPE=110
  - CICS_TERM, CICS_TTYPE, ELAPSED, EVENT_DATETIME, SUBRECORD, SUBRECORDNO, TRANSACTION, VTAMNET_IS_REMOTE, VTAMNETID
- SPECIALTYPE=OMEG
  - OMCMD_NAME, OMCMD_ALLOWED, OMCMD_TEXT, OMCMD_TYPE

© 2010 IBM Corporation

Newlist type=ACCESS

- Processing of Access Monitor files
- Fields from events and from RACF database
- Used to summarize access monitor files and produce usage reports

© 2010 IBM Corporation

Newlist type=RACF_ACCESS

- One line for each access path to a profile
  - ACL entries and UACC
- Simulated RACLIST
  - Grouping profile(s) memlst merged with transaction(s)
    - Field RACLIST_MERGE=YES
  - Duplicate members from several profiles
    - Field RACFLIST_MERGE=NO
- Access counts
  - From access monitor file(s)

© 2010 IBM Corporation

Simulate resource: merged members

```
simulate class=tcicstrn resource=(CEDA,CEMT,CEMA)

newlist type=racf_access title='Merged profiles matching CEMA',
  emptylist='Nothing matches CEMA'

  s class=%cicstrn resource=cema raclist_merge=yes

  sortlist member_class member_key(17),
           class profile(17) proftype id access
```

```
R A C F   A C C E S S   A U T H O R I Z A T I O N S
Merged profiles matching CEMA

MemClass Member key       Class    Profile          Type      Id       Access
TCICSTRN CEM*             GCICSTRN ER50414.RND2     GENERIC   -UACC-   NONE
```


© 2010 IBM Corporation

Compare snapshots

- Compare records from one or multiple sources
- Identify and show changes in selected fields
  - Give the compare option a newlist type
    - COMPAREOPT TYPE=RACF
  - Specify a label
    - e.g. NAME=PRIV_CHANGES
  - Identify the key of an observation
    - e.g. BY=(CLASS,PROFILE,SEGMENT)
  - Identify the base to compare against
    - e.g. BASE=(COMPLEX=GOLD)
  - Specify what to compare
    - e.g. COMPARE=(SPECIAL,OPERATION,AUDITOR)

© 2010 IBM Corporation

Compare snapshots

- Specify what to show
  - Additions, deletions, changes, changes that are improvements, changes that reduce security, differences

  – e.g. SHOW=DIFF

© 2010 IBM Corporation

Find profiles that were added with privileges

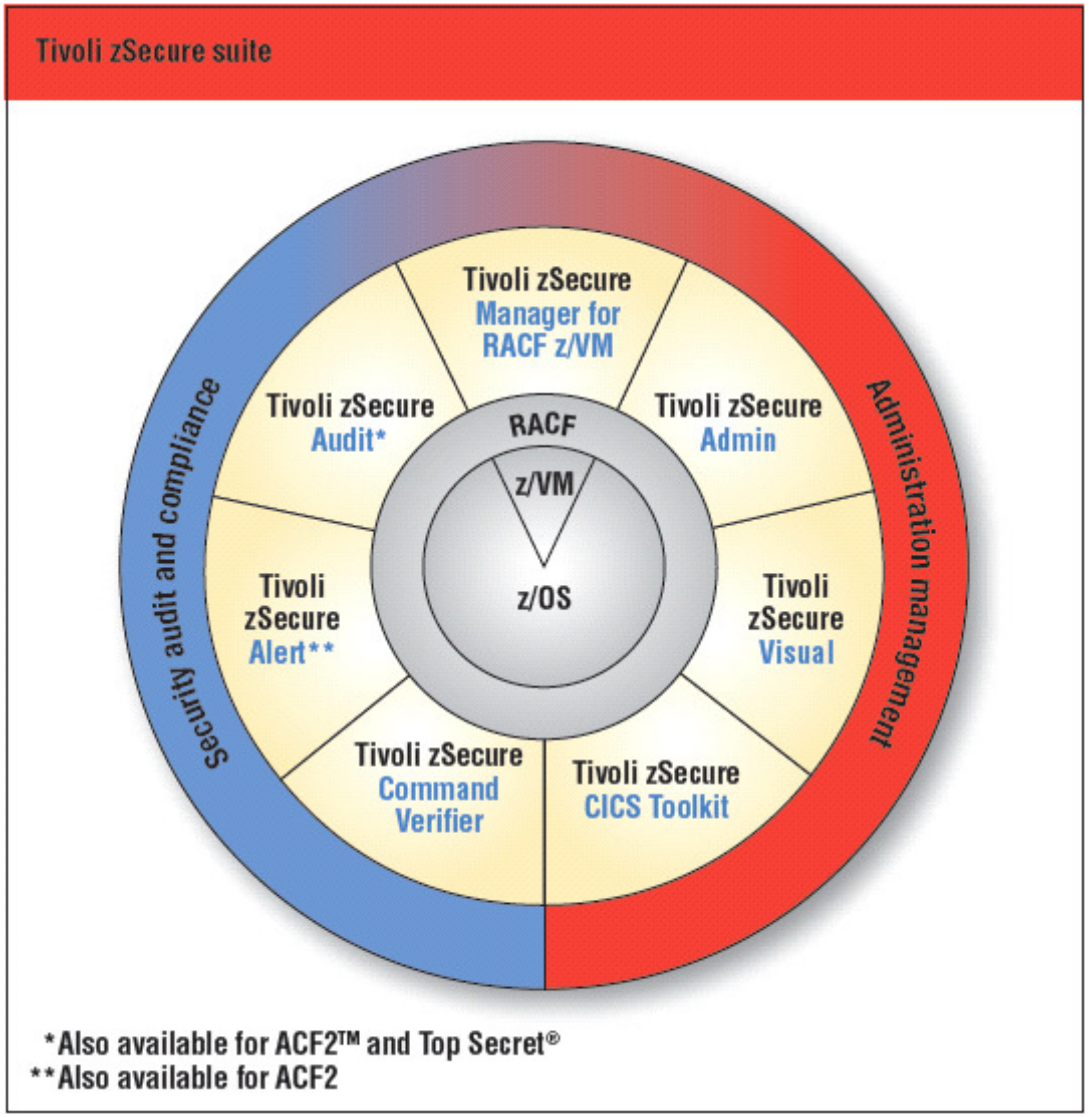
```
alloc type=unload complex=gold    dsn=CKR.BACK1DAY.UNLOAD
alloc type=racf   complex=current active
compareopt name=priv_add,
           type=racf,
           by=(class,profile,segment),
           base=(complex=gold),
           compare=(special,operations,auditor),
           show=add
newlist type=racf compareopt=priv_add
  select class=user segment=base complex=(gold,current),
         (special or operations or auditor)
  sortlist profile(8) special,operations,auditor
```

```
P R O F I L E S   T H A T   W E R E   A D D E D

Profile  Spc Opr Aud
NEWG     YES
NEWSA    YES
NEWTH    YES
```


© 2010 IBM Corporation

Availability and Support



© 2010 IBM Corporation

Supported platforms

- Supports z/OS 1.11
  - Also runs on (some) older z/OS releases
    - Formal support for z/OS 1.4 and newer
    - zSecure Visual server requires z/OS 1.6 and newer
- CICS TS 2.1 through 4.1
- CA ACF2 and CA TSS release 8 through 12
- DB2 up to release 9.1
- zSecure Visual
  - Tested with Windows XP SP2 and SP3, Vista, Windows 7

© 2010 IBM Corporation

Availability

- Announcement November 3, 2009
- GA November 6, 2009
  - Order via Shop z
    - https://www14.software.ibm.com/webapp/ShopzSeries/ShopzSeries.jsp
    - http://www.ibm.com/systems/z/os/zos/buy.html
- zSecure for RACF z/VM
  - Current version 1.8.1
    - PTF for z/VM 5.3 and 5.4 available
- Check for additional PTFs on Shop z

© 2010 IBM Corporation

Documentation

- Manuals in PDF and HTML format
  - See Tivoli zSecure Information Center
  - No more BookManager
- zSecure Visual help converted to Eclipse help plugin
- RACF Offline integrated into Admin+Audit manual
- Installation and Deployment guide
  - Access Monitor and RACF Offline setup added
  - Installation options and steps clarified
- Quick Reference Guide updated
  - CA TSS fields indicated
  - Available online

© 2010 IBM Corporation

Get involved

- A large percentage of new functions and features are driven by customer requirements
- We welcome your suggestions for improvements
  - submit them through **www.ibm.com**
- Join the zSecure Advisory Council to have your say on new release content
  - send an e-mail to **glinda@us.ibm.com**
- Want to share ideas, best practices, CARLa programs or how do I questions?
  - Join the zSecure forum at:-
    http://www.ibm.com/developerworks/forums/forum.jspa?forumID=1255

© 2010 IBM Corporation

Useful resources

zSecure Homepage: http://www-01.ibm.com/software/tivoli/products/zsecure/

zSecure 1.11 information center:
http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.zsecure.doc/welcome.html

zSecure release note information:
http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.zsecure.doc/releaseinfo/releaseinformation.html

zSecure forum: http://www.ibm.com/developerworks/forums/forum.jspa?forumID=1255

zSecure Redbook: http://www.redbooks.ibm.com/abstracts/sg247633.html?Open

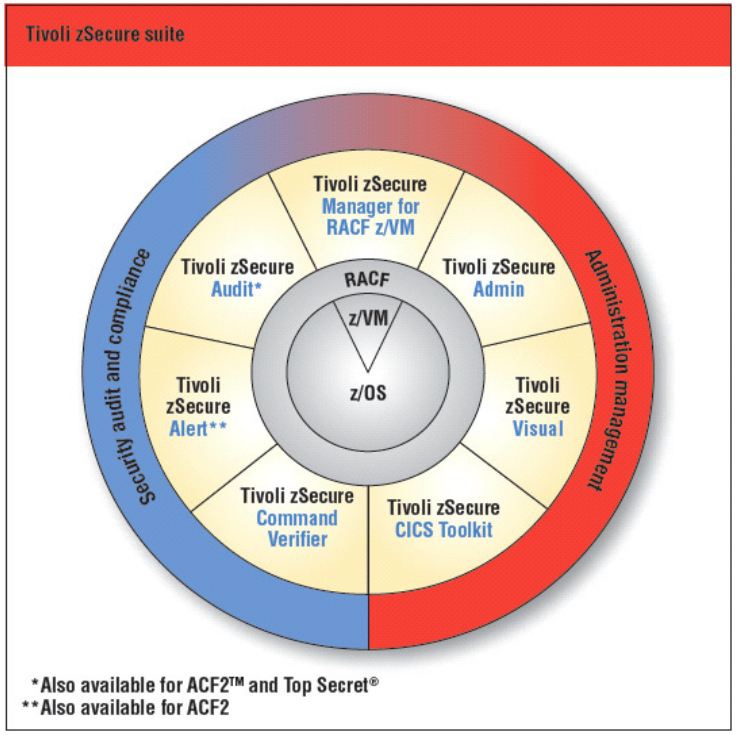
© 2010 IBM Corporation

Education

- Current education offerings for zSecure include:-
  - Basic Administration and Reporting (3 days)
  - RACF Management Workshop (2 days)
  - RACF and SMF Auditing (2 days)
  - z/OS UNIX System Services (USS) Security Overview (1 day)
  - CARLa Auditing and Reporting Language (3 days)
    - Classes can be run onsite or offsite
- For more details, please visit:-
  - http://www-01.ibm.com/software/tivoli/education/edu_prd.html

© 2010 IBM Corporation

Questions?



© 2010 IBM Corporation