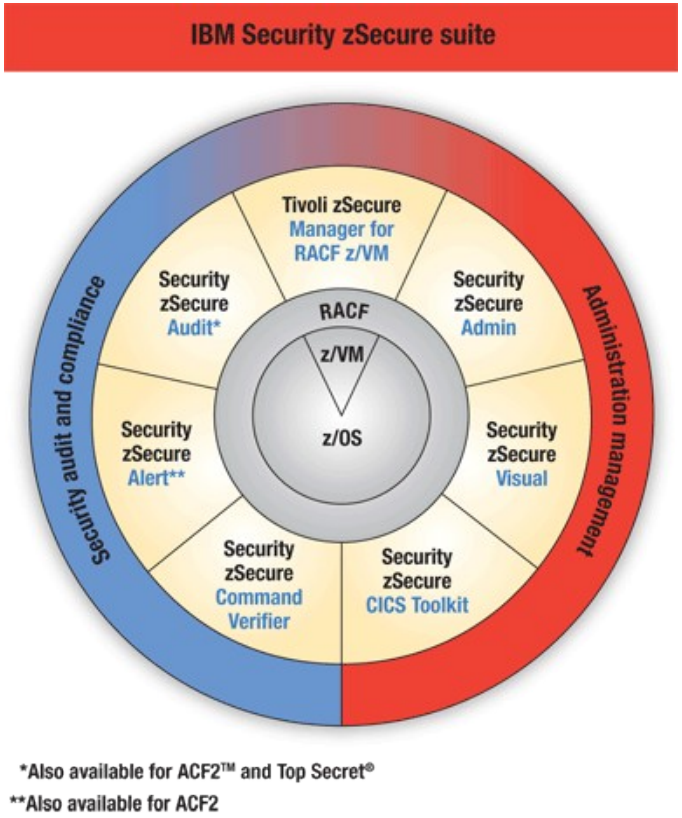
zSecure update

Multi-system support



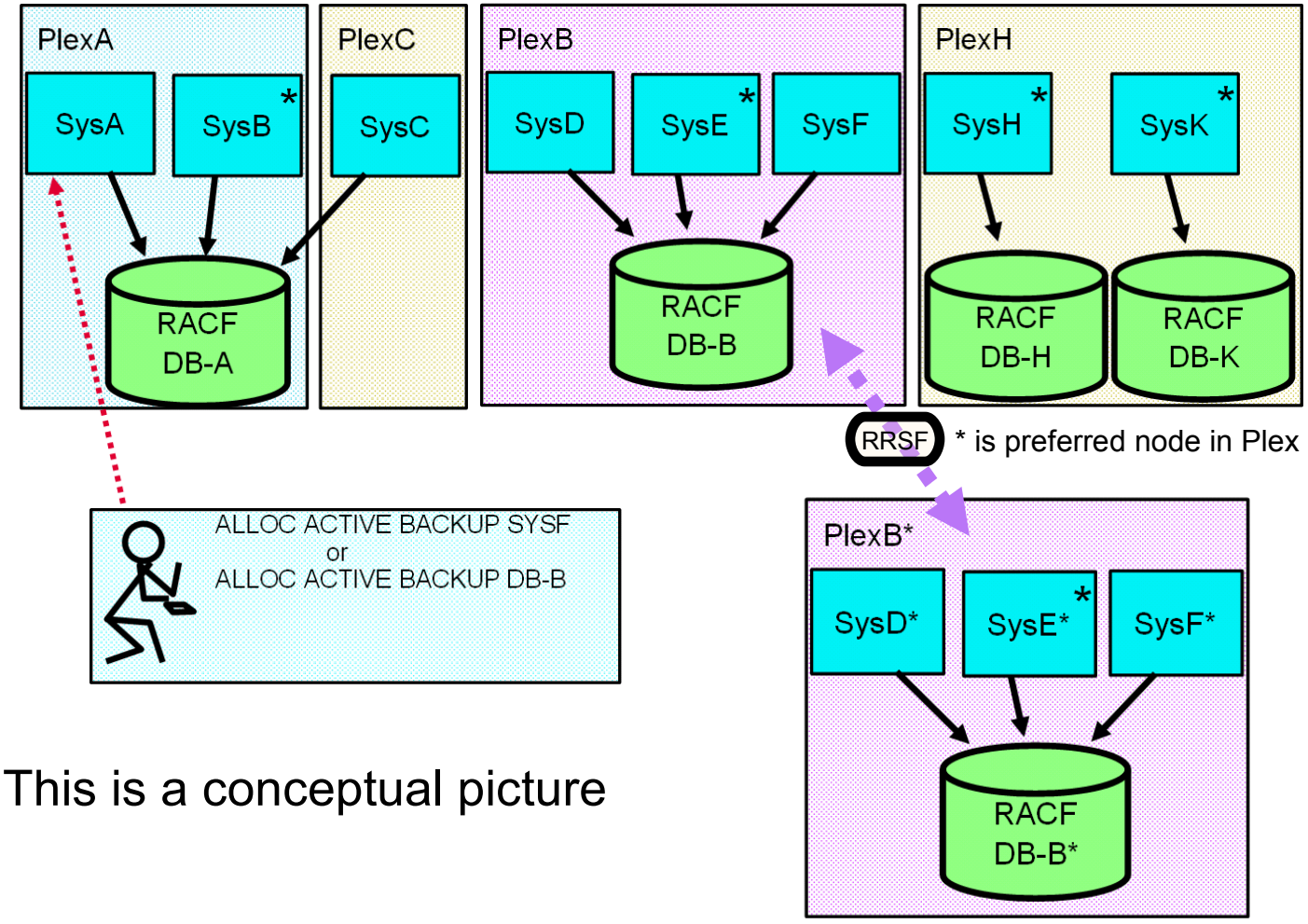
zSecure Admin

zSecure Audit

zSecure Visual

Release 1.12

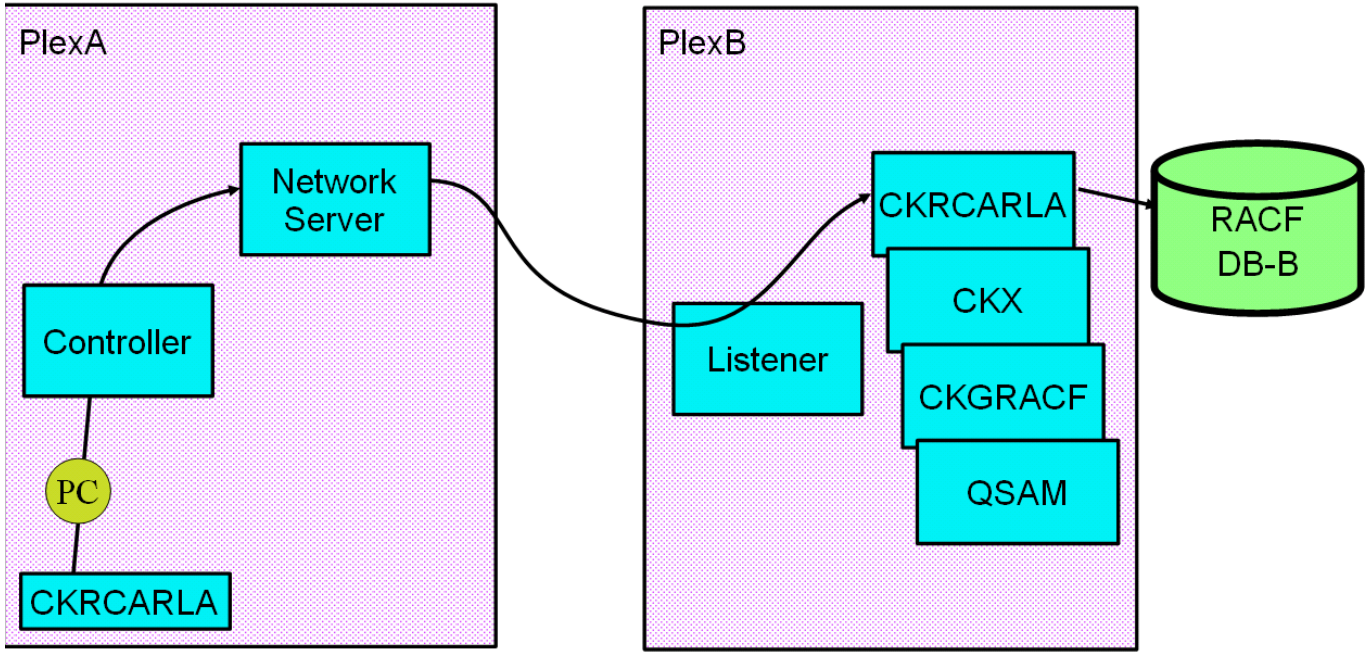
Multi-system support – Nodes and systems



- This is a conceptual picture

Multi-system support – zSecure server CKNSERVE

- zSecure Server network
  - CARLa engine talks to local server, which talks to remote server



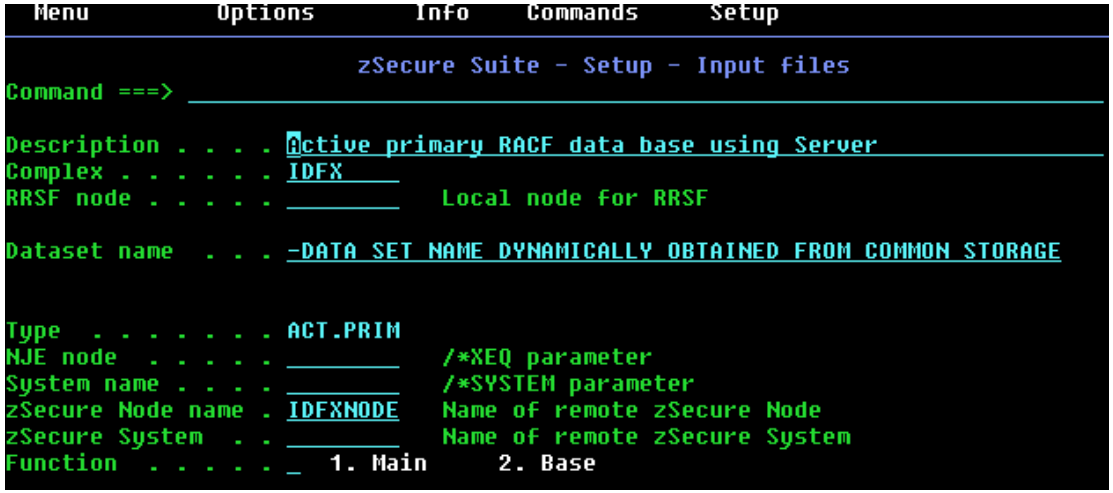
- The Controller and Listener are part of the CKNSERVE server program
  - Server Token field in SETUP RUN to specify name of the local server.

Data from multiple live systems in a single session Updates to multiple RACF databases with/out RRSF

- Multi-system support requirements
  - ✓ Administer multiple systems from a single application instance
    - ✓ Live data access
    - ✓ Fast data access
  - ✓ Allow sending the same commands to multiple systems
    - ✓ Use RACF Remote Sharing Facility network if present
      - ➢ Support for AT and for ONLYAT keywords
    - ✓ Without RRSF network
      - ➢ TCPIP connection
  - ✓ Use data encryption
  - ✓ Only minor modifications to the existing User Interface

Multi-system support – specifying data sources (1/4)

- The data set detail panel of the SETUP FILES menu allows specifying remote destinations



✓ zSecure Node – by Plex

✓ zSecure System – system

! When both zSecure Node and zSecure System are specified, they must belong together. Unless you want to enforce such a check, it is better to only specify zSecure Node for a database.

Multi-system support – specifying data sources (2/4)

- The following data sources are supported remotely
  - ✓ Active primary RACF database
  - ✓ Active backup RACF database
  - ✓ Backup ACF2 database
  - ✓ Active SMF
  - ✓ Active CKFREEZE (=system snapshot)
  - ✓ Catalogued data sets on request (by name)

! When ACTIVE is used – and information from an active CKFREEZE is needed – a remote mini-CKFREEZE is automatically allocated and used

Multi-system support – specifying data sources (3/4)

- If you do not specify a Complex name a default is assigned

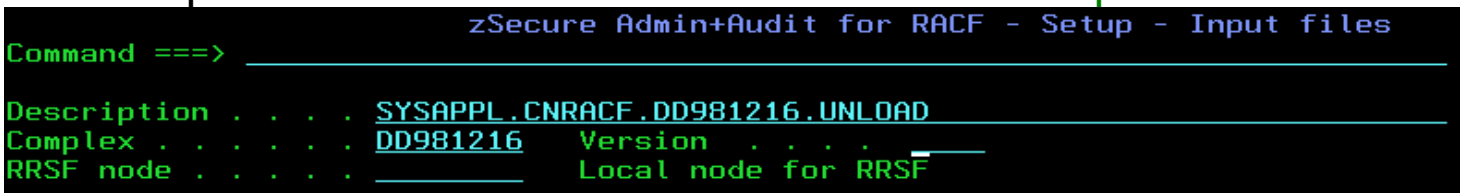
- Assignment of the default name has changed in this release.
  For CKFREEZE:
  1. RRSF node name
  2. Sysplex name
  3. Sysname
  - The default used to be the SYSID (“SMF id”)

  For a database the SYSID is used to link it to a CKFREEZE (etc.)

  For SMF files processing is (still) per record

Multi-system support – specifying data sources (4/4)

- The data set detail panel of the SETUP FILES menu now also allows specification of a Version in addition to Complex



- With different Versions data is treated as belonging to different points in time, thus causing DASD volumes to not be shared, RRSF nodes to be distinct, etc.
- To a large extent this means that Version acts much like Complex
- In most of the UI Version has not been added to the displays. Different Complex values must be used for report clarity

! Version *has* been added to the AU.S – MVS Extended - DASDVOL display, where Complex has a different function

Multi-system support – viewing reports

- The UI was already designed to work with multiple complexes
  - With shared DASD you could access foreign databases etc.

- In some places Complex was added

- E.g. menu option RA.3.G (Compare users):

```
Enter S in front of a class for more info       16 Dec 1998 00:05
   Class    Complex  Profiles C##MBJTI  C##BJT2
__ DATASET  DD981216       12 ALTER    ALTER
__ DATASET  DINO           48 ALTER    ALTER
__ FACILITY DD981216        6 READ     ALTER
__ FACILITY DINO           10 READ     ALTER
__ XFACILIT DINO            5 READ     ALTER
```

Multi-system support – compare databases

- SETUP VIEW has a new option for tweaking the RA.U/G/D/R menus:

  `/ Add summary to RA displays for multiple RACF sources (normally on)`

  This is a new kind of summary designed to highlight differences

  Flags and such: shows percentage of complexes for which it is true

  Text etc: shows value if all the same, or the *common prefix* followed by >

  Numbers and such: shows value if all the same, or <more>

- Let's look at two similar databases:

```
   User      # Name                 DfltGrp  Owner     Rev Ina Res Ptc Spc Opr
__ CERT004   2 TESTUSER DIG.CERT    C##B     SYSAUTH   100  50   0 100   0   0
s_ CERT005   2                      SYS>     <more>     50   0   0 100   0   0
```

  - ✓ These userids occur in both databases (the 2 under #)
  - ✓ CERT004 has all the same values, except for the `revoke_inactive` flag (50%)
  - ✓ CERT005 has two different owners, with no common prefix (hence <more>)

```
   User      Complex  Name                DfltGrp  Owner    RIRP SOA gC LCX Grp
__ CERT005   DD981216                    SYSPROG  C##BMR1                X   1
__ CERT005   DINO                        SYSAUTH  SYSAUTH  R             X   1
```

Multi-system support – command routing (1/2)

- SETUP CONFIRM has a new option for command routing:

```
                        zSecure Admin+Audit for RACF - Setup - Confirm
Command ===>

Action on command . . 2  1. Queue    2. Execute  3. Not allowed
Confirmation  . . . . 4  1. None     2. Deletes  3. Passwords      4. All
Command Routing . . . 2  1. Ask      2. Normal   3. Local only
```

'Local only' means that all commands go to the local system

'Ask' means that a prompt must always be shown to ask for the destination

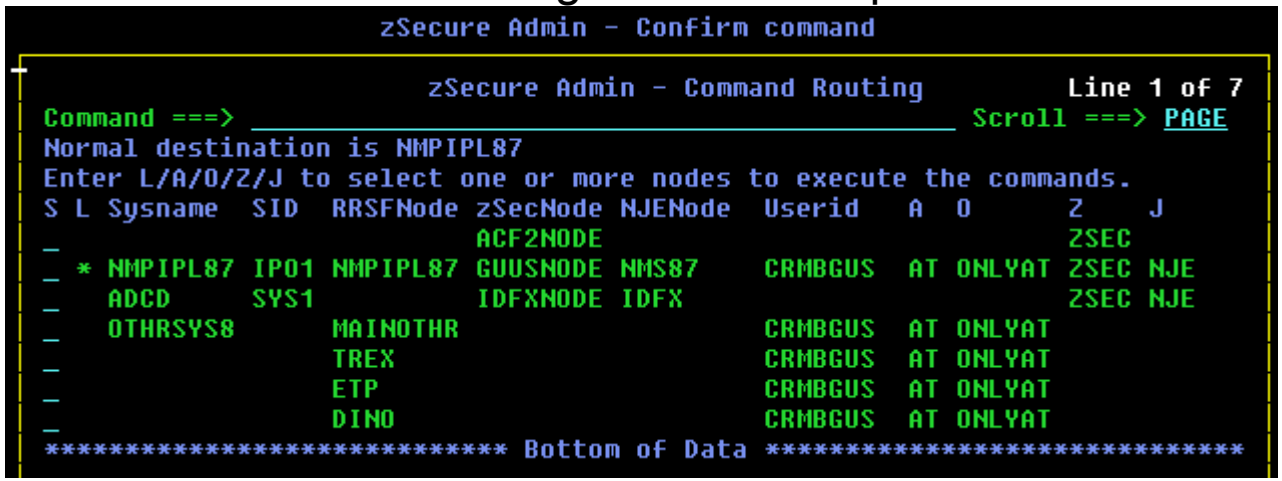
The default 'Normal' option means that

- ✓ Commands for a local data source go to the local system
- ✓ Remote routing order of preference:
  1. zSecure Node or zSecure System (for a database)
  2. RRSF node (for a database), with the AT keyword
  3. NJE node specified

! PTF warning: Action on command Execute will more often execute immediately, e.g. when copying a user (UA59956)

Multi-system support – command routing (2/2)

- In ‘Ask’ mode the following confirmation panel is shown:



Routing options are: Local, to an RRSF node using At or Onlyat, to a zSecure Node, or to an NJE (JES) node

- First the server is located, then the command is issued under the “user” authority, and feedback is passed back to the user.
- Routing can work on a single command or on a data set, in which case the zSecure Command Execution Utility (CKX) is used

RRSF support – RRSF nodes report

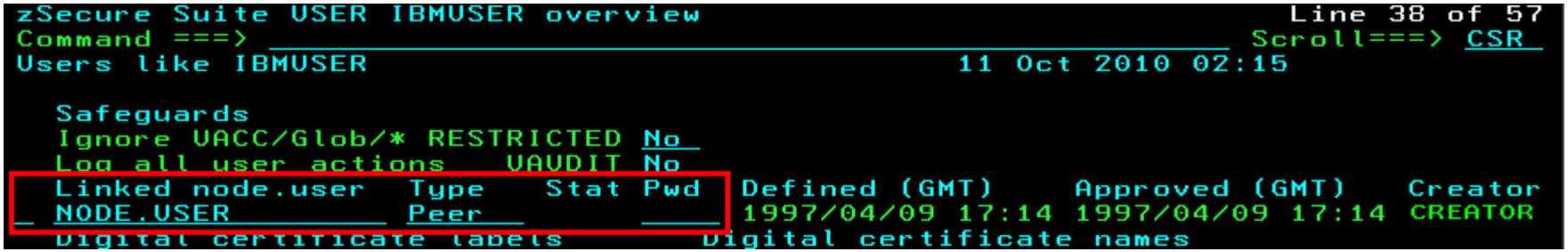
- Report on RRSF nodes added to AU.S – RACF control

```
RACF remote sharing facility nodes                                Line 1 of 12
Command ===>                                                   Scroll===> CSR
                                                    12 Oct 2010 00:07
   Complex  System   Local Node #Nodes
   DINO     EEND     EEND           12
   TargNode TargSysn TStat Loc Main Prot LUName   ModeName TPName   Description
__ EEND     EEND     O-A   Yes No   APPC EENDLU01          IRRRACF  EEND/GANS l
__ DINO              D-L   No  No   APPC DINOLU01          IRRRACF  RRSF NODE D
__ I522              D-L   No  No   APPC I522LU01          IRRRACF  RRSF NODE I
__ O110              D-L   No  No   APPC O110LU01          IRRRACF  RRSF NODE O
__ O130              D-L   No  No   APPC O130LU01          IRRRACF  RRSF NODE O
```

- The Target State shows D-L for Dormant-Local, O-A Operational-Active, etc.

- Additional details are available after zooming in

RRSF support – RACLINK overtype



- Admin: Line commands and overtype for RACLINK field

  A – approve pending user ID association

  C – copy existing association to define a new one

  D – undefine a user ID association

  I – define a new association

- This support allows e.g. to establish password synchronization between two user IDs for the same user

RRSF support – VERIFY and MERGE

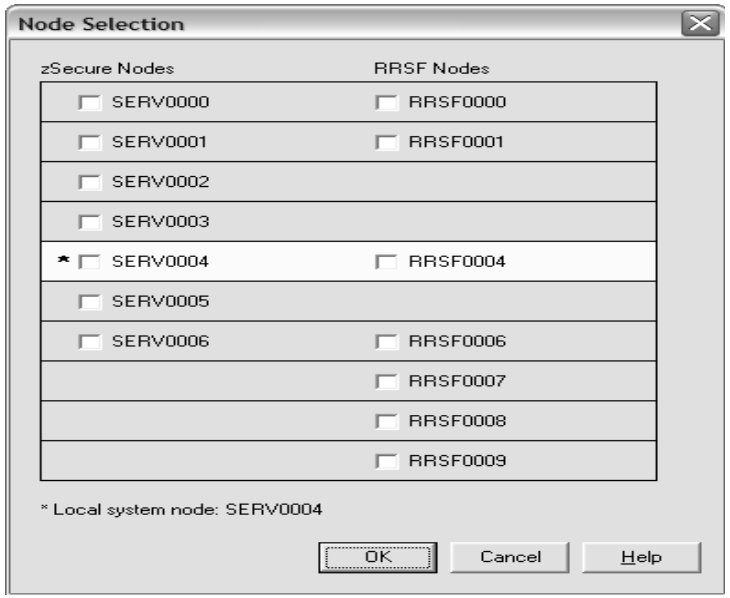
- VERIFY PERMIT, EMPTY, and ALLNOTEMPTY are now aware of RRSF
  - ✓ Userids and data sets will not be deleted when still in use on a connected RRSF node
    - ➢ Provided that information is available
    - ➢ Unless OPTION ONLYAT requests to do so
  - ✓ CKGRACF USER RACLINK UNDEF [(*node.id*)]
    - ➢ Can remove one-sided assocations
- MERGE will generate RACLINK DEFINE and RACLINK APPROVE as well as RACLINK UNDEFINE and CKGRACF… RACLINK UNDEFINE.

Multi-system and RRSF support – zSecure Visual

- Visual client can run with or without multi-system services

  Indicate the desired mode in the option form before logon

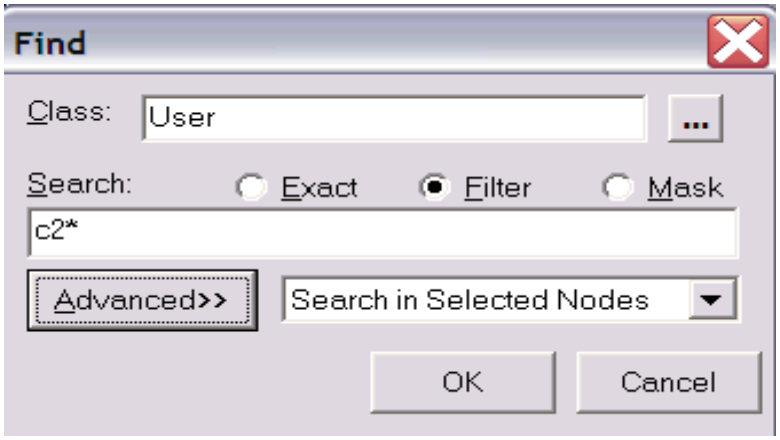
  - ➢ Checkbox ‘Use zSecure Server for multi-system services’
  - ! Must logoff and re-logon to change mode
- After logon, choose the zSecure and RRSF nodes to work with



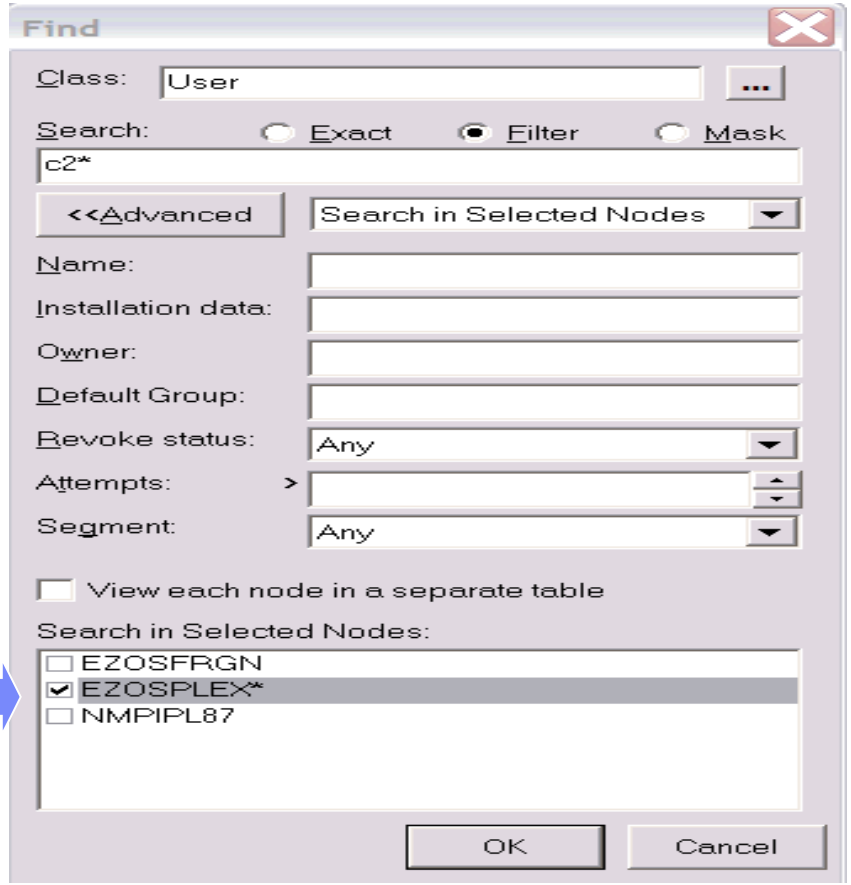
➢ During the session the ‘Available nodes’ menu option can be used to change the set of nodes being worked with

Multi-system and RRSF support – zSecure Visual

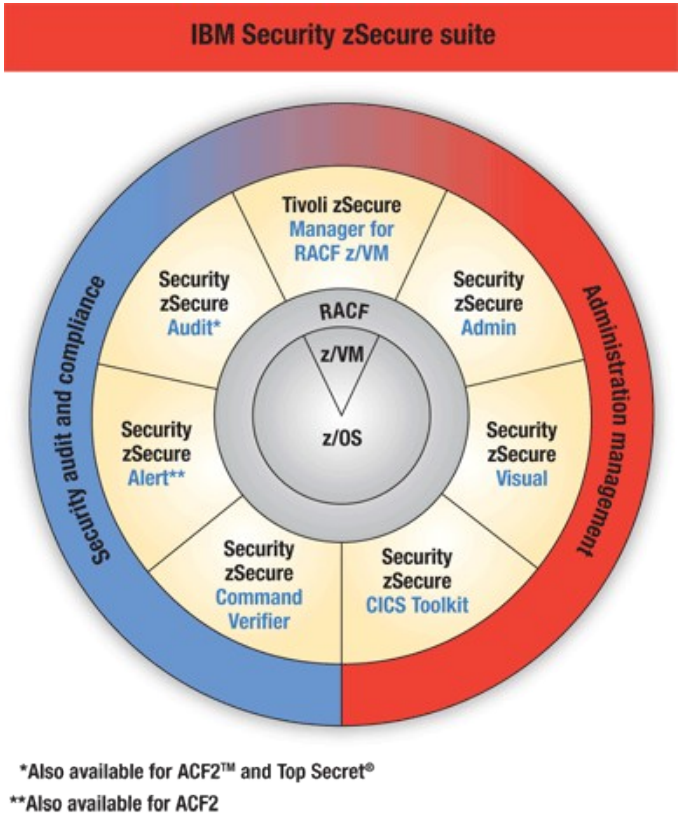
- Find dialog allows fine-tuning the search



- The basic Find dialog uses all nodes being worked with
- The Advanced Find dialog allows more specific search



Block commands



zSecure Admin

zSecure Audit

Release 1.12

Apply command to multiple records on a display

- zSecure 1.12 introduces block commands on ISPF displays:
  - Admin: RR..RR to Recreate multiple profiles
  - Admin: DD..DD to Delete multiple profiles
- Commands for all selected records are executed at once
  - *Also* when a single R or D command is used multiple times
  - Selection by R is combined with RR..RR, and D with DD..DD
- In addition a primary command FORALL is provided
  - With no selection, it applies a command to all records on the display
  - Z and ZZ..ZZ or X and XX..XX can be used to select/exclude records
  - Combining selections (Z) with exclusions (X) is not allowed

Block commands – FORALL (1/3)

- The command to be executed can either be specified after FORALL on the command line, or entered in the panel that opens when the command is issued without arguments.

- The command can specify substitution variables like !KEY

  These will be substituted in each record (e.g. by the profile key)

- The command is passed as entered, except it is scanned for exclamation marks(!) to replace the substitution variables

  To actually include an exclamation mark in the command, double it

- The period (.) can be used to explicitly end a variable name

  Like in JCL, double the period in this position if you want one

Block commands – FORALL (2/3)

```
zSecure Audit for RACF USER overview                          Line 325 of 1776
Command ===> forall                                            Scroll===> CSR
All users                                          8 Oct 2010 00:07
   User      Complex  Name                 DfltGrp  Owner    RIRP SOA gC LCX Grp
zz C##CY30   DINO     TEST USER            C##C     C##C     R              X   2
__ C##CY31   DINO     TEST USER            C##C     C##C     R              X   2
zz C##CY32   DINO     TEST USER            C##C     C##C     R              X   2
__ C##CY33   DINO     TEST USER            C##C     C##C     R              X   2
z_ C##CY34   DINO     TEST USER            C##C     C##C     R              X   2
__ C##CY35   DINO     TEST USER            C##C     C##C     R              X   2
```

- Selects users C##CY30, C##CY31, C##CY32, and C##CY34
- FORALL without parameters calls up the command entry panel

Block commands – FORALL (3/3)

```
                    zSecure Audit for RACF - FORALL Command Shell
Enter FORALL command below:


===> altuser_!key_owner(c##arob)_____________________________________________
_______________________________________________________________________________
_______________________________________________________________________________


Place cursor on choice and press enter to retrieve command
=> /* test !key !class !type */
=> altuser !key tso(maxsize(0))
=> list!class !key
```

- The command entry panel is similar to ISPF option 6
- The command is not limited to RACF, it could be your own REXX

Block commands – act on record level

- The FORALL command works on the record display level
  - ➢ Summary levels may require zooming in repeatedly
  - ✓ RA.R now has an option “Summarize by class”

    This will be **on** on initial migration to 1.12.0 for compatibility

    The setting is saved in the ISPF profile

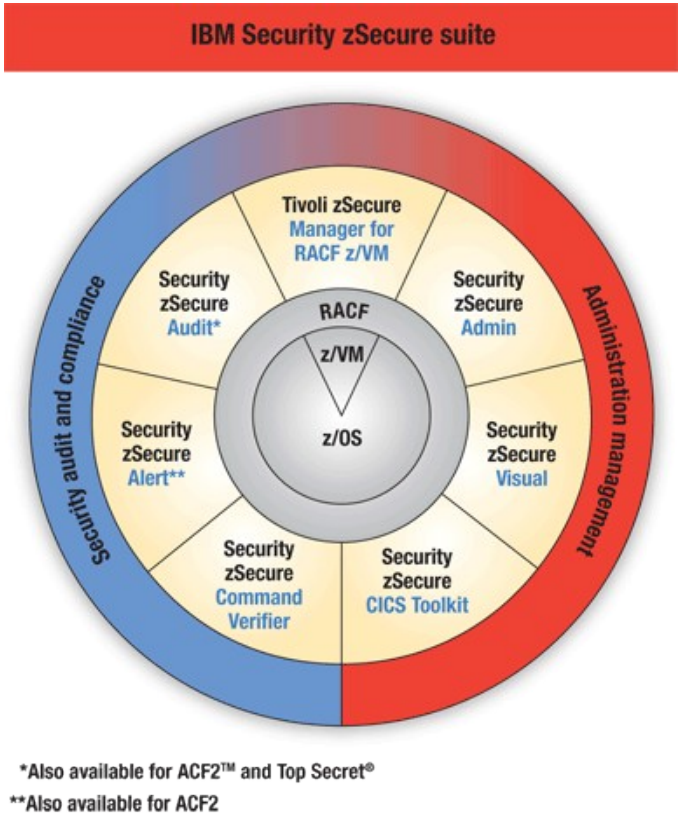
➢ If you run with multiple complexes, also think of SETUP VIEW

_ Add summary to RA displays for multiple RACF sources (normally on)

✓ Commands go into the appropriate CKRCMD for each complex

! PTF warning: These commands execute immediately (UA59956)

z/OS UNIX administration



zSecure Admin

Release 1.12

z/OS UNIX administration (1/2)

- z/OS UNIX reports are now available in zSecure Admin
  - Before, they were only available in zSecure Audit
  - The RE.U menu is extensively described in the zSecure 1.10.0 Global Overview

- U line command brings up ISPF's z/OS UNIX Directory List Utility, which can be used display directories and edit, browse, delete, rename, or copy files, as well as modify file mode fields and extended attributes, and execute commands.

```
IBM Tivoli zSecure UNIX summary                          11 s elapsed, 2.8 s CPU
Command ===> ____________________________________________________ Scroll===> CSR
Files for complex like :'tomo'c                  28 Nov 2008 00:07
   Complex  System   Count
   EEND     EEND         6
   Count FS mount point
       2 /u
   T FileMode  + apsl AuF Owner    Group    Relative pathname (within FS)
u_ d r-xr-xr-x        fff C##BHJ1  OMVSGRP  automount
__ d r-xr-xr-x        fff C##BHJ1  OMVSGRP  automount2
****************************** Bottom of Data ******************************
```

z/OS UNIX administration (2/2)

- On z/OS V1R12 this immediately brings up this panel:

```
                              z/OS UNIX Directory List            Row 1 to 3 of 3
Command ===>                                                     Scroll ===> PAGE

Pathname . : /u/automount

Command  Filename        Message          Type Permission Audit  Ext  Fmat
-------------------------------------------------------------------------------
________ .                                Dir  r-xr-xr-x  ------
________ ..                               Dir  rwxr-xr-x  fff---
/_______ c##bjti                          Dir  rwx------  fff---
```

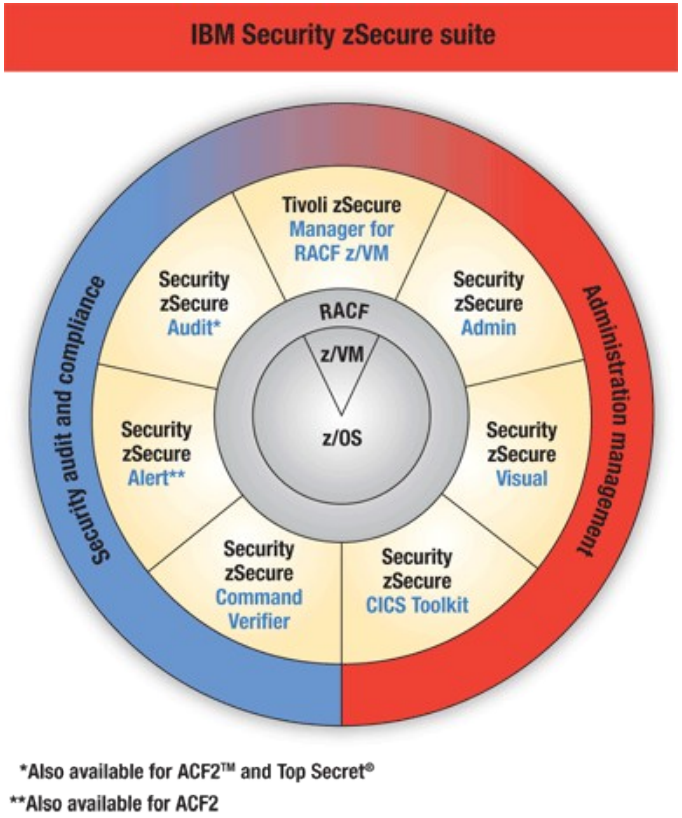
! The DIRLIST service invoked acts on directories. For a file the directory it is contained in will be shown; the end user must locate the file themselves.

! This service works on the local live z/OS UNIX

  - Requires read permission (file permission, or RACF auditor, UID(0), access to FACILITY BPX.SUPERUSER or UNIXPRIV BPX.FILESYS.**, …)

- Once here, / brings up the available commands
- Free form commands can be entered via 12 Execute command

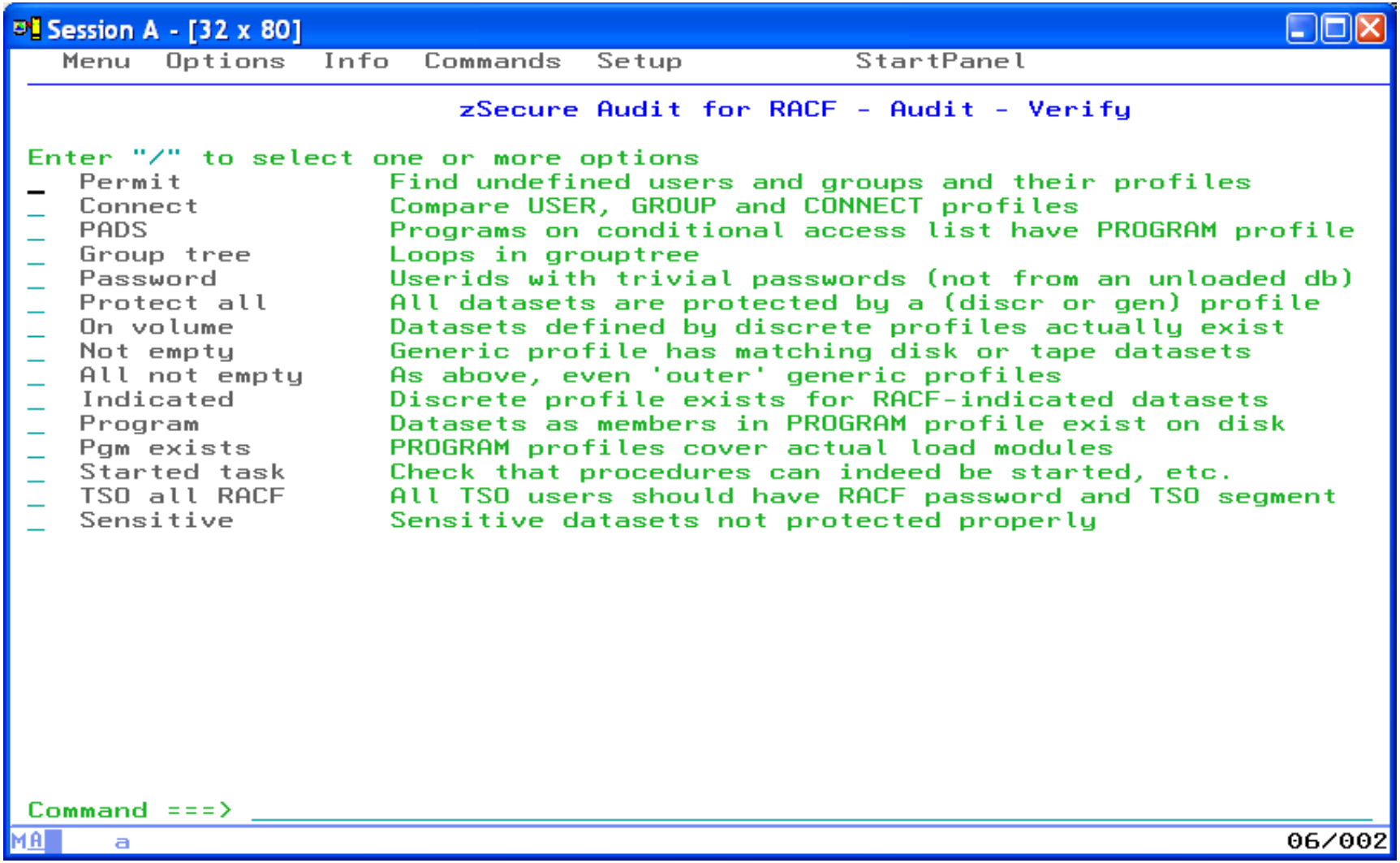
Access Monitor



zSecure Admin

Release 1.11

Verify consistency of RACF vs. z/OS



Analysis of Access Monitor files

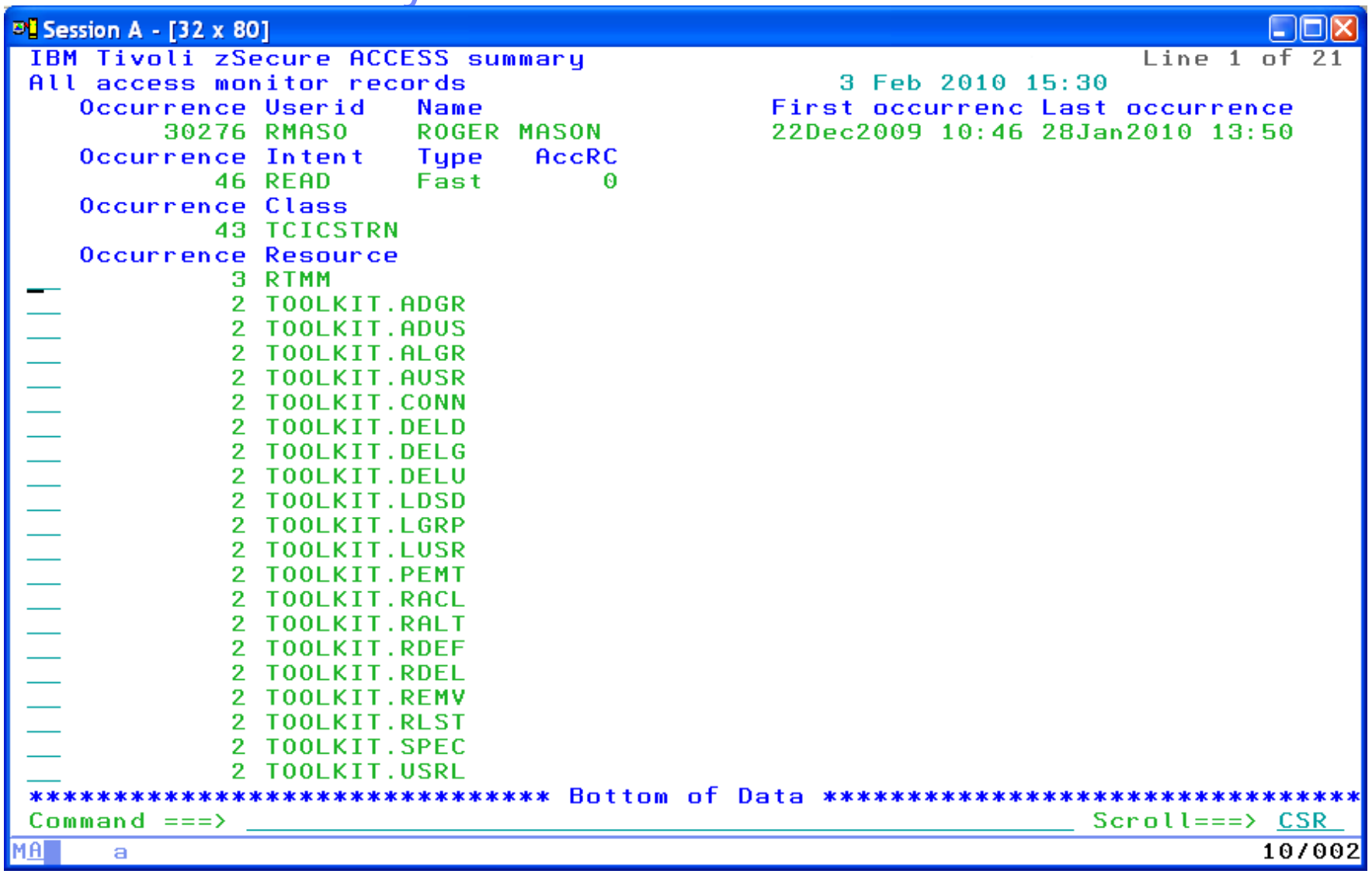
- New menu option in zSecure Admin
  - AM - Access Monitor
    - Analyzes Access Monitor file(s)
  - Which resources has a specific user accessed
    - In last month, in last year?
    - When was last access?
  - Who has accessed a given resource?

Access summary by user

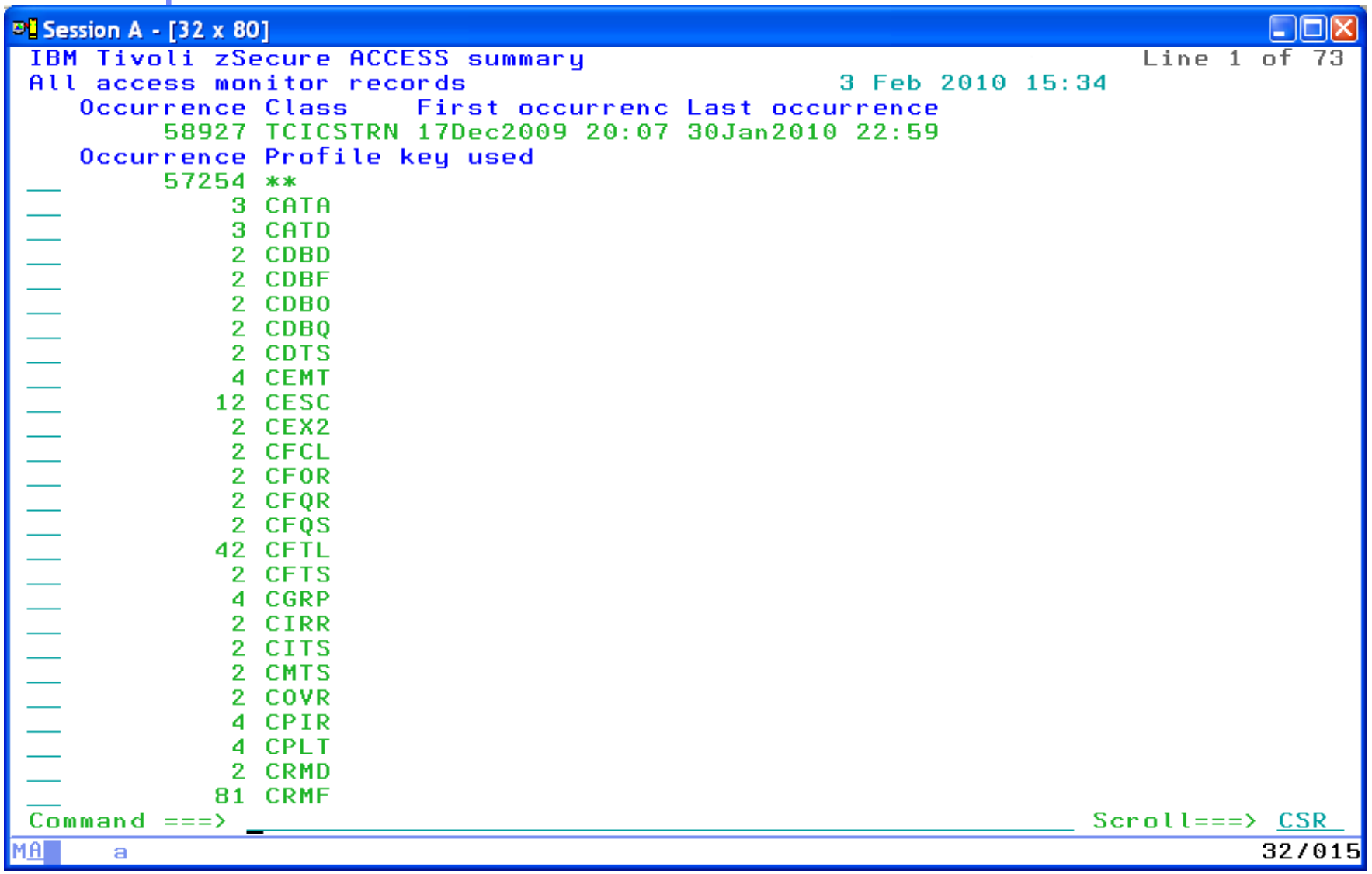
Session A - [32 x 80]

```
IBM Tivoli zSecure ACCESS summary                          1 s elapsed, 1.1 s CPU
All access monitor records                          3 Feb 2010 15:30
   Occurrence Userid   Name                    First occurrenc Last occurrence
__       1362                                 17Dec2009 21:57 30Jan2010 00:07
__          4 *                               18Dec2009 17:40 18Dec2009 17:41
__         37 *BYPASS*                        17Dec2009 20:06 19Jan2010 10:04
__          2 CICSUSER CICS DEFAULT USER      17Dec2009 20:07 19Jan2010 09:05
__       2654 CKR                             17Dec2009 23:00 30Jan2010 23:00
__      48725 C2PSUSER ZSECURE ALERT STC      17Dec2009 17:53 30Jan2010 23:00
__        533 C2RSERVE ZSECURE VISUAL SERV    17Dec2009 20:06 19Jan2010 09:36
__         48 DFS                             17Dec2009 20:06 26Jan2010 10:49
__         28 EREP     EREP                   17Dec2009 20:06 24Jan2010 00:00
__         16 FTPD                            25Dec2009 14:30 25Dec2009 14:48
__      14180 GEOFF    GEOFF ROUSELL MAIN     17Dec2009 18:24 26Jan2010 12:46
__        178 LDAPSRV  LDAP SERVER            17Dec2009 20:07 29Jan2010 23:59
__       7528 LENNIE   LENNIE DYMOKE-BRADSH   21Dec2009 11:43 22Dec2009 15:06
__       1904 LENNIE2  LENNIE DYMOKE-BRADSH   22Dec2009 10:48 22Dec2009 11:15
__        687 MILOS    MILOS KALJEVIC         25Dec2009 13:28  4Jan2010 09:11
__          3 OMVS     OMVS                   21Dec2009 11:45 21Dec2009 11:45
__     104678 PEASEJ   JAMIE PEASE GB TIV     17Dec2009 18:07 24Jan2010 18:21
__       1016 PEASEJ2  JAMIE PEASE - CV ID    17Dec2009 20:44  8Jan2010 13:21
__       1276 PEASEJ3  JAMIE PEASE - VIS ID   17Dec2009 21:24 22Dec2009 12:57
__      30276 RMASO    ROGER MASON            22Dec2009 10:46 28Jan2010 13:50
__       4104 ROBVH    ROB VAN HOBOKEN        13Jan2010 09:27 14Jan2010 13:01
__        228 ROBVH2   ROB VAN HOBOKEN        14Jan2010 13:03 14Jan2010 13:24
__       6551 SMTP     SMTP                   17Dec2009 20:19 30Jan2010 00:07
__        136 STC      STARTED TASK           17Dec2009 20:08 30Jan2010 00:00
__          6 STCRACF  CB390 TRACE WRITER     17Dec2009 20:06 19Jan2010 09:05
__        183 STSGJJB  JO JOHNSTON             6Jan2010 10:28  6Jan2010 10:28
__      59826 SYSSTC   SYSTEM STC              17Dec2009 20:06 30Jan2010 22:59
__         12 SYS1                            17Dec2009 20:07 19Jan2010 09:06
Command ===> _                                                Scroll===> CSR
MA    a                                                              32/015
```

Access summary for a user



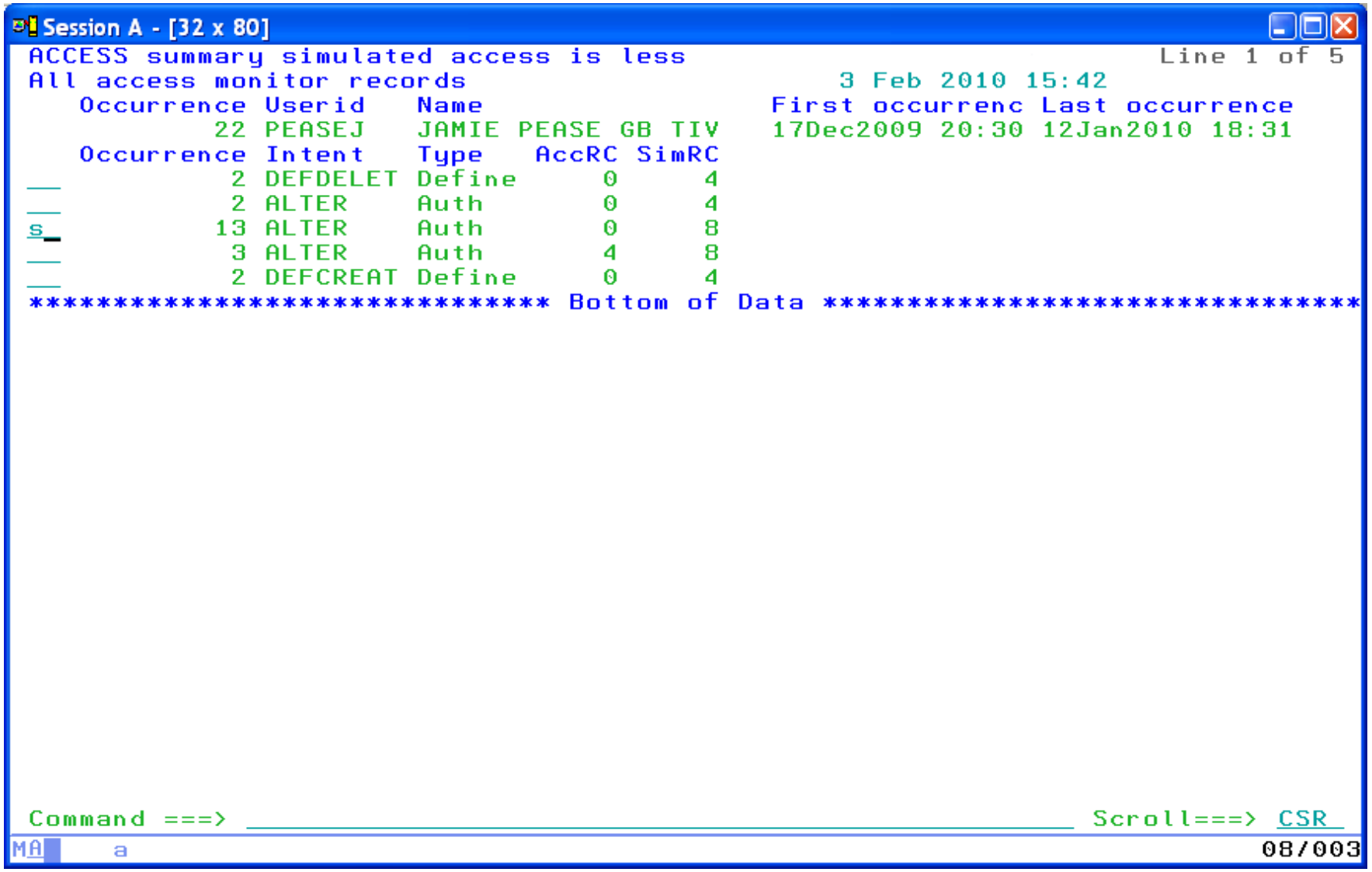
Active profiles and members within a class



Analysis of Access Monitor files

- Compare monitored access with RACF database
  - Active RACF database, *simulated* offline database, unload
  - 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

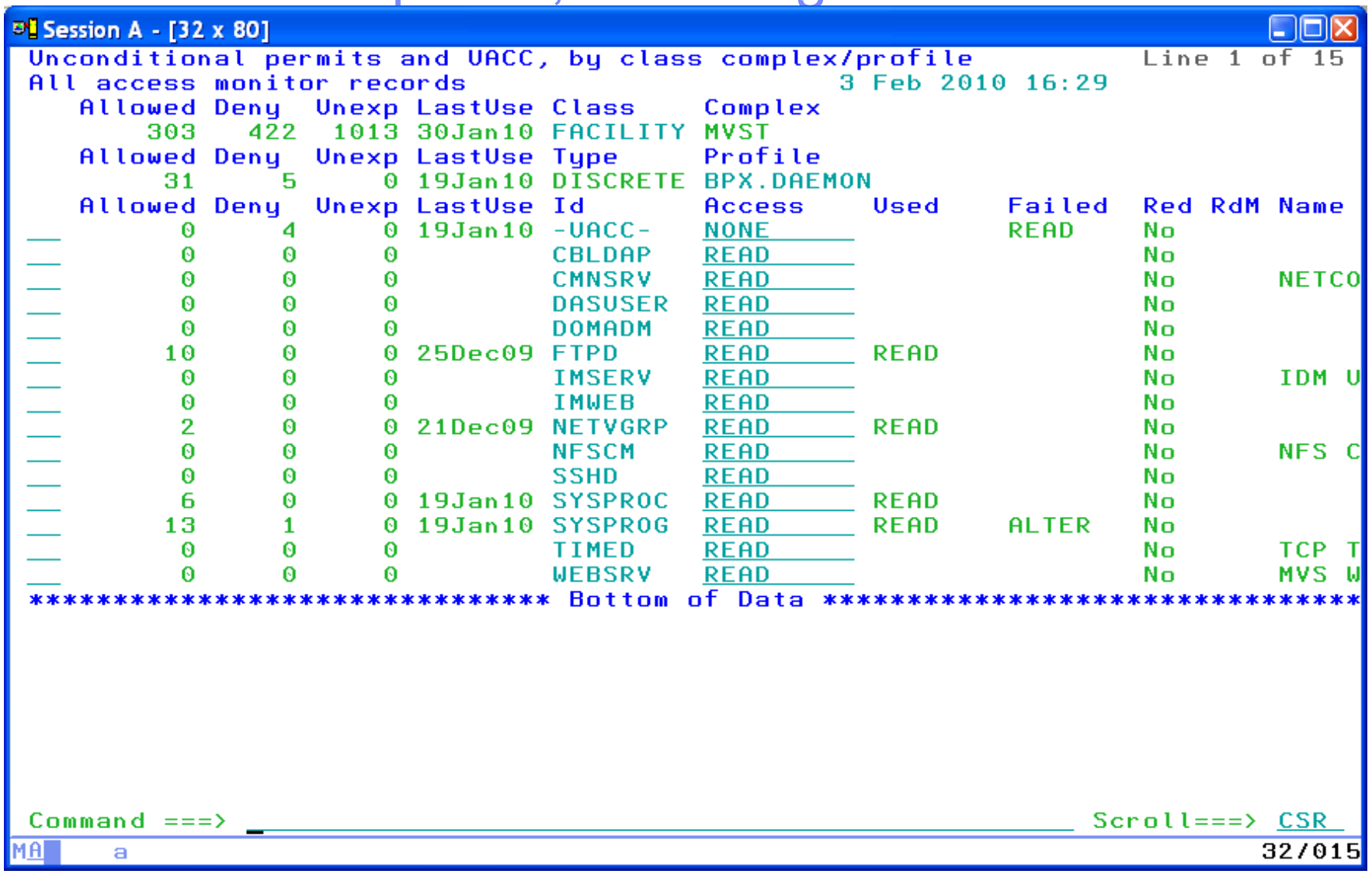
Allowed in Access Monitor, now denied in RACF



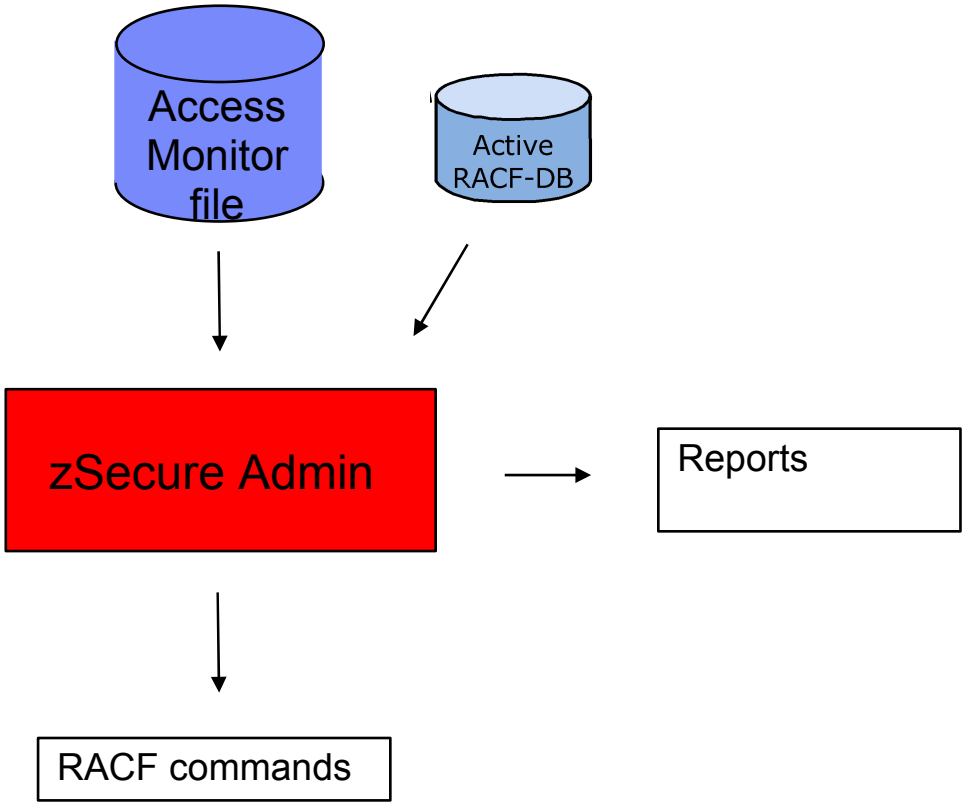
Analysis of Access Monitor files

- Analyze usage of RACF database entries
  - Which access list entries (permits) were referenced
    - Used to allow or deny access
  - Which connect groups were used
    - Used to allow or deny access
  - Which profiles were used
    - Normal profiles
    - Members of grouping profiles
    - Global profiles
  - Generate commands
    - Remove unused Permits, Connects, UACC and Profiles
    - Cleanup inconsistencies in RACF database

Access list of a profile, with usage info



Access Monitor overview



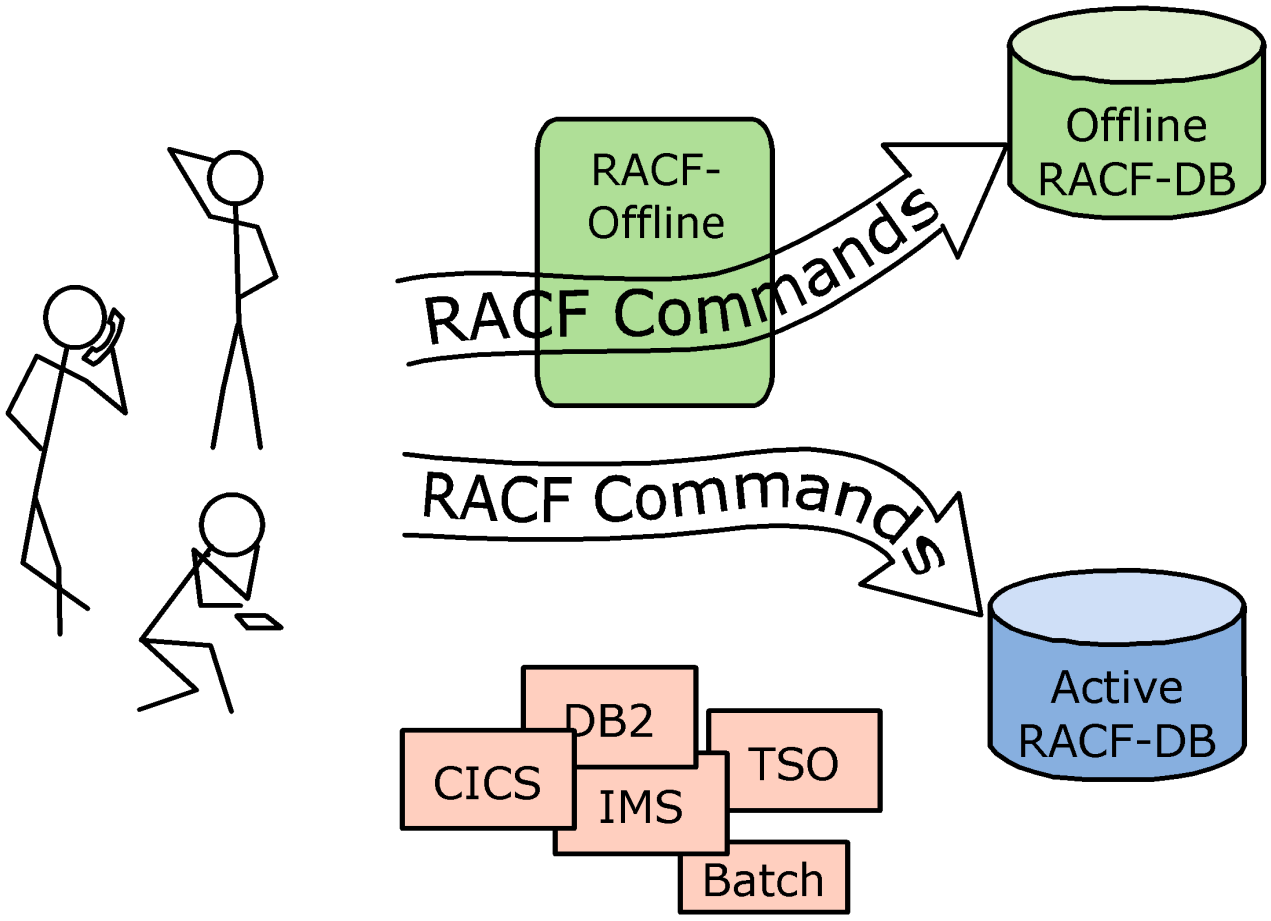
Test complex RACF changes

- Situation:
  - Complex changes to RACF
    - Merging groups
    - Merging RACF databases
- Best Solution Available?:
  - Use test system with separate RACF db
    - Planning, impact development
    - Not the same as production RACF db

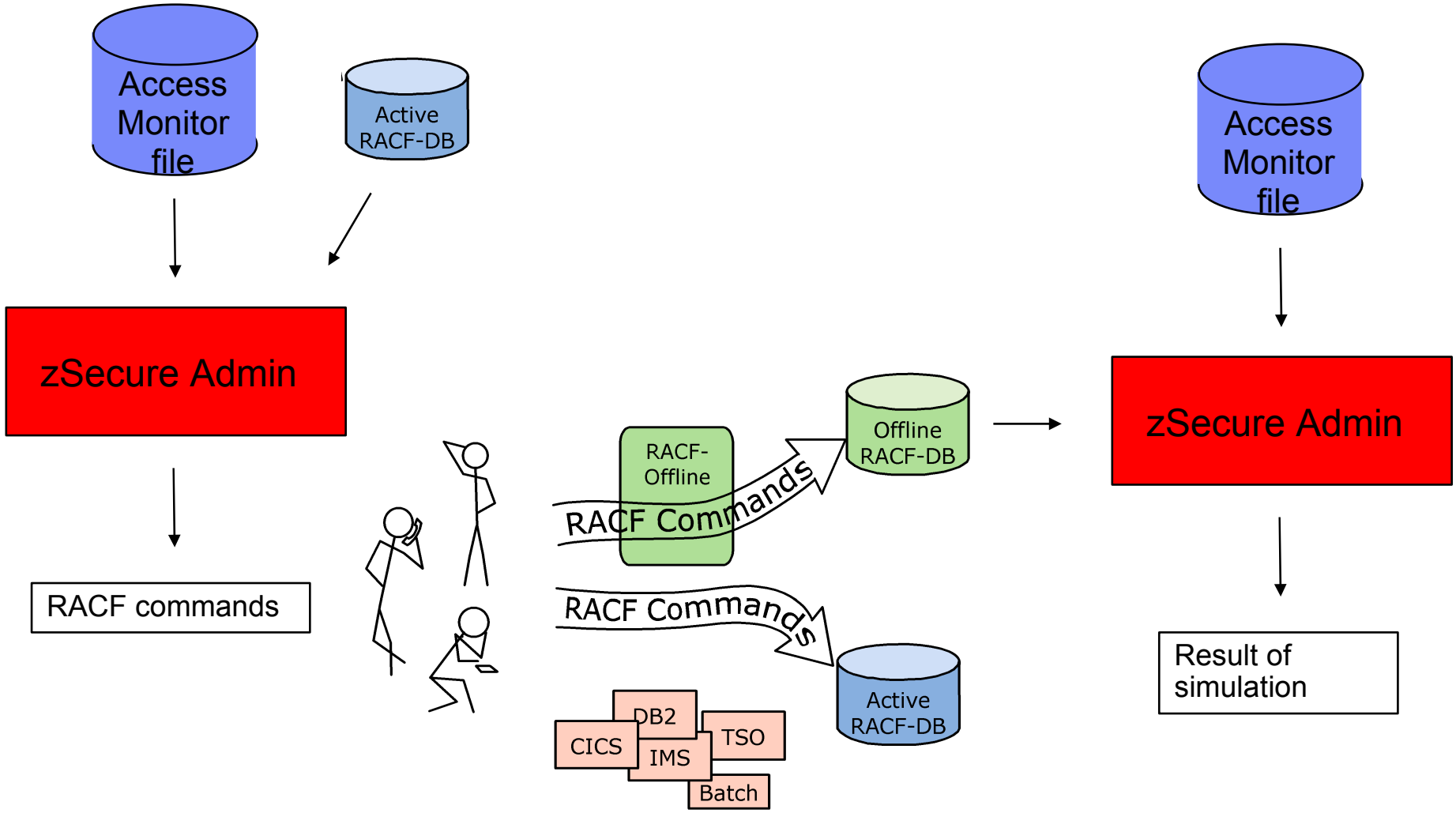
zSecure Solution

- Simulate RACF commands with RACF Offline
  - Create copy of RACF database, under group HLQ
  - Execute RACF commands that update this copy
  - Run zSecure reports on copy
  - Collect log of RACF commands to replay same actions on production
  - Part of zSecure Admin

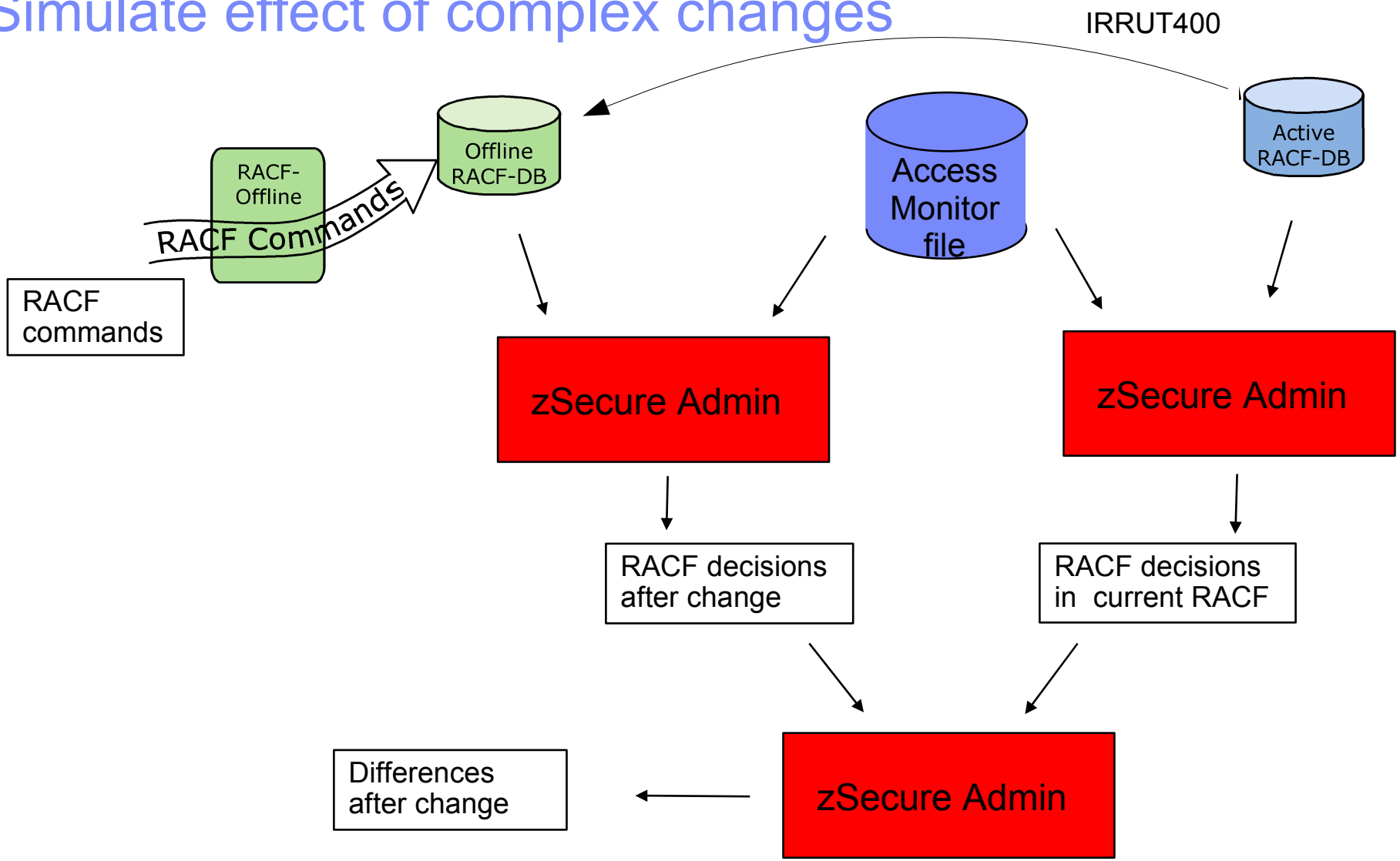
zSecure Admin: RACF Offline environment



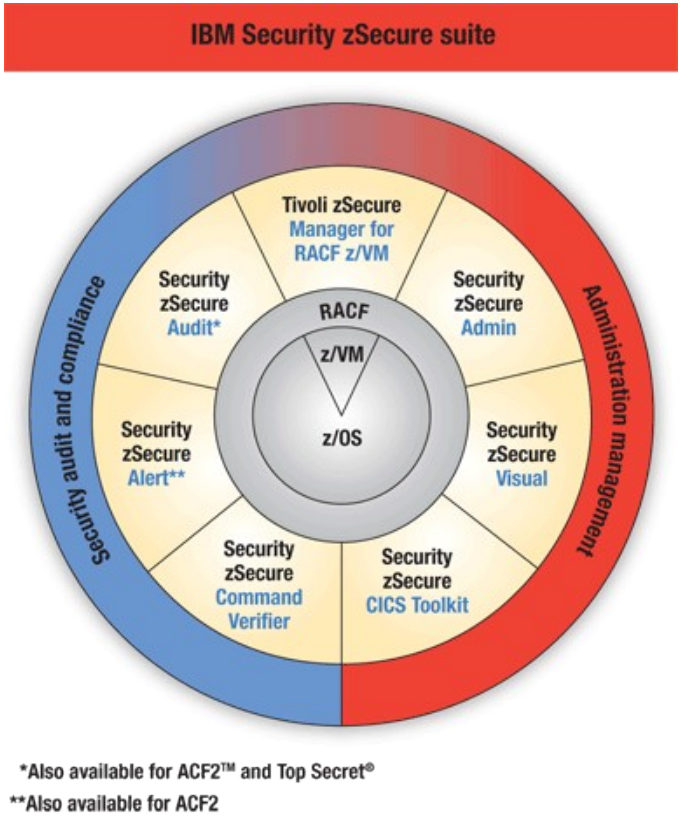
RACF Offline environment to test cleanup



Simulate effect of complex changes



SMF record support extensions



zSecure Audit

zSecure Alert

TCIM Enabler

Release 1.12

New SMF record types and fields – DB2 (1/2)

- DB2 V10R1 events (SMF record type 102)
  - New trace records of interest
    - IFCid 271 (Row and column access control)
    - IFCid 361 (Audit administrative authorities)
    - IFCid 362 (Begin audit trace with AUDITPOLICY)
  - Basic support for IFCids 357, 358, 359, 363, 364, 401, 402
  - New privileges added to IFCid 140
  - DB2 privilege translated to access intent (ALTER, CONTROL, …) by IFCids 140/361
  - New object type ‘session variable’
  - IFCids 142 enhanced to show row/column ACCESSCTRL information
  - IFCids 145 enhanced to show row/column enforcement

➢ Examples on next slide

New SMF record types and fields – DB2 (2/2)

Sample SMF 102-271 records

13Aug10 14:24:06.04 DB2 VA1A SECADM Drop column mask "DROP MASK M1"

13Aug10 14:24:06.26 DB2 VA1A SECADM Create column mask "CREATE MASK M1 ON ADMF001.EMP_E X1

- To see the full SQL command, zoom in to the detail display:

```
Description
DB2 VA1A SECADM Create column mask "CREATE MASK M1 ON ADMF001.EMP_E X1 FOR COLUMN
SSN RETURN CASE WHEN( VERIFY_ROLE_FOR_USER(SESSION_USER, 'ROLE1')=1 )
THEN SSN ELSE 'XXX-XX-' || SUBSTR(X1.SSN,8,4) END ENABLE"
```

Sample SMF 102-361 record

13Aug10 14:24:05.55 DB2 VA1A SECADM Audit administrative authority userauth for id SECADM with SECADM source SECADM.M1 by SQL "DROP MASK M1“

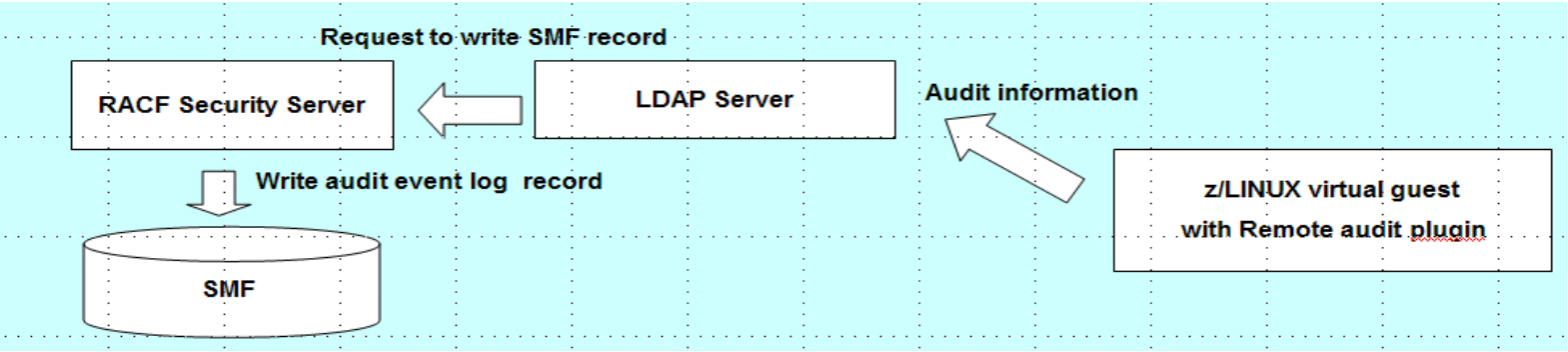
Sample SMF 102-362 record

22Mar10 10:21:55.43 DB2 VA1A SYSOPR START TRACE with AUDITPOLICY(TESTAUDP) Success RSN=0 SYSADMIN(S) DBADMIN(*)

Sample SMF 102-145 record

19Aug10 17:41:20.83 DB2 VA1A ADMF001 DML query CS by STLEC1 DSNTEP3.DSNTEP3 SQL stmt 2214 "SELECT * FROM ADMF001.EMP_E" enforced by SECADM.M1

New SMF record types and fields – Linux for System Z



- Linux for System Z events (SMF record type 83 subtype 4)

  SMF record type 83 subtypes have shared and individual data sections

  SMF record type 83-4 records remote audit events

  One application that can write them is a Linux plug-in (daemon) audispd

- New R_LOGDATA field - application-specific data from relocate section 114

  RACF_LINK_EVENT and RACF_LINK_AUDIT associate multiple records for the same event

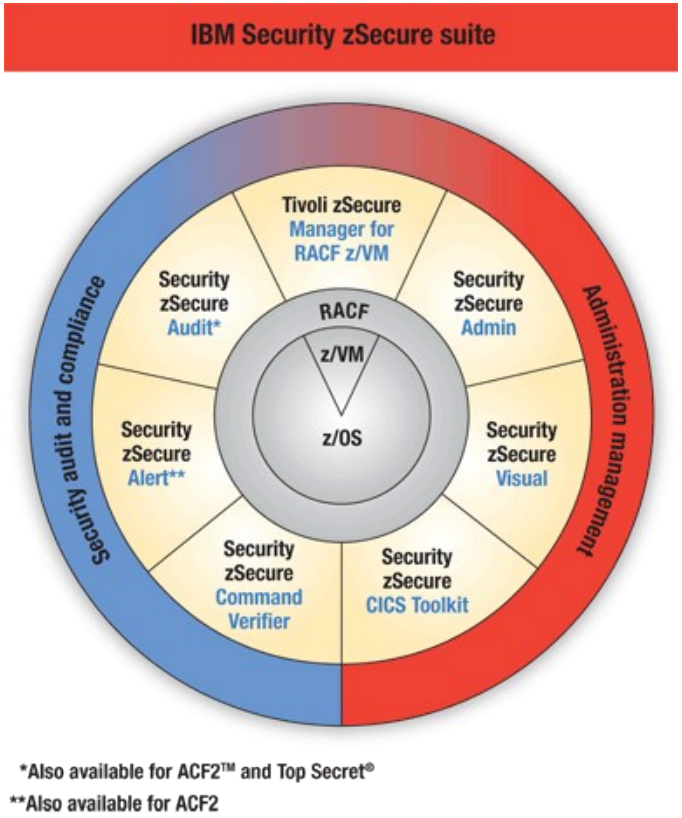
Sample SMF 83-4 records

R_auditx record from LDAPICTX logstr Remote audit request from BINDUSER. Linux (bobmcbob): type: SYSTEM_SHUTDOWN
R_auditx record from LDAPICTX logstr Remote audit request from BINDUSER. Linux (bobmcbob): type: USER_ACCT

Newlist type=SMF fields (1.11)

- 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

Send alerts to UNIX syslog



zSecure Alert

Release 1.12

Writing alerts to a UNIX syslog socket

- UNIX syslog added as an alert destination

  Syslog receivers are commonly used to collect messages from multiple systems, store them for log collection purposes and analyze them for alerting purposes. z/OS UNIX has a Syslog receiver that has been enhanced in z/OS V1R11, it can be used as a central point of log collection, e.g., for Linux for System Z systems. There are many cross-platform log collection solutions that zSecure Alert can now easily feed into.

- Specification works the same as for SNMP:

```
/ SNMP
  _ Write SNMP traps to C2RSNMP DD
  Specify SNMP receiver address(es) (multiple addresses in parentheses)
  Address . . . . . _____________________________________________________

/ UNIX syslog
  _ Write messages to C2RSYSLG DD
  Specify UNIX SYSLOG address(es) (multiple addresses in parentheses)
  Address(es) . . . _____________________________________________________
```

- Basic support as PTF for zSecure 1.11.0

zSecure Summary

- zSecure 1.12 available since November 2010