

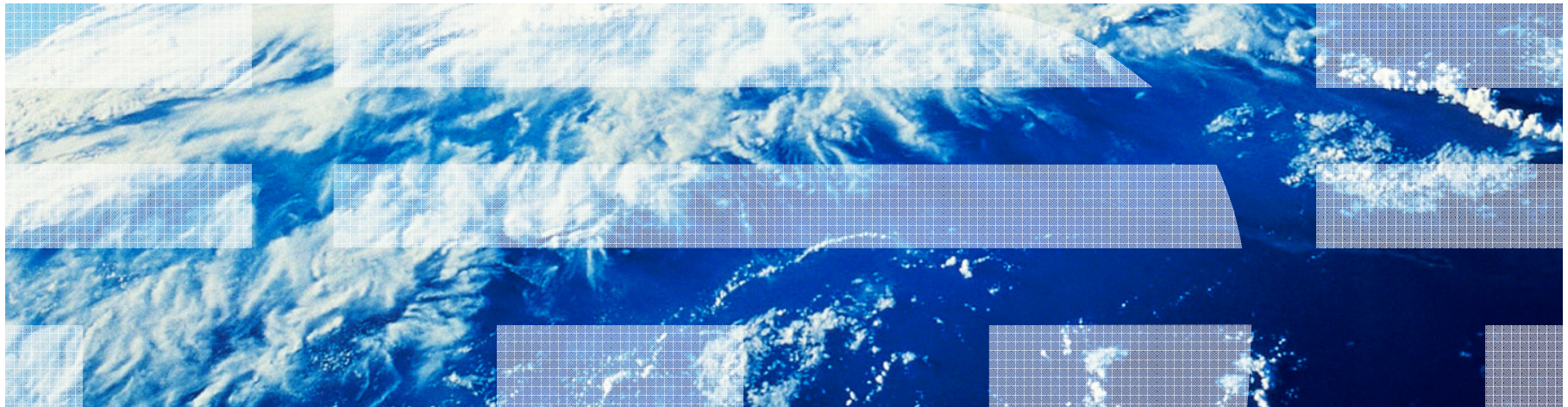
Jamie Pease, CISA, CISSP

IT Specialist, System z Security, IBM Software Group



IBM Tivoli zSecure Suite

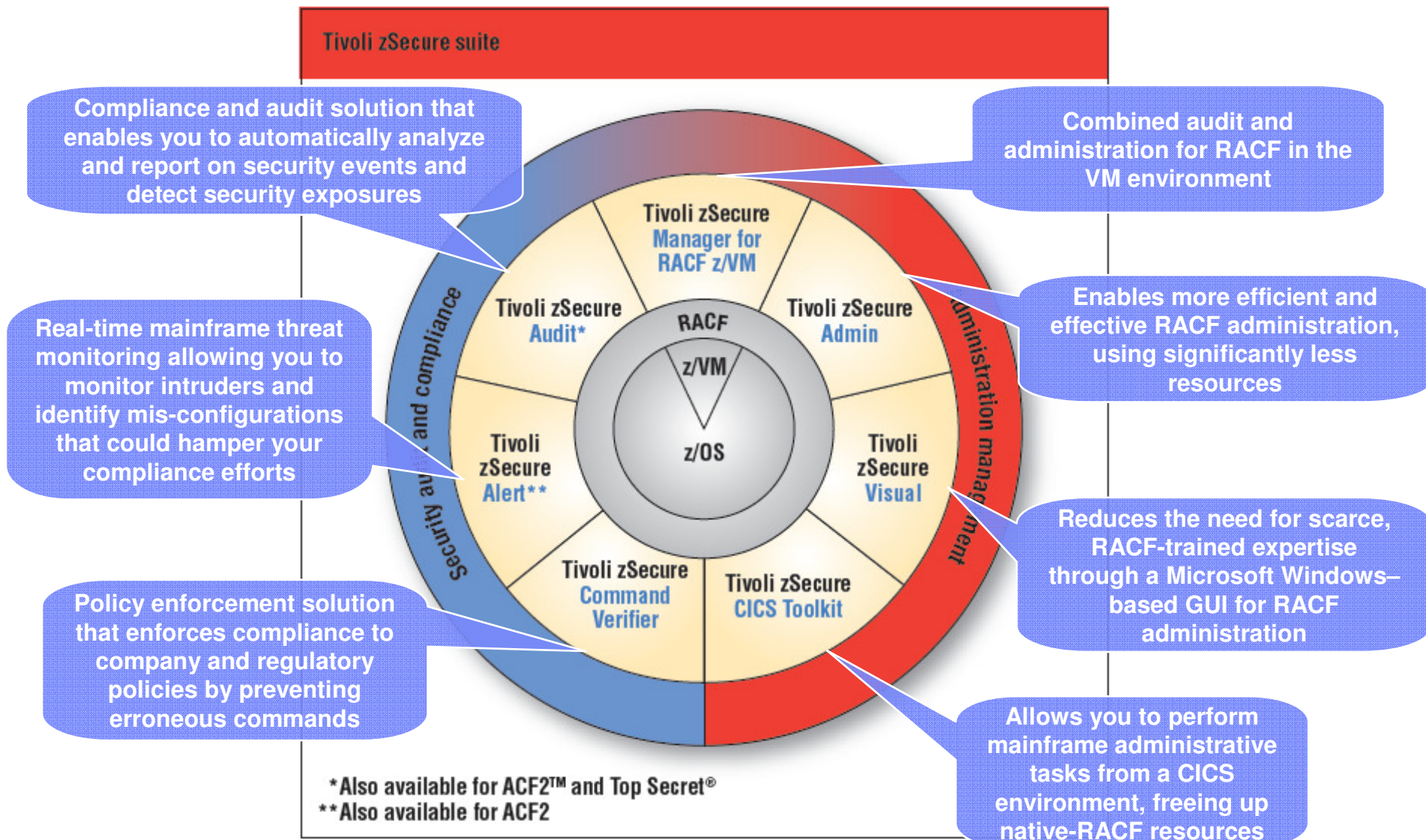
What is new in zSecure 1.11



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

IBM Tivoli zSecure Suite

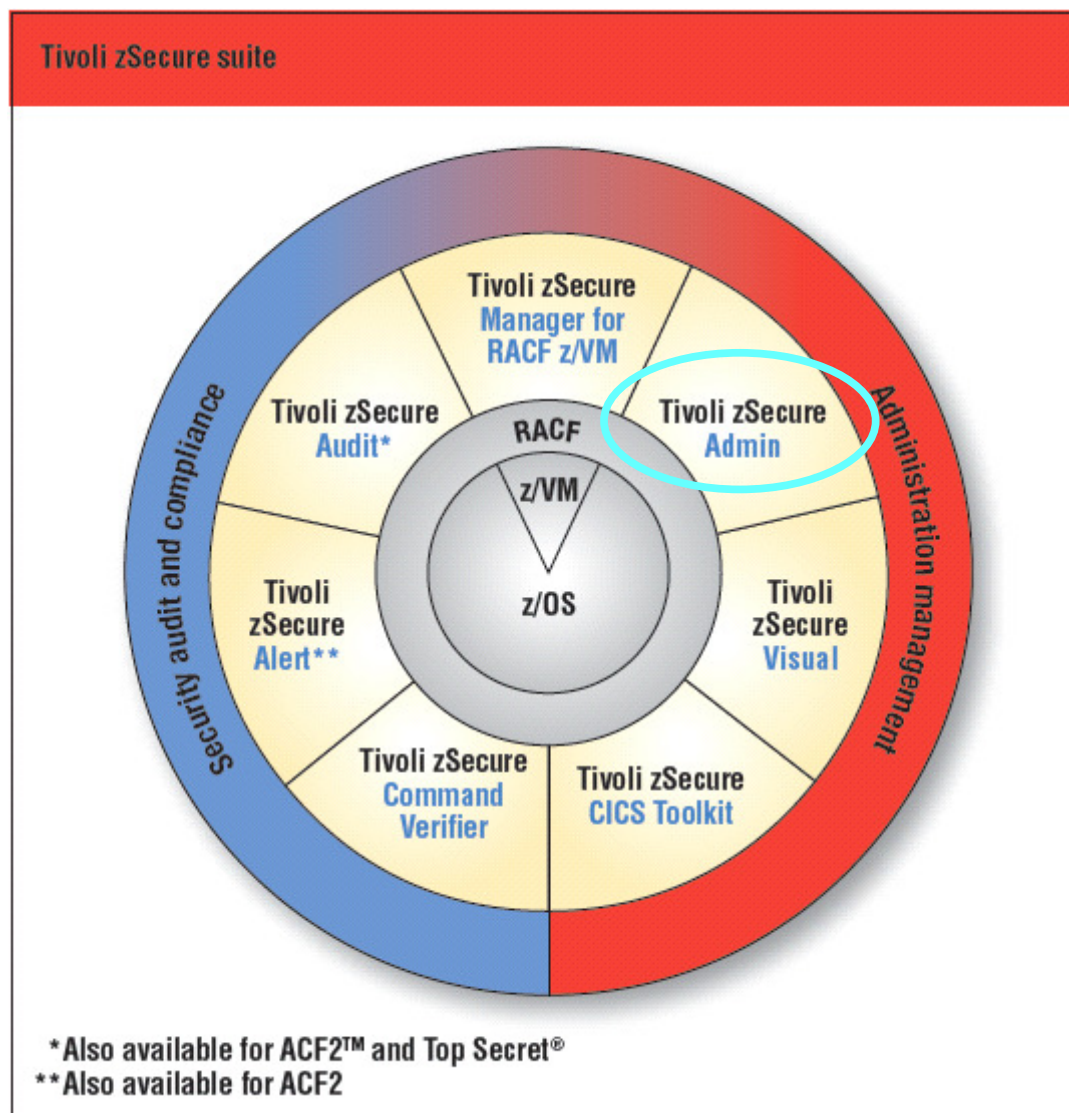


Note: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

zSecure 1.11 new functions and features

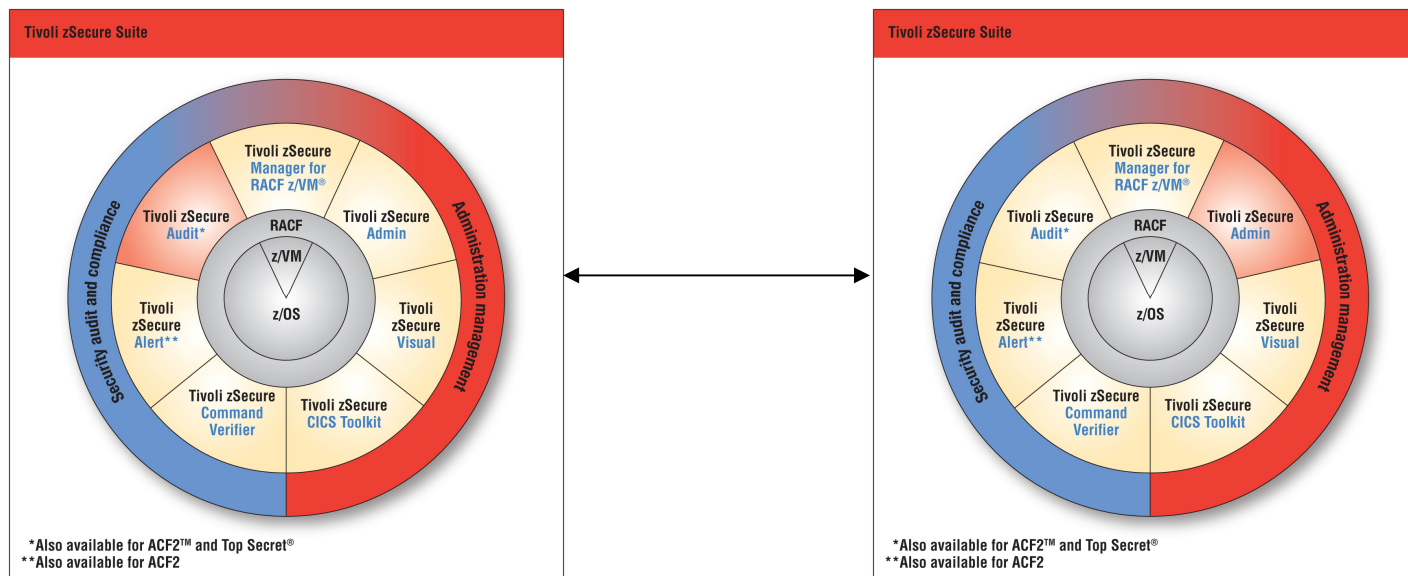
- New functions
 - Access Monitor for RACF
 - Finding RACF profiles with values in segment fields
 - TCPIP stack configuration
 - Support and Reporting of SMF records extended
 - Extended monitoring
 - z/OS and ACF2 currency
 - Globalization
 - and more

Access Monitor for RACF



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)



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

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 Analysis menu

```

Session A - [32 x 80]
Menu      Options      Info      Commands      Setup
-----
                zSecure Suite - Access

1      Access      Access summary by user or profile
2      Compare      Compare monitored access versus current database
3      Permit usage      Relate permit usage summary to current RACF database
4      Connect usage      Relate connect usage summary to current RACF database
5      Profile usage      Relate profile usage summary to current RACF database
6      Member usage      Relate member usage summary to current RACF database
7      Global usage      Relate Global usage summary to current RACF database
8      Remove      Remove unused profiles and authorizations
9      Cleanup      Remove permits, dataset and general resource profiles

Option ==>
MA a
32/014
  
```

Access summary by user

```

Session A - [32 x 80]
IBM Tivoli zSecure ACCESS summary
All access monitor records
1 s elapsed, 1.1 s CPU
3 Feb 2010 15:30

```

| Occurrence | Userid | Name | First occurrence | 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

```

Session A - [32 x 80]
IBM Tivoli zSecure ACCESS summary                               Line 1 of 21
All access monitor records                                     3 Feb 2010 15:30
Occurrence Userid Name                                         First occurrence Last occurrence
      30276 RMASO  ROGER MASON                                   22Dec2009 10:46 28Jan2010 13:50
Occurrence Intent Type AccRC
      46 READ    Fast      0
Occurrence Class
      43 TCICSTRN
Occurrence Resource
-----
      3 RTMM
-----
      2 TOOLKIT.ADGR
-----
      2 TOOLKIT.ADUS
-----
      2 TOOLKIT.ALGR
-----
      2 TOOLKIT.AUSR
-----
      2 TOOLKIT.CONN
-----
      2 TOOLKIT.DELD
-----
      2 TOOLKIT.DELG
-----
      2 TOOLKIT.DELU
-----
      2 TOOLKIT.LDSD
-----
      2 TOOLKIT.LGRP
-----
      2 TOOLKIT.LUSR
-----
      2 TOOLKIT.PEMT
-----
      2 TOOLKIT.RACL
-----
      2 TOOLKIT.RALT
-----
      2 TOOLKIT.RDEF
-----
      2 TOOLKIT.RDEL
-----
      2 TOOLKIT.REMV
-----
      2 TOOLKIT.RLST
-----
      2 TOOLKIT.SPEC
-----
      2 TOOLKIT.USRL
***** Bottom of Data *****
Command ==> _____ Scroll==> CSR
MA a
10/002

```

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

Allowed in Access Monitor, now denied in RACF

```

Session A - [32 x 80]
ACCESS summary simulated access is less
All access monitor records
Occurrence Userid Name First occurrence Last occurrence
22 PEASEJ JAMIE PEASE GB TIV 17Dec2009 20:30 12Jan2010 18:31
Occurrence Intent Type AccRC SimRC
2 DEFDELETE Define 0 4
2 ALTER Auth 0 4
s 13 ALTER Auth 0 8
3 ALTER Auth 4 8
2 DEFCREAT Define 0 4
***** Bottom of Data *****

Command ==>
Scroll==> CSR
MA a 08/003

```

Access list of a profile, with usage info

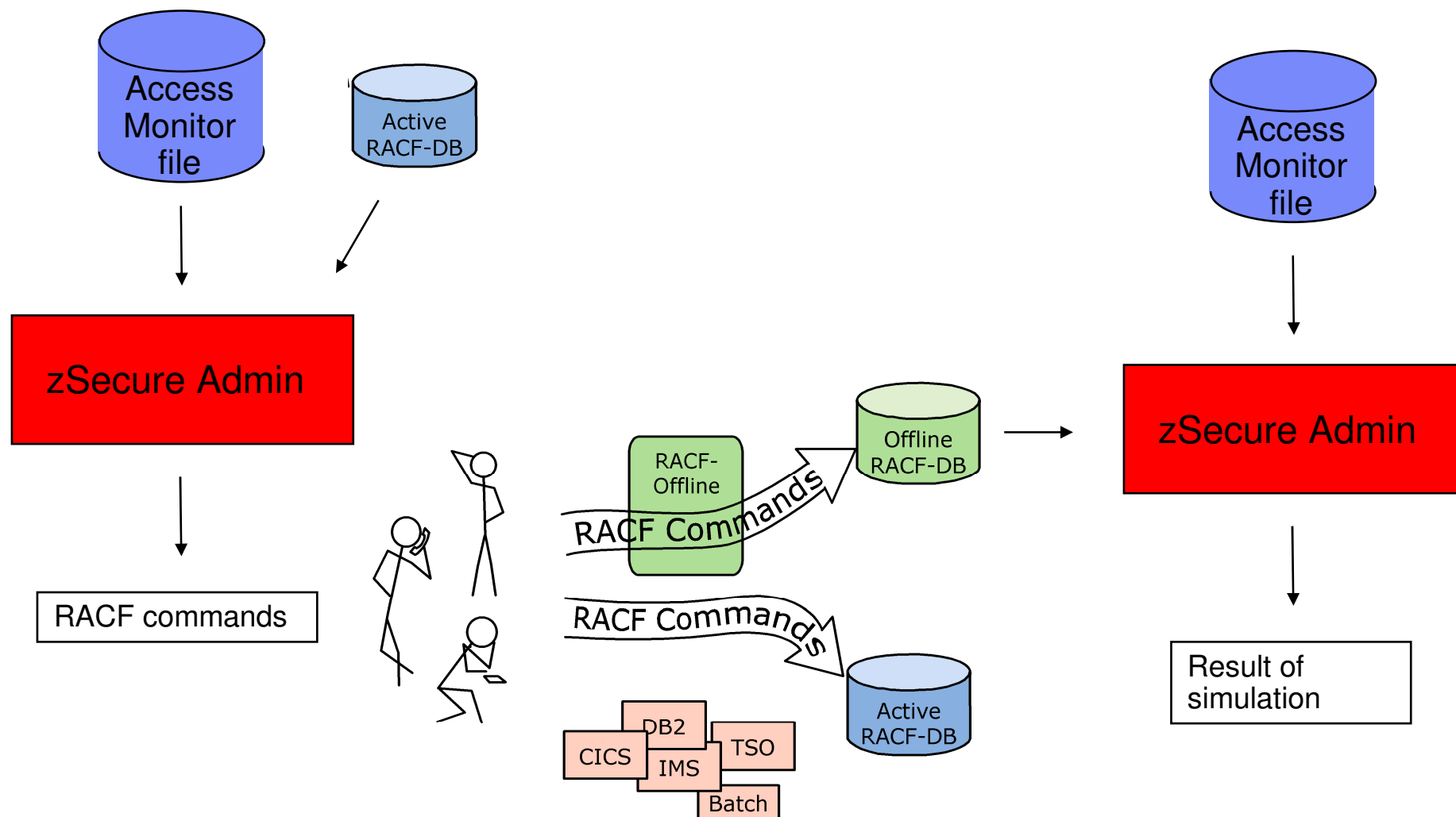
```

Session A - [32 x 80]
Unconditional permits and UACC, by class complex/profile Line 1 of 15
All access monitor records 3 Feb 2010 16:29
  Allowed Deny Unexp LastUse Class Complex
    303 422 1013 30Jan10 FACILITY MVST
  Allowed Deny Unexp LastUse Type Profile
    31 5 0 19Jan10 DISCRETE BPX.DAEMON
  Allowed Deny Unexp LastUse Id Access Used Failed Red RdM Name
-----
    0 4 0 19Jan10 -UACC- NONE READ No
    0 0 0 CBLDAP READ No
    0 0 0 CMNSRV READ No NETCO
    0 0 0 DASUSER READ No
    0 0 0 DOMADM READ No
    10 0 0 25Dec09 FTPD READ READ No
    0 0 0 IMSERV READ No IDM U
    0 0 0 IMWEB READ No
    2 0 0 21Dec09 NETVGRP READ READ No
    0 0 0 NFSCM READ No NFS C
    0 0 0 SSHD READ No
    6 0 0 19Jan10 SYSPROC READ READ No
    13 1 0 19Jan10 SYSPROG READ READ ALTER No
    0 0 0 TIMED READ No TCP T
    0 0 0 WEBSRV READ No MVS W
***** Bottom of Data *****

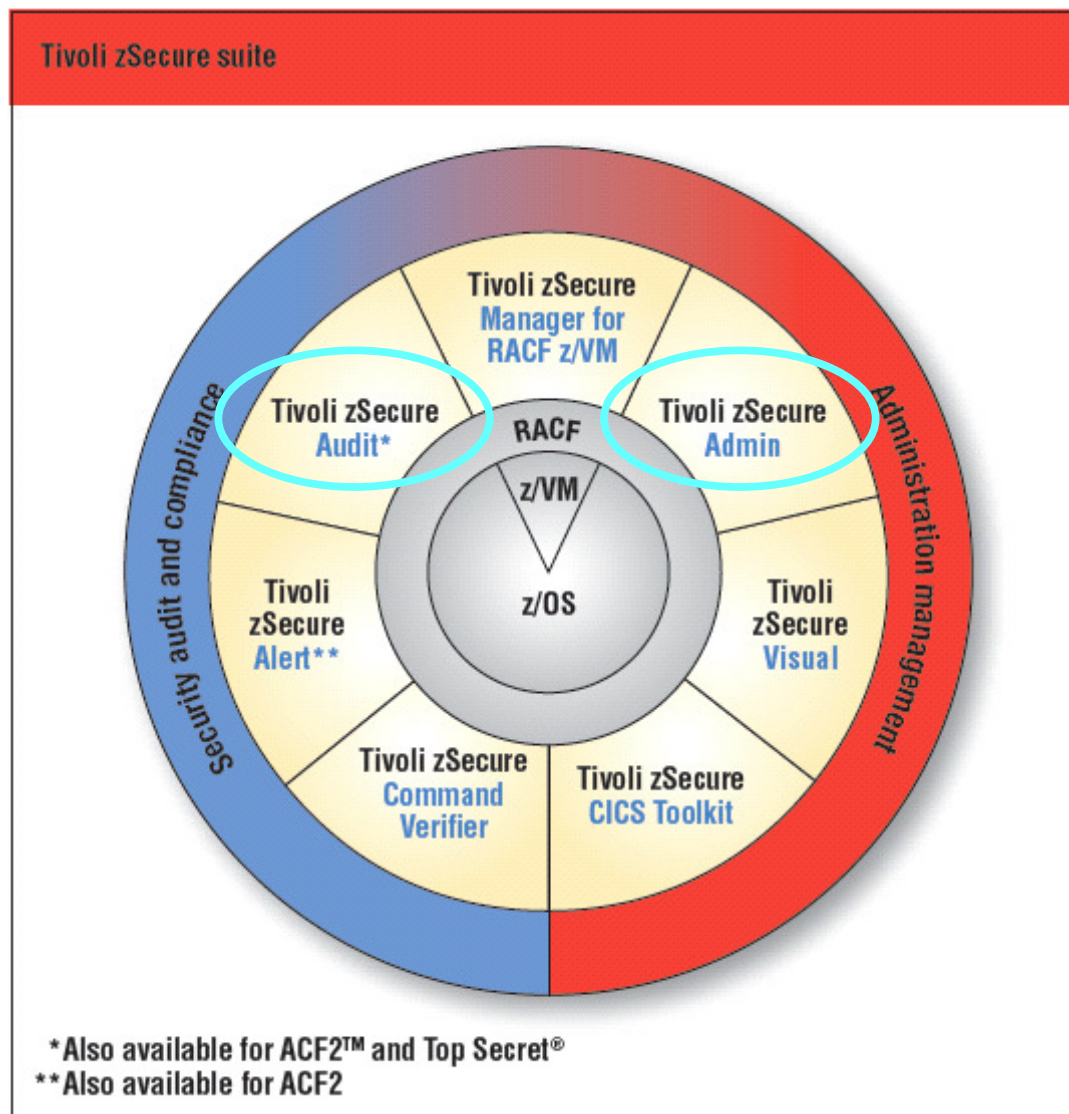
Command ==>
Scroll==> CSR
MA a 32/015

```


RACF Offline environment to test cleanup



Find field values in RACF application segments



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

Research UID(0) users...

```

Session A - [32 x 80]
Menu      Options      Info      Commands      Setup
-----
zSecure Suite - RACF - User Selection

_  Add new user or segment

Show userids that fit all of the following criteria
Userid . . . . . _____ (user profile key or filter)
Name . . . . . _____ (name/part of name, no filter)
Installation data . _____ (data scan, no filter except *)
Owned by . . . . . _____ (group or userid, or filter)
Default group . . . _____ (group or filter)
Connect group . . . _____ (group or filter)

Additional selection criteria
_  Other fields      _  Attributes      /  Segment presence  _  Absence

Output/run options
/  Show segments      -  All              -  Specify scope
_  Print format      -  Customize title  -  Send as e-mail
_  Background run    -  Full page form   -  Sort differently   -  Narrow print

Command ==> _____ _ start panel
MA a
19/024

```

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

```

Session A - [32 x 80]
Menu      Options      Info      Commands      Setup

zSecure Suite - User - Segment selection

USER OMVS segment selection
s UNIX user (uid) . . . . . = 0 (operator: < <= > >= = <> ^= )
x UNIX home path . . . . . / (path or filter)
- Initial program . . . . . (program or filter)
Max. address space size . . . . . (operator: < <= > >= = <> ^= )
Maximum CPU time . . . . .
Max. files open per proc . . . . .
Max. data space for mapping . . . . .
Max. nr. of active procs . . . . .
Max. nr. of active threads . . . . .

Command ==>

MA a 07/035
  
```

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

```

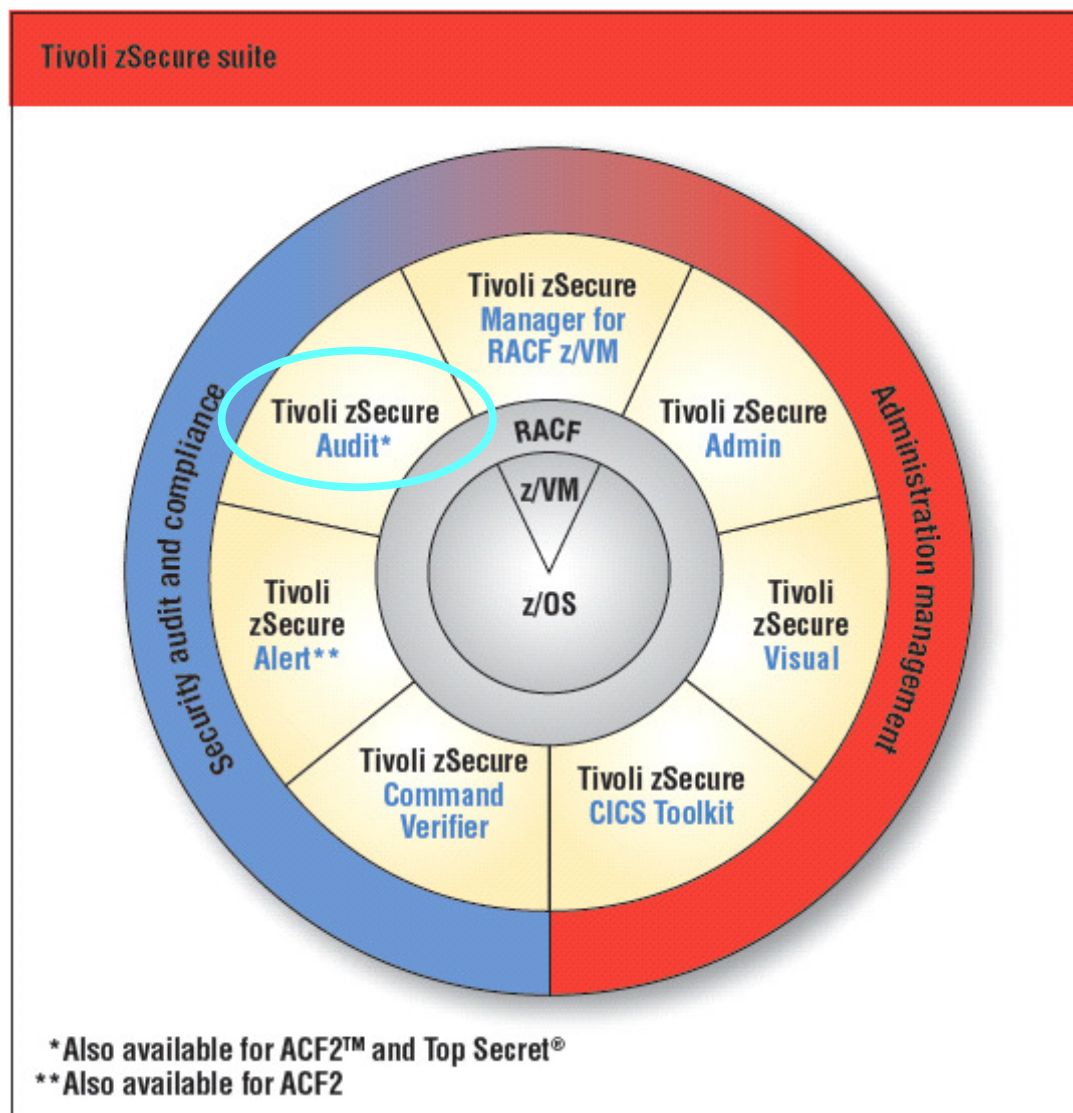
Session A - [32 x 80]
zSecure Suite USER OMVS segments          1 s elapsed, 0.3 s CPU
All users with segment OMVS, uid=0x home=/ 29 Sep 2009 15:07

  User      Complex  Uid      Home directory      Initial progr
  ---      -
  ██████████  PROD      0      /u/██████████      /bin/sh
  CRMQA097  PROD      0      / /sub1/sub2/sub3/sub4/sub5/sub6 /;/sub1/sub2/
  LDAPSRV   PROD      0
  ██████████  PROD      0      /u/██████████      /bin/sh
  SKRBKDC   PROD      0
  STRCONS   PROD      0
  STRTASK   PROD      0

***** Bottom of Data *****

Command ==>
Scroll==> CSR
MA a 32/015
  
```


TCPIP Stack Configuration reporting



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

TCPIP Stack Configuration

```

Session A - [32 x 80]
zSecure Suite Display Selection Line 1 of 8

  Name      Summary Records Title
- IPSTACK   1          1 IBM Tivoli zSecure IP_STACK summary
- IPPORT    1          72 IBM Tivoli zSecure IP_PORT summary
- IPRULE    1          1 IBM Tivoli zSecure IP_RULE summary
- IPVIPA    0          0 IBM Tivoli zSecure IP_VIPA summary
- IPINTFD   1          4 IBM Tivoli zSecure IP_INTERFACE summary
- IPRROUTE  1          2 IBM Tivoli zSecure IP_ROUTE summary
- IPNETACC  0          0 IBM Tivoli zSecure IP_NETACCESS summary
- IPAUTOL   1          1 IBM Tivoli zSecure IP_AUTOLOG summary
***** Bottom of Data *****

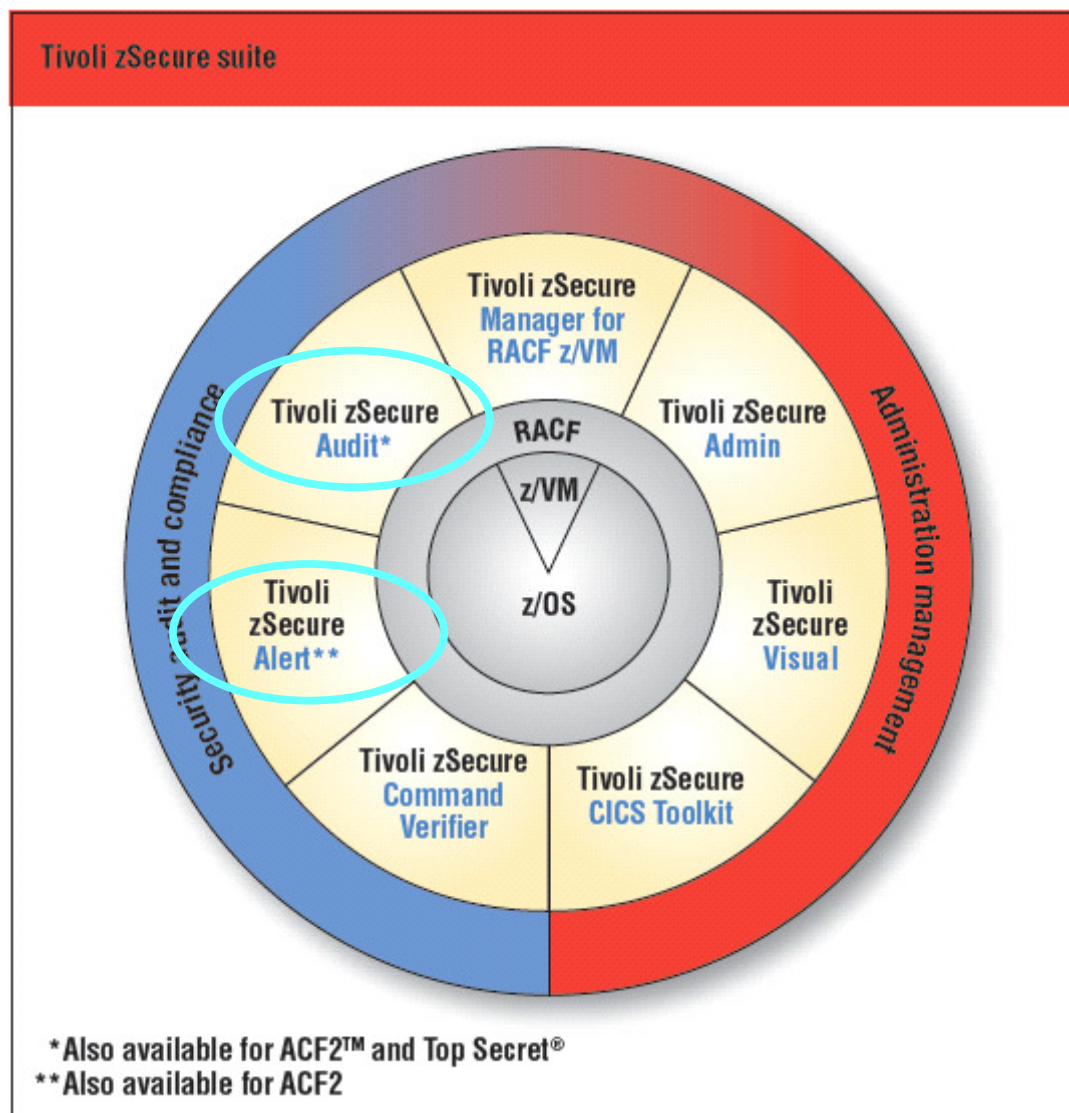
Command ==> _____ Scroll==> CSR
MA a 04/002
  
```

TCPIP Stack Configuration

```

Session A - [32 x 80]
IBM Tivoli zSecure IP_PORT summary                               Line 32 of 72
All TCP/IP stack information                                     6 Aug 2009 10:03
  Complex Sysplex Syst      Stack      Count
  EZOS    EZOSRD2R EZOS    TCPIP    72
Stack    BPort  EPort  Prt  Bind IP  address replacement
___ TCPIP    723   723   TCP
___ TCPIP    724   731   TCP
___ TCPIP    750   750   TCP
___ TCPIP    750   750   UDP
___ TCPIP    751   751   TCP
___ TCPIP    751   751   UDP
___ TCPIP    823   823   TCP
___ TCPIP   1023  1023  TCP
___ TCPIP   1023  1023  UDP
___ TCPIP   1024  1024  TCP
___ TCPIP   1415  1415  TCP
___ TCPIP   3000  3000  TCP
___ TCPIP   7000  7009  TCP
___ TCPIP   7050  7059  TCP
___ TCPIP   7100  7109  TCP
___ TCPIP   8000  8009  TCP
___ TCPIP   8010  8019  TCP
___ TCPIP   8020  8029  TCP
___ TCPIP   8030  8039  TCP
___ TCPIP   8040  8049  TCP
___ TCPIP   8050  8059  TCP
___ TCPIP   8060  8069  TCP
___ TCPIP   8070  8079  TCP
___ TCPIP   8080  8089  TCP
___ TCPIP   8090  8099  TCP
___ TCPIP   8801  8801  TCP
Command ==>
Scroll==> CSR
MA a
21/002
  
```

SMF record support and reporting



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)

CICS SMF records

Session A - [32 x 80] Line 14 of 174

Event log record detail information 26Mar09 03:58 to 1Apr09 05:00

| Date/time | Description |
|---------------------|--|
| 27Mar09 03:06:40.67 | CICSA CICS transaction CICS CPLT |
| 27Mar09 03:06:40.77 | CICSA CICS transaction CICS CSSY |
| 27Mar09 03:06:40.82 | CICSA CICS transaction CICS CGRP |
| 27Mar09 03:06:40.82 | CICSA CICS transaction CICS CSSY |
| 27Mar09 03:06:40.82 | CICSA CICS transaction CICS CSSY |
| 27Mar09 03:06:40.82 | CICSA CICS transaction CICS CSSY |
| 27Mar09 03:06:40.97 | CICSA CICS transaction CICS CSSY |
| 27Mar09 03:06:40.97 | CICSA CICS transaction CICS CSSY |
| 27Mar09 03:06:41.02 | CICSA CICS transaction CICS CSSY |
| 27Mar09 03:06:41.11 | CICSA CICS transaction CICS CSSY |
| 27Mar09 03:06:41.15 | CICSA CICS transaction CICS CSSY |
| 27Mar09 03:07:22.41 | CICSA CICS transaction CICS CPIR |
| 27Mar09 03:07:22.46 | CICSA CICS transaction CICS CISC |
| 27Mar09 03:07:22.47 | CICSA CICS transaction CICS CATA |
| 27Mar09 03:07:22.93 | CICSA CICS transaction CICS CWBG |
| 27Mar09 03:07:23.08 | job CICSA CICS appl CICS monitor performance dictionary |
| 27Mar09 03:07:23.08 | job CICSA CICS appl CICS monitor performance data 12 tra |
| 27Mar09 03:07:23.24 | CICSA CICS transaction CICS CEJR |
| 27Mar09 03:07:23.24 | CICSA CICS transaction CICS CSFU |
| 27Mar09 03:07:23.39 | CICSA CICS transaction CICS CXRE |
| 27Mar09 03:07:24.11 | CICSUSER CICS transaction CICS CQRY from L702 |
| 27Mar09 03:07:25.63 | CICSUSER CICS transaction CICS CSGM from L702 |
| 27Mar09 03:07:29.97 | CICSUSER CICS transaction CICS CESN from L702 |
| 27Mar09 03:07:34.90 | CICSUSER CICS transaction CICS CESN from L702 |
| 27Mar09 03:07:37.85 | BCSCGB1 CICS transaction CICS CEMN from L702 |
| 27Mar09 03:14:24.22 | CICSA CICS transaction CICS CATR |
| 27Mar09 03:14:24.28 | job CICSA CICS appl CICS monitor performance data 12 tra |
| 31Mar09 22:36:37.30 | CICSA CICS transaction CICS CISR |

Command ==> CSR Scroll==>

MA a 30/002

CICS SMF records

```

Session A - [32 x 80]
Event log record detail information
Line 1 of 93
26Mar09 03:58 to 1Apr09 05:00

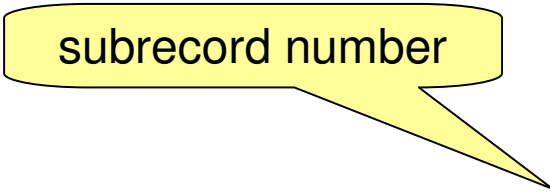
Description
BCSCGB1 CICS transaction CICS CEMN from L702

Record identification
Jobname + id: CICSA
SMF date/time: Fri 27 Mar 2009 03:14:24.28
Event date/time: 27Mar2009 03:07:37.85
SMF system: SYS1 record type: 110-1 record no: CKR1SM00 10 1

CICS address space data
Subsys: CICS
Applid: CICS
Specific applid: CICS

CICS transaction data
Transaction name: CEMN
Transaction type: T0
Completion:
Elapsed: 00:01:17.973034

Subject identification
- User: BCSCGB1
  Name:
  CICS terminal L702
  LU name: LCL702 Vtam net: ADCD
- Source IP:
  Remote network:
Command ==>
Scroll==> CSR
MA a 32/015
  
```



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

Member level changes

```

Session A - [32 x 80]
Event log record detail information                                0 s elapsed, 0.2 s CPU
                                                                15Jul08 17:42 to 17Jul08 19:43

  Date/time      Description
  ___
  15Jul08 17:42  SYSPRG1 Delete member EFFE in DMTP13 IBMUSER.ISPF.CNTL
  15Jul08 18:45  SYSPRG1 Rename member $$README to $$README in DMTP13 IBMUSER.I
  15Jul08 18:45  SYSPRG1 Add member EFFE in DMTP13 IBMUSER.ISPF.CNTL
  15Jul08 18:46  SYSPRG1 Rename member $$README to $$README in DMTP13 IBMUSER.I
  15Jul08 18:46  SYSPRG1 Delete member EFFE in DMTP13 IBMUSER.ISPF.CNTL
  15Jul08 19:11  SYSPRG1 Add member SMFUNL in DMTP13 IBMUSER.ISPF.CNTL
  15Jul08 19:12  SYSPRG1 Replace member SMFUNL in DMTP13 IBMUSER.ISPF.CNTL
  17Jul08 17:31  SYSPRG1R Replace member AA25068 in DMTA11 DLIB.SYS1.SMPPTS
  17Jul08 17:31  POCST1M Add member BA25068R in DMTP13 IBMUSER.ISPF.CNTL
  17Jul08 17:32  POCST1M Add member BA25068S in DMTP13 IBMUSER.ISPF.CNTL
  17Jul08 17:33  POCST1M Add member BA25068A in DMTP13 IBMUSER.ISPF.CNTL
  17Jul08 17:34  POCST1M Replace member BA25068A in DMTP13 IBMUSER.ISPF.CNTL
  17Jul08 17:35  SYSPRG1A Replace member IGG0210B in DMTRES SYS1.LPALIB
  17Jul08 17:35  SYSPRG1A Replace member IGWCCA00 in DMTRES SYS1.LPALIB
  17Jul08 17:35  SYSPRG1A Replace member IGWCDRTR in DMTRES SYS1.LPALIB
  17Jul08 17:35  SYSPRG1A Replace member IGC0002A in DMTRES SYS1.LPALIB
  17Jul08 19:34  POCST1M Replace member AA250681 in DMTP13 IBMUSER.ISPF.CNTL
  17Jul08 19:36  POCST1M Replace member PRSMF42 in DMTP13 IBMUSER.ISPF.CNTL
  17Jul08 19:39  POCST1M Replace member PRSMF42 in DMTP13 IBMUSER.ISPF.CNTL
  17Jul08 19:41  POCST1M Replace member AA250681 in DMTP13 IBMUSER.ISPF.CNTL
  17Jul08 19:42  POCST1M Replace member PRSMF42 in DMTP13 IBMUSER.ISPF.CNTL
  17Jul08 19:43  POCST1M Replace member SMFUNL in DMTP13 IBMUSER.ISPF.CNTL
  ***** Bottom of Data *****

Command ==>
Scroll==> CSR
MA a 32/015
  
```

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 |

New ISPF options for Event selection and reporting

```

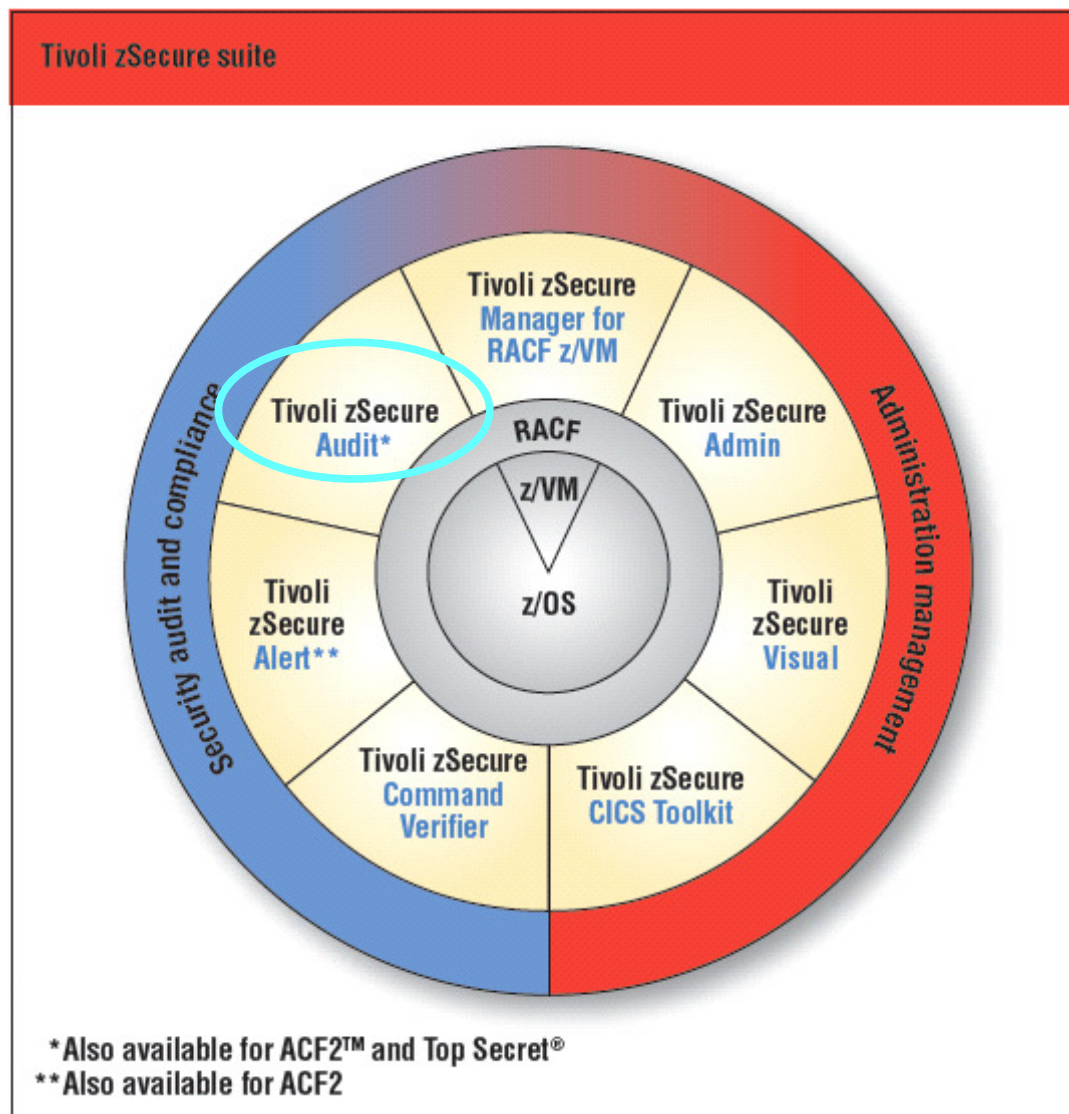
Session A - [32 x 80]
Menu      Options      Info      Commands      Setup
-----
                                zSecure Admin+Audit for RACF - Main menu
                                More      +
SE  Setup      Options and input data sets
RA  RACF       RACF Administration
AU  Audit      Audit security and system resources
RE  Resource   Resource reports
AM  Access     RACF Access Monitor
EV  Events     Event reporting from SMF and other logs
  U  User      User events from SMF
  G  Group     Group events from SMF
  D  Data set  Data set events from SMF
  R  Resource  General resource events from SMF
  F  Filesystem Unix filesystem events from SMF and other logs
  I  IP        IP events from SMF and other logs
  1  SMF reports Predefined analysis reports
  2  RACF events RACF logging for specific events
  4  DB2       DB2 events from SMF
  5  CICS     CICS events from SMF
  6  Omegamon Omegamon events from SMF
  C  Custom    Custom report
CO  Commands  Run commands from library
IN  Information Information and documentation
LO  Local     Locally defined options
X   Exit      Exit this panel

Input complex:  none selected

Product/Release
5655-T01 IBM Tivoli zSecure Admin 1.11.0
Option ==>
MA  a

```

Other enhancements to Audit



Other enhancements to Audit

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

```

Session A - [32 x 80]
Menu      Options      Info      Commands      Setup

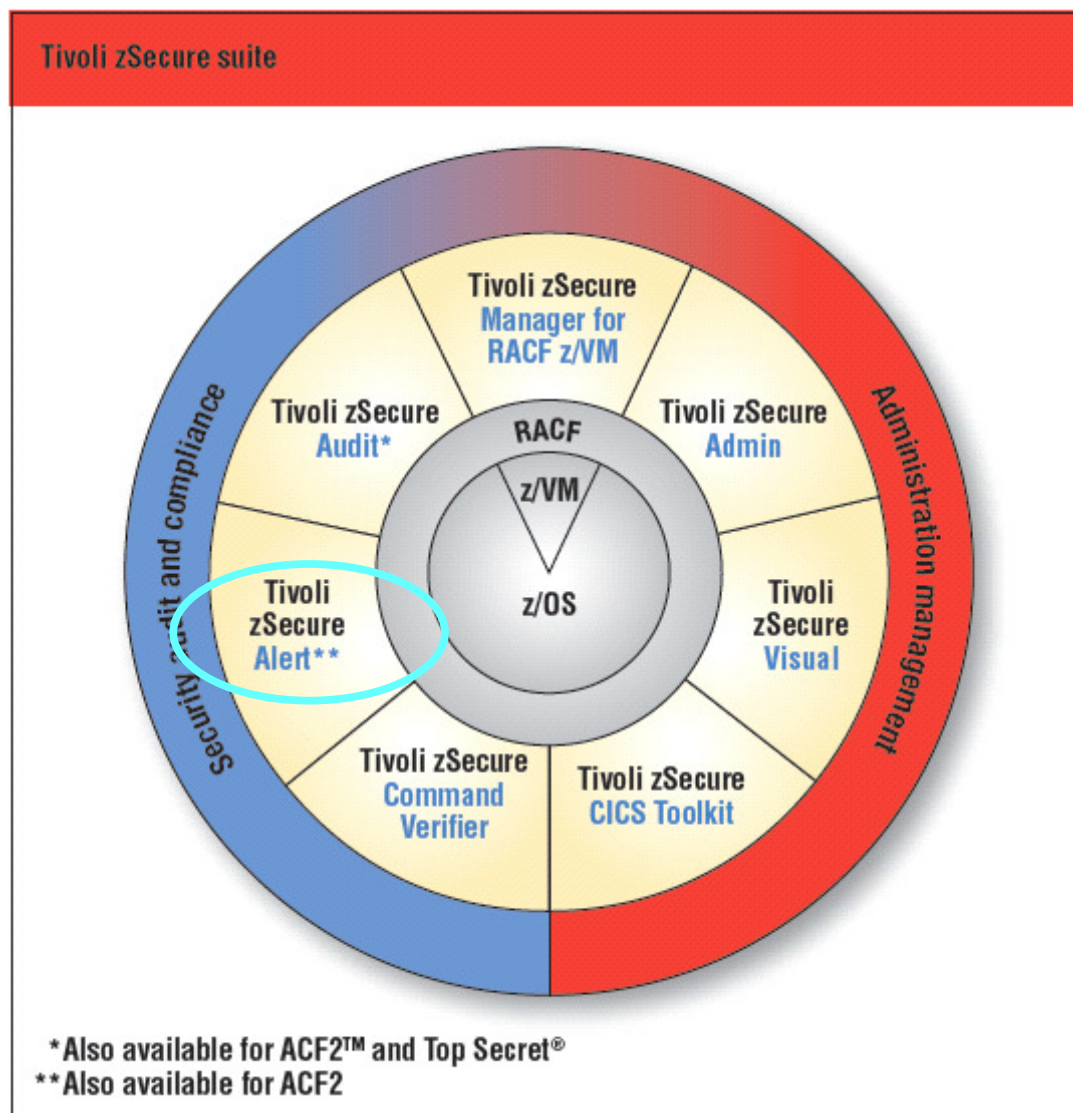
zSecure Admin+Audit for RACF - Audit - Status

Enter / to select report categories
- MVS tables           MVS oriented tables (reads first part of CKFREEZE)
- MVS extended         MVS oriented tables (reads whole CKFREEZE)
- RACF control         RACF oriented tables
- RACF user            User oriented RACF tables and reports
- RACF resource        Resource oriented RACF tables and reports

Select options for reports:
/ Select specific reports from selected categories
- Include audit concern overview in overall prio order
- Only show reports that may contain audit concerns
20 Minimum audit priority for audit concerns (1-99)
- Print format          - Concise (short) report
- Background run

Audit policy
/ zSecure
- C1
- C2
- B1
  
```


Extended Monitoring



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

Extended Monitoring: configuring

```

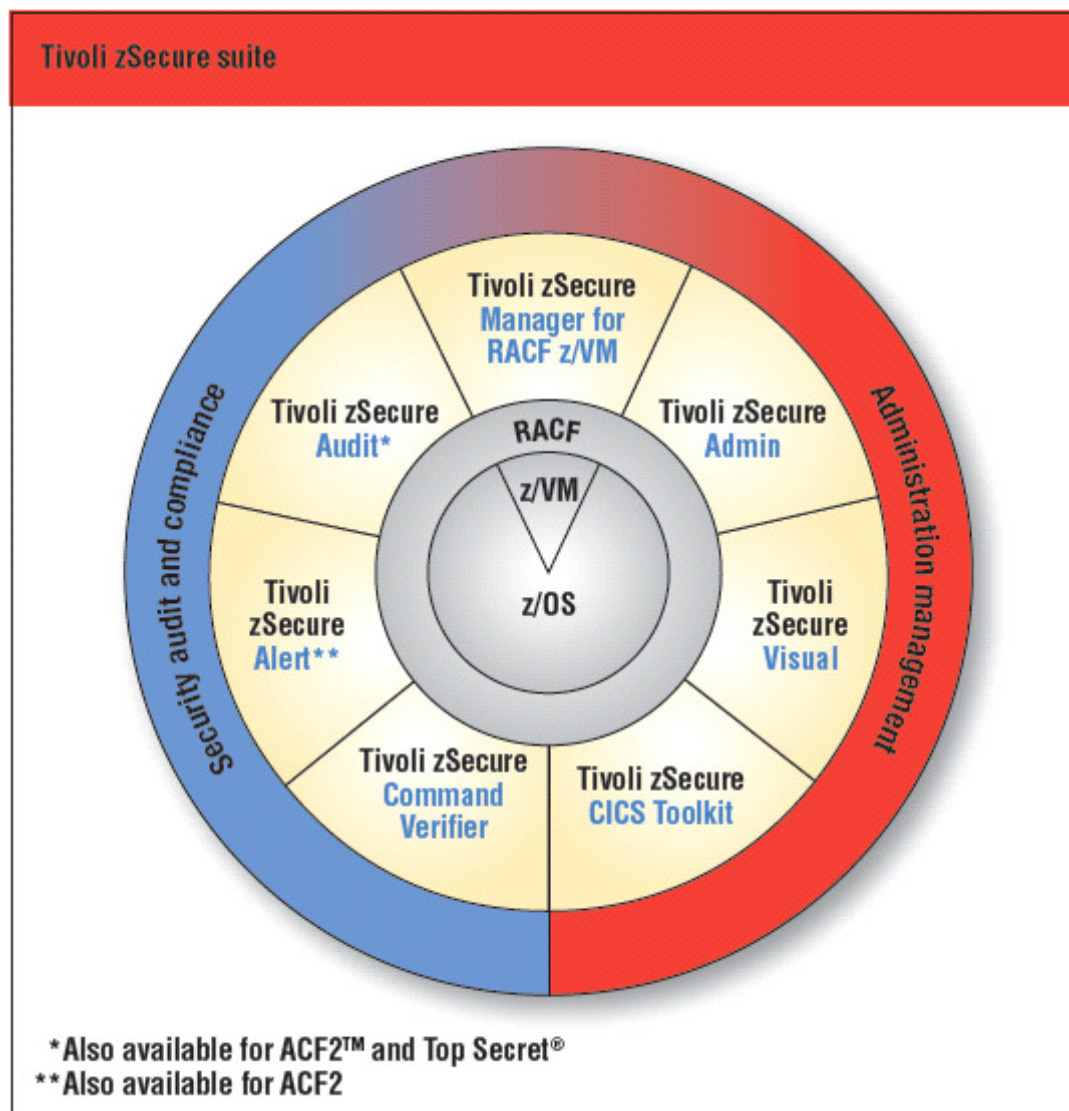
Session A - [32 x 80]
Menu      Options      Info      Commands      Setup
-----
zSecure Suite - Setup - Alert      Row 1 to 5 of 5

RACF control alerts
Select the alert you want to work with.
The following line commands are available: A(Preview), C(opy), D(elete),
E(dit), I(nsert), W(Who/Where), S(elect), U(nselect), B(rowse)
-----
Alert                                     Id      Sel      gECSW      C      EM
- Global security countermeasure activated 1501    No      gE W        N
- Global security countermeasure deactivated 1502    No      gE W        N
- Global security countermeasure or option changed 1503    No      gE W        N
- RACF resource class has been activated 1504    Yes     gE W        Y
- RACF resource class has been inactivated 1505    Yes     gE W        Y
***** Bottom of data *****
-----
Alert                                     Id      Sel      gECSW      C      EM
- SMF data loss started 1601    No      gE W        N
- SMF logging resumed after failure 1602    No      gE W        N
- SVC definition changed 1603    Yes     gE W        Y
***** Bottom of data *****

Command ==> _____ Scroll ==> CSR
MA a
11/002

```

z/OS currency



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)

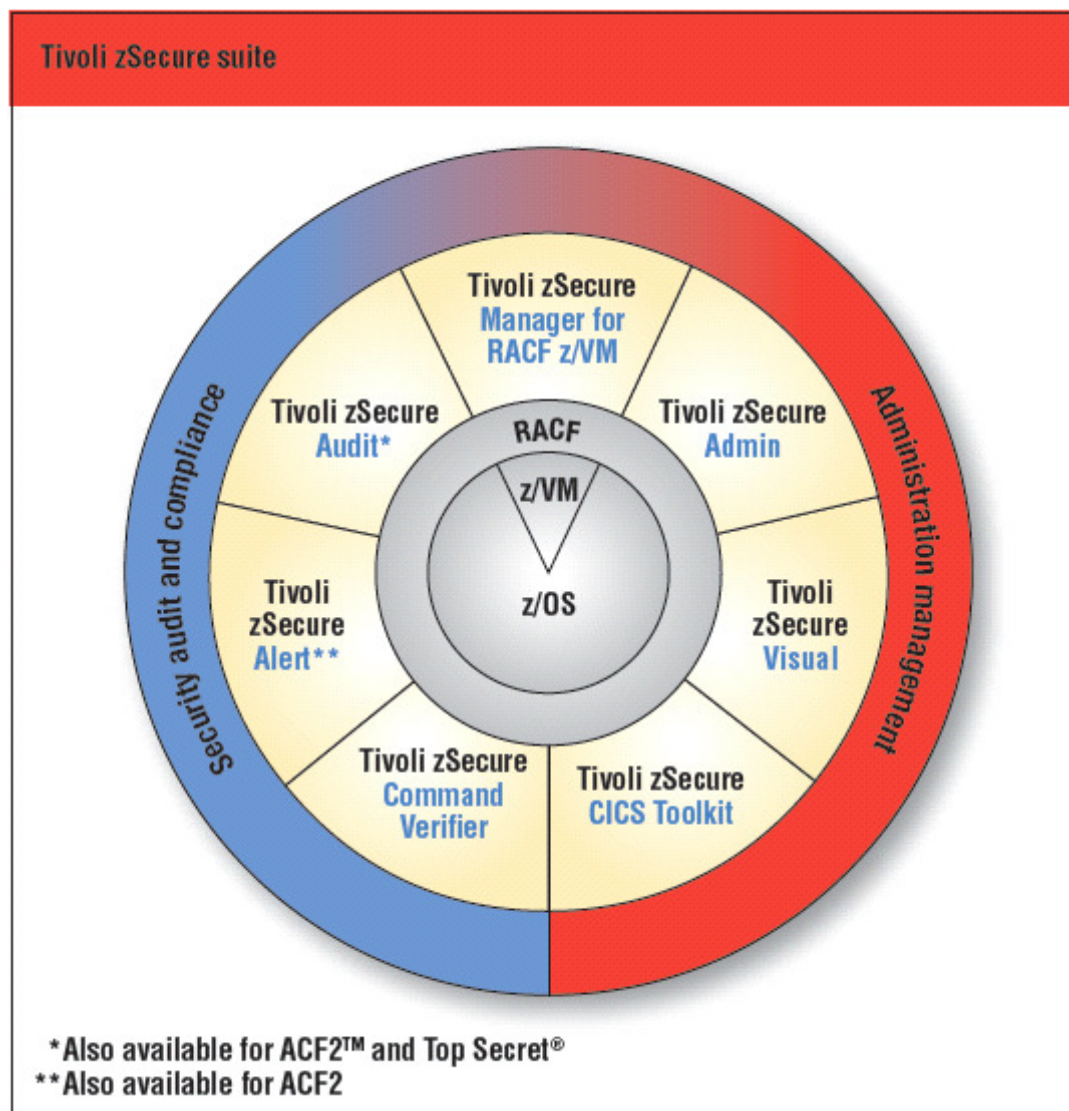
z/OS currency support

- 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)

z/OS currency support

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

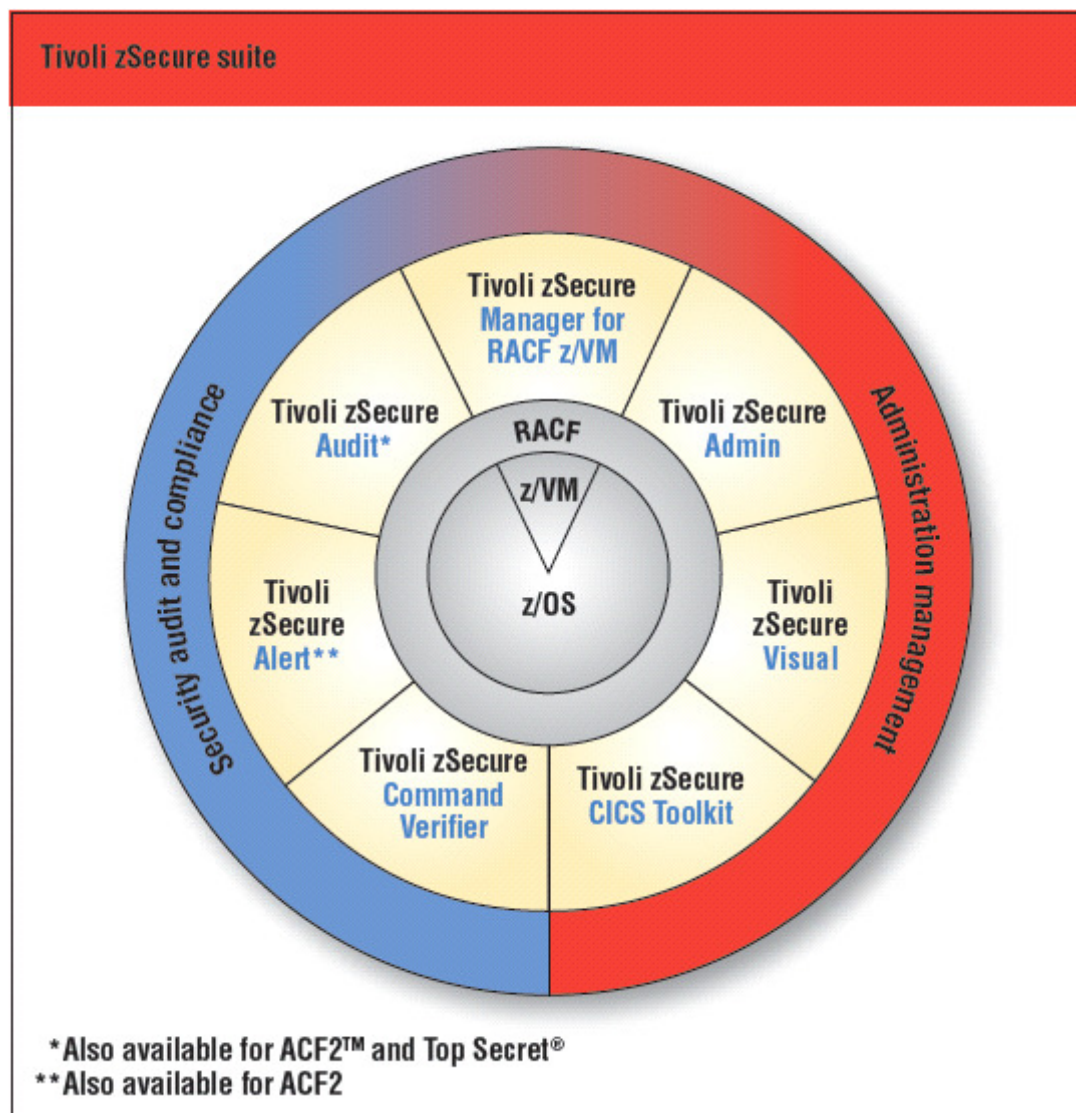
ACF2 currency



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)

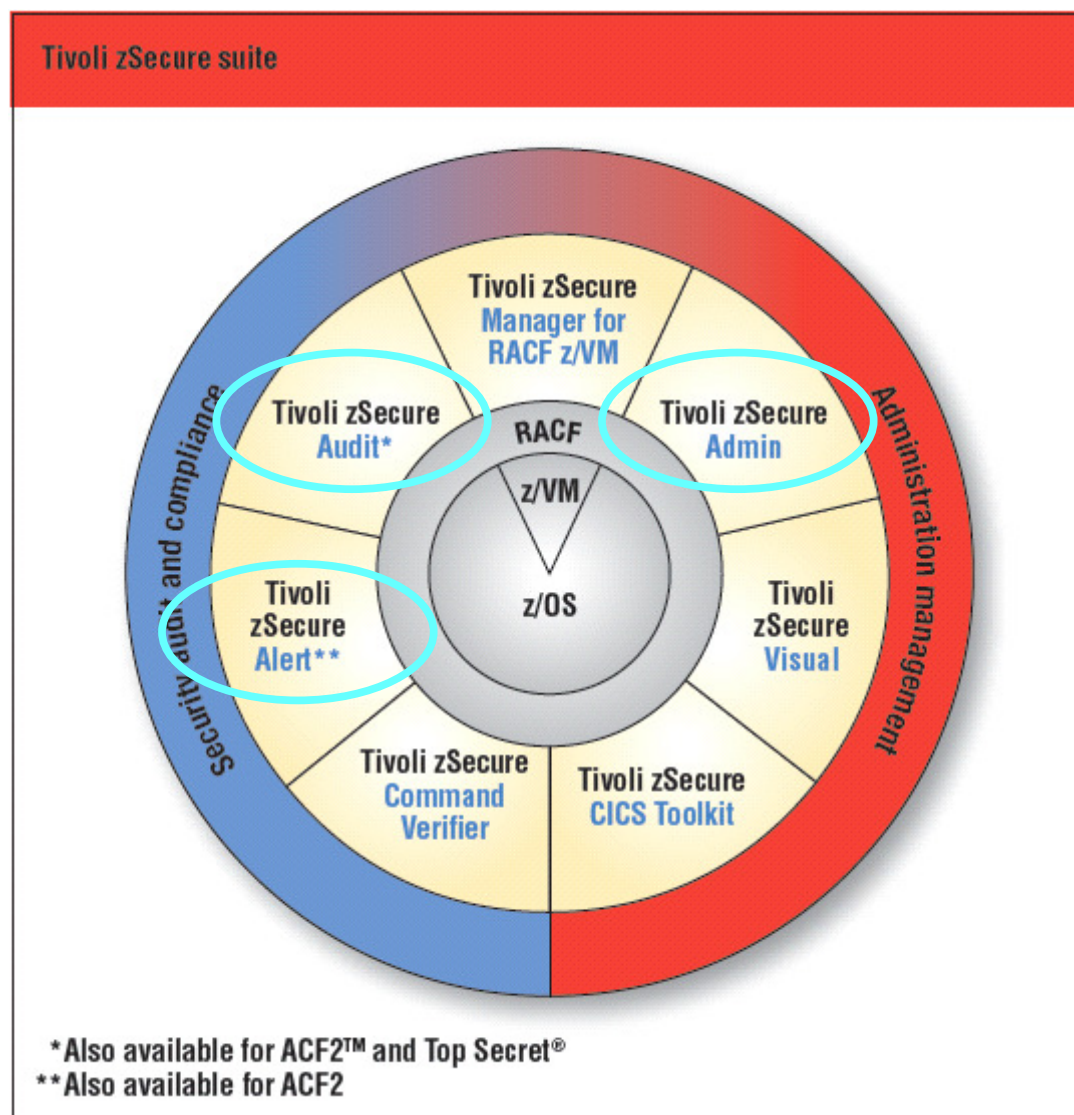
Globalization



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

CARLa update



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

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

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)

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 |

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)

Compare snapshots

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

- e.g. SHOW=DIFF

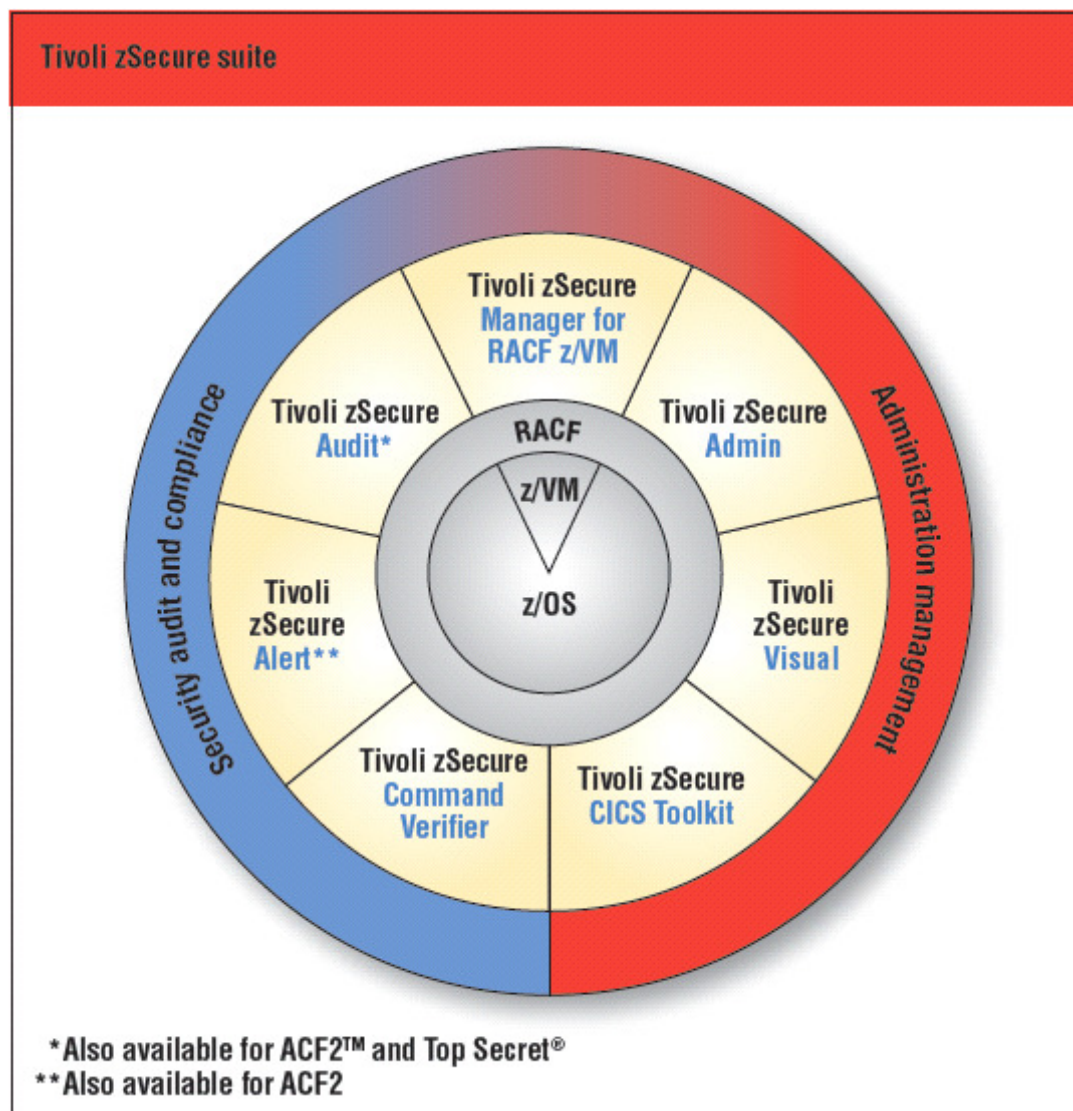
Find profiles that were added with privileges

```
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 | | |

Availability and Support



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

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

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

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>

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>

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

Questions?

