#SHAREorg

SHARE
Technology • Connections • Results

How zSecure 1.13 Increases Audit Capability and Reduces Audit Effort

Mark S Hahn
IBM

March 14, 2012
Session Number 10340

Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

- z/OS
- RACF

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- Introduce zSecure 1.13
- zSecure Audit and Admin
- Enhancements to CICS, IMS and DB2 collection
- Access Monitor – Uses and Don’ts
- Multiple System Communication
- TCP/IP / Increased SMF coverage
- Summary

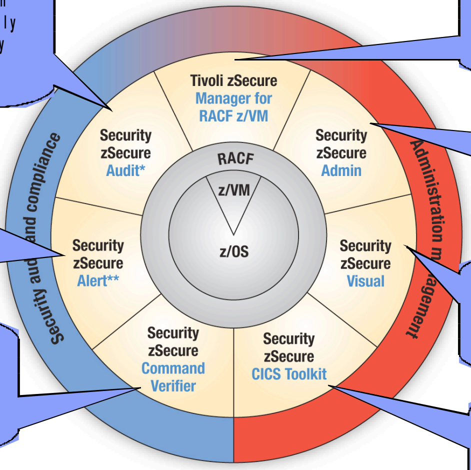
IBM Security zSecure Suite

IBM Security zSecure suite

Compliance and audit solution that enables you to automatically analyze and report on security events and detect security exposures

Real-time mainframe threat monitoring allowing you to monitor intruders and identify configuration mistakes that could hamper your compliance efforts

Policy enforcement solution that enforces compliance to company and regulatory policies by preventing erroneous commands



Combined audit and administration for RACF in the VM environment

Enables more efficient and effective RACF administration, using significantly less resources

Reduces the need for scarce, RACF-trained expertise through a Microsoft Windows-based GUI for RACF administration

Allows you to perform mainframe administrative tasks from a CICS environment, freeing up native-RACF resources

*Also available for ACF2™ and Top Secret®

**Also available for ACF2

zSecure 1.13 – Enhancements

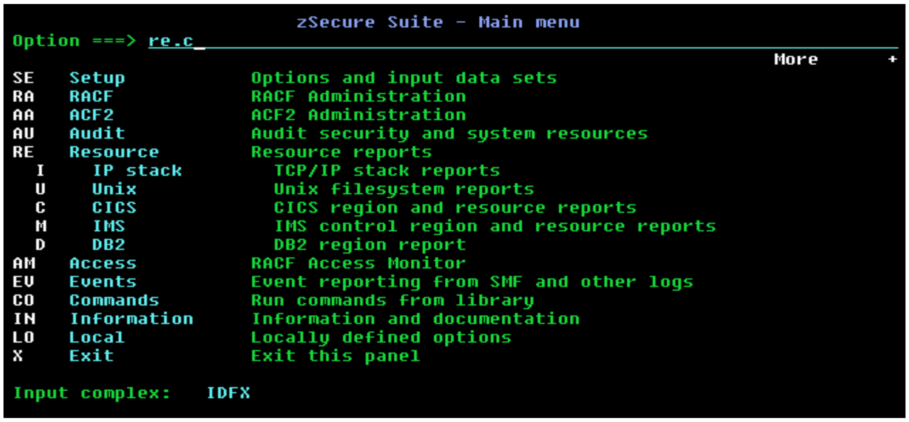
- Expanded collection of strategic subsystem information
  - CICS
  - IMS
  - DB2
- Enhanced Access Monitor data collection
- TCP/IP reporting enhanced

CICS, IMS and DB2

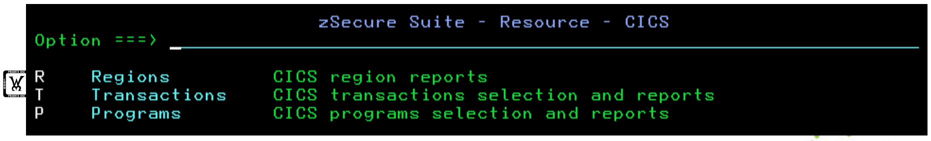
- Data now collected by periodic CKFREEZE
  - CICS datasets (DFHRPL, DFHCSD, etc.)
    - Also CICS CAT1/CAT2 transactions
  - IMS datasets (matrix, modblks, etc)
  - DB2 datasets (BSDS)
- Collect by default
- Ensure XMEM in effect
- Output used for:
  - SENSTRUS – Sensitive and TRUSTED report
  - Resources (C – CICS M – IMS D – DB2)

CICS, IMS, and DB2 Resource reports

- New menu options RE.C, RE.M, and RE.D



```
                          zSecure Suite - Main menu
Option ===> re.c_
                                                                More       +
SE    Setup                 Options and input data sets
RA    RACF                  RACF Administration
AA    ACF2                  ACF2 Administration
AU    Audit                 Audit security and system resources
RE    Resource              Resource reports
  I     IP stack              TCP/IP stack reports
  U     Unix                  Unix filesystem reports
  C     CICS                  CICS region and resource reports
  M     IMS                   IMS control region and resource reports
  D     DB2                   DB2 region report
AM    Access                RACF Access Monitor
EV    Events                Event reporting from SMF and other logs
CO    Commands              Run commands from library
IN    Information           Information and documentation
LO    Local                 Locally defined options
X     Exit                  Exit this panel

Input complex:    IDFX
```



```
                          zSecure Suite - Resource - CICS
Option ===> _

R     Regions               CICS region reports
T     Transactions          CICS transactions selection and reports
P     Programs              CICS programs selection and reports
```

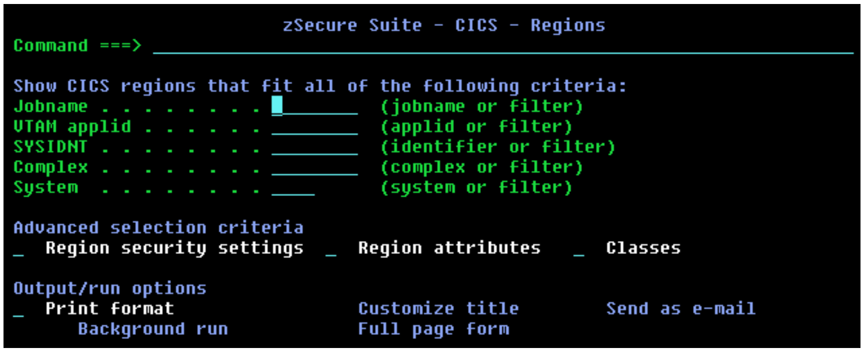
CICS, IMS, and DB2 Resource reports

- What can they drill in for?
  - Regions
  - Transactions
  - Programs / PSBs
  - RACF control specifics

- Key point
  - _ Print format
    - Enables batch run
    - Enables email results

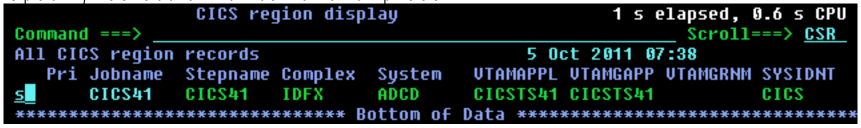
CICS region reports

- Go to menu option RE.C.R



```
                         zSecure Suite - CICS - Regions
Command ===> _________________________________________________________________

Show CICS regions that fit all of the following criteria:
Jobname . . . . . . . . ________  (jobname or filter)
VTAM applid . . . . . . ________  (applid or filter)
SYSIDNT . . . . . . . . ________  (identifier or filter)
Complex . . . . . . . . ________  (complex or filter)
System  . . . . . . . . ____      (system or filter)

Advanced selection criteria
_  Region security settings  _  Region attributes    _  Classes

Output/run options
_  Print format              Customize title        Send as e-mail
      Background run         Full page form
```

- Specify selection criteria and press ENTER



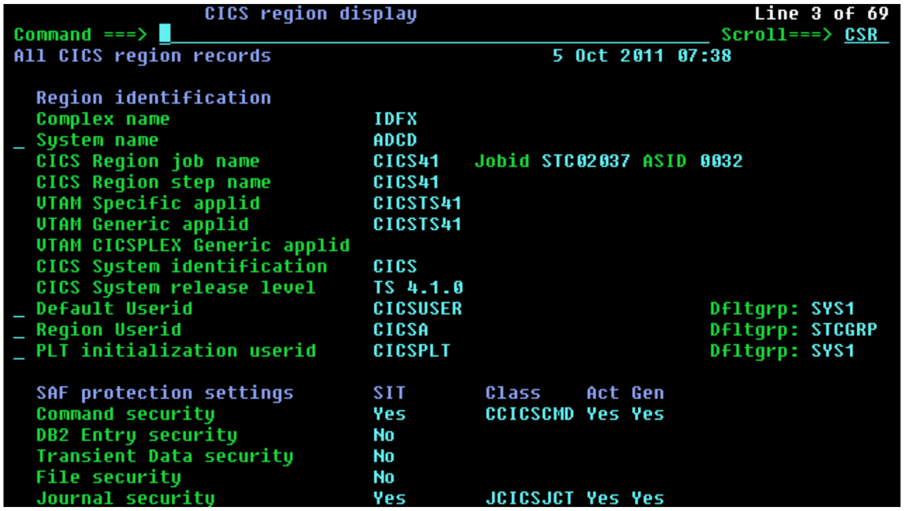
```
                 CICS region display                     1 s elapsed, 0.6 s CPU
Command ===> ____________________________________________________ Scroll===> CSR
All CICS region records                                  5 Oct 2011 07:38
   Pri Jobname  Stepname Complex  System   VTAMAPPL VTAMGAPP VTAMGRNM SYSIDNT
s         CICS41   CICS41   IDFX     ADCD     CICSTS41 CICSTS41          CICS
******************************* Bottom of Data ********************************
```

- Type 'S' against the CICS region you want to display

SHARE in Atlanta 2012

CICS region reports

This results in a CICS region display, including. SAF class info

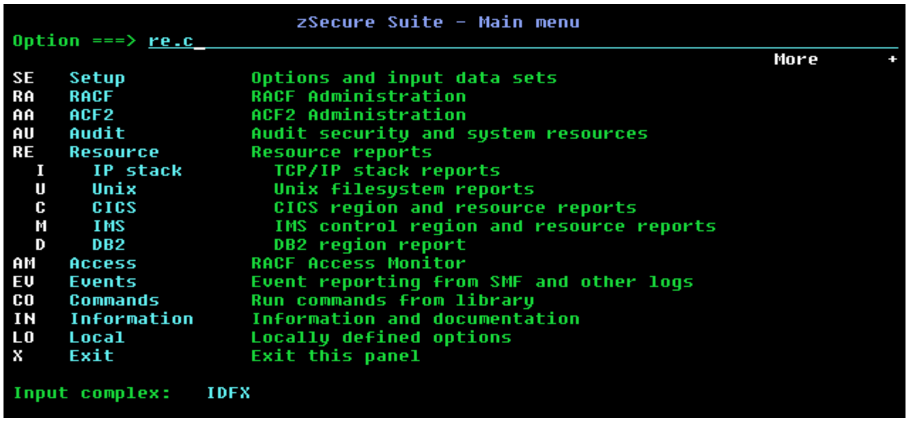


```
                  CICS region display                          Line 3 of 69
Command ===> _______________________________________________ Scroll===> CSR
All CICS region records                              5 Oct 2011 07:38

  Region identification
  Complex name                 IDFX
_ System name                  ADCD
  CICS Region job name         CICS41   Jobid STC02037 ASID 0032
  CICS Region step name        CICS41
  VTAM Specific applid         CICSTS41
  VTAM Generic applid          CICSTS41
  VTAM CICSPLEX Generic applid
  CICS System identification   CICS
  CICS System release level    TS 4.1.0
_ Default Userid               CICSUSER                     Dfltgrp: SYS1
_ Region Userid                CICSA                        Dfltgrp: STCGRP
_ PLT initialization userid    CICSPLT                      Dfltgrp: SYS1

  SAF protection settings      SIT       Class    Act Gen
  Command security             Yes       CCICSCMD Yes Yes
  DB2 Entry security           No
  Transient Data security      No
  File security                No
  Journal security             Yes       JCICSJCT Yes Yes
```

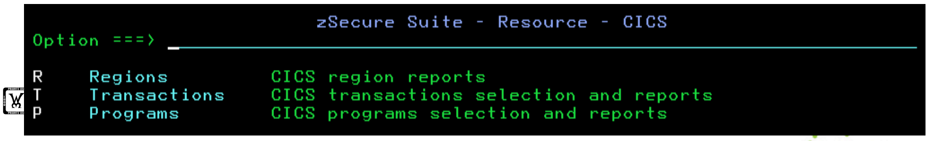
SHARE in Atlanta 2012

CICS reports

- New menu options RE.C, RE.M, and RE.D

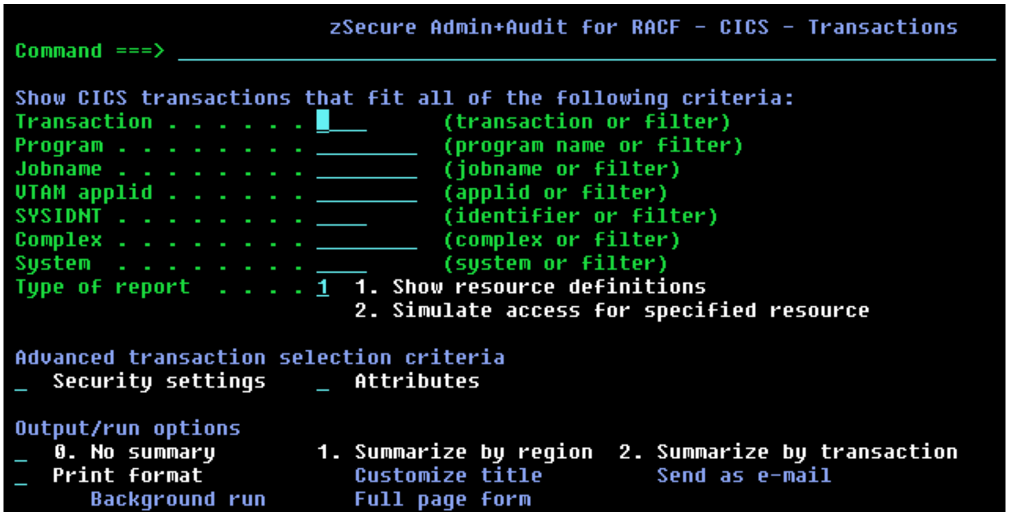


```
                                 zSecure Suite - Main menu
Option ===> re.c_
                                                                        More     +
SE    Setup                Options and input data sets
RA    RACF                 RACF Administration
AA    ACF2                 ACF2 Administration
AU    Audit                Audit security and system resources
RE    Resource             Resource reports
  I     IP stack             TCP/IP stack reports
  U     Unix                 Unix filesystem reports
  C     CICS                 CICS region and resource reports
  M     IMS                  IMS control region and resource reports
  D     DB2                  DB2 region report
AM    Access               RACF Access Monitor
EV    Events               Event reporting from SMF and other logs
CO    Commands             Run commands from library
IN    Information          Information and documentation
LO    Local                Locally defined options
X     Exit                 Exit this panel

Input complex:    IDFX
```



```
                                 zSecure Suite - Resource - CICS
Option ===> _

R     Regions              CICS region reports
T     Transactions         CICS transactions selection and reports
P     Programs             CICS programs selection and reports
```

CICS transactions reports

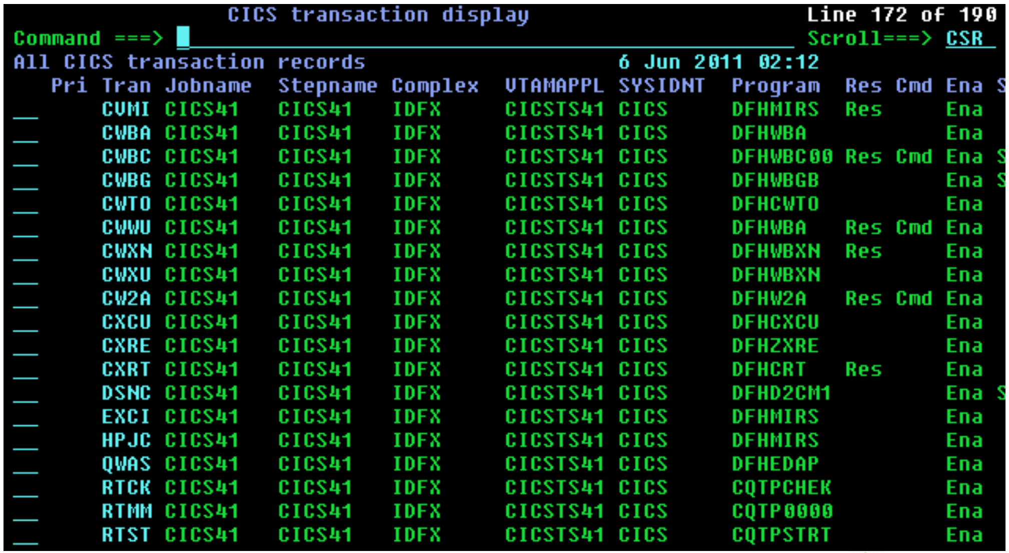


```
                          zSecure Admin+Audit for RACF - CICS - Transactions
Command ===> ________________________________________________________________

Show CICS transactions that fit all of the following criteria:
Transaction . . . . . . ____         (transaction or filter)
Program . . . . . . . . ________     (program name or filter)
Jobname . . . . . . . . ________     (jobname or filter)
VTAM applid . . . . . . ________     (applid or filter)
SYSIDNT . . . . . . . . ____         (identifier or filter)
Complex . . . . . . . . ________     (complex or filter)
System  . . . . . . . . ____         (system or filter)
Type of report  . . . . 1  1. Show resource definitions
                           2. Simulate access for specified resource

Advanced transaction selection criteria
_  Security settings       _  Attributes

Output/run options
_  0. No summary           1. Summarize by region   2. Summarize by transaction
_  Print format            Customize title          Send as e-mail
      Background run       Full page form
```

Summary options: None, By region, By transaction
Simulation option: Show access for uncaptured (non-existent) resources
Specify selection criteria and press ENTER

CICS transactions reports

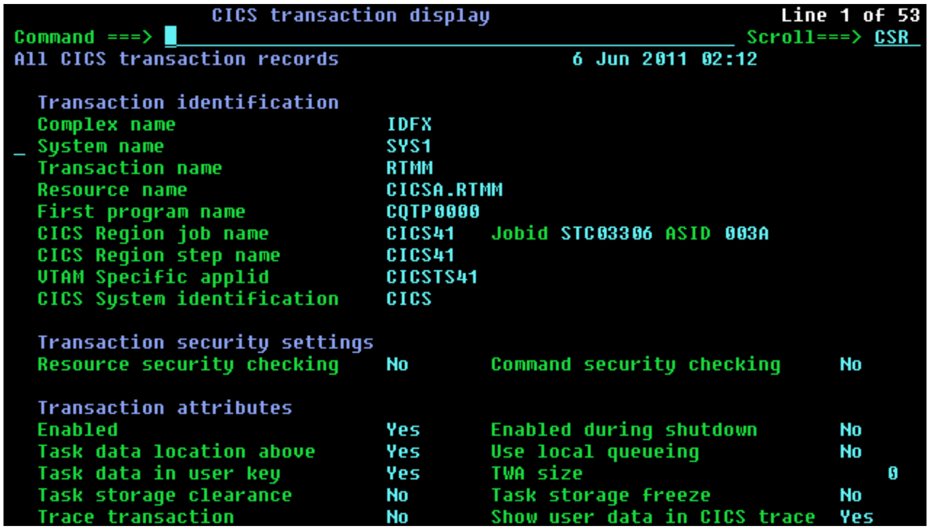
This results in a CICS transaction overview



```
                 CICS transaction display                      Line 172 of 190
Command ===> _                                                 Scroll===> CSR
All CICS transaction records                    6 Jun 2011 02:12
   Pri Tran Jobname  Stepname Complex  VTAMAPPL SYSIDNT  Program  Res Cmd Ena S
__      CVMI CICS41   CICS41   IDFX     CICSTS41 CICS     DFHMIRS  Res     Ena
__      CWBA CICS41   CICS41   IDFX     CICSTS41 CICS     DFHWBA           Ena
__      CWBC CICS41   CICS41   IDFX     CICSTS41 CICS     DFHWBC00 Res Cmd Ena S
__      CWBG CICS41   CICS41   IDFX     CICSTS41 CICS     DFHWBGB          Ena S
__      CWTO CICS41   CICS41   IDFX     CICSTS41 CICS     DFHCWTO          Ena
__      CWWU CICS41   CICS41   IDFX     CICSTS41 CICS     DFHWBA   Res Cmd Ena
__      CWXN CICS41   CICS41   IDFX     CICSTS41 CICS     DFHWBXN  Res     Ena
__      CWXU CICS41   CICS41   IDFX     CICSTS41 CICS     DFHWBXN          Ena
__      CW2A CICS41   CICS41   IDFX     CICSTS41 CICS     DFHW2A   Res Cmd Ena
__      CXCU CICS41   CICS41   IDFX     CICSTS41 CICS     DFHCXCU          Ena
__      CXRE CICS41   CICS41   IDFX     CICSTS41 CICS     DFHZXRE          Ena
__      CXRT CICS41   CICS41   IDFX     CICSTS41 CICS     DFHCRT   Res     Ena
__      DSNC CICS41   CICS41   IDFX     CICSTS41 CICS     DFHD2CM1         Ena S
__      EXCI CICS41   CICS41   IDFX     CICSTS41 CICS     DFHMIRS          Ena
__      HPJC CICS41   CICS41   IDFX     CICSTS41 CICS     DFHMIRS          Ena
__      QWAS CICS41   CICS41   IDFX     CICSTS41 CICS     DFHEDAP          Ena
__      RTCK CICS41   CICS41   IDFX     CICSTS41 CICS     CQTPCHEK         Ena
__      RTMM CICS41   CICS41   IDFX     CICSTS41 CICS     CQTP0000         Ena
__      RTST CICS41   CICS41   IDFX     CICSTS41 CICS     CQTPSTRT         Ena
```

Type 'S' against the CICS transaction you want to display

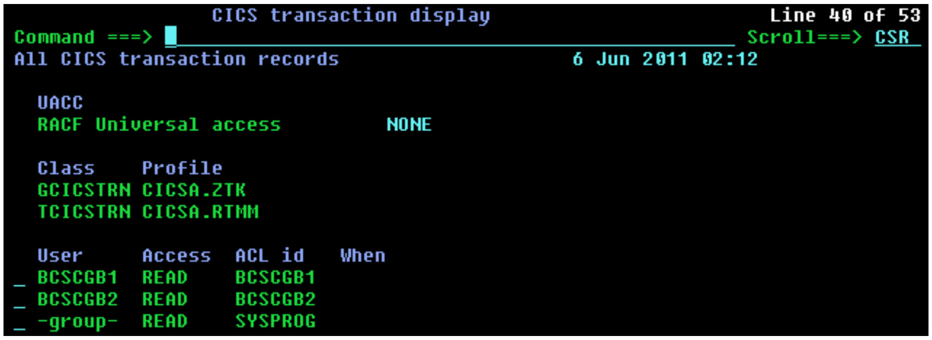
CICS transactions reports



```
                 CICS transaction display                        Line 1 of 53
Command ===> _                                                 Scroll===> CSR
All CICS transaction records                    6 Jun 2011 02:12

  Transaction identification
  Complex name                  IDFX
_ System name                   SYS1
  Transaction name              RTMM
  Resource name                 CICSA.RTMM
  First program name            CQTP0000
  CICS Region job name          CICS41   Jobid STC03306 ASID 003A
  CICS Region step name         CICS41
  VTAM Specific applid          CICSTS41
  CICS System identification    CICS

  Transaction security settings
  Resource security checking    No       Command security checking     No

  Transaction attributes
  Enabled                       Yes      Enabled during shutdown       No
  Task data location above      Yes      Use local queueing            No
  Task data in user key         Yes      TWA size                          0
  Task storage clearance        No       Task storage freeze           No
  Trace transaction             No       Show user data in CICS trace  Yes
```

Scroll down for additional details

CICS transactions reports



```
                  CICS transaction display                          Line 40 of 53
Command ===> _                                                      Scroll===> CSR
All CICS transaction records                           6 Jun 2011 02:12

  UACC
  RACF Universal access          NONE

  Class    Profile
  GCICSTRN CICSA.ZTK
  TCICSTRN CICSA.RTMM

  User     Access  ACL id   When
_ BCSCGB1  READ    BCSCGB1
_ BCSCGB2  READ    BCSCGB2
_ -group-  READ    SYSPROG
```

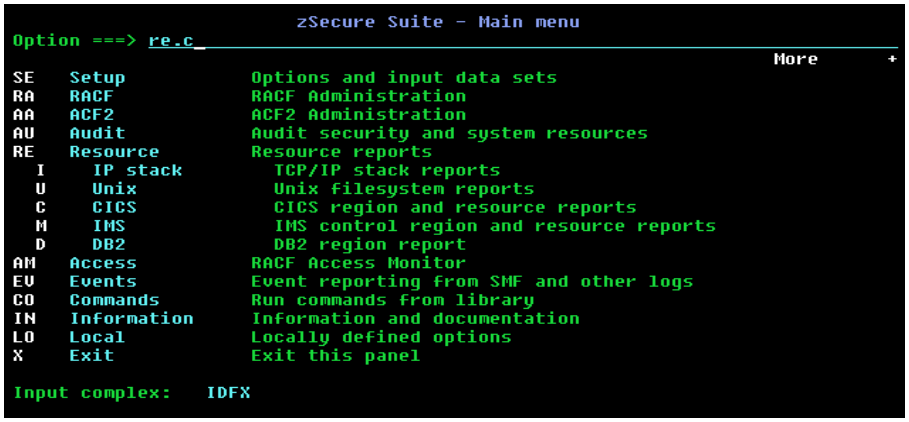
Contributing profiles (grouping-class and member-class)

Effective access to the “merged profile”

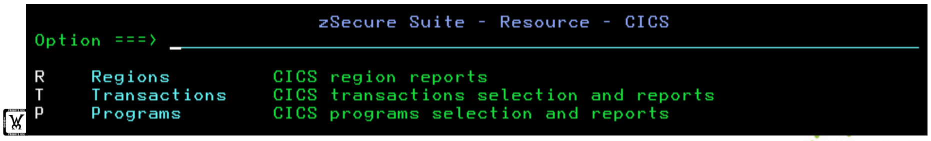
- ACL command to explode/resolve/effective
- ACL command to sort access list

CICS reports

- New menu options RE.C, RE.M, and RE.D

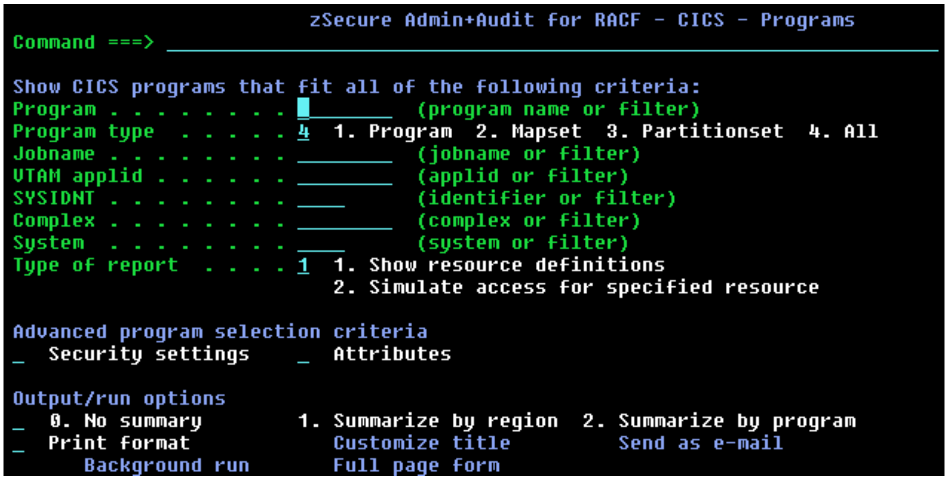


```
                        zSecure Suite - Main menu
Option ===> re.c_
                                                                More       +
SE   Setup                Options and input data sets
RA   RACF                 RACF Administration
AA   ACF2                 ACF2 Administration
AU   Audit                Audit security and system resources
RE   Resource             Resource reports
  I    IP stack             TCP/IP stack reports
  U    Unix                 Unix filesystem reports
  C    CICS                 CICS region and resource reports
  M    IMS                  IMS control region and resource reports
  D    DB2                  DB2 region report
AM   Access               RACF Access Monitor
EV   Events               Event reporting from SMF and other logs
CO   Commands             Run commands from library
IN   Information          Information and documentation
LO   Local                Locally defined options
X    Exit                 Exit this panel

Input complex:   IDFX
```



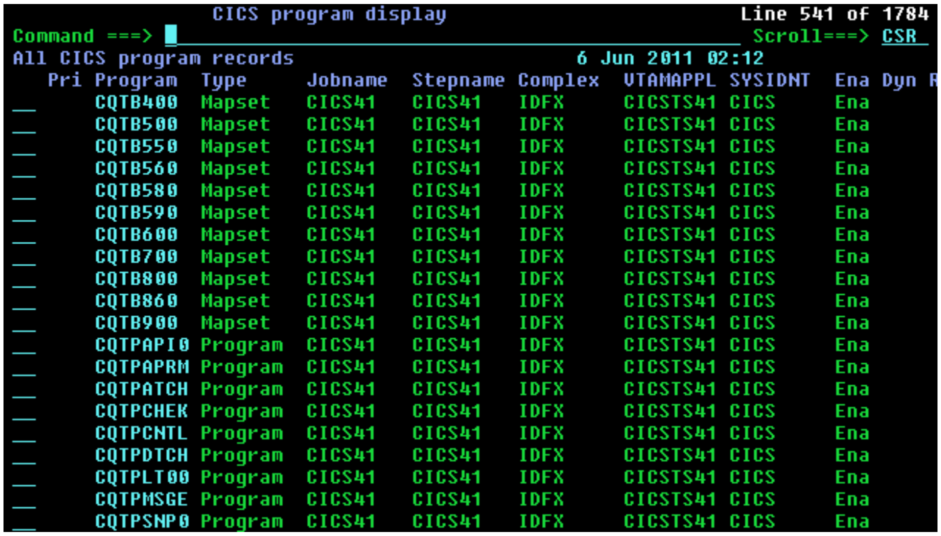
```
                        zSecure Suite - Resource - CICS
Option ===> _

R    Regions              CICS region reports
T    Transactions         CICS transactions selection and reports
P    Programs             CICS programs selection and reports
```

CICS Program reports



```
                          zSecure Admin+Audit for RACF - CICS - Programs
Command ===> __________________________________________________________________

Show CICS programs that fit all of the following criteria:
Program . . . . . . . . ________  (program name or filter)
Program type  . . . . . 4  1. Program  2. Mapset  3. Partitionset  4. All
Jobname . . . . . . . . ________  (jobname or filter)
VTAM applid . . . . . . ________  (applid or filter)
SYSIDNT . . . . . . . . ____      (identifier or filter)
Complex . . . . . . . . ________  (complex or filter)
System  . . . . . . . . ____      (system or filter)
Type of report  . . . . 1  1. Show resource definitions
                           2. Simulate access for specified resource

Advanced program selection criteria
_  Security settings     _  Attributes

Output/run options
_  0. No summary        1. Summarize by region  2. Summarize by program
_  Print format            Customize title         Send as e-mail
      Background run       Full page form
```

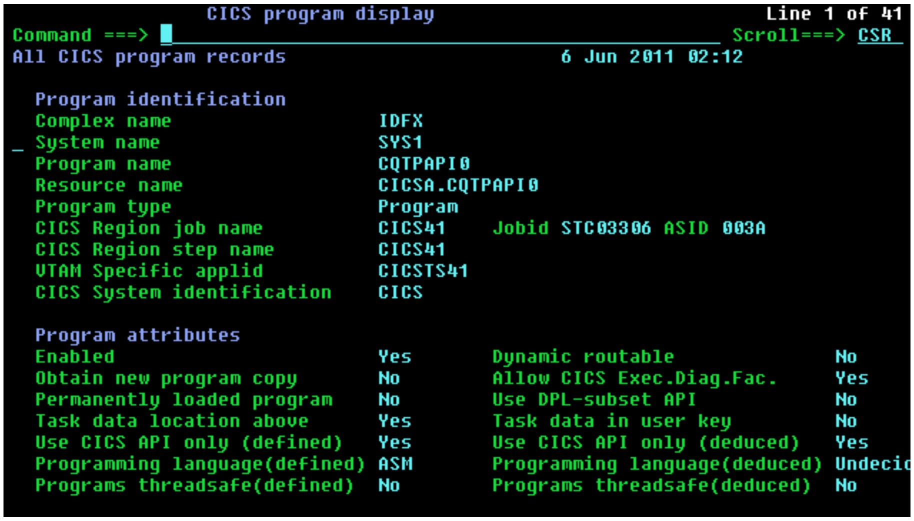
CICS Program Reports



```
                 CICS program display                            Line 541 of 1784
Command ===> _______________________________________________________ Scroll===> CSR
All CICS program records                               6 Jun 2011 02:12
   Pri Program  Type     Jobname  Stepname Complex  VTAMAPPL SYSIDNT  Ena Dyn R
__     CQTB400  Mapset   CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTB500  Mapset   CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTB550  Mapset   CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTB560  Mapset   CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTB580  Mapset   CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTB590  Mapset   CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTB600  Mapset   CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTB700  Mapset   CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTB800  Mapset   CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTB860  Mapset   CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTB900  Mapset   CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTPAPI0 Program  CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTPAPRM Program  CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTPATCH Program  CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTPCHEK Program  CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTPCNTL Program  CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTPDTCH Program  CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTPLT00 Program  CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTPMSGE Program  CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
__     CQTPSNP0 Program  CICS41   CICS41   IDFX     CICSTS41 CICS     Ena
```

This results in a CICS programs overview
Type 'S' against the CICS program you want to display

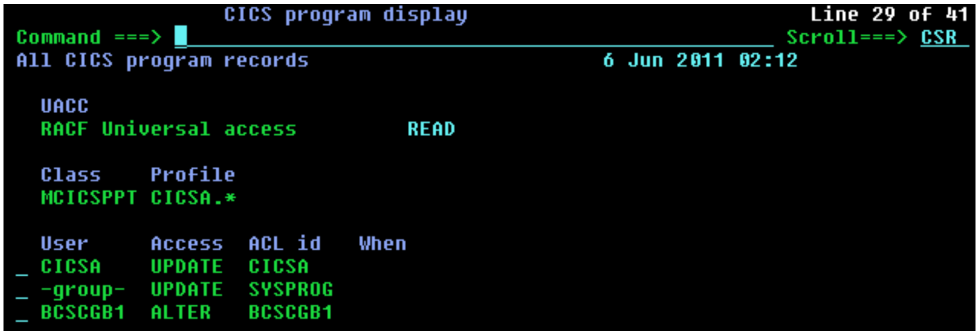
CICS Program Reports



```
                 CICS program display                              Line 1 of 41
Command ===> █                                                  Scroll===> CSR
All CICS program records                              6 Jun 2011 02:12

  Program identification
  Complex name                  IDFX
_ System name                   SYS1
  Program name                  CQTPAPI0
  Resource name                 CICSA.CQTPAPI0
  Program type                  Program
  CICS Region job name          CICS41     Jobid STC03306 ASID 003A
  CICS Region step name         CICS41
  VTAM Specific applid          CICSTS41
  CICS System identification    CICS

  Program attributes
  Enabled                       Yes        Dynamic routable              No
  Obtain new program copy       No         Allow CICS Exec.Diag.Fac.     Yes
  Permanently loaded program    No         Use DPL-subset API            No
  Task data location above      Yes        Task data in user key         No
  Use CICS API only (defined)   Yes        Use CICS API only (deduced)   Yes
  Programming language(defined) ASM        Programming language(deduced) Undecid
  Programs threadsafe(defined)  No         Programs threadsafe(deduced)  No
```

This results in a CICS program display
Scroll down for further details

CICS Program Report



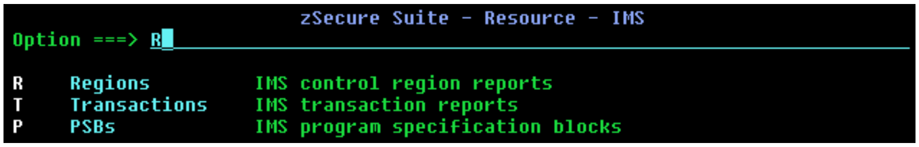
```
                 CICS program display                              Line 29 of 41
Command ===> █                                                  Scroll===> CSR
All CICS program records                              6 Jun 2011 02:12

  UACC
  RACF Universal access         READ

  Class     Profile
  MCICSPPT  CICSA.*

  User      Access   ACL id    When
_ CICSA     UPDATE   CICSA
_ -group-   UPDATE   SYSPROG
_ BCSCGB1   ALTER    BCSCGB1
```

Contributing profiles (grouping-class and member-class)

Effective access to the “merged profile”
- ACL command to explode/resolve/effective
- ACL command to sort access list

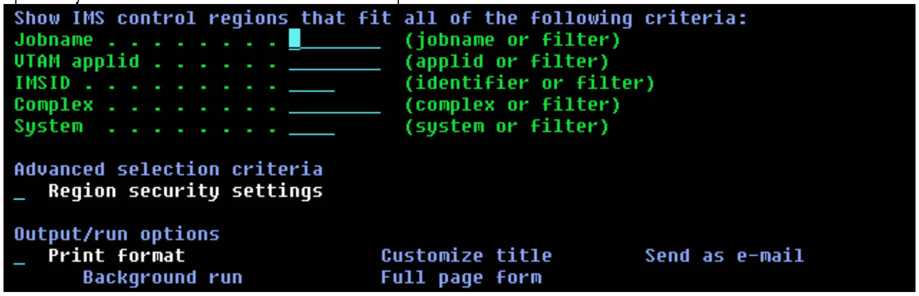
IMS control region reports

- Go to menu option RE.M.R



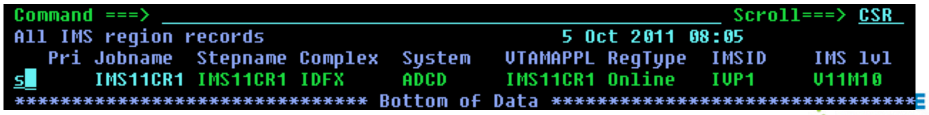
```
                             zSecure Suite - Resource - IMS
Option ===> R

R     Regions          IMS control region reports
T     Transactions     IMS transaction reports
P     PSBs             IMS program specification blocks
```

- Specify selection criteria and press ENTER



```
Show IMS control regions that fit all of the following criteria:
Jobname . . . . . . . . ________  (jobname or filter)
VTAM applid . . . . . . ________  (applid or filter)
IMSID . . . . . . . . . ____      (identifier or filter)
Complex . . . . . . . . ________  (complex or filter)
System  . . . . . . . . ____      (system or filter)

Advanced selection criteria
_  Region security settings

Output/run options
_  Print format                 Customize title        Send as e-mail
     Background run             Full page form
```

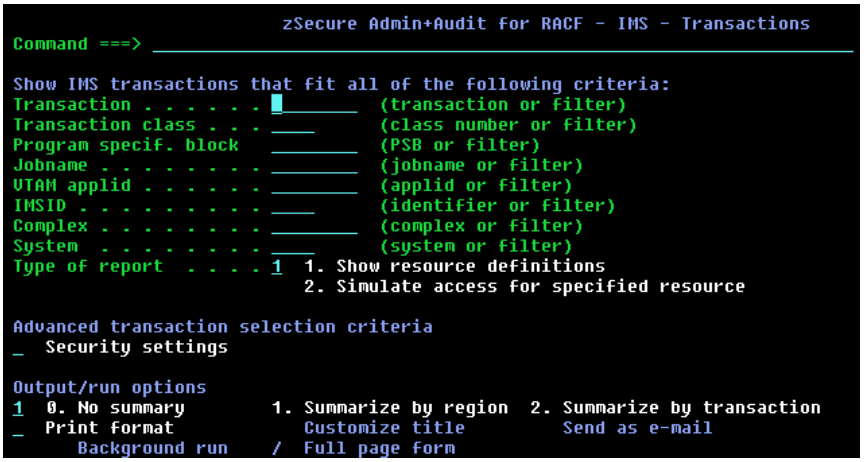
- Type 'S' against the IMS control region you want to display



```
Command ===> _______________________________________________ Scroll===> CSR
All IMS region records                            5 Oct 2011 08:05
   Pri Jobname  Stepname Complex  System  VTAMAPPL RegType  IMSID    IMS lvl
s       IMS11CR1 IMS11CR1 IDFX     ADCD    IMS11CR1 Online   IVP1     V11M10
******************************* Bottom of Data ********************************
```

IMS control region reports

- Go to menu option RE.M.T

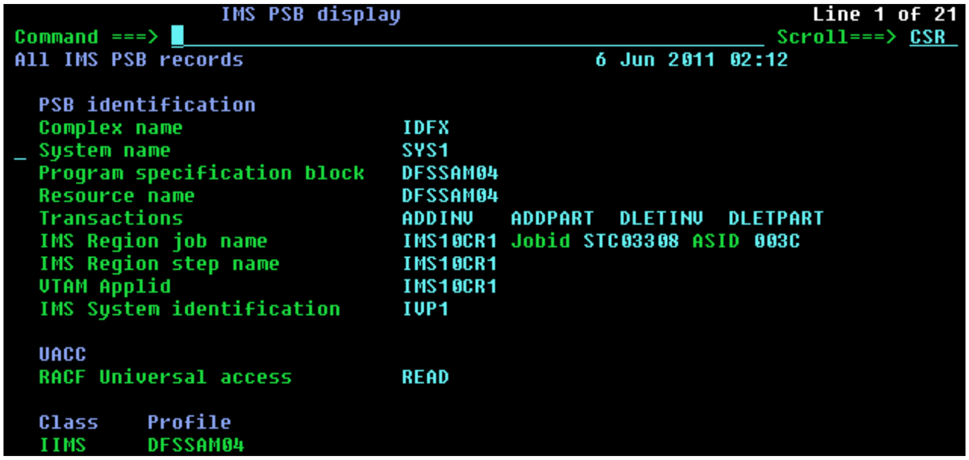


```
                        zSecure Admin+Audit for RACF - IMS - Transactions
Command ===> ____________________________________________________________

Show IMS transactions that fit all of the following criteria:
Transaction . . . . . . ________  (transaction or filter)
Transaction class . . . ____      (class number or filter)
Program specif. block   ________  (PSB or filter)
Jobname . . . . . . . . ________  (jobname or filter)
VTAM applid . . . . . . ________  (applid or filter)
IMSID . . . . . . . . . ____      (identifier or filter)
Complex . . . . . . . . ________  (complex or filter)
System  . . . . . . . . ____      (system or filter)
Type of report  . . . . 1  1. Show resource definitions
                           2. Simulate access for specified resource

Advanced transaction selection criteria
_  Security settings

Output/run options
1  0. No summary          1. Summarize by region   2. Summarize by transaction
_  Print format           Customize title          Send as e-mail
     Background run     / Full page form
```

- Summary options: None, By region, By transaction
- Simulation option: Show access for uncaptured (non-existent) resources
- Specify selection criteria and press ENTER

IMS PSB Report

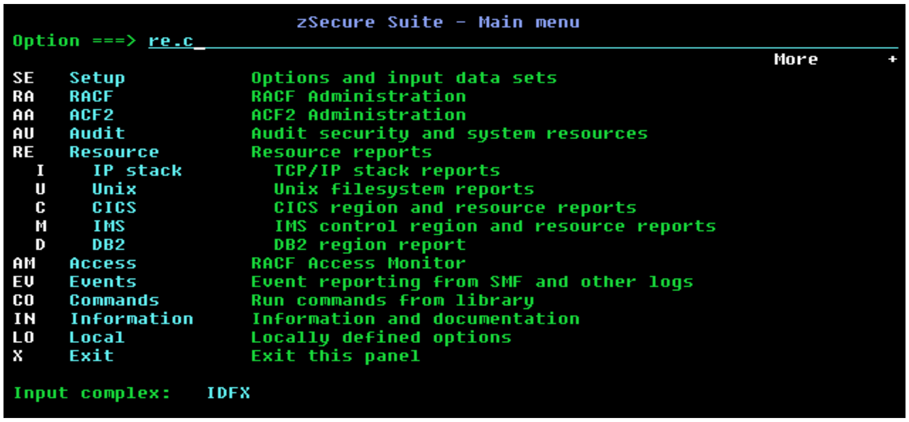
In addition – IMS PSB Report



```
                 IMS PSB display                                 Line 1 of 21
Command ===> _______________________________________________  Scroll===> CSR
All IMS PSB records                                 6 Jun 2011 02:12

  PSB identification
  Complex name                  IDFX
_ System name                   SYS1
  Program specification block   DFSSAM04
  Resource name                 DFSSAM04
  Transactions                  ADDINV   ADDPART   DLETINV   DLETPART
  IMS Region job name           IMS10CR1 Jobid STC03308 ASID 003C
  IMS Region step name          IMS10CR1
  VTAM Applid                   IMS10CR1
  IMS System identification     IVP1

  UACC
  RACF Universal access         READ

  Class    Profile
  IIMS     DFSSAM04
```

CICS, IMS, and DB2 Resource reports

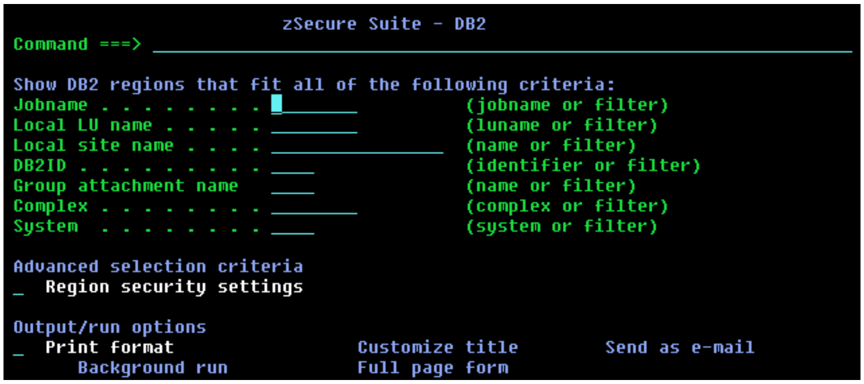
- New menu options RE.C, RE.M, and RE.D



```
                         zSecure Suite - Main menu
Option ===> re.c_
                                                            More     +
SE    Setup               Options and input data sets
RA    RACF                RACF Administration
AA    ACF2                ACF2 Administration
AU    Audit               Audit security and system resources
RE    Resource            Resource reports
  I     IP stack            TCP/IP stack reports
  U     Unix                Unix filesystem reports
  C     CICS                CICS region and resource reports
  M     IMS                 IMS control region and resource reports
  D     DB2                 DB2 region report
AM    Access              RACF Access Monitor
EV    Events              Event reporting from SMF and other logs
CO    Commands            Run commands from library
IN    Information         Information and documentation
LO    Local               Locally defined options
X     Exit                Exit this panel

Input complex:   IDFX
```

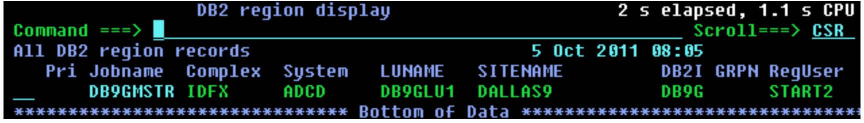
DB2 region reports

- Go to menu option RE.D



```
                         zSecure Suite - DB2
Command ===> ________________________________________________________________

Show DB2 regions that fit all of the following criteria:
Jobname . . . . . . . . . ________         (jobname or filter)
Local LU name . . . . . . ________         (luname or filter)
Local site name . . . . . ________________ (name or filter)
DB2ID . . . . . . . . . . ____             (identifier or filter)
Group attachment name   . ____             (name or filter)
Complex . . . . . . . . . ________         (complex or filter)
System  . . . . . . . . . ____             (system or filter)

Advanced selection criteria
_  Region security settings

Output/run options
_  Print format                Customize title        Send as e-mail
      Background run           Full page form
```

- Specify selection criteria and press ENTER

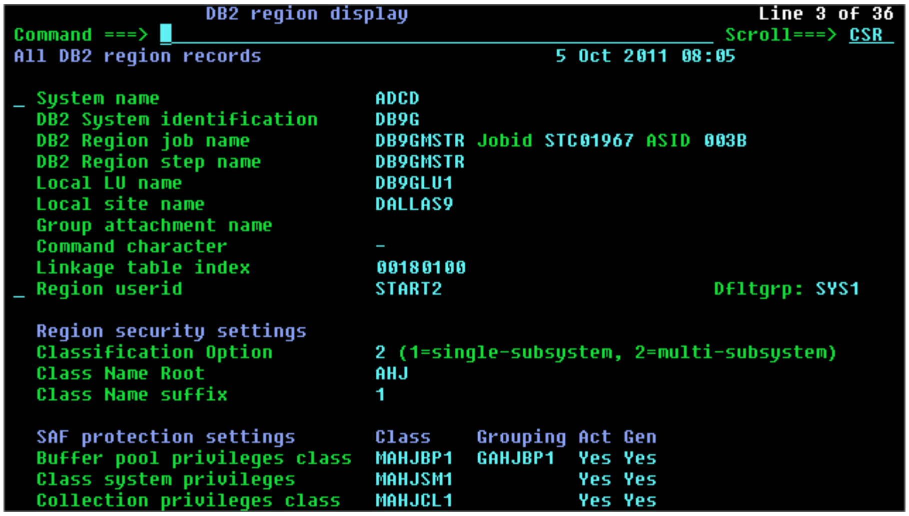


```
                 DB2 region display                        2 s elapsed, 1.1 s CPU
Command ===> _                                                   Scroll===> CSR
All DB2 region records                                     5 Oct 2011 08:05
   Pri Jobname  Complex  System   LUNAME    SITENAME         DB2I GRPN RegUser
___     DB9GMSTR IDFX     ADCD     DB9GLU1   DALLAS9          DB9G      START2
******************************* Bottom of Data ********************************
```

- Type 'S' against the DB2 region you want to display

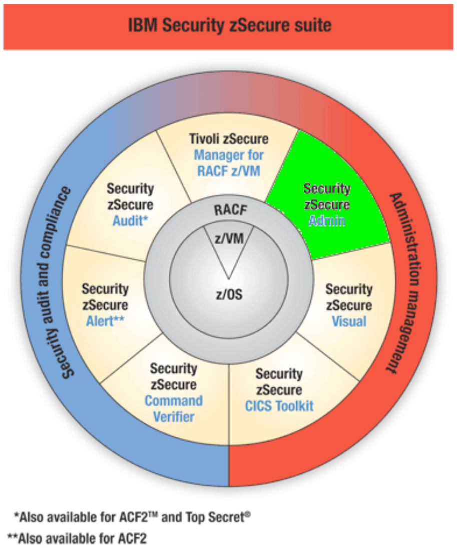
DB2 region reports

- ✔ This results in a DB2 region display



```
                  DB2 region display                                Line 3 of 36
Command ===> _                                                   Scroll===> CSR
All DB2 region records                                   5 Oct 2011 08:05

_ System name                     ADCD
  DB2 System identification       DB9G
  DB2 Region job name             DB9GMSTR Jobid STC01967 ASID 003B
  DB2 Region step name            DB9GMSTR
  Local LU name                   DB9GLU1
  Local site name                 DALLAS9
  Group attachment name
  Command character               -
  Linkage table index             00180100
_ Region userid                   START2                         Dfltgrp: SYS1

  Region security settings
  Classification Option           2 (1=single-subsystem, 2=multi-subsystem)
  Class Name Root                 AHJ
  Class Name suffix               1

  SAF protection settings         Class    Grouping Act Gen
  Buffer pool privileges class    MAHJBP1  GAHJBP1  Yes Yes
  Class system privileges         MAHJSM1           Yes Yes
  Collection privileges class     MAHJCL1           Yes Yes
```

Access Monitor


IBM Security zSecure suite
Tivoli zSecure Manager for RACF z/VM
Security zSecure Admin
Security zSecure Audit*
RACF
z/VM
z/OS
Security zSecure Alert**
Security zSecure Visual
Security zSecure Command Verifier
Security zSecure CICS Toolkit
Security audit and compliance
Administration management
*Also available for ACF2™ and Top Secret®
**Also available for ACF2

zSecure Admin

Access Monitor – Improved consolidation

- New ACCESS record format (V1.13 format)
  - Created in daily consolidation (C2PAMCVT)
  - Enables parallel reading and consolidation
- Consolidation improved
  - Very little virtual storage
  - Very fast process
- Reporting unaffected
  - Any combination of V1.11 format and V1.13 format
  - No performance changes

Access Monitor – Gotchas

- What Access Monitor is
  - Tool for finding which profiles or ACLs are unused
  - PERIOD
- What Access Monitor is NOT
  - A RACHECK tracing tool
  - A microscope into RACF calls

Access Monitor – Gotchas

- SMF v Access Monitor
  - Trust SMF trail
    - AM sees (interim) “nolog” calls
    - SMF sees final result calls.
  - ALTER v READ access experience
    - zSecure Forum question*
      http://www.ibm.com/developerworks/forums/forum.jspa?forumID=1255
- 3rd party calls
  - Before z/OS 1.13 POE support
    - Deceptive interpretation – info accurate, but interim (3rd party calls) cause cloudy interpretation
- Maximize consolidation
  - Especially with 1.13 support

Access Monitor –
Gotchas – ALTER Access reporting

Access Monitor reports INTENT=ALTER ACCESS_ALLOWED=NONE for datasets in a CHECKDSN statement in a CNFCOLL run. The RACF profile gives the userid READ access to this dataset.
I dumped all the relevant fields within TYPE=ACCESS:

Indeed, CKFCOLL uses a RACROUTE STATUS=ACCESS to find out what access it has to sensitive system data sets and to the data sets specified on the CHECKDSN statement. If the task is APF authorized, it then bypasses RACF and processes the data sets to obtain member names and to calculate checksums. If the task is not APF authorized, it only processes the data sets to which it has READ access or higher.

Access Monitor does not currently recognize the difference between a regular request for ALTER access and a STATUS=ACCESS request. That means that for all the above data sets, Access Monitor reports that CKFCOLL tries to ALTER the data set.

Access Monitor –
Gotchas

- Consolidation data set names
  - Plan to use DPREF=
  - Set HLQs to useful pattern
    - like using yyyymmdd instead of mmddyyyy
    - Prefixing interval (Dyyy or Myyy or Yyyy) for brevity
  - XXX.YYY.Dyymmdd – daily
    DPREF=XXX.YYY.D1202 will give all existing Feb 2012
    and you can go for DPREF=XXX.YYY.D12 for all 2012
  - XXX.YYY.Myymm – for monthly consolidations

Access Monitor –
Collect job name/port of entry

- Sometimes difficult to match recorded access to process
  - Especially for batch workloads (TWS)
- Sometimes info needed for restructure of access
  - When splitting workloads based on application.
  - When reorganizing generic profiles based on access
  - Conditional access
- Collect additional information
  - Jobname (or stcname)
  - Port of entry

- Extra fields in ACCESS newlist
- Extra selection and reporting fields in ISPF user interface.

Access Monitor –
Collect job name/port of entry

- Extra information has some costs
  - More space in Access Monitor data sets
  - Consolidation gets less efficient (more than offset)
- Collection only for specific events
  - Default is **no** detail collection
  - Jobname only for listed userids
  - POE name only for listed classes and listed POE class
- Three new control/configuration files
  - C2PAMJOB - Userids for which to collect job names
  - C2PAMPCL - POE classes for which to collect POE names
  - C2PAMRCL - Resource classes for which to collect POE names

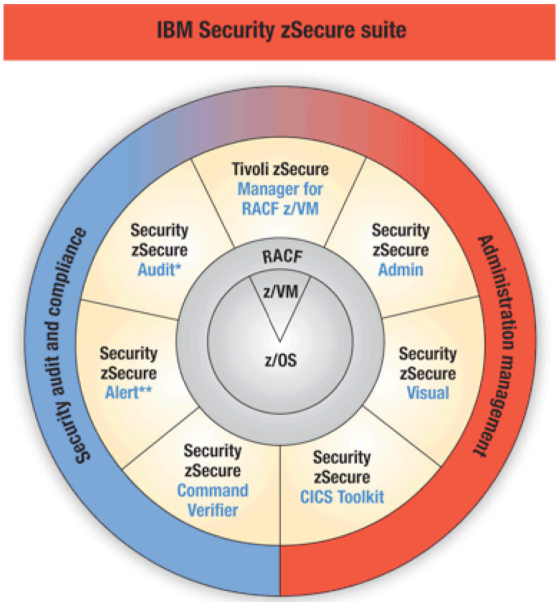
Access Monitor –
Data reduction JESSPOOL, GDGs

- Improve efficiency of Access Monitor consolidation
- Unique parts of resource names flattened
- JESSPOOL
  - IDFX.C2PSUSER.C2PACMON.STC02236.D0000102.?
    - JOBID =STC02236
    - DSID =D0000102
    - Replace by x (lowercase letter x)
  - IDFX.C2PSUSER.C2PACMON.Sxxxxxxx.Dxxxxxxx.?
- GDG
  - IBMUSER.GDGDATA.G0001V00
    - Generation and version number
    - Replace by n (lowercase letter n)
  - IBMUSER.GDGDATA.GnnnnVnn
- Most efficient in daily consolidation (C2PAMCOL)

Access Monitor –
Collect “Authority Used”

- Had to wait for z/OS & RACF to provide this information
- Collect use of OPERATIONS/SPECIAL attribute
- Collect authority granted by EXIT
- Collect status of OPERATIONS/SPECIAL at time of event
- Needs RACF support
  - z/OS 1.13
  - PTF on z/OS 1.12 (UA61826 – SAF, UA61827 – RACF)
- New flags in Access Monitor records.
  If present, records are consolidated separately
- New fields in ACCESS NEWLIST
  - ACCESS_OPERATIONS
  - ACCESS_SPECIAL
  - ACCESS_USED_EXIT
  - ATTRIB_OPERATIONS
  - ATTRIB_SPECIAL

TCP/IP security extensions


IBM Security zSecure suite
Tivoli zSecure Manager for RACF z/VM
Security zSecure Audit*
Security zSecure Admin
Security zSecure Alert**
Security zSecure Visual
Security zSecure Command Verifier
Security zSecure CICS Toolkit
RACF
z/VM
z/OS
Security audit and compliance
Administration management

*Also available for ACF2™ and Top Secret®
**Also available for ACF2

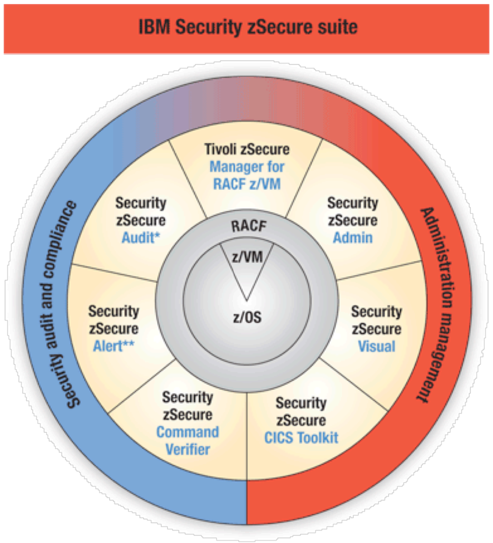
TCP/IP – auditing enhancements

- Communications Server (CS) Resolver settings
  - zSecure Collect can retrieve these on z/OS V1R13 and up
  - Settings shown in the CS Resolver (IPRESOLV) report
  - Implied trust is shown in Trusted/Trustees reports
  - which users can redirect all DNS queries from the users' own address spaces
  - which users can control CS Resolver configuration parameters, and thus redirect all IP traffic to host names from all users' address spaces after the next CS Resolver setup modification
- z/OS V1R13 introduces SAF resources to control whether an application can create and delete an application-specific Dynamic VIPA
  - zSecure can report these from CKFREEZE or SMF 119 records
- z/OS V1R13 SMF type 119 IPSec records can show NAT traversal information for IKE v2 in the RECORDDESC

TCP/IP – Dynamic VIPA

- New information added to TCP/IP VIPA configuration (IP_VIPA) reports:
  - RESOURCE – SERVAUTH resource of the form EZB.MODDVIPA.*sysname.tcpname.resname*
    - *sysname* is MVS &SYSNAME system symbol
    - *tcpname* is the name of the procedure that started the stack
    - *resname* is the value after ‘SAF’ on a SAFNAME statement
  - RESNAME – the *resname* in the above
- Also to SMF reports as IP_VIPA_RESOURCE and IP_VIPA_RESNAME, and IP_VIPA_RACF_PROFILE contains the matching profile for SMF 119 TCP/IP stack records
- With READ access a user can
  - Create or delete an application-specific DVIPA specified by a specific VIPARANGE statement, and a SIOCSVIPA(6) IOCTL call or the MODDVIPA utility

SMF record support extensions


IBM Security zSecure suite
Tivoli zSecure Manager for RACF z/VM
Security zSecure Audit*
Security zSecure Admin
Security zSecure Alert**
Security zSecure Visual
Security zSecure Command Verifier
Security zSecure CICS Toolkit
RACF
z/VM
z/OS
Security audit and compliance
Administration management

*Also available for ACF2™ and Top Secret®
**Also available for ACF2

zSecure Audit
zSecure Alert

New SMF record types and fields

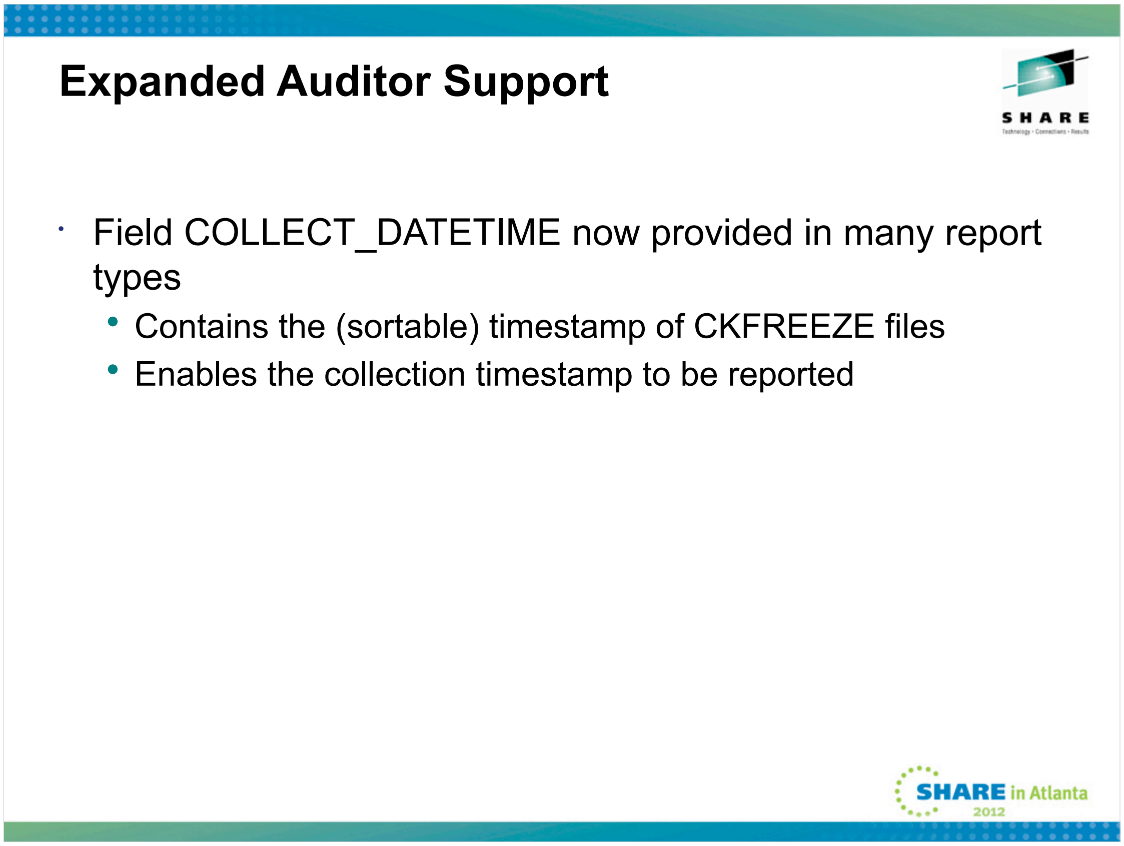
- Support for LDAP events written to SMF as record type 83-3
  - Recognized EVENTs:
  - 1 ADD 7 EXTENDED
  - 2 BIND 8 MODIFY
  - 3 COMPARE 9 MODIFYDN
  - 4 CONNECT 10 SEARCH
  - 5 DELETE 11 UNBIND
  - 6 DISCONNECT
  - New fields LDAP_CONN_ID, LDAP_CLIENT_SECL, and LDAP_ENTRY_NM for the connection ID, the LDAP client seclabel, and the target entry (Distinguished Name) of the operation: BIND, DELETE, ADD, etc.

- Additional SMF updates shown later under z/OS currency

Expanded SMF Reporting

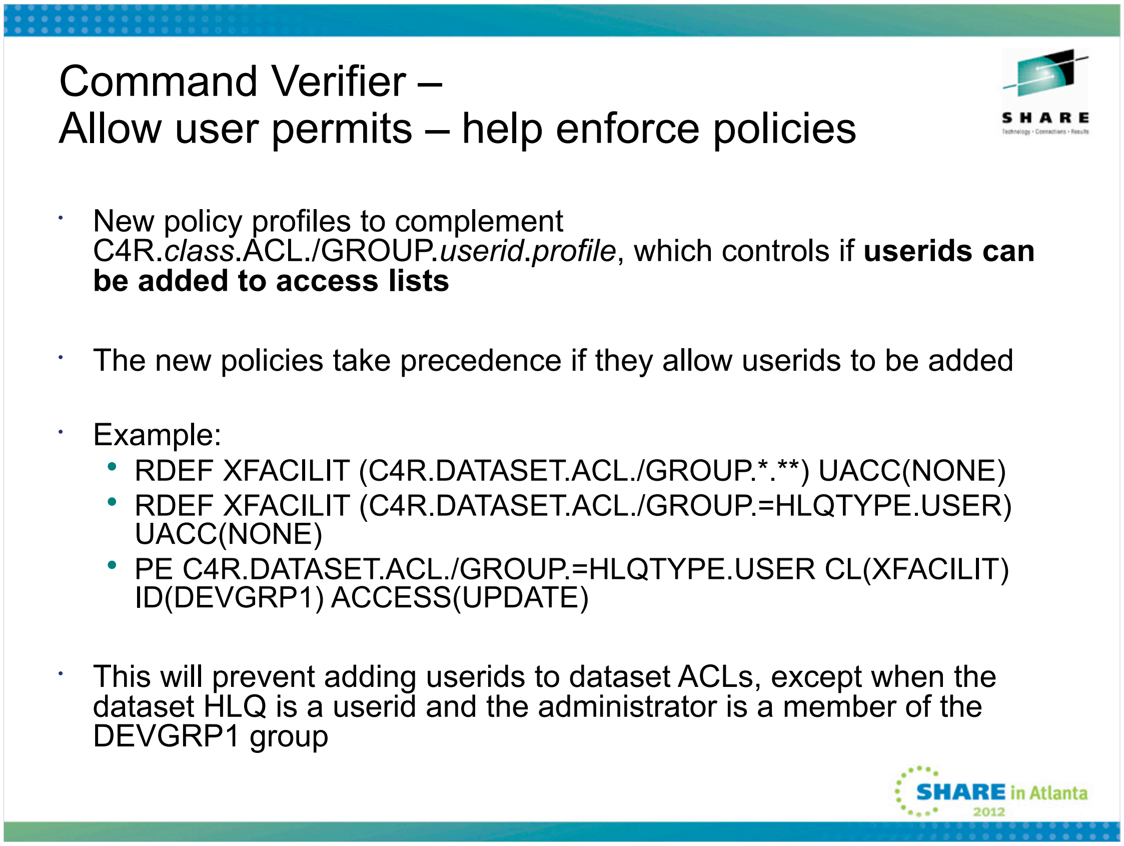
- Support for SMF record **type 89 subtype 1** Product Intersection Data
  - for products registered with the IFAUSAGE service
  - when a program at ADDRSP level invokes one at the TASK level

- Support for SMF record **type 42 subtype 26** extended to UNIX_* fields
  - Written for create/remove/rename of file object for NFS
  - Provides the NFS client's information, the type of operation and object descriptive information
  - Extensions to fields RECORDDESC, UNIX_* and others
    - more details in speaker notes
- SMF recording for SMF record **type 92** (z/OS UNIX) and **type 80** (RACF) records need to be enabled in order to derive the UNIX path name.



Expanded Auditor Support

- Field COLLECT_DATETIME now provided in many report types
  - Contains the (sortable) timestamp of CKFREEZE files
  - Enables the collection timestamp to be reported



Command Verifier –
Allow user permits – help enforce policies

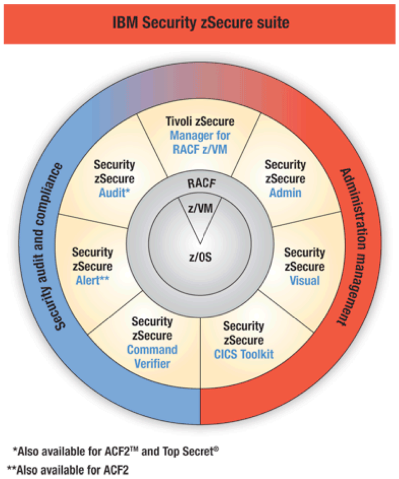
- New policy profiles to complement C4R.*class*.ACL./GROUP.*userid.profile*, which controls if **userids can be added to access lists**

- The new policies take precedence if they allow userids to be added

- Example:
  - RDEF XFACILIT (C4R.DATASET.ACL./GROUP.*.**) UACC(NONE)
  - RDEF XFACILIT (C4R.DATASET.ACL./GROUP.=HLQTYPE.USER) UACC(NONE)
  - PE C4R.DATASET.ACL./GROUP.=HLQTYPE.USER CL(XFACILIT) ID(DEVGRP1) ACCESS(UPDATE)

- This will prevent adding userids to dataset ACLs, except when the dataset HLQ is a userid and the administrator is a member of the DEVGRP1 group

Multi-system support


IBM Security zSecure suite
Tivoli zSecure Manager for RACF z/VM
Security zSecure Audit*
Security zSecure Admin
Security zSecure Alert**
Security zSecure Visual
Security zSecure Command Verifier
Security zSecure CICS Toolkit
RACF
z/VM
z/OS
Security audit and compliance
Administration management
*Also available for ACF2™ and Top Secret®
**Also available for ACF2

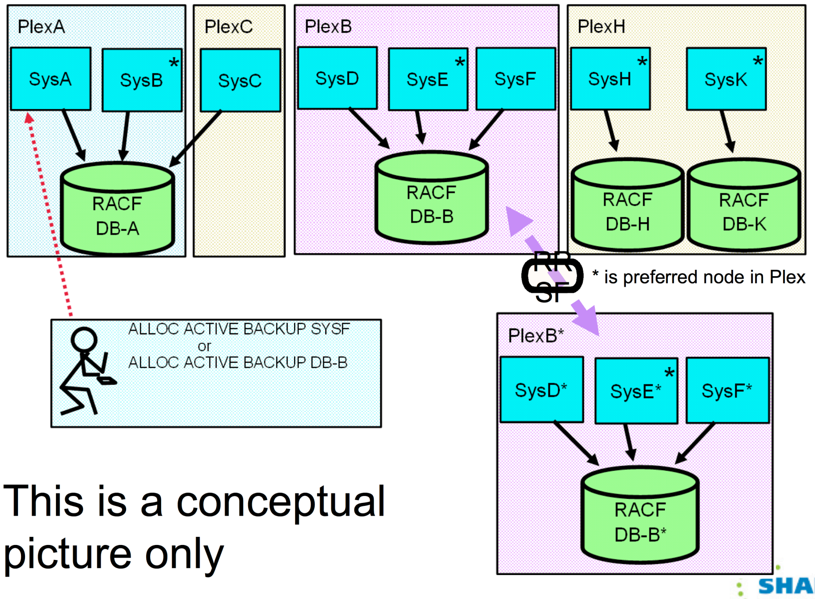
zSecure Admin

zSecure Audit

Multi-system connection - Update multiple RACFs 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*
    - ✓Do not require RRSF network
    - ✓Provides encryption
  - ✓Only minor modifications to the existing User Interface

Multi-system support – Nodes and systems



- This is a conceptual picture only

Multi-system support – Specifying data sources

- 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)

Multi-system support – Viewing reports

- **For example, menu option RA.3.G (Compare users):**

```
Enter S in front of a class for more info  16 Dec 2011
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 at a glance

- 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 and such: shows value if all the same, or the *common prefix* followed by >
    - Numbers and such: shows value if all the same, or `<more>`

Multi-system support – Compare databases at a glance

- 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>`)

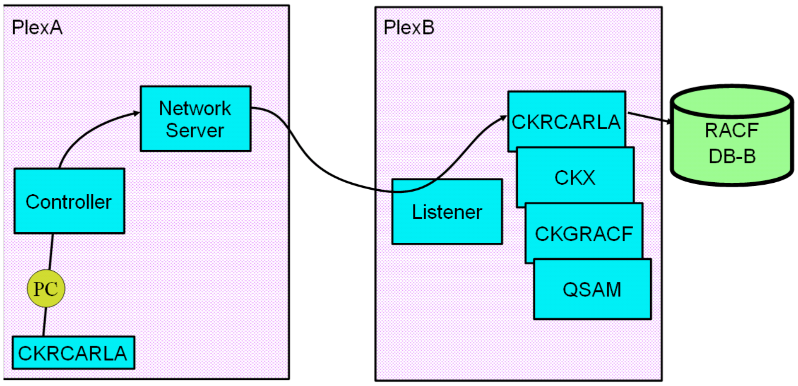
```
     User       Complex   Name                    DfltGrp   Owner     RIRP  SOA  gC  LCX  Grp

__   CERT005    DD981216                          SYSPROG   C##BMR1                   X    1

__   CERT005    DINO                              SYSAUTH   SYSAUTH   R               X    1
```

Multi-system support – Remote data limitations

- ✓ The information returned from a remote RACF database is limited in the same way as an UNLOAD file
  - ❖ E.g. sensitive data such as passwords is not present
- ✓ The remote RACF database also has characteristics similar to a local database:
  - ❖ Two-pass database read is not allowed—use an UNLOAD
  - ❖ RECNO will be 0
- ✓ MERGE is not allowed with a remote database
- A remote UNLOAD is just an UNLOAD
  - ➢ It is treated like a regular file and is not processed by a remote CKRCARLA

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

Summary

- Welcome to zSecure 1.13 – GA Nov 2011
- Suite of products, focused on
  - zSecure Audit for RACF
  - zSecure Admin
- Enhancements to CICS, IMS and DB2 collection
- Access Monitor – Uses and Don’ts
- Multiple System Communication
- TCP/IP / Increased SMF coverage
- And many more auditor-friendly features