#SHAREorg

SHARE
Technology · Connections · Results

What zSecure Manager for RACF z/VM 1.11.1 Can Do For You

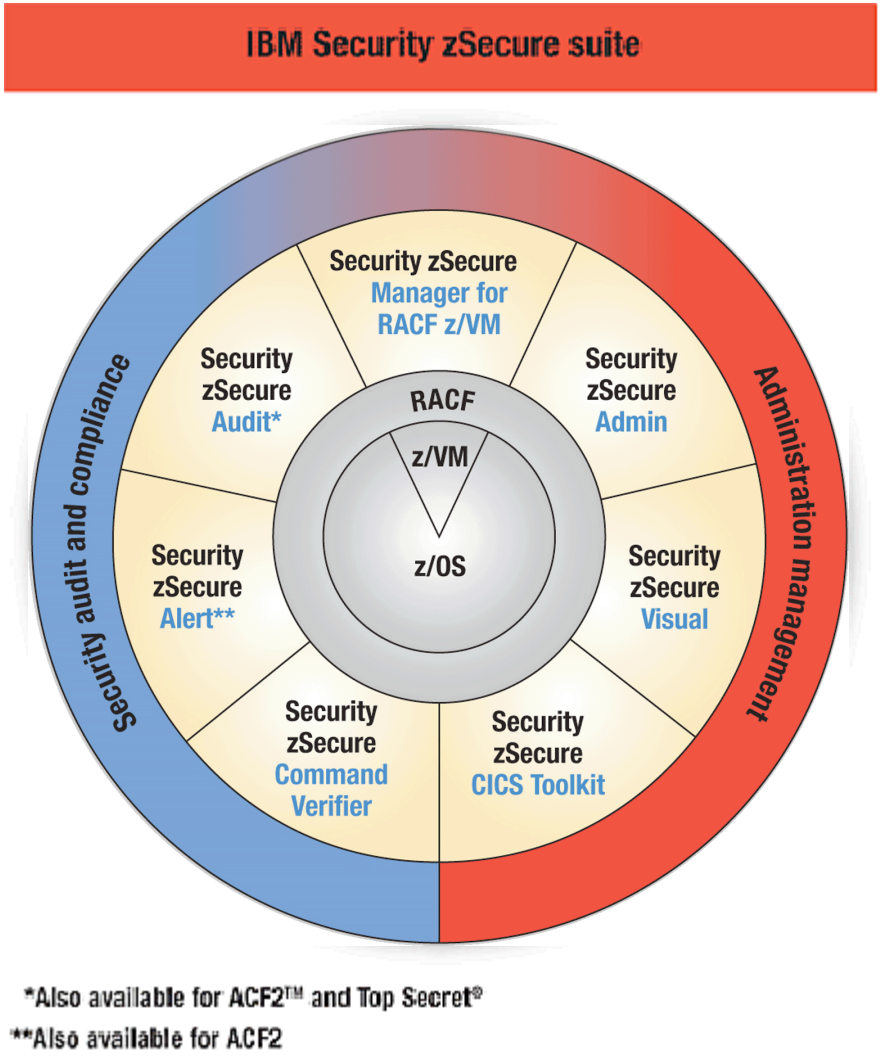
Mark S Hahn
IBM

Thursday, August 9, 2012
Session 11848

SHARE in Anaheim 2012

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

ibm.com/security



IBM Security zSecure suite

IBM Security zSecure suite

Simplify administration and automate audit and compliance reporting

Capabilities:

- Administration and provisioning:
  - **Admin** enhances security administration and user management for RACF
  - **Visual** offers a Windows GUI to RACF
  - **CICS Toolkit** for Extensibility with CICS support
- Audit, monitoring and compliance:
  - **Command Verifier** offers automated security monitoring, protection
  - **Alert** provides intrusion detection and alerting
  - **Audit** provides event detection, analysis & reporting and system integrity audit & analysis

Benefits:

- Administration and provisioning:
  - Reduce administration time, effort and cost
  - Enable decentralized administration
  - Quick response time, enabling business
  - Reduce training time needed for new administrators
- Audit, monitoring and compliance:
  - Pass audits more easily, improve security posture
  - Save time and costs through improved security and incident handling
  - Increase operational effectiveness

zSecure 1.11.1

- New release z/VM offering

5655-T13 IBM Security zSecure Manager for RACF z/VM 1.11.1

- Current releases for z/OS products (GA as of 11/11/11)

5655-T01 IBM Security zSecure Admin 1.13.0

5655-T02 IBM Security zSecure Audit 1.13.0

5655-T09 IBM Security zSecure Visual 1.13.0

5655-T11 IBM Security zSecure Alert 1.13.0

5655-T05 IBM Security zSecure CICS Toolkit 1.13.0

5655-T07 IBM Security zSecure Command Verifier 1.13.0

5655-T15 IBM Tivoli Compliance Insight Manager Enabler for z/OS 1.13.0

zSecure 1.13.0 Solution Packages

- 5655-SE1 IBM Security zSecure Administration
  - IBM Security zSecure Admin
  - IBM Security zSecure Visual
- 5655-SE2 IBM Security zSecure Compliance and Auditing
  - IBM Security zSecure Audit (RACF, CA ACF2, CA Top Secret)
  - IBM Security zSecure Alert (RACF, CA ACF2)
  - IBM Security zSecure Command Verifier
- 5655-SE3 IBM Security zSecure Compliance and Administration
  - IBM Security zSecure Administration package
  - IBM Security zSecure Compliance and Auditing package
- General Availability date: June 1, 2012

z/VM Authorization

- Authorization is based on
  - Who you are: your VM user ID
    - Unix UID/GID
    - privilege class
    - directory authorizations
    - ESM access control list
  - What you know: a password
    - If minidisks not protected by ESM

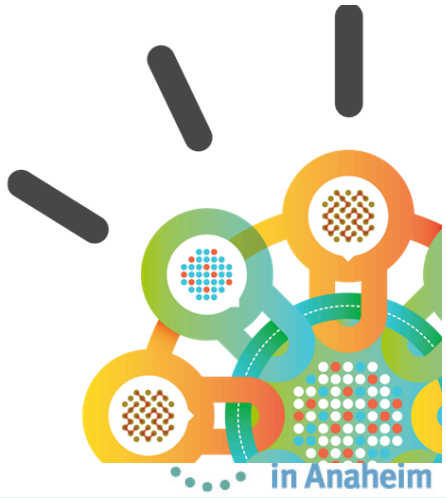
The CP Directory – sample entry

```
USER RACFU01   MYPWD 100M    100M       G
  INCLUDE   TESTUSER
  OPTION DIAG88
  NAMESAVE GCS
  IUCV      ANY
  OPTION LNKSTABL LNKEXCLU
  OPTION DEVMAINT DEVINFO
  POSIXINFO UID 32 GID 1
  POSIXINFO FSROOT '/../VMBFS:RESEARCH:BFSTEST/'
  POSIXINFO IWDIR /u/RACFU01
  POSIXINFO IUPGM /bin/sh
  CONSOLE   009 3215 T IBMUSER
  LINK      MAINT     19C     19C      RR
  MDISK 191   3380    1000    50       U01DSK MR READ WRITE MULTI
```

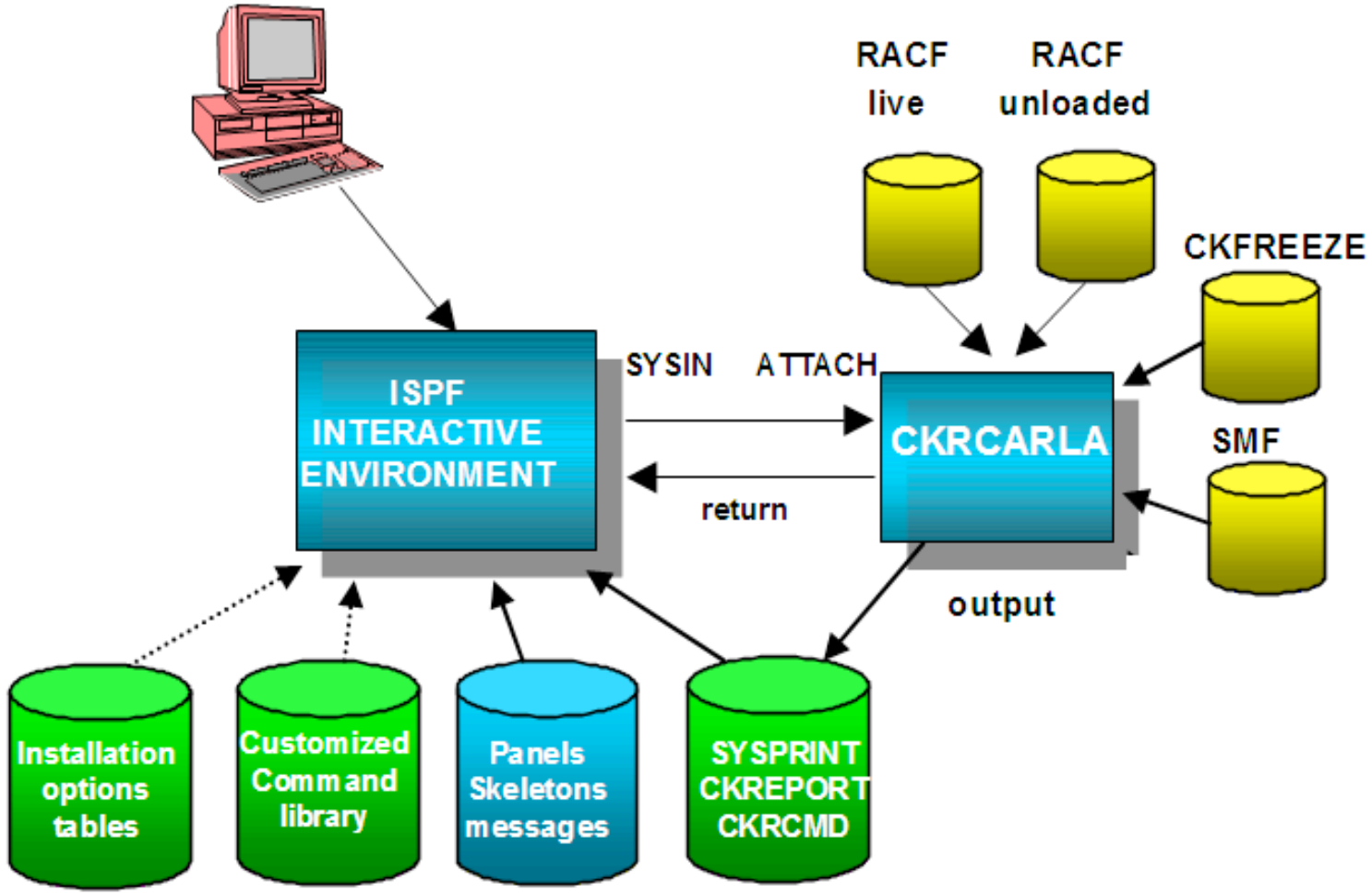
*Stuff in bold can be overridden by RACF

zSecure Manager for RACF z/VM …

- Combined administration and audit functionality for the VM environment:
  - Automate complex, time consuming z/VM security management tasks with simple, one-step actions that can be performed without detailed knowledge of RACF commands
  - Create comprehensive audit trails without substantial manual effort (RACF SMF records)
  - Quickly identify and prevent problems in RACF before they become a threat to security and compliance
  - Help ease the burden of database consolidation
  - Generate customized reports
  - Use archived data or latest (live) data



Architecture – Manager and the CARLa engine

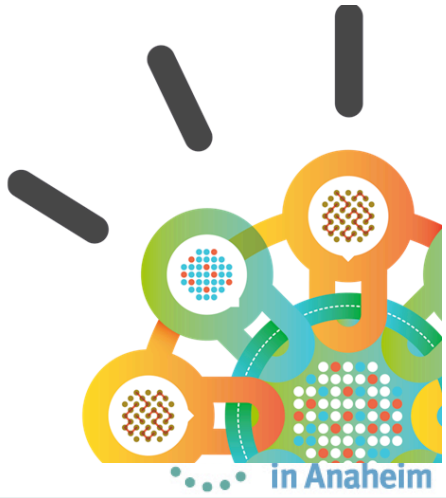


CKRCARLA is the main engine. The CKFREEZE file used as input is created by CKVCOLL.

What's new in 1.11.1

zSecure Manager for RACF z/VM 1.11.1

- Support for live data
  - active RACF database,
  - active SMF data
- z/VM resource collection
- z/VM V6R2 support and exploitation
- Compare interface
- User Interface improvements
- and more…



Data sources

- ✓ RACF data: RACF DB, DB-Copy, DB-Unload
  SMF data: Active file, archived records
  CKFREEZE: File with configuration info

- ✓ Specified in User Interface (UI) in SETUP FILES
- ✓ Specified using FILEDEFs
- ✓ Specified in CARLa using ALLOC statement

- ➢ User needs authorization to link in READ mode

Active RACF and SMF

- ✓Either specify link information in SETUP files, or
- ✓Let program determine link information (z/VM 6.2 and sufficient authorization)

- CARLa Syntax:

```
alloc type=RACF dsn=RACF.DATASET cmsmode=H
alloc type=RACF backup active
alloc type=SMF active
```

- ➢ Automatic only on z/VM 6.2, and user needs either class B or access to VMCMD DIAG0A0.RACONFIG

Active RACF and SMF (UI)

- Three new sets of input files

```
Command ===> _____________________________________________ Scroll ===> CSR

(Un)select (U/S/C/M) set of input files or work with a set (B, E, R, I, D or F)

   Description                                          Complex
_  Default RACF database                                selected
_  VM30V06  CKFREEZE A1                                 selected
_  Active backup RACF data base
_  Active backup RACF data base and live SMF data sets
_  Active primary RACF data base
******************************* BOTTOM OF DATA ********************************
```

- Three new types of input files

```
Select the type of data set or file

    Type              Description
_   ACT.BACK          The backup RACF database of your active system
_   ACT.PRIM          The primary RACF database of your active system
_   ACT.SMF           The live SMF data set(s)
_   ACT.SYSTEM        Live settings
_   CKFREEZE          System resource information data set
```

zSecure Collect for z/VM

- Information is collected from
  - ✓ USER DIRECT
    (file that defines all users and their static resources,
    often managed using DIRMAINT)
    - ✓ As specified by user
    - ✓ Created using DIRM USER (NO)PASS
    - ➢ Supports users defined via USER, PROFILE, POOL, IDENTITY, SUBCONFIG.
    - ➢ Must be single file (non-clustered)
  - ✓ Real devices (using CP QUERY commands)
  - ✓ RACF
    - ➔ Only if z/VM 6.2, using DIAG A0-50

zSecure Collect for z/VM

- Information is stored in CKFREEZE
- Authorization needed:
  - ✓ For real devices, user needs class BE.
  - ✓ For RACF, user needs class AB or VMCMD DIAG0A0.RACONFIG
- Suggest to run in XAUTOLOGed machine with class ABEG

New newlists: VM_MDISK (1/6)

- VM_MDISK shows information about defined minidisks
  - ➢ Based on USER DIRECT from CKFREEZE
  - ✓ Include RACF access data:
    - ✓ VMMDISK resource,
    - ✓ VMMDISK profile, and
    - ✓ RACF ACL
  - ✓ Include GLBLDSK info from HCPRWA (z/VM 6.2)

New newlists: VM_MDISK (5/6)

- This results in a minidisk overview

```
                  VM minidisks overview                    0 s elapsed, 0.0 s CPU
Command ===> _                                                Scroll===> CSR
All minidisks                                      19 Apr 2012 01:10
   Complex  System   #Mdisks
   dup1     TIVMEM1      546
   Pri VM user  Devn RDev RVolSr ACIGROUP DskTyp Md MdS DevTyp DvA Lcl Glb
__  15 DATAMOV2  155  000 V3V082          MDISK  MR     3390   CKD
__  15 DATAMOV2  1AA  000 V3V082          MDISK  MR     3390   CKD
__  15 DATAMOV2  1FA  000 V3V082          MDISK  MR     3390   CKD
__  15 DATAMOV2  2AA  000 V3V082          MDISK  MR     3390   CKD
__  15 DATAMOV2  5F0  000 $$$$$$          MDISK  MR     3380   CKD
__  15 DATAMOV2  5FF  000 $$$$$$          MDISK  MR     3380   CKD
__  15 DIRMSAT2  155  000 V3V082          MDISK  MR     3390   CKD
__  15 DIRMSAT2  1AA  000 V3V082          MDISK  MR     3390   CKD
__  15 DIRMSAT2  1DE  000 V3V082          MDISK  MR     3390   CKD
__  15 DIRMSAT2  1FA  000 V3V082          MDISK  MR     3390   CKD
__  15 DIRMSAT2  2AA  000 V3V082          MDISK  MR     3390   CKD
```

- Type 'S' against the minidisk you want to display

New newlists: VM_DEV (1/6)

- VM_DEV shows information about real devices
  - Information from CKFREEZE
  - ✓ Include RACF access data (z/VM 6.2)
    - ✓ VMDEV resource,
    - ✓ VMDEV profile, and
    - ✓ RACF ACL

New newlists: VM_DEV (3/6)

- New menu option RE.V (also available under AU.S – VM Extended)

```
                        zSecure Suite - Resource - VM
Option ===> _____________________________________________________________

M    Minidisks        VM minidisks reports
RD   Real devices     VM real devices reports
```

- Go to menu option RE.V.RD:

```
                        zSecure Suite - VM - Real devices Selection
Command ===> ____________________________________________________________

Show devices that fit all of the following criteria:
Device number . . . . . ____       (number or filter)
Volume serial . . . . . ______     (volser or filter)
Attached to user. . . . ________   (user or filter)
Virtual device number . ____       (number or filter)
Complex . . . . . ________         (complex or filter)
System  . . . . . ________         (system or filter)

Advanced selection criteria
_  Security settings
Show differences
_  ADD   _  DEL   _  CHG+   _  CHG-   _  CHGu   _  SAME   _  BASE
Output/run options
_  Summarize by user
_  Output in print format     Customize title
     Run in background
```

- Specify selection criteria and press Enter

New newlists: VM_DEV (4/6)

- RE.V.RD Advanced selection criteria
  - ✓ Security settings

```
                        zSecure Suite - VM - Real devices Selection
Command ===> ____________________________________________________________________
All real devices
Show devices that fit all of the following security criteria:
SAF resource name  . . _________________________  (resource name or filter)
RACF profile name  . . _________________________  (profile or filter)
RACF Universal access  __  _  1. None     3. Update   5. Alter
                              2. Read     4. Control  6. Ignore
IDStar access  . . . . __  _  1. None     3. Update   5. Alter
                              2. Read     4. Control  6. Ignore
Global access  . . . . __  _  1. None     3. Update   5. Alter
                              2. Read     4. Control  6. Ignore
                              (operator: < <= > >= = <> ¬= )
Read Only  . . . . . . . _    (Y/N)
```

New newlists: VM_DEV (5/6)

- ✓ This results in a real devices overview

```
                    VM real devices overview                  0 s elapsed, 0.0 s CPU
Command ===> _____________________________________________________ Scroll===> CSR
All real devices                                  10 Feb 2012 11:21
   Complex  Syst     #Dev
   VM       ZVM620     35
   Pri Devi VDev Volume Userid   DevC Status   Size  R/O Profile
__     0A80 0000 610RES          DASD FREE      3339     RDEV.0A80.ZVM620
__     0A81 0000 610PAG          DASD FREE      3339     RDEV.0A81.ZVM620
__     0A82 0000 610SPL          DASD FREE      3339     RDEV.0A82.ZVM620
__     0A83 0000 PRODPK          DASD FREE      3339     **
__     0A84 0000 VTAMPK          DASD FREE      3339     **
__     0A85 0000 610W01          DASD FREE      3339     **
__     0A86 0000 610W02          DASD FREE      3339     **
__     0400 0000                 OSA  FREE               **
__     0401 0000                 OSA  FREE               **
__     0402 0000                 OSA  FREE               **
```

- ➢ Type 'S' against the device you want to display

New newlists: VM_DEV (6/6)

- ✓ This results in a real device detail display

```
                VM real devices overview
Command ===> ____________________________________________________________
All real devices


  Device identification
  Real device address             0520
  Virtual device address          0000
  Device volume serial            M01RES
  Associated userid
  Device class                    DASD
  Device status                   CPOWNED
  Read Only access                No
  Complex name                    ZAHJB
  System name                     ZVM620

  Device security settings
  VMDEV resource name             RDEV.0520.ZVM620
  RACF universal access           NONE
  RACF Global access              NONE
  RACF ID * access

  Class     Profile
  VMDEV     **

  User      Access  ACL id    When
_ IBMUSER   ALTER   IBMUSER
```

Live data support

- z/VM V6R2 RACF supports DIAG A0-50

✓Information about RACF

- ✓HCPRWA (including GLBLDSK, SYSSEC),
- ✓RCVT, RCVX,
- ✓CDT, Router,
- ✓RACF DSNT and RRNG,
- ✓Templates, Dynamic Parse,
- ✓RACF Exits

CLASS, OPTIONS and SETUP from active system (1/2)

- Previously, only the RACF options and classes from the RACF database were available.
- Now information from the active system
  - Requires z/VM 6.2
  - AU.S – VM Extended
    - ✓EXITS
  - AU.S – RACF Control
    - ✓SETROPTS, SETROPAU, ROUTER, RANGE,
    - ✓RACFDSN, RACFCLAS, TEMPLATE
- RACF database based reports are still included
  - ✓ SETROPTD, SETROPAD, RACFDCLS

CLASS, OPTIONS and SETUP from active system (2/2)

- AU.S – VM extended – with 'Select specific reports' leads to

```
                zSecure Manager for RACF - Audit - Status VM  extended
Command ===> _____________________________________________________________

Enter "/" to select report(s)

_  EXITS           - Exit and table overview
_  DASDVOL         - DASD Volume Protection and Sharing
_  VMMDISK         - VM minidisks
_  VMDEV           - VM real devices
```

- AU.S – RACF control – with 'Select specific reports' leads to

```
              zSecure Manager for RACF - Audit - Status RACF control
Command ===> _____________________________________________________________

Enter "/" to select report(s)
_  SETROPTS        - RACF SETROPTS settings
_  ROUTER          - SAF router table (ICHRFR01)
_  RANGE           - RACF Range Table
_  RACFDSN         - RACF Current database data set names and settings
_  RACFCLAS        - RACF class info
_  GLOBAL          - Global profile overview
_  TEMPLATE        - RACF template definitions
```

- Note that SETROPTS generates 4 reports, RACFCLAS generates 2

New newlists: EXIT (z/VM 6.2)

- EXITS report is existing z/OS report, but new for z/VM
- ➔ If data is in CKFREEZE (or live), RACF exits and data modules (ROUTER, CDT) now available
- ➢ Added to AU.S – VM Extended

```
                    Exit and table overview                          Line 1 of 2
Command ===> _                                                 Scroll===> CSR
                                                        10 Feb 2012 11:21
   Complex  System   Exits Audit concerns Priority
   VM       ZVM620       2              0
   Pri Program  Applic   Subs Dynamic exitname Eff Description
__     ICHRRCDx RACF                            Class descriptor table
__     ICHRRNG  RACF                            RACF range table
******************************* Bottom of Data ********************************
```

RACF SETROPTS settings report (z/VM 6.2)

- SETROPTS report shows ACTIVE Options

➔Added to AU.S – RACF Control

```
                                                                Line 2 of 62
RACF system, ICHSECOP, and general SETROPTS settings
Command ===> _____________________________________________ Scroll===> CSR
                                                 21 May 2012 06:00
   Complex  System   Collect timestamp
   TIVMEM1  TIVMEM1  21 May 2012 06:00

General RACF properties                  Data set protection options
Access Control active          Yes       Pre
Force storage below 16M        No        Pro
Check all connects  GRPLIST    Yes       Aut
Check genericowner for create  No        Enh
NOADDCREATOR is active         No        Pre
Dynamic CDT active             No        Pre
Primary Language               ENU       GDG
Secondary Language             ENU       USE
VMXEVENT control profile       NOVMRDR   GRO
RACF software release level
RACF DB template level

DASD data set protection                 Ter
Volume level permits DASDVOL   No        Ter
Erase-on-scratch               None      Und
```

```
Auditing options
Audit SPECIAL users                 Yes
Audit OPERATIONS users              No
Audit USER profile changes          No
Audit GROUP profile changes         No
Audit SECLABELed resources          No
Audit command violations            Yes
Audit from security level           None
Real datasetnames in SMF            No
Dataset logoptions                  Profile
APPLAUDIT is active                 No
VMXEVENT audit profile

Identification/Authentication options
Remember dates INITSTATS            Yes
Prevent logon if unused days        No
Revoke after password attempt       No
```

RACF SETROPTS audit concerns report (z/VM 6.2)

- SETROPAU report shows Audit concerns

➔Added to AU.S – RACF Control

```
                SETROPTS settings - audit concerns              Line 1 of 10
Command ===> _                                                  Scroll===> CSR
                                                    21 May 2012 06:00
   Pri Complex  System   Count
    30 TIVMEM1  TIVMEM1     10
   Pri Parameter                 Value    Audit concern
__  30 REVOKE                    No       Too many password violations allowed
__  20 OPERAUDIT                 No       OPERATIONS activity undetectable
__  15 AUDIT_GROUP               No       Profile changes in GROUP class are not
__  15 AUDIT_USER                No       Profile changes in USER class are not
__  15 HISTORY                   No       Users can use the same passwords over
__  15 INACTIVE                  No       Apparently unused userids increase ris
__  11 RVARYSTATUSPWSET          No       Password to deactivate RACF still at I
__  10 GENERICOWNER              No       User with CLAUTH can bypass generic pr
__  10 RACF release                       Security/integrity flaw remediation no
__  10 RVARYSWITCHPWSET          No       Password to switch RACF database still
******************************* Bottom of Data ********************************
```

New newlists: RACF Class (z/VM 6.2)

- RACFCLAS report shows ACTIVE CDT and options

➔Added to AU.S – RACF Control

```
                                                                Line 110 of 127
RACF CDT, SETROPTS class info and number of profiles
Command ===> _____________________________________________________ Scroll===> CSR
                                                  21 May 2012 06:00
   Complex  System   Classes Active Nonempty Profiles Audit concerns Priority
   TIVMEM1  TIVMEM1      127     11       11      997           127       31
   Pr Class    Pos Grouping Members  Protect  Glbl Generic  Profiles RC Oper RF
__ 31 VMBATCH   15                    Noaudit       Discrete      199  4 OPER Ye
__  4 VMBR     120 VMEVENT           Inactive      Discrete           4       Ye
__ 31 VMCMD     14                    Noaudit                     5  4 OPER Ye
__  5 VMDEV    594                    Inactive                    3  4       Ye
__  4 VMEVENT  120           VMBR     Inactive      Discrete           4       Ye
__ 31 VMLAN     64                    Noaudit       Discrete      1  4       Ye
__  3 VMMAC     91                    Inactive                    8       Ye
__ 31 VMMDISK   18                    Noaudit                   529  4 OPER Ye
__  5 VMNODE    16                    Inactive      Discrete           4 OPER Ye
__  5 VMPOSIX   63                    Inactive      Discrete     18    4       Ye
__  5 VMRDR     17                    Inactive      Discrete    199    4 OPER Ye
__ 31 VMSEGMT   90                    Noaudit       Discrete           4       Ye
__ 31 VMXEVENT  96           VXMBR    Noaudit       Discrete      7    4       Ye
__ 23 VTAMAPPL 114                    Inactive      Discrete           4       Ye
__ 31 VXMBR     96 VMXEVENT           Noaudit       Discrete           4       Ye
__  4 WIMS     101           OIMS     Inactive      Discrete           4       Ye
__  4 WRITER   111                    Inactive      Discrete           8       Ye
```

z/VM currency

- Various knowledge bases updated
  - ✓ For example, recognition of software version levels, end of service dates
- Treat ALTER on **discrete** VMMDISK profile the same as ALTER on **generic** VMMDISK profile

✓ Also available as toleration maintenance for Manager 1.11.0

- ➢ PTF UV61155 for APAR VM17762

Compare interface

Visual RACF database compare

- When running with multiple RACF input sources
  - ✓ Additional summary level (specify in SETUP VIEW)

```
/  Add user/group info to view
   (Selecting this will use some additional storage - normally on )
/  Add summary to RA displays for multiple RACF sources (normally on)
_  Add connect date and owner to RA.U connect group section
```

- ➢ This will highlight differences between the databases
  - ✓ Flags shown as percentage
  - ✓ Numbers shown if everywhere the same, otherwise as <more>
  - ✓ Text shown as common value, or as common prefix followed by >

```
                                                                Line 86 of 203
zSecure Manager for RACF USER overview
Command ===> _____________________________________________ Scroll===> CSR
All users                                        29 May 2012 08:58
   User      # Name                 DfltGrp  Owner    Rev Ina Res Ptc Spc Opr
__ GSKADMIN  2                      SYS1     IBMUSER    0   0   0   0   0   0
__ IBMUSER   2                      SYS1     IBMUSER  100   0   0   0   0   0
__ IMAP      2                      SYS1     IBMUSER    0   0   0   0   0   0
__ IMAPAUTH  2                      SYS1     IBMUSER    0   0   0   0   0   0
```

Compare interface – Results Details (8/9)

- ✓Fields changed (Compare Changes) are shown on detail display

```
                    zSecure Suite USER overview                    Line 1 of 60
Command ===> _____________________________________________ Scroll===> CSR
All users                                  13 Mar 2009 12:33

_ Identification of AUTO1                                          RECOVERY
  User name                  NETVIEW USER
  Installation data          ____________________________________________
_ Owner                      CRBEHEER                    SYSTEEMBEHEER
_ User's default group       CRBEHEER                    SYSTEEMBEHEER

  Changes
  HAS_PASSWORD(->YES)
  OWNER(SYSPROG->CRBEHEER)
  PROTECTED(YES->)

  Group    Auth    R SOA AG Uacc    Revokedt    Resumedt    ConnectDa ConOwner
_ CRBEHEER USE     _ ___ __ NONE    ___________ ___________ 28Apr1998 CRBEHEER

  System access                          Statistics
  Revoked (may be by date)     No        Creation date                 28Apr98
  Inactive, revoked or pending Yes       Last RACINIT current connects  5May98
  Days of week user can logon  SMTWTFS   User's last use date           5May98
  Time of day user can logon   _________ User's last use time          15:53
```

Compare interface (9/9)

- Compare function is available on:
  - ✓ RA.U/G/D/R
  - ✓ RA.3.A/B/C
  - ✓ RA.S
  - ✓ AU.S
  - ✓ RE.T
  - ✓ RE.V.M
  - ✓ RE.V.RD

Apply command to multiple records on a display

- Block commands on ISPF displays:
  - RR..RR to Recreate multiple profiles
  - 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 (1/4)

- 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

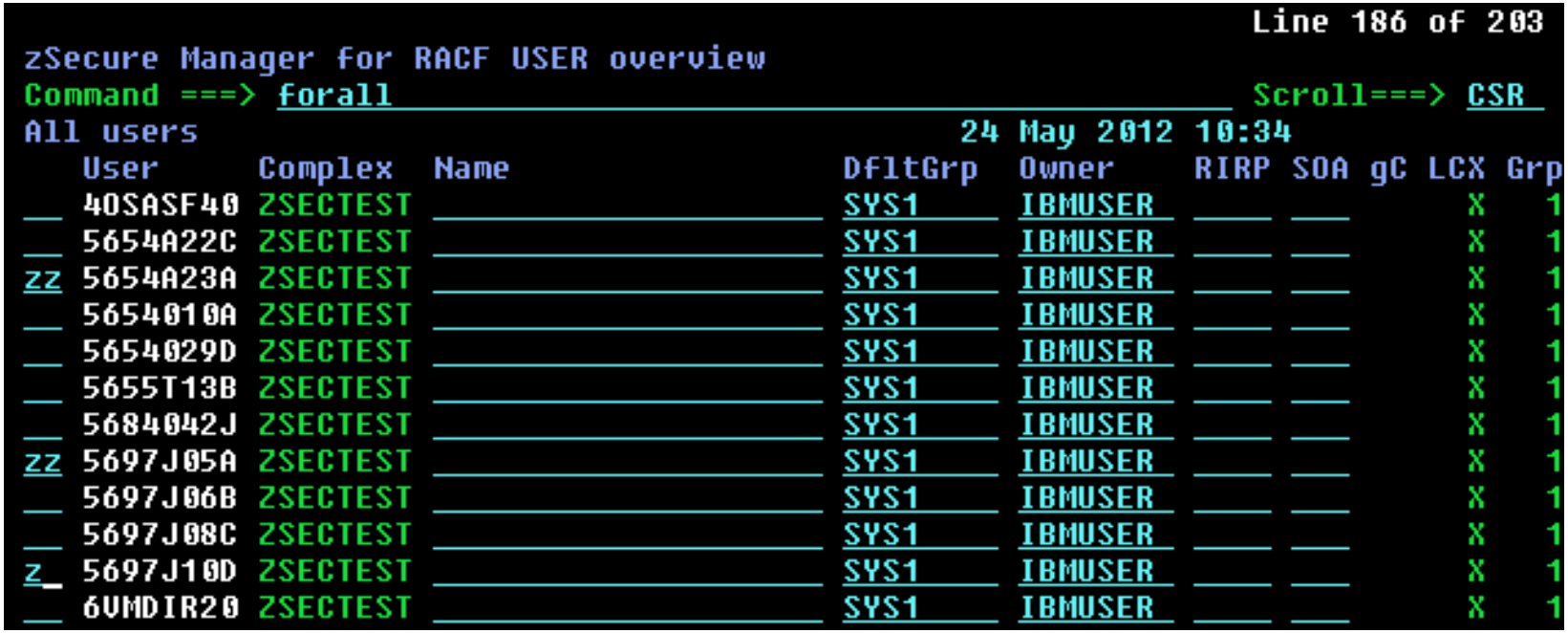
  These will be substituted in each record (e.g. by the profile key)

- 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

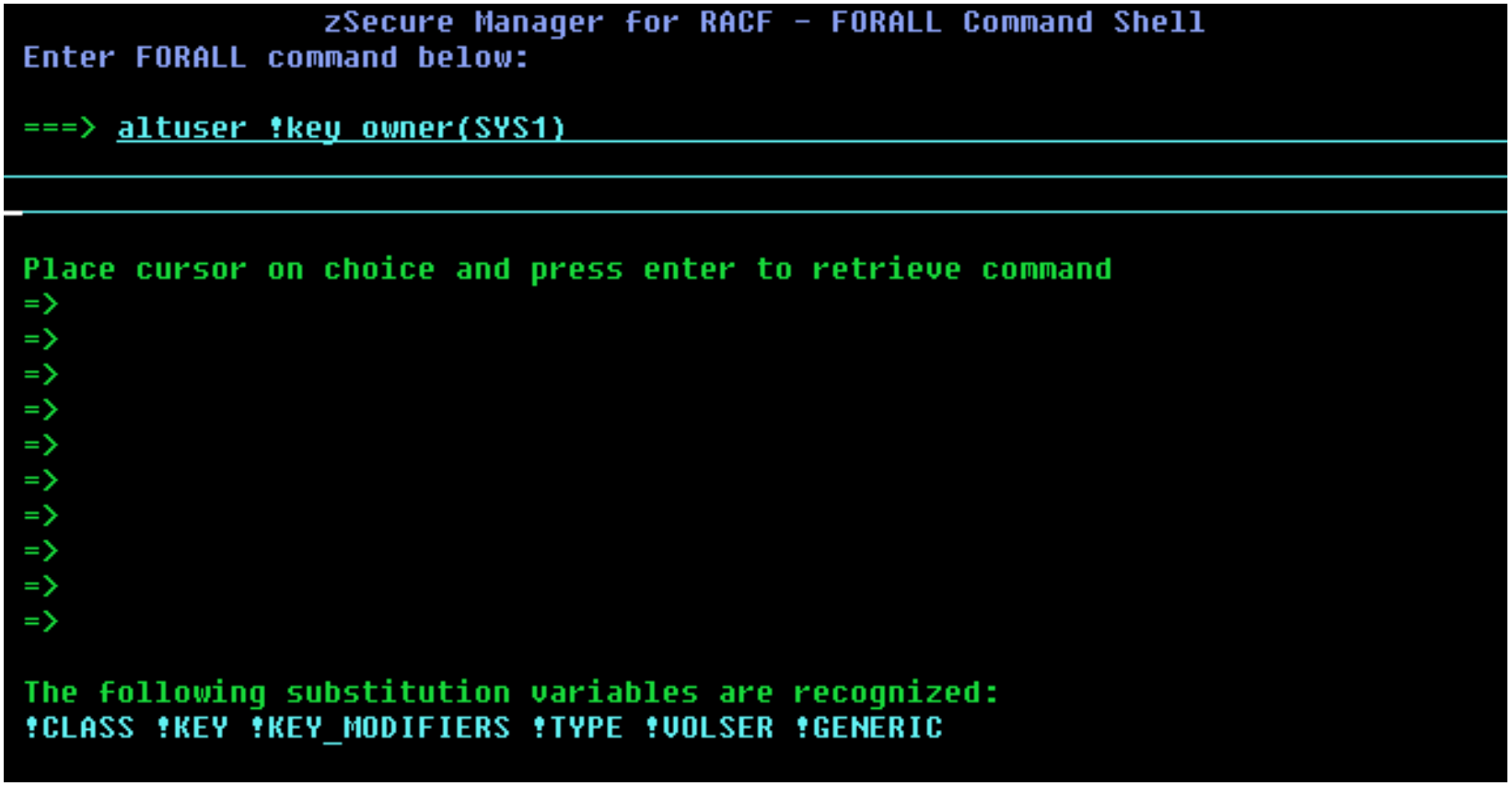
Block commands – FORALL (2/4)



```
                                                              Line 186 of 203
zSecure Manager for RACF USER overview
Command ===> forall                                          Scroll===> CSR
All users                                        24 May 2012 10:34
   User     Complex  Name                 DfltGrp  Owner    RIRP SOA gC LCX Grp
__ 40SASF40 ZSECTEST ____________________ SYS1     IBMUSER                X   1
__ 5654A22C ZSECTEST ____________________ SYS1     IBMUSER                X   1
zz 5654A23A ZSECTEST ____________________ SYS1     IBMUSER                X   1
__ 5654010A ZSECTEST ____________________ SYS1     IBMUSER                X   1
__ 5654029D ZSECTEST ____________________ SYS1     IBMUSER                X   1
__ 5655T13B ZSECTEST ____________________ SYS1     IBMUSER                X   1
__ 5684042J ZSECTEST ____________________ SYS1     IBMUSER                X   1
zz 5697J05A ZSECTEST ____________________ SYS1     IBMUSER                X   1
__ 5697J06B ZSECTEST ____________________ SYS1     IBMUSER                X   1
__ 5697J08C ZSECTEST ____________________ SYS1     IBMUSER                X   1
z_ 5697J10D ZSECTEST ____________________ SYS1     IBMUSER                X   1
__ 6VMDIR20 ZSECTEST ____________________ SYS1     IBMUSER                X   1
```

- Selects users 5654A23A, 5654010A, 5654029D, 5655T13B, 5684042J, 5697J05A, and 5697J10D
- FORALL without parameters calls up the command entry panel

Block commands – FORALL (3/4)



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

Block commands – FORALL (4/4)

- With Action on Command set to Queue, generated commands are in CKRCMD:

```
 CKR1CMD  CKRCMD   A1  F 80  Trunc=80 Size=8 Line=0 Col=1 Alt=0

00000 * * * Top of File * * *
00001  /* CKRCMD file CKR1CMD complex ZSECTEST generated 24 May 2012 10:34 */
00002 altuser 5654A23A owner(SYS1)
00003 altuser 5654010A owner(SYS1)
00004 altuser 5654029D owner(SYS1)
00005 altuser 5655T13B owner(SYS1)
00006 altuser 5684042J owner(SYS1)
00007 altuser 5697J05A owner(SYS1)
00008 altuser 5697J10D owner(SYS1)
00009 * * * End of File * * *
```

- Most RACF profile displays support FORALL with variables:
  - !KEY (profile key),
  - !CLASS (profile class),
  - !TYPE (profile type),
  - !VOLSER (volume serial – for discrete profiles),
  - !GENERIC ('GENERIC' for fully qualified generic profiles),
  - !KEY_MODIFIERS (to make a profile key unique (like volser(*volume*))

Block commands – act on record level display

- 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 1.11.1 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

Other ISPF UI enhancements

UI – CMS Batch interface (1/3)

- Background option available on reports
  - ✓ Runs CKRESUB EXEC to punch job to specified CMSBATCH machine
  - ✓ Input file created on user's A-disk
  - ➢ CMSBATCH machine must have READ access

UI – CMS Batch interface (2/3)

- ✓Background option available on selection panels:

```
Output/run options
_  Show segments      _  All               _  Specify scope
/  Print format       _  Customize title
   /  Background run  _  Full page form    _  Sort differently  _  Narrow print
```

- ✓Batch submit menu:

```
                        zSecure Manager for RACF - Submit menu
Option ===> _____________________________________________________________________

1  Edit          Edit JCL
2  Submit        Submit JCL for execution
3  Cancel        Do not submit the JCL
4  Select        Select an alternate set of input files


Batch input files   *NONAME*

Job statement information:  (Verify before proceeding)
Userid . . . . . . . CRMBMR1
Account info . . . . 9999999
Jobname  . . . . . . ________
VM batch userid  . . CRMBATCH
```

UI - CMS Batch interface (3/3)

- Generates two files
  - ✓ CARLa input file on user's A-disk
  - ✓ “Submit REXX”

```
CKR1BICH EXEC     A1  V 130  Trunc=130 Size=19 Line=0 Co

00000 * * * Top of File * * *
00001 /* rexx */
00002 'CP SPOOL PUNCH TO CRMBATCH CONT'
00003 punch = 'EXECIO 1 PUNCH (STRING'
00004 punch '/JOB CRMBGUS 99999999 CRMBGUS '
00005 punch 'VMLINK  '
00006 punch 'VMLINK RACFVM 200  <* R>'
00007 punch 'VMLINK CRMBGUS 191 <* B-Z>'
00008 punch 'FILEDEF SYSPRINT TERMINAL'
00009 punch 'FILEDEF CKREPORT PR'
00010 punch 'FILEDEF SYSTERM  TERMINAL'
00011 punch 'FILEDEF CKRCMD   TERMINAL'
00012 punch 'FILEDEF SYSIN    DISK CKR1BTSI SYSIN *'
00013 punch 'FILEDEF CKRCARLA DISK ISPNULL CARLA *'
00014 punch 'GLOBAL LOADLIB CKRCARLA'
00015 punch 'OSRUN CKRCARLA'
00016 punch 'CP SPOOL PRT to CRMBGUS '
00017 punch 'CP SPOOL CON to CRMBGUS '
00018 punch '/*'
00019 'CP SPOOL PUNCH NOCONT CLOSE'
00020 * * * End of File * * *
```

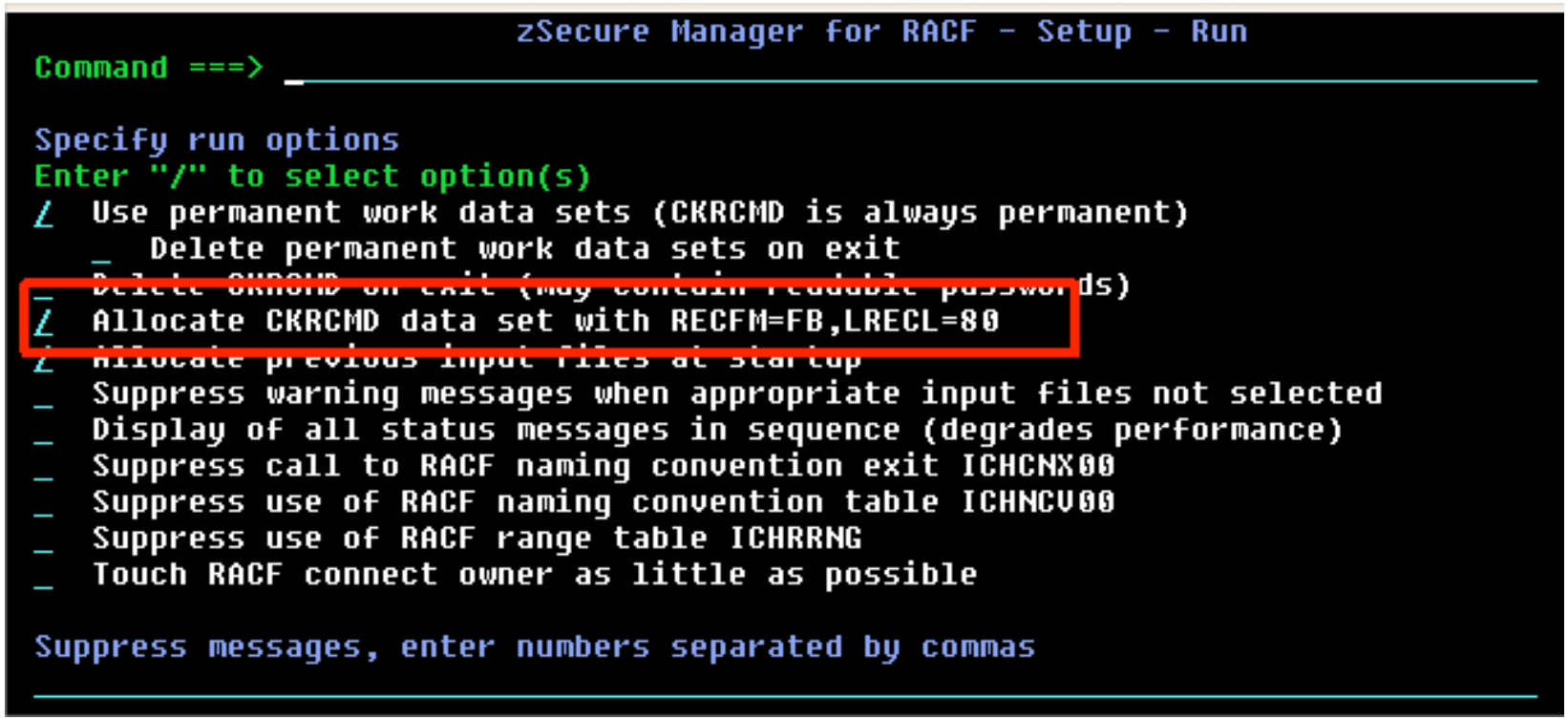
```
CKR1BTSI SYSIN    A1  V 80  Trunc

00000 * * * Top of File * * *
00001 PRINT DD=CKREPORT
00002 I M=C2RXDEF1
00003 alloc type=RACF dsn=RACF.DAT
00004 alloc type=CKFREEZE cmsfile=
00005
00006 n n=baseu1 segment=BASE requ
00007  ,
00008  tt="zSecure Manager for RAC
00009  st="All users"
00010  s s=base c=user
00011  sortlist " - complex"(tt,pa
00012  ,
00013 key(8,"User") name dfltgrp o
00014  restricted(1,hb) | protecte
00015  spec(hb,1) | oper(1,hb) | a
00016 any_link | any_cert | passwo
00017  passint_effective("Int",3)
00018 cggrpnm(sort,hor,wordwrap,25
00019  instdata(0,wrap),
00020    / "     Concern: "(notemp
00021 * * * End of File * * *
```

UI – z/VM specific UI startup options

- New options for ISPF usage in Configuration Parameters
  - ✓ MODE=LINE | ISPF | ISPFPDF
    - ➢ MODE(ISPF) now uses CMS XEDIT
      - ➔ In 1.11.0 used PDF when available
      - ➔ Use new value ISPFPDF for that now
  - ✓ ISPFMiniDisk=ISPVM 192
    - ➢ To automatically link to ISPF disk
- More dynamic use of minidisk address and access mode

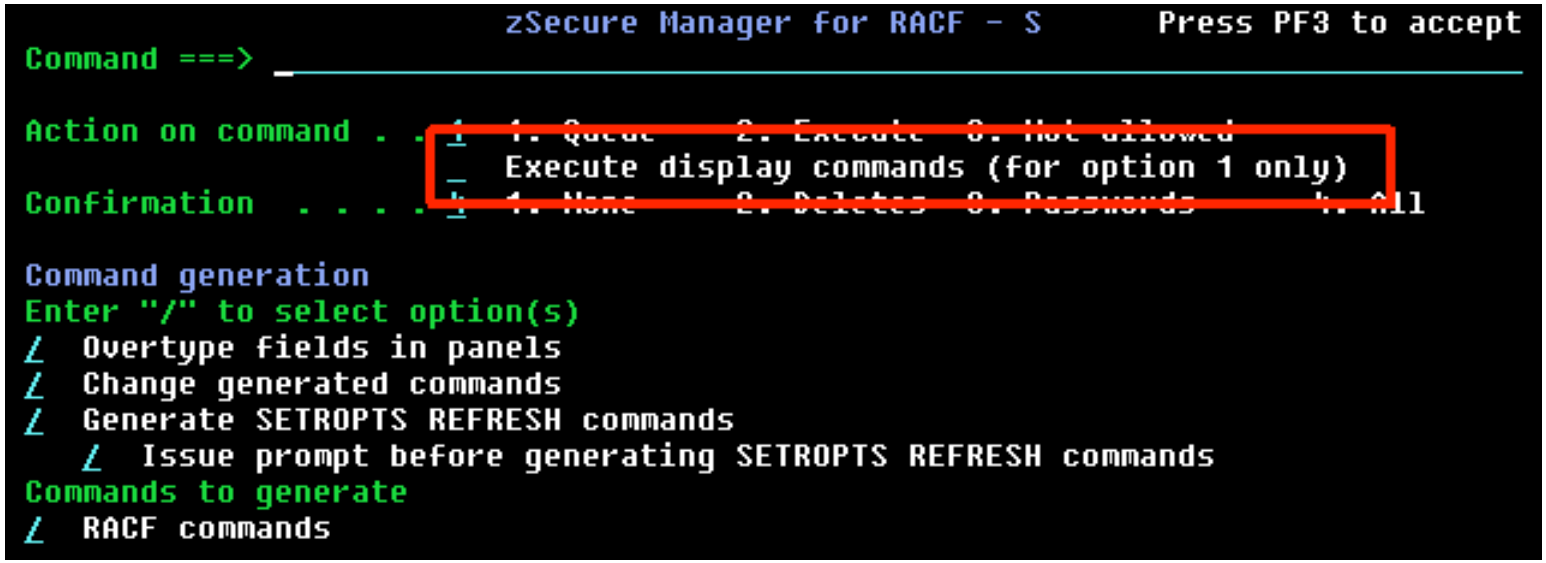
UI - Generate CKRCMD cmds in first 72 positions

- Command output files are now by default FB80
  - Existing users need to select record format



UI – Intermediate 'Action on command' setting

- New SETUP CONFIRM option to execute “list” commands only



UI – Add connect information

- New option in SETUP VIEW:

```
/  Add user/group info to view
   (Selecting this will use some additional storage - normally on )
/  Add summary to RA displays for multiple RACF sources (normally on)
/  Add connect date and owner to RA.U connect group section
```

- Example output:

```
                                                                Line 1 of 57
zSecure Manager for RACF USER overview
Command ===> _____________________________________________ Scroll===> CSR
All users                                    29 May 2012 10:14


_ Identification of IBMUSER                                        DFLT
  User name                  ____________________
  Installation data          ________________________________________________
_ Owner                      IBMUSER
_ User's default group       SYS1

  Group    Auth     R SOA AG Uacc     Revokedt    Resumedt    ConnectDa ConOwner
_ SYSCTLG  JOIN     _ ___ __ READ     ____________ ____________ 18Jan2012 IBMUSER
_ SYS1     JOIN     _ ___ __ READ     ____________ ____________ 18Jan2012 IBMUSER
_ VSAMDSET JOIN     _ ___ __ READ     ____________ ____________ 18Jan2012 IBMUSER
```

UI - Other display and action enhancements

- Revoked connect indication (RvC) in ACL display

```
Access   ACL id    When                  RI Name                   DfltGrp   RvC
ALTER    SYSPROG                                                  SYSPROG   No
```

- PE line command allows (*) for ID(*) PERMIT
  - Using just * brings up the list of defined Ids

- Recreate now generates SETROPTS REFRESH commands

```
****** ********************************************************************** Top of Data **********
==MSG> -Warning- The UNDO command is not available until you change
==MSG>           your edit profile using the command RECOVERY ON.
000001          /* CKRCMD file CKR1CMD complex NANO generated 26 May 2011 11:19 */
000002          /* CKRCMD file CKRT1CMD complex NANO generated 26 May 2011 11:19 */
000003         rdefine FACILITY $$TEST$$ owner(IBMUSER) audit(failures(READ)) uacc(NONE    )
000004         rdefine FACILITY $$TEST$$.XYZZY11 owner(IBMUSER) audit(failures(READ)) uacc(NONE    )
000005         permit $$TEST$$ class(FACILITY)  id(IBMSYS1) access(NONE)
000006         permit $$TEST$$ class(FACILITY)  id(IBMSYS2) access(READ)
000007         permit $$TEST$$ class(FACILITY)  id(IBMUSER) access(READ)
000008         permit $$TEST$$ XYZZY11 class(FACILITY)  id(IBMSYS3) access(NONE)
000009         setropts refresh raclist(FACILITY)
****** ******* ************************** Bottom of Data **********
```

UI – Changes to FIND and RFIND in reports

- Enhanced zSecure User Interface FIND and RFIND function
  - ✓ After FIND PREV command RFIND is more intuitive:
    It now searches from bottom to top, right to left.
  - ✓ Repeated FIND/RFIND is not confused by intermediate scrolling
  - ✓ Introduced Bottom-of-data and Top-of-data messages
  - ➢ This applies to data displays. Menu and selection panels use the native ISPF function.

UI – Selection for TRUSTED reports (1/3)

- Available in new option RE.T
  - ✓ Selection on Trust level, Users, Resources
  - ✓ Summary on User or Resource
  - ➢ No change in reported information

UI – Selection for TRUSTED reports (2/3)

- New menu option RE.T (Trust reports)

```
AU   Audit            Audit security and system resources
RE   Resource         Resource reports
  T    Trusted          Trusted users and sensitive resources reports
  V    VM               VM resource reports
EV   Events           Event reporting from SMF and other logs
CO   Commands         Run commands from library
```

➢ Go to RE.T:

```
                          zSecure Manager for RACF - Trusted
Command ===> _____________________________________________________________

Show trust relations that fit all of the following criteria:
Complex . . . . . ________  (complex or filter)
Trust level . . . . . __  __    (operator: < <= > >= = <> ¬= , number 1-10)

Selection criteria
_  Select/exclude users and access types
_  Select resources

Output/run options
_  1. Summarize by resource  2. Summarize by user
/  Print format              _  Customize title
   _  Background run
```

➢ Specify additional selection criteria and summarize category

UI – Selection for TRUSTED reports (3/3)

- Select/exclude users and access types

```
Selection criteria (use of filters allowed)
Userid . . . . . _________ ________ ________ ________ ________ _ More
Userid default group  ________ ________ ________ ________ ________ _ More
Userid owner . . . . . ________ ________ ________ ________ ________ _ More
Access via group . . . ________ ________ ________ ________ ________ _ More
Access level . . . . . __ _________ (operator: < <= > >= = <> ¬= )
Scan Privilege for . . _________ (for example OWNER, UACC, Permit, Unix, ..)

Exclusion criteria (use of filters allowed)
Userid . . . . . ________ ________ ________ ________ ________ _ More
Userid default group  ________ ________ ________ ________ ________ _ More
Userid owner . . . . . ________ ________ ________ ________ ________ _ More
Access via group . . . ________ ________ ________ ________ ________ _ More
Access level . . . . . __ _________ (operator: < <= > >= = <> ¬= )
```

- ✓ More box allows you to specify up to 25 selection criteria

- Select resources

```
Show trusted resources that fit all of the following criteria:
Resource . . . . . _____________________________________ (resource or filter)
Class  . . . . . ________ (class or filter)
Scan Sensitivity for ___________ (for example APF, CICS, TSO, HSM, MSTR, ...)
Profile name . . . . _____________________________________ (profile or filter)
Profile owners . . . ________ ________ ________ ________ ________ _ More
```

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 — connection ID
    - LDAP_CLIENT_SECL — LDAP client seclabel
    - LDAP_ENTRY_NM — target entry name (DN)

Other – VMBATCH access added to TRUSTED

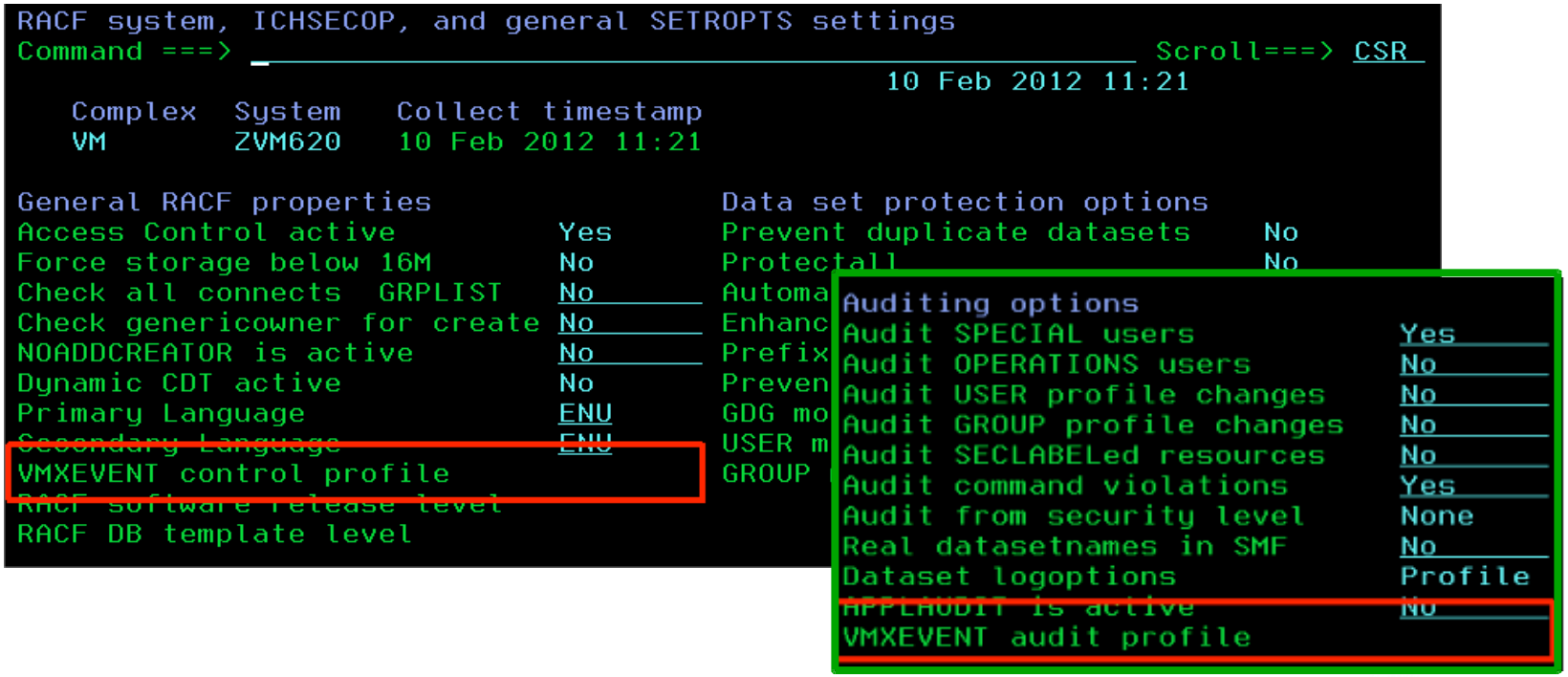
- Alternate user support in TRUSTED
  - ✓ Access to VMBATCH <userid>

```
                Sensitive data trustees                                 Line 1 of 2
Command ===> _____________________________________________ Scroll===> PAGE
All trusted records                              21 May 2012 06:00
   Pri Complex  System   Trust relations
    44 TIVMEM1  TIVMEM1              359
   Pri Sensitivity Class    Resources Trust relations
    10 SetAltUser  VMBATCH         19              20
   Pri Resource                                    VolSer Trust relations
    10 CRMBCNT                                                        2
   Pri Userid   Name                 From     Audit concern
__  10 CRMBTCH7                      TIVMEM1  Can run with authorizations of vi
__  10 DIRMAINT                      TIVMEM1  Can run with authorizations of vi
******************************** Bottom of Data ********************************
```

Other – Protection of CP commands and diagnose API

- Extra VMXEVENT fields in SETROPTS display

```
VM_SETEVENT_CTL                 Profile_name
  VM_SETEVENT_AUDIT             Profile_name
```



Other – SYSSEC settings

- SYSSEC info from HCPRWA in RACFCLAS report

```
  SYSSEC_F_VIOLATION          DEFER | FAIL
SYSSEC_M_MESSAGE              Yes | No
SYSSEC_P_SUCCESS              ALLOW | DEFER
SYSSEC_U_UNDEFINED            ALLOW | DEFER | FAIL
SYSSEC_W_WARNING              DEFER | FAIL
```

```
                                                                Line 30 of 50
RACF CDT, SETROPTS class info and number of profiles
Command ===> _____________________________________________ Scroll===> CSR
                                                10 Feb 2012 11:21
   Complex  System    Classes Active Nonempty Profiles Audit concerns Priority
   VM       ZVM620        127      8       10      542            127       31
   Pr Class     Pos Grouping Members  Protect  Glbl Generic  Profiles RC Oper RF
   31 VMBATCH    15                   Noaudit                    124  4 OPER Ye

  SYSSEC settings
  SYSSEC Permit setting          ALLOW    SYSSEC Undefined setting      DEFER
  SYSSEC Warning setting         DEFER    SYSSEC Message setting
  SYSSEC Failure setting         FAIL
```

```
  Audit concern
  SYSSEC setting SYSSEC_W_WARNING=DEFER violates protection by default
  principle / not OSPP compliant, SYSSEC setting SYSSEC_U_UNDEFINED=DEFER
  violates protection by default principle / not OSPP compliant, Profile
  changes in class are not audited, OPERATIONS honored (IBM default)
********************************* Bottom of Data ********************************
```

Other CARLa enhancements (1/3)

- Interpretation of masking has changed for RA.U and other panels
  - ✓ An asterisk followed by characters now works as expected
  - ✓ For data sets and resources the match is for one qualifier
  - ➢ Note: ** in the first position will **not** match 0 qualifiers

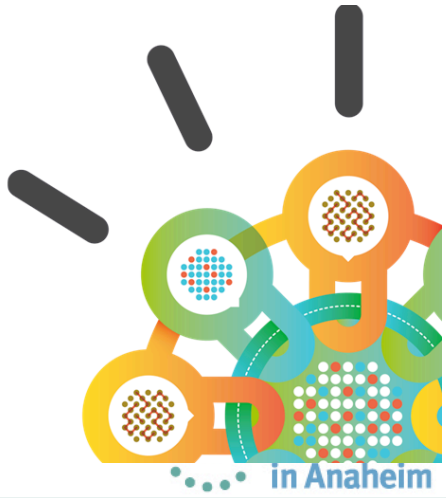
- `OPTION NOWARNING` sets program RC to 0 if it is 4

- Field modifier `COMMON_PREFIX, CPRX`
  - summary statistic that contains the common prefix of the records

- `AVG`, `MAX`, `MIN`, and `FREQ` allowed as field modifiers
  - ➔ Use of FREQ is more strict (needs a boolean)

z/VM 6.2 Installation

- z/VM 6.2 VMSES has changed for SSI cluster support
  - Products can now be installed once in the cluster
  - Names of SFS Filepools have changed
- Production disk cannot be in SFS. Minidisk only.
- Program Directory has been adapted
- ✓ Install on minidisks is unchanged



z/VM deployment

- Some areas that may need attention
  - Use the correct disk sizes from the Program Directory
  - Ensure a normal user has access to the product minidisk
  - Access to the RACF database OS-formatted disk (RACFVM 200/300)
  - Access to the RACF SMF records (RACFVM 301/302)
  - Access to the ISPF product minidisk to bring up ISPF (ISPVM 192 disk)
  - Access to the minidisk where the customized CKV EXEC and configuration file are placed
  - Ensure the userid that is used for the COLLECT function has A, B, E and G privileges.
    As the COLLECT function can use a virtual machine that is invoked via XAUTOLOG, granting such privileges is usually not an issue.
    It will also need access to a current copy of the VM Directory.
    This can be obtained via DIRM with the (NO)PASS option.

Dropped support

- zSecure 1.11.1 no longer provides service for z/VM V5R3

Availability

- General Availability date: June 15, 2012
- Supports releases: z/VM V5R4 through z/VM V6R2