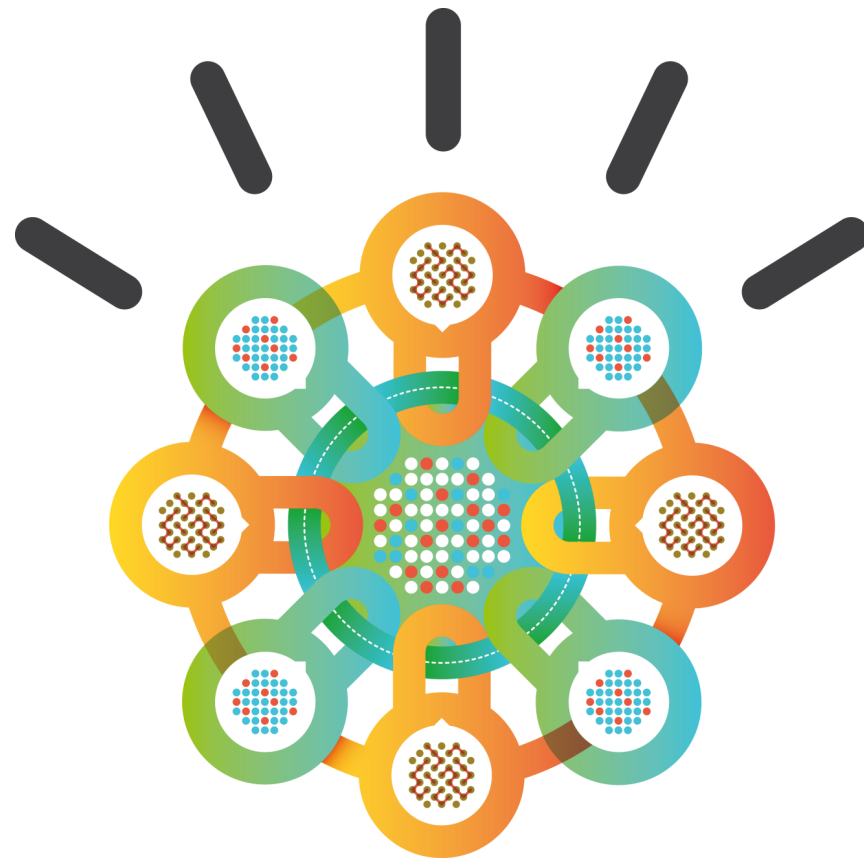


IBM Security zSecure update

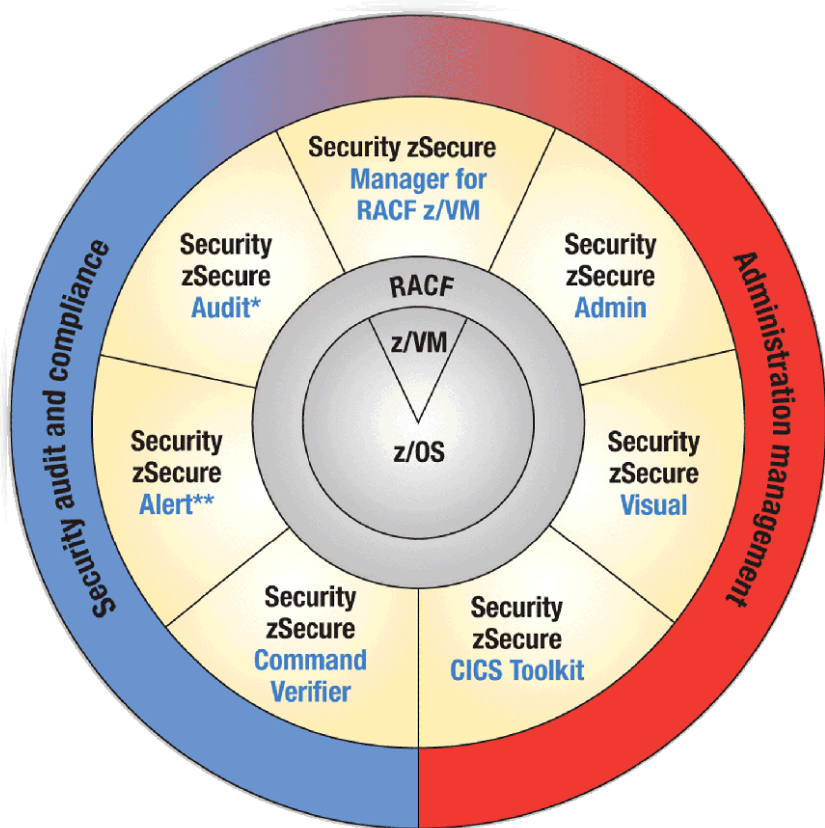
Rob van Hoboken
zSecure architect

rob.vanhoboken@nl.ibm.com



© 2012 IBM Corporation

IBM Security zSecure suite



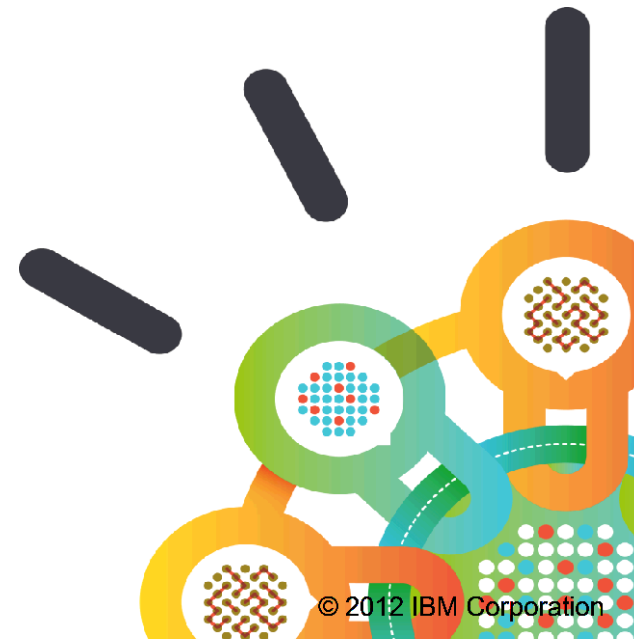
IBM Security zSecure

*Also available for ACF2™ and Top Secret®

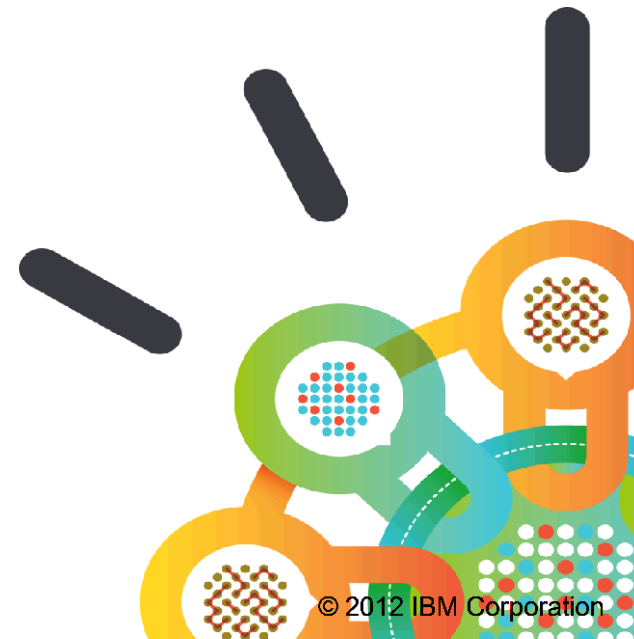
**Also available for ACF2

Agenda

- zSecure integration with Qradar SIEM
- What's new in zSecure 1.13.1
- zSecure Manager for RACF z/VM 1.11.1
- Availability



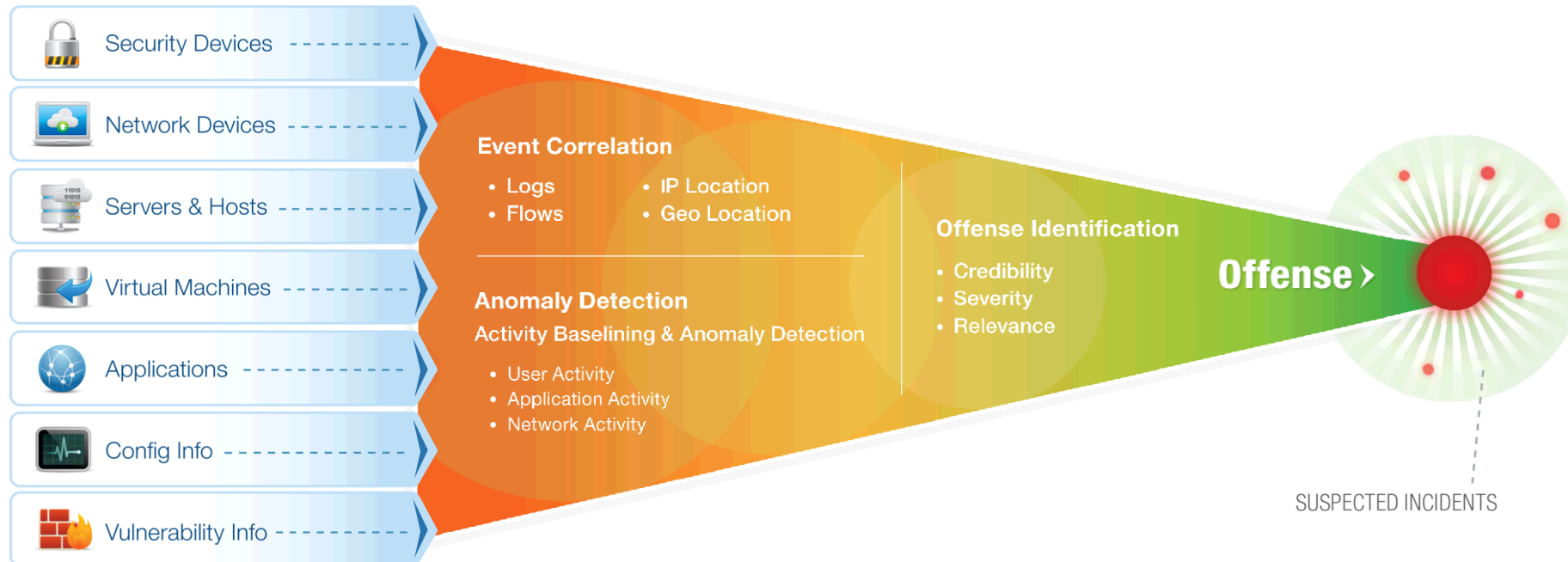
Qradar Integration



An Introduction to QRadar SIEM

- A next-gen SIEM product
(Security Information and Event Management)
- Offers:
 - Integrated log, threat, risk & compliance management
 - Sophisticated event analytics
 - Asset profiling and flow analytics
 - Offense management and workflow

An Introduction to QRadar SIEM



QRadar accepts data from a wide variety of sources to provide visibility into a customer's environment

An Introduction to QRadar SIEM – DSMs and Protocols

- ‘Log Source’ is the name for instances of a given product from which QRadar receives logs.
- A DSM (Device Support Module) is the code module QRadar uses to identify and understand events from a given log source.
 - There is one DSM per Log Source Type
- ‘Protocols’ are the components that handle the different methods of getting events from log sources to QRadar. Examples are Syslog, Log File, JDBC.



QRadar/zSecure Integration - DSMs

- DSMs and Protocols are pluggable components
 - they are shipped via rpm package
 - can be installed on a running QRadars system
- 6 new DSMs added for integration with zSecure Audit:
z/OS, RACF, DB2, CICS, Top Secret, ACF2
- These DSMs must be installed and deployed on QRadars

QRadar/zSecure Integration – ADD the Log Source

Add a log source

Log Source Name	z/OS
Log Source Description	z/OS mainframe1
Log Source Type	IBM z/OS
Protocol Configuration	Log File
Log Source Identifier	172.16.30.157 - zOS
Service Type	FTP
Remote IP or Hostname	172.16.30.157
Remote Port	21
Remote User	qaiteam
Remote Password
Confirm Password
Remote Directory	zOS_files
Recursive	<input type="checkbox"/>
FTP File Pattern	zOS.*gz
FTP Transfer Mode	BINARY
Start Time	00:00
Recurrence	1H
Run On Save	<input checked="" type="checkbox"/>
EPS Throttle	100
Processor	GZIP
Ignore Previously Processed File(s)	<input checked="" type="checkbox"/>
Change Local Directory?	<input type="checkbox"/>
Event Generator	LINEBYLINE



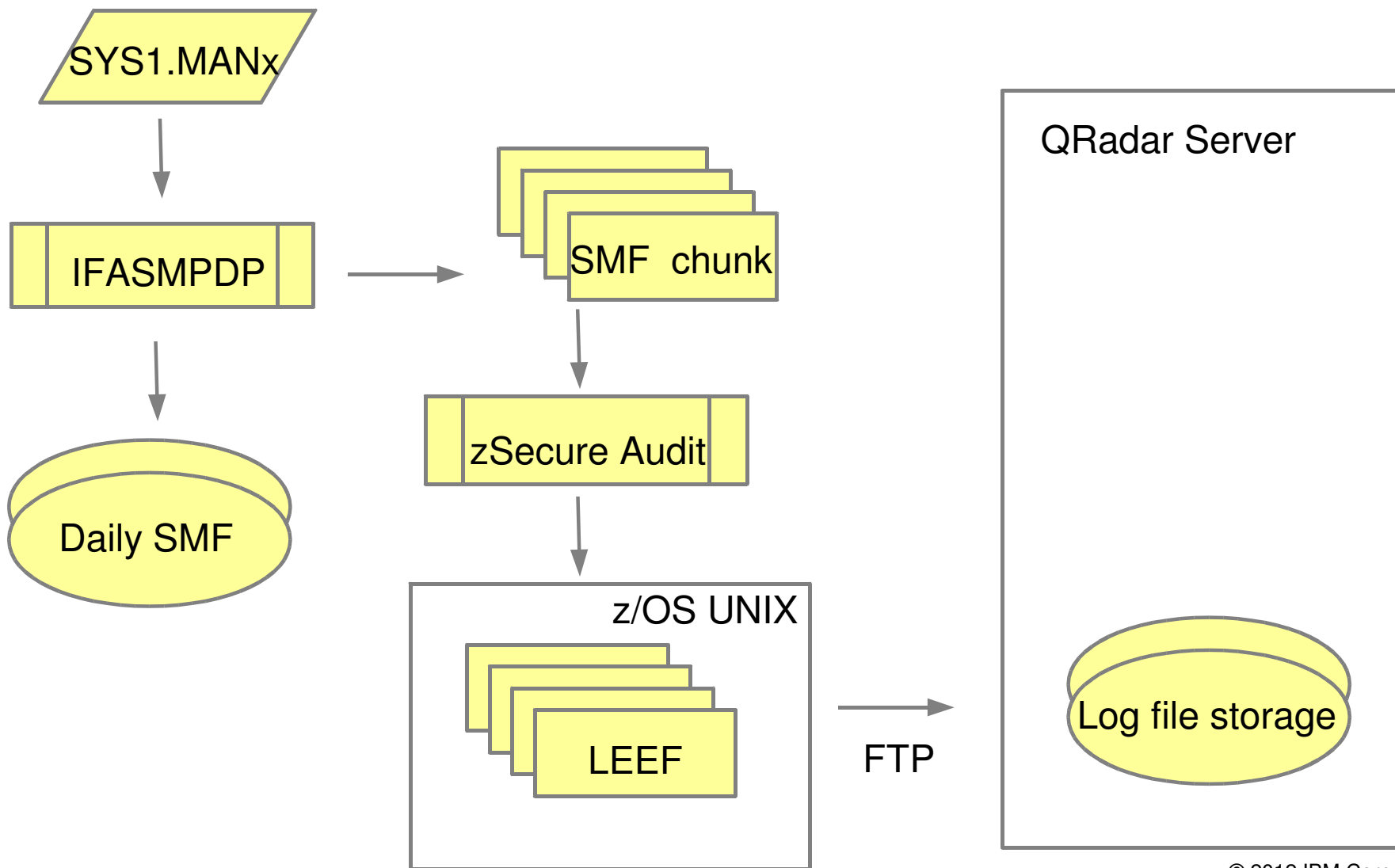
zSecure side – Prepare Log Source Data

- SMF is the source for QRadar Log Source
- Asynchronous zSecure Audit step to process SMF
 - Convert SMF to Log Event Enhanced Format (LEEF).
 - Header, fields separated by |
 - label=value<TAB>
 - Create data (LEEF files) for multiple DSMs:
e.g., z/OS, RACF, DB2, CICS.
 - Decide which SMF to process and when.

zSecure side – Sample Log Source Data

```
LEEF:1.0|IBM|RACF|1.13|80 2.0|devTimeFormat=yyyy-  
MM-dd'T'HH:mm:ss.SSSZ devTime=2012-08-21T13:37:45  
.240+0100 usrName=KCARR name=KRYSTAL CARRINGTON  
usrPriv=special superuser usrGroups=SYSPROG  
DEMOUSR ICTXname= ICTXreg= job=ZT01 21 Aug  
2012 11:51:24.66 DYNASTY intent=UPDATE  
allow=ALTER class=DATASET prof=USER.PROCLIB  
res=USER.PROCLIB vol=*SMS* dsn=USER.PROCLIB  
sens=STC proclib own= box=IBM-75-  
0000000GP091-1F37 terminal=ISZ002 poe= LU  
ISZ002 logstr= auth=Normal desc=Success  
appl= sum=RACF ACCESS success for KCARR:  
(UPDATE,ALTER) on DATASET USER.PROCLIB cmd=
```

zSecure side – Data flow



QRadar view of z/OS log activity from zSecure Audit

Welcome, admin [logout]
Dashboard Offenses Log Activity Network Activity Assets Reports Admin
System Time: 19:05 Preferences Help

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions Quick Filter...

Viewing events from 2012-07-05 18:51:00 to 2012-07-05 19:06:00 View: Select An Option: Display: Default (Normalized)

Current Filters:
Log Source is z/OS (Clear Filter)

Current Statistics

(Show Charts)

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
Non-VSAM data set input	z/OS	4	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	4
PDS member add/replace	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
Non-VSAM data set output	z/OS	4	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	4
VSAM data set open	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
Non-VSAM data set input	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
Job start	z/OS	1	18:59	Service Started	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
Non-VSAM data set input	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
VSAM data set close	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
Delete from catalog	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
Scratch data set	z/OS	1	18:59	File Deleted	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
Non-VSAM data set input	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
UDP Socket Close	z/OS	1	18:59	Session Terminated	172.16.30.157	0	172.16.30.157	28644	OMVS	1
PDS member add/replace	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
PDS member add/replace	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
Non-VSAM data set output	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
Non-VSAM data set output	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
Define in catalog	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
UDP Socket Close	z/OS	1	18:59	Session Terminated	172.16.30.157	0	172.16.30.157	28643	OMVS	1
PDS member add/replace	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
Non-VSAM data set output	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
UDP Socket Close	z/OS	1	18:59	Session Terminated	172.16.30.157	0	172.16.30.157	28642	OMVS	1
Job end	z/OS	1	18:59	Service Stopped	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
Job step result	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1
VSAM data set close	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	1


displaying 1 to 24 of 24 items (Elapsed time: 0:00:00.070)
Copyright © 2012 Q1 Labs Inc. All rights reserved.

RACF – RACHECK Access Violation Details

Welcome, admin [logout]

Dashboard
Offenses
Log Activity
Network Activity
Assets
Reports
Admin

System Time: 08:28 | Preferences | Help



Search...
Quick Searches
Add Filter
Save Criteria
Save Results
Cancel
False Positive
Rules
Actions
Quick Filter...

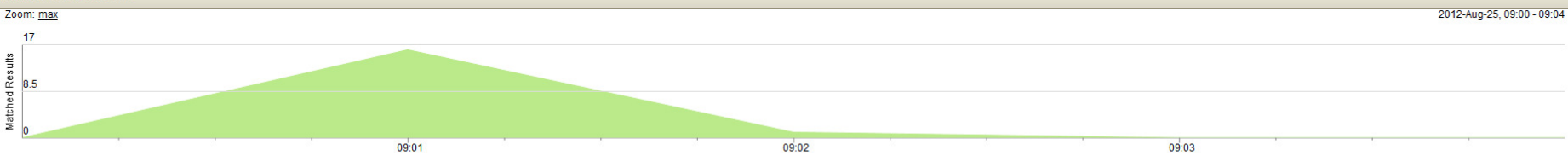
Viewing events from 2012-08-25 09:00:00 to 2012-08-25 09:04:00
View: Select An Option:
Display: Custom

Using Search: RACF - RACHECK Access Violations Details

Completed

Current Filters:
Log Source Group is IBM (Clear Filter), Event Name is RACHECK Insufficient authority (Clear Filter), Log Source is IBM RACF (Clear Filter)

Current Statistics

Records Matched Over Time
Zoom: max
2012-Aug-25, 09:00 - 09:04


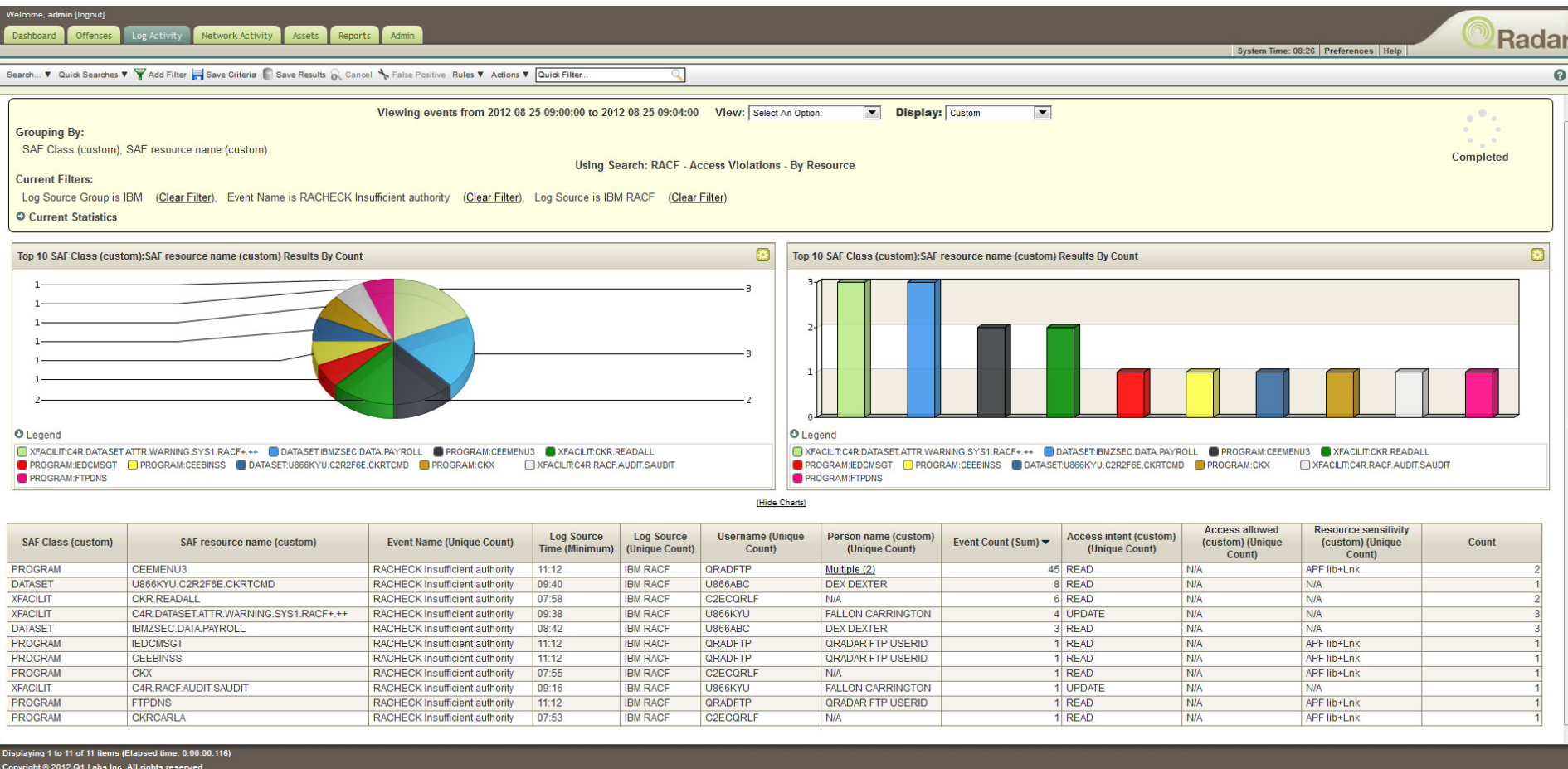
Update Details

Hide Charts


Event Name ▼	Log Source Time	Log Source	Event Count	Username	Person name (custom)	SAF Class (custom)	SAF resource name (custom)	Access intent (custom)	Access allowed (custom)	Resource sensitivity (custom)
RACHECK Insufficient authority	09:38	IBM RACF	2	U866KYU	FALLON CARRINGTON	XFACILIT	C4R.DATASET.ATTR.WA...	UPDATE	N/A	N/A
RACHECK Insufficient authority	09:40	IBM RACF	8	U866ABC	DEX DEXTER	DATASET	U866KYU.C2R2F6E.CK...	READ	N/A	N/A
RACHECK Insufficient authority	09:38	IBM RACF	1	U866KYU	FALLON CARRINGTON	XFACILIT	C4R.DATASET.ATTR.WA...	UPDATE	N/A	N/A
RACHECK Insufficient authority	09:38	IBM RACF	1	U866KYU	FALLON CARRINGTON	XFACILIT	C4R.DATASET.ATTR.WA...	UPDATE	N/A	N/A
RACHECK Insufficient authority	09:16	IBM RACF	1	U866KYU	FALLON CARRINGTON	XFACILIT	C4R.RACF.AUDIT.SAUDIT	UPDATE	N/A	N/A
RACHECK Insufficient authority	08:42	IBM RACF	1	U866ABC	DEX DEXTER	DATASET	IBMZSEC.DATA.PAYROLL	READ	N/A	N/A
RACHECK Insufficient authority	08:42	IBM RACF	1	U866ABC	DEX DEXTER	DATASET	IBMZSEC.DATA.PAYROLL	READ	N/A	N/A
RACHECK Insufficient authority	08:42	IBM RACF	1	U866ABC	DEX DEXTER	DATASET	IBMZSEC.DATA.PAYROLL	READ	N/A	N/A
RACHECK Insufficient authority	11:12	IBM RACF	21	QRADFTP	QRADAR FTP USERID	PROGRAM	CEEMENU3	READ	N/A	APF lib+Lnk
RACHECK Insufficient authority	11:12	IBM RACF	1	QRADFTP	QRADAR FTP USERID	PROGRAM	IEDCMSGT	READ	N/A	APF lib+Lnk
RACHECK Insufficient authority	11:12	IBM RACF	1	QRADFTP	QRADAR FTP USERID	PROGRAM	CEEBINSS	READ	N/A	APF lib+Lnk
RACHECK Insufficient authority	11:12	IBM RACF	1	QRADFTP	QRADAR FTP USERID	PROGRAM	FTPDNS	READ	N/A	APF lib+Lnk
RACHECK Insufficient authority	07:58	IBM RACF	5	C2ECQRLF	N/A	XFACILIT	CKR.READALL	READ	N/A	N/A
RACHECK Insufficient authority	07:58	IBM RACF	1	C2ECQRLF	N/A	XFACILIT	CKR.READALL	READ	N/A	N/A
RACHECK Insufficient authority	07:55	IBM RACF	1	C2ECQRLF	N/A	PROGRAM	CKX	READ	N/A	APF lib+Lnk
RACHECK Insufficient authority	07:53	IBM RACF	1	C2ECQRLF	N/A	PROGRAM	CKRCARLA	READ	N/A	APF lib+Lnk
RACHECK Insufficient authority	11:12	IBM RACF	24	QRADFTP	N/A	PROGRAM	CEEMENU3	READ	N/A	APF lib+Lnk

Displaying 1 to 17 of 17 items (Elapsed time: 0:00:00.147)
Copyright © 2012 Q1 Labs Inc. All rights reserved.

RACF – Access Violations by Resource



RACF – Access Violations by Username

Welcome, admin [logout]
Dashboard
Offenses
Log Activity
Network Activity
Assets
Reports
Admin
System Time: 08:27
Preferences
Help


Search...
Quick Searches
Add Filter
Save Criteria
Save Results
Cancel
False Positive
Rules
Actions
Quick Filter...

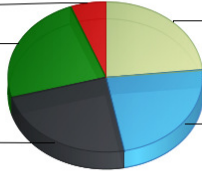
Viewing events from 2012-08-25 09:00:00 to 2012-08-25 09:04:00
View: Select An Option:
Display: Custom
Completed

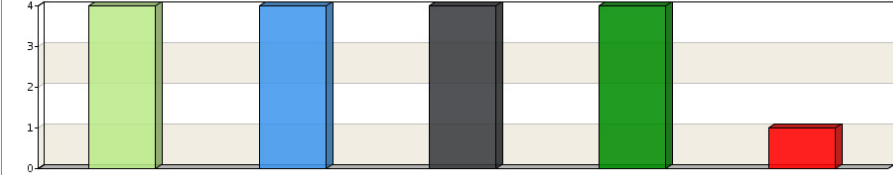
Grouping By:
Username, Person name (custom)

Using Search: RACF - Access Violations - By Username

Current Filters:
Log Source Group is IBM (Clear Filter), Event Name is RACHECK Insufficient authority (Clear Filter), Log Source is IBM RACF (Clear Filter)

Current Statistics

Top 10 Username:Person name (custom) Results By Count


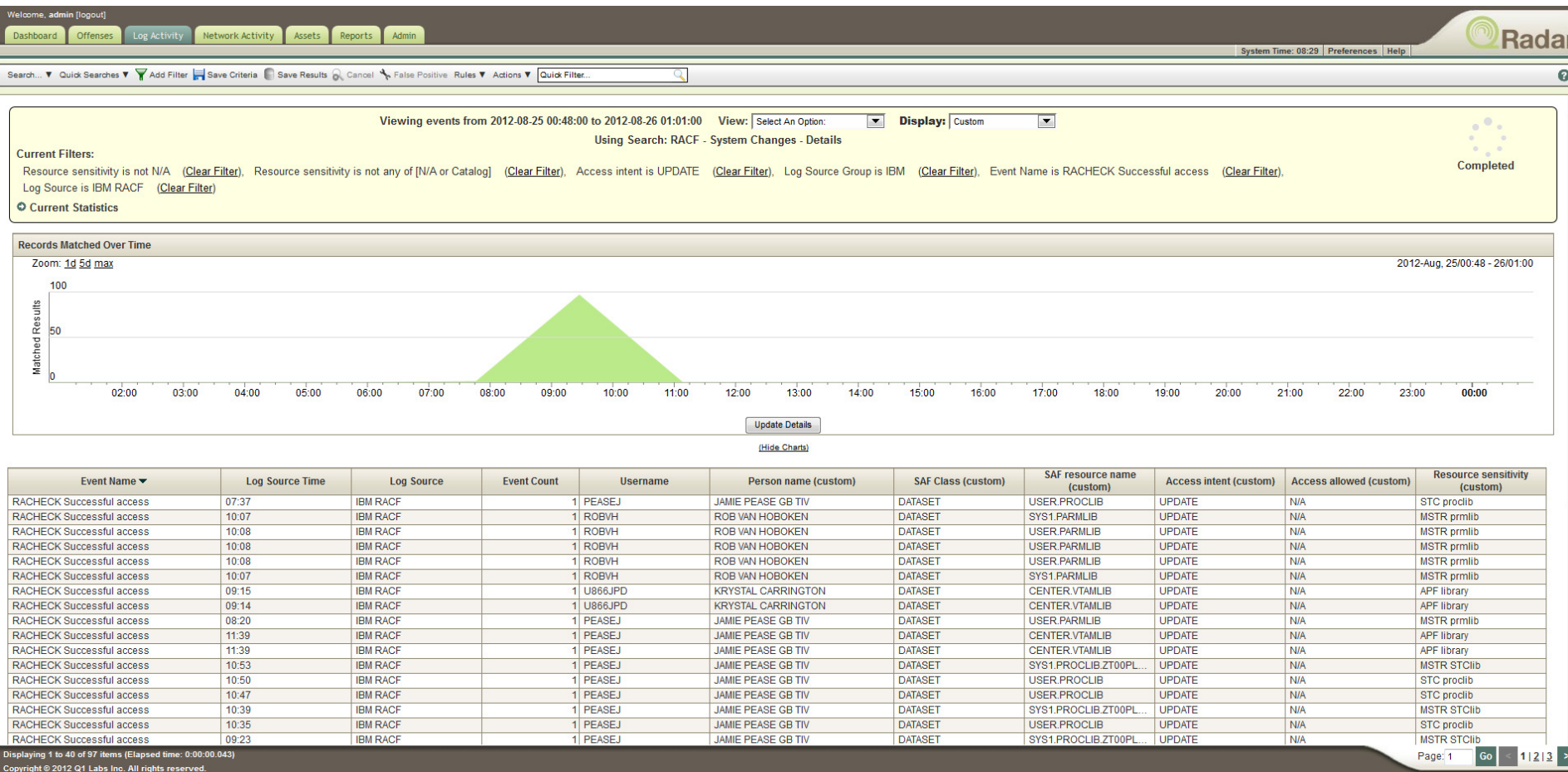
Top 10 Username:Person name (custom) Results By Count


(Hide Charts)

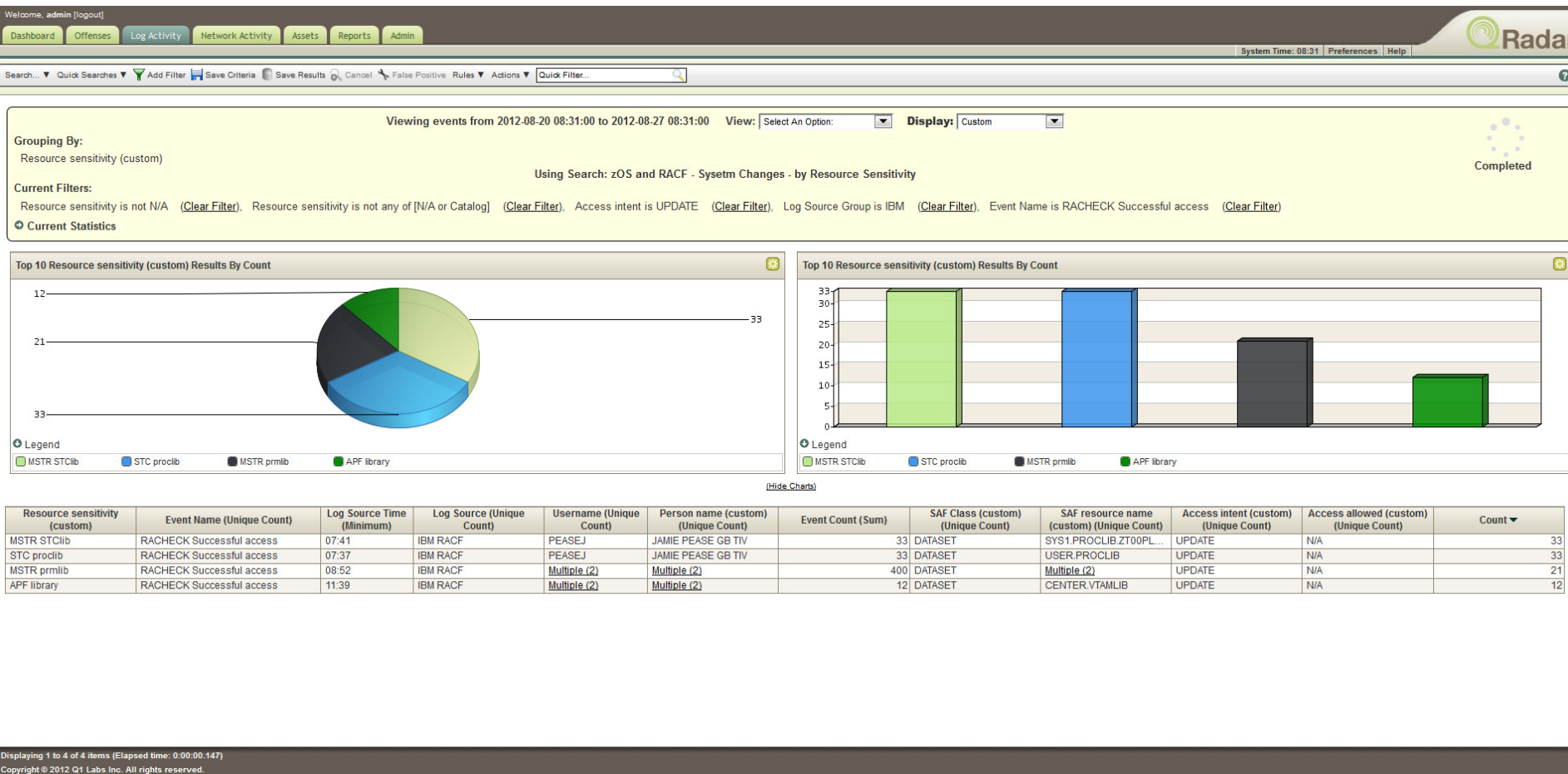
Username	Person name (custom)	Event Name (Unique Count)	Log Source Time (Minimum)	Log Source (Unique Count)	Event Count (Sum)	SAF Class (custom) (Unique Count)	SAF resource name (custom) (Unique Count)	Access intent (custom) (Unique Count)	Access allowed (custom) (Unique Count)	Resource sensitivity (custom) (Unique Count)	Count
C2ECQRLF	N/A	RACHECK Insufficient authority	07:53	IBM RACF	8	Multiple (2)	Multiple (3)	READ	N/A	Multiple (2)	4
U866KYU	FALLON CARRINGTON	RACHECK Insufficient authority	09:16	IBM RACF	5	XFACILIT	Multiple (2)	UPDATE	N/A	N/A	4
QRADFTP	QRADAR FTP USERID	RACHECK Insufficient authority	11:12	IBM RACF	24	PROGRAM	Multiple (4)	READ	N/A	APF lib+Lnk	4
U866ABC	DEX DEXTER	RACHECK Insufficient authority	08:42	IBM RACF	11	DATASET	Multiple (2)	READ	N/A	N/A	4
QRADFTP	N/A	RACHECK Insufficient authority	11:12	IBM RACF	24	PROGRAM	CEEMENU3	READ	N/A	APF lib+Lnk	1

Displaying 1 to 5 of 5 items (Elapsed time: 0:00:00.142)
Copyright © 2012 Q1 Labs Inc. All rights reserved.

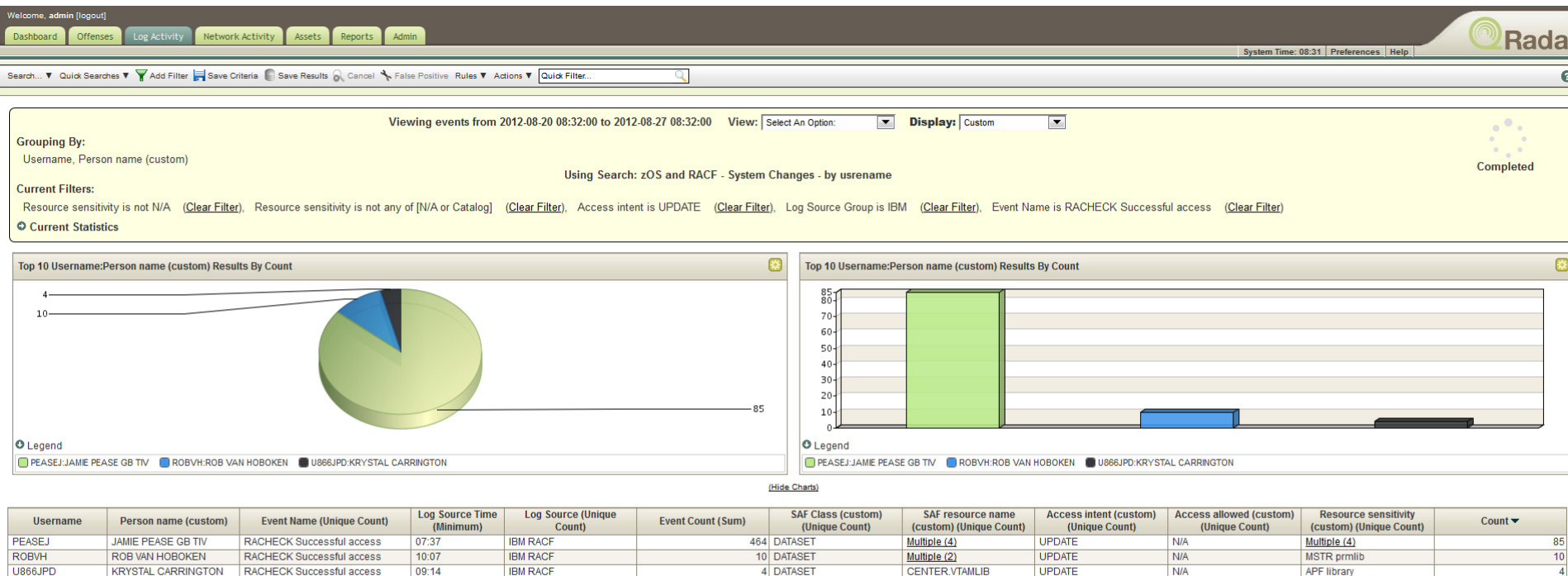
RACF - RACHECK Successful Access



zOS and RACF – System Changes by Resource Sensitivity



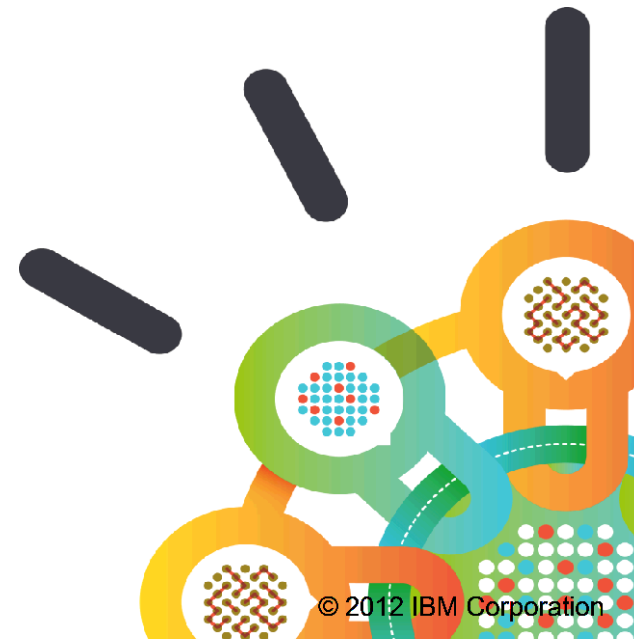
zOS and RACF – System Changes by Username



zSecure and QRadar Security Intelligence integration

- Strengthen mainframe security operations and help improve protection for critical mainframe environment
- Improve compliance visibility real-time with standards and regulations by simplifying audit and management efforts
- Consolidate enterprise security view allowing the identification and remediation of excess mainframe access, threats and concerns.
- Store event data in forensically secure database to address regulation mandates.
- Trigger complex correlation of threats, insider fraud and business risk as easy to understand “offenses” for further investigation and follow-ups

What's new in 1.13.1

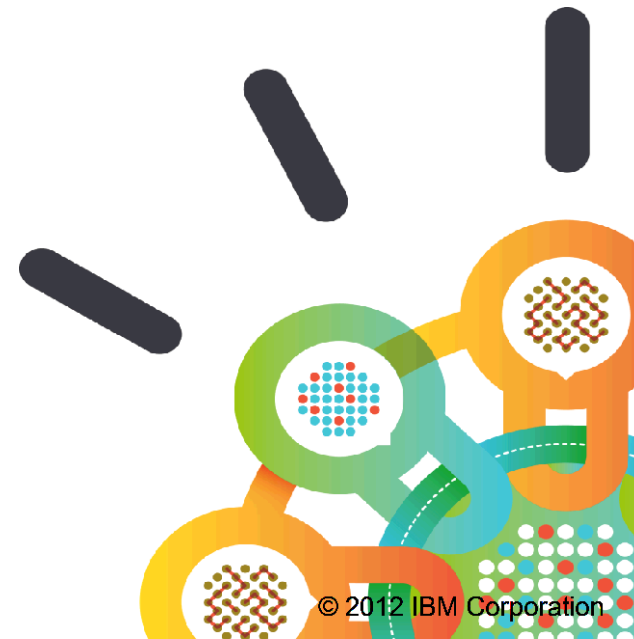




zSecure Admin and Audit 1.13.1 – Themes

- Access Monitor Improvements
- User Interface improvements
 - Compare function
- DB2 resource collection
- Compliance reporting

Access Monitor Enhancements



New field in ACCESS Newlist: SIM_VIA

(1/8)

- SIM_VIA shows authority used to decide access
 - Calculated by CKRCARLA
 - Based on current RACF database
- Possible values are:
ID_User, ID_Group, ID_Star, UACC,
Qual_Own, Create, Global, Grp_UACC,
Sys_Oper, Sys_Spec, Grp_Oper, Grp_Spec,
Inactive, DfltRC, No_CDT, Noprot, ProtFail,
PrivTrus, No_Prof, APF, <blank>

New field in ACCESS Newlist: SIM_VIA

(2/8)

- Sample output when used in summary

```

                                IBM Security zSecure ACCESS summary
Command ==> _
All access monitor records
  Occurrence Via      First occurrence Last occurrence
---
      51 ID_USER  17Apr2012 14:50 17Apr2012 14:55
      15 ID_GROUP 17Apr2012 14:51 17Apr2012 14:51
      85 UACC     17Apr2012 14:51 17Apr2012 14:55
     118 GLOBAL   17Apr2012 14:51 17Apr2012 14:52
      23 QUALOWN  17Apr2012 14:51 17Apr2012 14:52
      14 SYS_OPER 17Apr2012 14:51 17Apr2012 14:51
       1 SYS_SPEC 17Apr2012 14:51 17Apr2012 14:51
       2 PROTFAIL 17Apr2012 14:51 17Apr2012 14:52
      18 DFLTRC   17Apr2012 14:50 17Apr2012 14:52
       2 PRIVTRUS 17Apr2012 14:51 17Apr2012 14:51
*****
  
```



New field in ACCESS Newlist: SIM_VIA

(4/8)

- Process for UACC/ID(*) cleanup
Replace access by a functional group
 - 1) Select all users/resources that are likely to be grouped together
 - 2) Generate commands that connect all users that access via UACC to the functional group
 - 3) If no more access to resource via UACC, generate commands to reset UACC to NONE

New field in ACCESS Newlist: SIM_VIA

(5/8)

1) Connect users to new group

Start at AM.9

Use option 4 to convert UACC to a functional group

Use option 5 to convert ID(*) to a functional group

```
zSecure Suite - Access - Cleanup
Option ==> █
1  User permit      Redundant permits to userids
2  Dataset          Redundant dataset profiles
3  Empty            Generic profiles without matching disk or tape datasets
4  UACC             Generate permits/connects to convert UACC access
5  ID(*)            Generate permits/connects to convert ID(*) access
```

New field in ACCESS Newlist: SIM_VIA

(6/8)

- 1) Select users/resource that are likely to be grouped together
Specify intended access to convert specific access
Provide info for the (new) functional group

```

zSecure Suite - Cleanup - UACC
Command ==> █

Generate permits/connects to convert UACC selection criteria:
Userid . . . . . BCSC*      (userid or EGN mask)
Complex . . . . .          (complex or EGN mask)
SAF resource class . . . DATASET (class or EGN mask)
SAF resource name . . . a*.*
RACF match on . . . . .
Intended access . . . . >= 1 1. Read    2. Update  3. Control  4. Alter

Date selection
From date . . . . .      Until date . . . . .

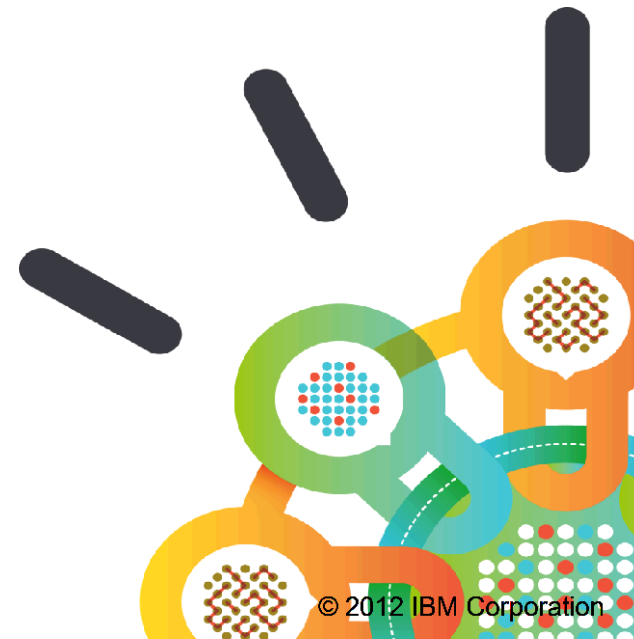
Specify data for group for which permit/connect commands are generated
Group for permit/connect BCSCUACC (group name; required, no mask allowed)
Superior group . . . . .      (group name; optional for new group)
Owner for new group . . .      (owner name; optional for new group)
Instdata new group . . .
  
```



Other enhancements

- Improved access simulation for OPERATIONS users
 - Access via System-OPERATIONS is now simulated
 - In ACCESS newlist shown in SIM_VIA, SIM_RESULT
 - In RACF_ACCESS newlist counted as ALTER-O
 - Also support for SPECIAL attribute
- Improved search for matching GLOBAL profiles
 - Better handling of &RACUID qualifier

ISPF UI enhancements





COMPARE functions

(1/10)

- Option in UI to designate an input set as a baseline
 - Enables use of “Show compare differences”.
 - Extra column (Compare Result) added to overview display.
 - Extra field (Compare Changes) added to detail display.

Compare Interface – Where to start ?

(3/10)

- New line commands in SETUP FILES
 - C to use set as Compare Base ('baseline')
 - M to use set as Merge Source (unused in UI)

```

zSecure Manager for RACF - Setup - Input      ROW 1 OF 5
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)

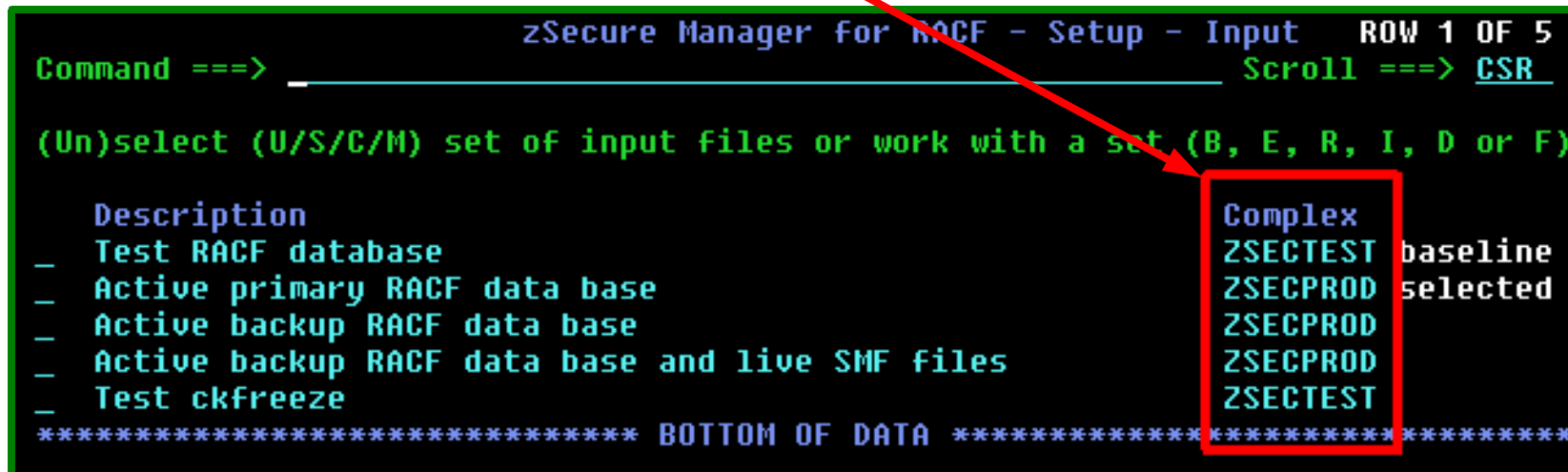
      Description                                Complex
- Active backup RACF data base and live SMF data sets      merge
- Active backup RACF data base                             baseline
- Default RACF database                                   selected
- VM30V06 CKFREEZE A1                            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

- “Function=” removed from data set details

Compare Interface – Where to start ?

(4/10)

- Always specify a **Complex** name



```

zSecure Manager for RACF - Setup - Input   ROW 1 OF 5
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
- Test RACF database                       ZSECTEST baseline
- Active primary RACF data base            ZSECPROD selected
- Active backup RACF data base             ZSECPROD
- Active backup RACF data base and live SMF files ZSECPROD
- Test ckfreeze                           ZSECTEST
***** BOTTOM OF DATA *****
  
```

- Omitting a Complex
 - Makes result hard to interpret
 - Sometimes leads to error messages

Compare Interface – Next step

(5/10)

- With a BASELINE set and a regular (MAIN) set, you can select the **Show differences** selection fields to compare RACF sources and/or CKFREEZE files.

```

Menu      Options      Info      Commands      Setup

zSecure Suite - RACF - User Selection

Command ==> _ start panel

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

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

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

Compare Interface – Next step

(6/10)

- When checked, additional panel allows specification which compare results to show.

```

Menu      Options      Info      Commands      Setup

zSecure Suite - Show differences

Command ==>

Select the type(s) of difference for display
/ ADD     Entries that were added into selected set
/ DEL     Entries that were deleted from selected set
/ CHG+    Changes that improve security
/ CHG-    Changes that reduce security
/ CHGu    Changes without impact on the security compliance level
- SAME    Identical entries
- BASE    Baseline records

Note: For comparing input sources, you need to select one baseline input set
(by using the SETUP FILES C action command),
and at least one regular main set (by using the SETUP FILES S action command)

```

- Some panels show direct selection line

```

Show differences
/ ADD / DEL / CHG+ / CHG- / CHGu _ SAME _ BASE
Output/Run options

```

Compare Interface – Results Overview

(8/10)

- If at least one difference type is selected, COMP (Compare Result) column in overview display

zSecure Suite USER overview Line 21 of 2056

Command ==> CSR Scroll==> CSR

All users 13 Mar 2009 12:33

User	Complex	Name	Comp	DfltGrp	Owner	RIRP	SOA	gC	LC
irrcerta	RECOVERY	CERTAUTH Anchor	CHG		irrcerta	R			C
irrmulti	RECOVERY	Criteria Anchor	CHG		irrmulti	R			
irrsitec	RECOVERY	SITE Anchor	CHG		irrsitec	R			C
AB5200A	NANO		DEL	CRMDTEST	CRMDTEST	P			
AB5201A	NANO		DEL	CRMDTEST	CRMDTEST	P			
AB5240A	NANO		DEL	CRMDTEST	CRMDTEST	P			
AB5241A	NANO		DEL	CRMDTEST	CRMDTEST	P			
AB5392A	NANO		DEL	CRMDTEST	CRMDTEST	P			
AB5393A	NANO		DEL	CRMDTEST	CRMDTEST	P			
AB5394A	NANO		DEL	CRMDTEST	CRMDTEST	P			
AB5396A	NANO		DEL	CRMDTEST	CRMDTEST	P			
AB5397A	NANO		DEL	CRMDTEST	CRMDTEST	P			
AB5398A	NANO		DEL	CRMDTEST	CRMDTEST	P			
AB5399A	NANO		DEL	CRMDTEST	CRMDTEST	P			
AB5499A	NANO		DEL	CRMDTEST	CRMDTEST	P			
ACFQAC90	RECOVERY		ADD	CRMQ	CRMQ	RI			
ACFSTCID	NANO	DO NOT LOGON	DEL	SYS1	SYS1	P			
ADM@ACL	RECOVERY	KERBEROS AUTH DS	ADD	KERBEROS	KERBEROS	P			
ADM@SRV	RECOVERY	KERBEROS ADMIN	ADD	KERBEROS	KERBEROS	I			
ADM1	RECOVERY	USR =QA OW=ADMIN	CHG	ADMIN	ADMIN	R P			

Compare Interface – Results Details

(9/10)

- 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 AUT01                                         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
Revoked (may be by date)   No
Inactive, revoked or pending   Yes
Days of week user can logon   SMTWTFS
Time of day user can logon   _ _ _ _ _

Statistics
Creation date              28Apr98
Last RACINIT current connects   5May98
User's last use date         5May98
User's last use time         15:53
  
```



Compare Interface

(10/10)

- Compare function is available on:
 - RA.U/G/D/R – RACF User/Group/Dataset/Resource
 - RA.2/5 – RACF digital certificates
 - RA.3.A/B/C/D/E/F – RACF special purpose
 - RA.S – RACF setropts
 - AU.S – Audit status
 - RE.T/I/U/C/M/D – Resource views
 - AA.I/L/R/S – ACF2 database

Selection and Summary in TRUSTED reports

(1/3)

- Trust relation
 - Any way a subject can access a sensitive object
 - Both RACF and ACF2 support
- Available in new option RE.T
 - ✓ Selection on Trust level, Users, Resources
 - ✓ Summary on User or Resource
 - No change in reported information

Selection and Summary in TRUSTED reports

(2/3)

- New option RE.T (Sensitive Resources)

```

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
  T   Trusted         Trusted users and sensitive resources reports
AM   Access          RACF Access Monitor
  
```

- Specify additional selection criteria and summarize category

```

                                zSecure Suite - 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
- Show differences
- Print format             Customize title       Send as e-mail
  
```


Selection and Summary in 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
```

Additional UI enhancements

- Improve Field Value verification
 - ✓ Error messages are issued earlier
 - ✓ Avoid (cryptic) failures in CKRCARLA
 - ✓ Done for most input selection fields

```

                                zSecure Suite - RACF - User
Command ==> _____ Invalid character
                                _ start panel

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

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

The following characters are not supported for this field: embedded blanks,
commas, parentheses, single quotes, double quotes, back quotes, and
semicolons

Background run Full page form Sort differently Narrow print
  
```

Additional UI enhancements

- Select on absence of ACL id

```

Menu      Options      Info      Commands      Setup

zSecure Suite - RACF - Data set Selection

Command ==>
All profiles
Specify additional selection criteria:
Find a combination of the following in the access list
# permits . . . . . (operator: < <= > >= = <> ^= )
# conditional permits . . . . . (operator: < <= > >= = <> ^= )
Id on access list . . <> IBMUSER_ (=, ^= or <> + id, or filter)
When resource . . . . . (resource name or filter)
Access level . . . . . 1. None      When class . . . 1. PROGRAM
                        2. Execute   2. CONSOLE
                        3. Read       3. APPCPORT
                        4. Update     4. TERMINAL
                        5. Control    5. JESINPUT
                        6. Alter      6. SERVAUTH
                        7. Ignore     7. Present
                        8. Ignore     8. Ignore

Access list filtering
_ Only show matching ACL entries

B 10/036
Connected to remote server/host wlaa.tivlab.raleigh.ibm.com using lu/pool TCPA0536 and port 23

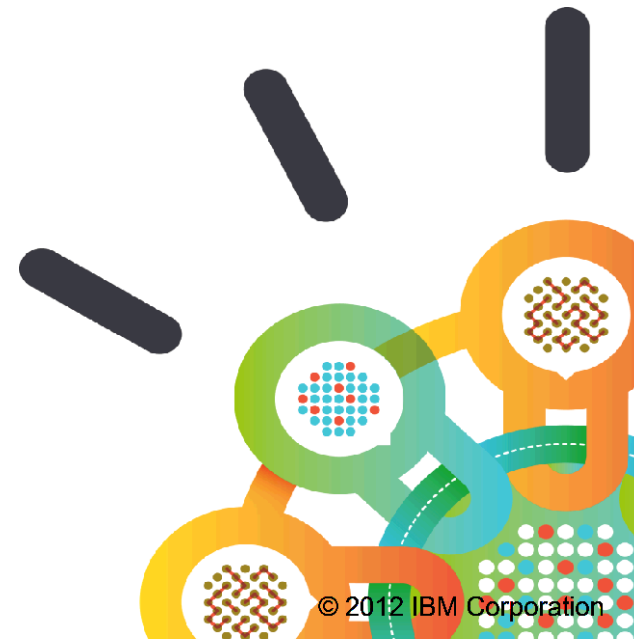
```

→ If operator is omitted, presence is tested

Additional UI enhancements

- P line command on application segment
 - Shows the profile belonging to the segment

DB2 Resource Collection





DB2 Resource Collection

- Collect more data from
 - ✓ DB2 region
 - ✓ Startup (dsnzparm) parameters
 - ✓ DB2 catalog tables
 - ✓ Tables, Plans, Packages
 - ✓ User authorizations
- Show access and authorizations
 - ✓ Internal DB2 privileges
 - ✓ RACF defined attributes
 - ✓ RACF defined authorizations



DB2 Resource Collection

- ✓ Extra keyword for CKFCOLL
 - DB2CAT option to collect
Tables, Plans, Packages, Userauth
- ✓ Extra records in CKFREEZE data set
- ✓ Reported in existing and new newlists
- ✓ Available in UI using options
RE.D.R/TB/PK/PN



DB2 Region Reporting

- New fields in DB2_REGION newlist
 - ✓ CLASS_ADMIN, CLASS_DSNR,
 - ✓ DB2_LEVEL, START_DATETIME, SYSPARM_STARTUP
SYSPARM_ACTIVE, SYSPARM_ACTIVE_DATETIME,
 - ✓ ZPRM_SYSADM, ZPRM_SYSADM2, ZPRM_SYSOPR1,
ZPRM_SYSOPR2, ZPRM_SECADM1, ZPRM_SECADM2,
ZPRM_SEPARATE_SECURITY
 - ✓ ZPRM_SCCSID, ZPRM_MCCSID, ZPRM_MIXED
 - ✓ ZPRM_SMFACCT, ZPRM_SMFSTAT, ZPRM_AUDITST
 - ✓ DB2_ACL, RACF_DB2_ACL, ...
- ISPF primary command ACL ORIGIN | NOORIGIN toggles individual GRANT lines versus one line per authid where date and grantor show most recent change.

DB2 Region Reporting Overview

DB2 region display

Command ==>

All DB2 region records

Pri	Jobname	Complex	System	DB2I	LUNAME	SITENAME	GRPN	CMDCHAR	PCLX	RegUser	St
—	DBA2MSTR	SP12	SP12	DBA2	DB2DBA2	DBA2		:DBA2	00003500	DCUSER	DB
—	D81KMSTR	SP12	SP12	D81K	DB2D81K	D81K		:D81K	00002600	DCUSER0	D8
—	D81VMSTR	SP12	SP12	D81V	DB2D81V	D81V		:D81V	00002700	DCUSER0	D8
—	D81WMSTR	SP12	SP12	D81W	DB2D81W	D81W	D81G	:D81W	00002800	DCUSER0	D8
—	D91DMSTR	SP12	SP12	D91D	DB2D91D	D91C	D91G	:D91D	00002A00	DCUSER	D9
—	D91IMSTR	SP12	SP12	D91I	DB2D91I	D91I		:D91I	00002D00	DCUSER	D9

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

➤ Scroll right for additional data:

Line 1 of 6

Scroll==> CSR

9 Jun 2012 19:31

GRPN	CMDCHAR	PCLX	RegUser	StrtSprm	ActvZprm	StrtTime	ActvTime	DB2 lvl	A
	:DBA2	00003500	DCUSER	DBA2PARM	DBA2PARM	4Jun12 10:41:34	4Jun12 10:41:34	V10.1.0	
	:D81K	00002600	DCUSER0	D81KPARM	D81KPARM	4Jun12 10:41:43	4Jun12 10:41:43	V8.1.0	
	:D81V	00002700	DCUSER0	D81VPARM	D81VPARM	4Jun12 12:33:29	4Jun12 12:33:29	V8.1.0	
	D81G :D81W	00002800	DCUSER0	D81WPARM	D81WPARM	4Jun12 10:07:49	4Jun12 10:07:49	V8.1.0	
	D91G :D91D	00002A00	DCUSER	D91DPARM	D91DPARM	4Jun12 10:07:49	4Jun12 10:07:49	V9.1.0	
	:D91I	00002D00	DCUSER	D91IPARM	D91IPARM	4Jun12 10:07:49	4Jun12 10:07:49	V9.1.0	

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

DB2 Region Reporting Details

➤ Zoom in to a particular DB2 region

```

                                DB2 region display                                Line 1 of 78
Command ===> _____ Scroll===> PAGE
All DB2 region records                                24 May 2012 07:53

Region identification
Complex name                WLAA
System name                 PL87
DB2 System identification    DBA1
DB2 Region job name         DBA1MSTR Step Jobid STC02094 ASID 0045
DB2 Region step name       DBA1MSTR
Local LU name              DBA1LU
Local site name            DBA1
Group attachment name
Command character          -DBA1
Linkage table index        00180700
Region userid              SYSDSP                                Dfltgrp:
Startup system zparm module DBA1PARM
Active system zparm module DBA1PRMZ
Subsystem startup timestamp 22May12 01:00:11
Last SET SYSPARM timestamp 23May12 05:46:29
DB2 system release level   V10.1.0

Region security settings
DB2 authorization checking  No          Extended security      Yes
  
```

DB2 Region Reporting Details

```

                                DB2 region display                                Line 19 of 78
Command ==> _                               Scroll==> PAGE
All DB2 region records                               24 May 2012 07:53

Region security settings
DB2 authorization checking      No      Extended security      Yes
DBA can create for others      No
Authorization exit module      DSN3@ATH Access control module      DSNX@XAC
Signon exit module             DSN3@SGN
Classification Option          2 (1=single-subsystem, 2=multi-subsystem)
Class Name Root               DSN      Class Name suffix          1

Region user      Id      RI Name      DfltGrp  InstData
System administrator id      IBMUSER      NONAME      SYS1
System administrator id 2    DB2ADM
Console operator id 1        IBMUSER      NONAME      SYS1
Console operator id 2        GROUP1
_ System default id          IBMUSER      NONAME      SYS1
RLF authorization id         IBMUSER      NONAME      SYS1
Security administrator id 1
Security administrator id 2
Separate security tasks      No
  
```

DB2 Region Reporting Details

```

DB2 region display                                     Line 40 of 78
Command ==> _____ Scroll==> PAGE
All DB2 region records                               24 May 2012 07:53

Region auditing settings
Audit trace start                                   No
SMF accounting data                                1
SMF statistics data                                1 3 4 5 6
Compress SMF trace records                          No

SAF protection settings
Subsystem access class                             Class   Grouping Act  Gen
Admin authorization class                           DSNR     N/A      Yes Yes
Buffer pool privileges class                         MDSNBP   GDSNBP   Yes Yes
Class system privileges                             MDSNSM   GDSNSM   Yes Yes
Collection privileges class                         MDSNCL   GDSNCL   Yes Yes
Stored proc privileges class                        MDSNSP   GDSNSP   Yes Yes
Database privileges class                          MDSNDB   GDSNDB   Yes Yes
Sequences class                                     MDSNSQ   GDSNSQ   Yes Yes
Java archive files class                           MDSNJR   GDSNJR   Yes Yes
Table/index/view priv. class                       MDSNTB   GDSNTB   Yes Yes
Package privileges class                           MDSNPK   GDSNPK   Yes Yes
Tablespace privileges class                        MDSNTS   GDSNTS   Yes Yes
Plan privileges class                              MDSNPN   GDSNPN   Yes Yes
  
```

DB2 Region Reporting Details

```

DB2 region display                                     Line 60 of 78
Command ==> _____ Scroll==> PAGE
All DB2 region records                               24 May 2012 07:53

Schema privileges class      MDSNSC   GDSNSC   Yes Yes
User type privileges class   MDSNUT   GDSNUT   Yes Yes
Storage group privilege class MDSNSG   GDSNSG   Yes Yes

Archive log settings
Add timestamp to archive log No
Archive log 1 dsn prefix     DSN101.ARCHLOG1
Archive log 2 dsn prefix     DSN101.ARCHLOG2

Resource name translation from UTF8
Mixed byte character set     65534   Use mixed character set      No
Single byte character set     37

Miscellaneous settings
IRLM procedure name          DBA1IRLM IRLM subsystem name          IRA1
New version uses BINDADD     Yes      Utility temp storage class

Pri Audit concern

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

```

DB2 Tables Reporting

- New DB2_TABLE newlist with fields
 - ✓ COMPLEX, SYSTEM, DB2ID, SCHEMA, NAME
LOCATION, DBID, OBID, DATABASE,
TABLESPACE, TABLE_TYPE,
 - ✓ ROW_MLS, LABEL, OWNER, OWNER_TYPE,
CREATEDBY, CONTROL
 - ✓ CREATE_TIMESTAMP, ALTER_TIMESTAMP,
RELATED_SCHEMA, RELATED_TABLE
 - ✓ CLASS, RESOURCE_PREFIX, AUDITING,
DB2_ACL, RACF_DB2_ACL
 - ✓ . . .

DB2 Tables Reporting

➤ Now available as RE.D.TB

```
zSecure Suite - Resource - DB2
Option ==> █
R   Regions      Region overview and system privileges (DSNADM, MDSNSM)
PK  Packages     Packages (pre-bound SQL statements)
PN  Plans        Plans (control structures created during BIND)
TB  Tables/views  Tables and views
```

➔ Tables and Views are combined in single report type

DB2 Tables Reporting

- Selection criteria
- Summary options

```

zSecure Suite - DB2 - Tables/views

Command ==> _____

Show DB2 tables/views that fit all of the following criteria:
Table/view name . . . . . 
Table type . . . . . _ A/C/G/H/M/P/T/U/X (default all types)
DB2ID . . . . . _____ (identifier or filter)
Database name . . . . . _____ (database or filter)
Schema name . . . . . _____
Complex . . . . . _____ (complex or filter)
System . . . . . _____ (system or filter)

Advanced selection criteria
_ Security settings      _ Authids and tablespace

Output/run options
_ 0. No summary          2. Summary by table name  4. Summary by schema
_ 1. Summary by region   3. Summary by table type  5. Summary by database
_ Show differences
_ Print format           Customize title          Send as e-mail
_ Background run         Full page form
  
```

- All fields can be used as selection criteria

DB2 Tables Reporting Overview Display

DB2 tables display					
Command ==> ■					
All DB2 table/view records					
Table	Complex	OBID	T	DB2I	Database
ADMIN_TASKS	IDFX	3	T	DB9G	DSNADMDB
ADMIN_TASKS_HIST	IDFX	8	T	DB9G	DSNADMDB
AGEGROUP	IDFX	40	T	DB9G	DSN8D91Y
ALA_RESTART	IDFX	3	T	DB9G	SYSTOOLS
APPLICANT	IDFX	5	T	DB9G	DSQ1STBB
AUX_BMP_PHOTO	IDFX	14	X	DB9G	DSN8D91L
AUX_EMP_RESUME	IDFX	20	X	DB9G	DSN8D91L
AUX_PSEG_PHOTO	IDFX	8	X	DB9G	DSN8D91L
BIN_REC_INPUT	IDFX	0	G	DB9G	DSNDB06
BIN_REC_OUTPUT	IDFX	0	G	DB9G	DSNDB06
BP_TBL	IDFX	0	G	DB9G	DSNDB06
BUFFERPOOL_STATUS	IDFX	0	G	DB9G	DSNDB06
CATALOG	IDFX	49	T	DB9G	DSN8D91X
CITY	IDFX	24	T	DB9G	DSN8D91Y
CMDMSG_TBL	IDFX	0	G	DB9G	DSNDB06
COMMAND_SYNONYMS	IDFX	22	T	DB9G	DSQDBCTL
CUSTOMER	IDFX	21	T	DB9G	DSN8D91X
CUSTOMERS	IDFX	49	T	DB9G	DSN8D91Y
DATA_SHARING_GROUP	IDFX	0	G	DB9G	DSNDB06
DB2_CMD_OUTPUT	IDFX	0	G	DB9G	DSNDB06
DB2_SYSPARM	IDFX	0	G	DB9G	DSNDB06
DB2_THREAD_STATUS	IDFX	0	G	DB9G	DSNDB06
DBSTATUS_TBL	IDFX	0	G	DB9G	DSNDB06
DB_STATUS	IDFX	0	G	DB9G	DSNDB06
DDF_CONFIG	IDFX	0	G	DB9G	DSNDB06
DDF_TBL	IDFX	0	G	DB9G	DSNDB06

DB2 Tables Reporting Detail Display

```

DB2 tables display
Command ==> █
All DB2 table/view records

Identification
System name                AHJB      complex IDFX
DB2 System identification   DB9G
Database id and name       294 RACFDB2
Schema name                USER01
Table/view id and name     6 GROUP_SUBGROUPS
Table type                 T
Tablesapce name            IRRDBU00
Authid of table owner      BCSCGB1
Owner type (L for role)
Authid of creator          BCSCGB1
Label

Based on
Related schema name
Related table name
Location

Properties                  Statistics
Audit level                Alter timestamp      3Jul12 06:24
Row/column access control  Creation timestamp   3Jul12 06:24
Multi-level security by row

Resource prefix
DB9G.USER01.GROUP_SUBGROUPS
  
```

DB2 Tables Reporting Detail Display

```

DB2 tables display
Command ==> _
DB2 table/view records for tables/views like group_*

Resource prefix
DB9G.USER01.GROUP_SUBGROUPS

Class Resource name
_ MAHJTB1 DB9G.USER01.GROUP_SUBGROUPS.SELECT
_ MAHJTB1 DB9G.USER01.GROUP_SUBGROUPS.UPDATE
_ MAHJTB1 DB9G.USER01.GROUP_SUBGROUPS.INSERT
_ MAHJTB1 DB9G.USER01.GROUP_SUBGROUPS.ALTER
_ MAHJTB1 DB9G.USER01.GROUP_SUBGROUPS.DELETE
_ MAHJTB1 DB9G.USER01.GROUP_SUBGROUPS.REFERENCES
_ MAHJTB1 DB9G.USER01.GROUP_SUBGROUPS.TRIGGER

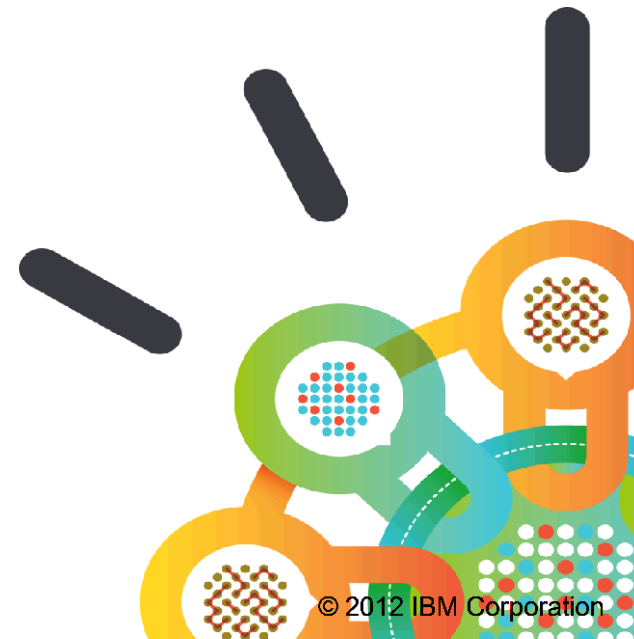
Userid SUIADRT Grantee>>LastGranted H L Grantor
-role- s..... REALLYLONGROLENAME 12Jul12 13:03:00 BCSCGB1
-authid- s..... CONNECTINFOCONSTRAINT 12Jul12 03:13:14 BCSCGB1
BCSCGB1 SUIADRT BCSCGB1 3Jul12 06:24:26 BCSCGB1

Userid SUIADRT Id
-other- SUIADRT -uacc-
BCSCGB2 SUIADRT BCSCGB2

***** Bottom

```

Compliance Reporting





Compliance reporting

- Automate reporting about security settings
- Match against external standard
- Combine information from multiple NEWLISTS
- Allow exceptions to the rule
- Report percentage of reaching target
- Example:
 - APF data sets should only allow UPDATE by system programming group
 - Need info from Newlist Type=Sensdsn, R_Sensitive and RACF_Access
 - With 100s of data sets, want to report e.g. 99%

Provide Compliance Testing Framework

- Use a meta-newlist to report about records in other newlists.
- STANDARD Statement
 - Defines the standards, and the rules
 - Intended to be provided in fixed external members
- Newlist type=compliance
 - Shows the results
- SUPPRESS Statement
 - Installation specific (temporary) exclusions
- Provides a framework for adding standards and tests.
- No standards and compliance tests are yet provided.



Sample policy: APF data set protection

standard Demo version(0.1)

```
domain APFlib select(sensdsn(apf=yes) r_sensitive racf_access)
```

```
rule APFprofile domain(APFlib) desc("APF access+auditing")
```

```
test uacc          r_sensitive(uacc<update)
```

```
test successAudit  r_sensitive(audits=update)
```

```
test failureAudit  r_sensitive(auditf=read)
```

```
endrule
```

```
rule APFupdate domain(APFlib) desc("APF access"),
```

```
  exempt(racf_access(id=sys*))
```

```
test updateAccess racf_access(access>=update) noncompliant
```

```
test readAccess   racf_access(access<update)
```

```
endrule
```

```
endstandard
```

Sample report: APF data set protection

newlist type=compliance

summary standard(8) * domain(8) * rule(16) * test(16),

test_compliant(freq),

test_noncompliant(freq)

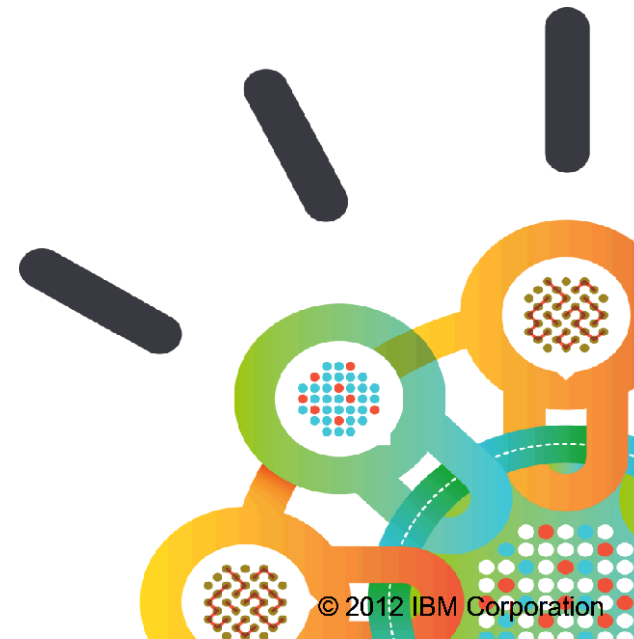
Standard	Domain	n	Rule	Test name	Cmp	Non
Demo					43	56
	APFlib				43	56
			APFprofile		65	34
				failureAudit	100	0
				successAudit	0	100
				uacc	97	2
			APFupdate		38	61
				readAccess	38	61
				updateAccess	38	61

Sample report: APF data set protection

```
newlist type=compliance
define rcount("Profiles",8) sumcount
summary standard(8) * domain(8) * rule(16) * test(16),
test_compliant,
test_noncompliant(freq),
count(np),
rcount(np) * resource(nd)
```

Domain	n	Rule	Test name	Cmp	Non	Count	Profiles
					56		
APFlib					56		
		APFprofile			34		
			failureAudit	Yes	0	134	134
			successAudit	No	100	134	134
			uacc	No	100	4	4
			uacc	Yes	0	130	130
		APFupdate			61		
			readAccess	No	100	484	134
			readAccess	Yes	0	301	131
			updateAccess	No	100	484	134
			updateAccess	Yes	0	301	131

zSecure Command Verifier

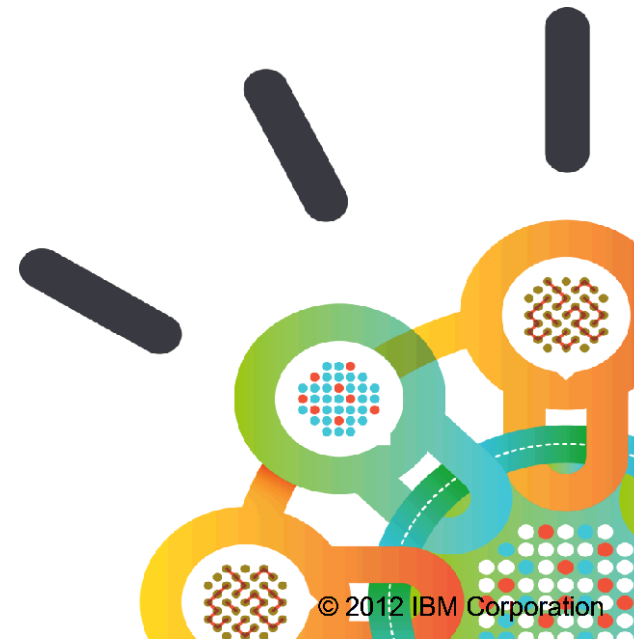


Command Verifier

- Universal groups don't keep track of connected users
 - Possible to DELGROUP the group, even with users still being connected.
 - Result might be many “connection errors”
 - Always use zSecure Admin to delete groups
- New GROUP policy
C4R.GROUP.DELETE.=UNIVERSAL
- Only authorized users can delete a universal group

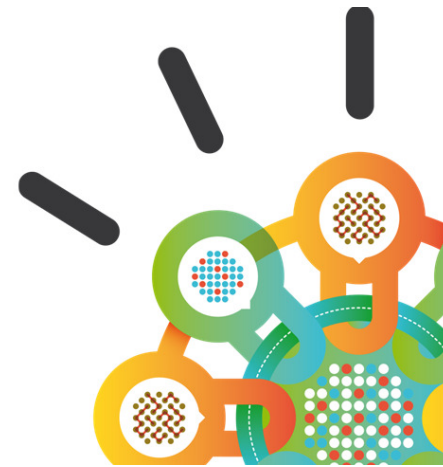


zSecure Manager for RACF z/VM 1.11.1



zSecure Manager for RACF z/VM 1.11.1 – Themes

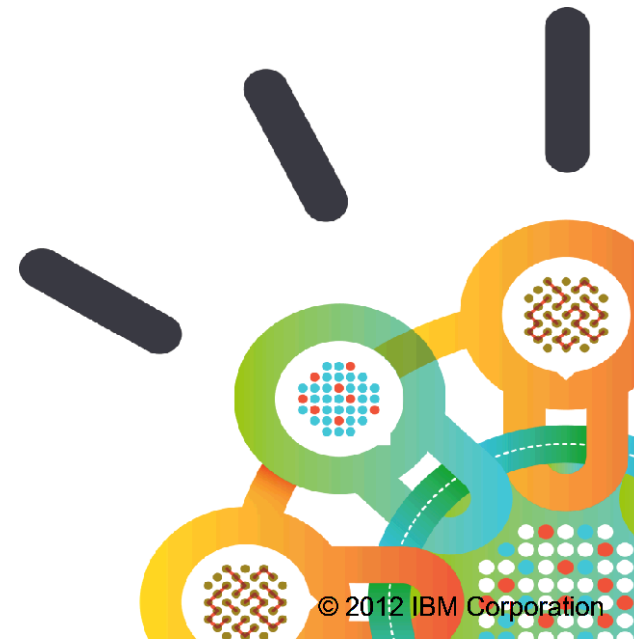
- Support for active RACF database, and active SMF data access
- z/VM resource collection
- z/VM V6R2 support and exploitation
- Compare interface
- User Interface improvements
- and more...



© 2012 IBM Corporation



Active RACF database and SMF





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)

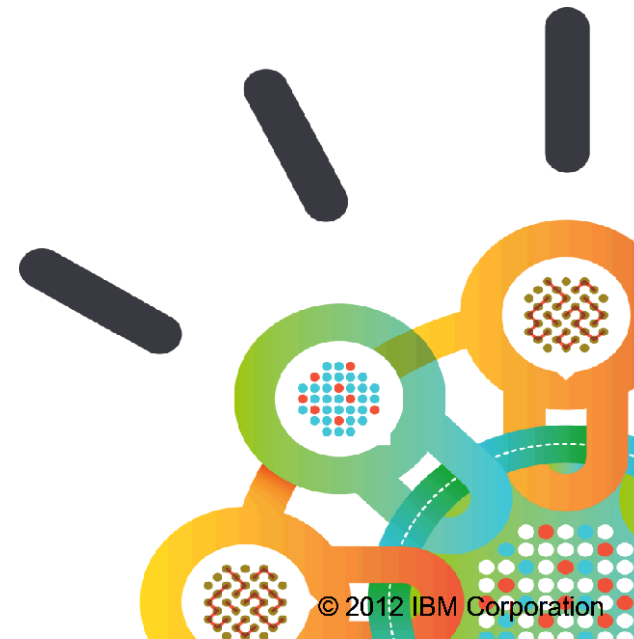
Description                                Complex
_ Default RACF database                      selected
_ VM30V06 CKFREEZE A1                       selected
_ Active backup RACF data base
_ Active backup RACF data base and live SMF data sets
_ Active primary RACF data base
***** BOTTOM OF DATA *****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

➤ 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
```

z/VM resource collection





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 CKFFREEZE
 - ✓ Include RACF access data:
 - ✓ VMMDISK resource,
 - ✓ VMMDISK profile, and
 - ✓ RACF ACL
 - ✓ Include GLBLDSK info from HCPRWA (z/VM 6.2)

New newlists: VM_MDISK

(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.M:

```

zSecure Suite - VM - Minidisks Selection
Command ==> _____

Show minidisks that fit all of the following criteria:
Userid . . . . . (userid or filter)
Device number . . . . . (number or filter)
Real device number. . . . . (number or filter)
Real volume . . . . . (volser or filter)
ACIGROUP name . . . . . (name or filter)
Complex . . . . . (complex or filter)
System . . . . . (system or filter)

Advanced selection criteria
_ Minidisk attributes _ Security settings
Show differences
_ ADD _ DEL _ CHG+ _ CHG- _ CHGu _ SAME _ BASE
Output/run options
_ 0. No summary          1. Summarize by user      2. Summarize by volume
_ Output in print format Customize title
Run in background

```

- Specify selection criteria and press Enter

New newlists: VM_MDISK

(4/6)

➤ RE.V.M Advanced selection criteria

✓ Minidisk attributes selection panel

```
Minidisk type . . . . . _ 1. MDISK 2. V-DISK 3. T-DISK 4. FULLPK 5. All
Device type . . . . . _ 1. 3380 2. 3390 3. 9936 4. FB-512 5. All
Device architecture . . . . . _ 1. CKD 2. FBA 3. Both
Access mode . . . . . _ R _ RR _ W _ WR _ M _ MR _ MW
Local to this system . . . . . _ (Y/N)
```

✓ Minidisk security settings selection panel

```
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: < <= > >= = <> ^= )
In HCPRWA GLBLDSK table _ (Y/N)
Read password . . . . . _ Unused _ Set _ All _ AllOrSet
Write password . . . . . _ Unused _ Set _ All _ AllOrSet
Multiwrite password . . . . . _ Unused _ Set _ All _ AllOrSet
```

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_MDISK

(6/6)

✓ This results in a minidisk detail display

```

Minidisk identification
- Virtual machine userid      GNORR      Number of cylinders or blocks      2
Virtual device address      191      Size of minidisk
Volume serial
Real device address      E005      Start of minidisk
Real volume serial      U3U075      Last of minidisk
Minidisk type      MDISK      Device
Access mode      MR      Device
Local to this system      Yes      Access
Complex name      ZSECTEST      ACIGRA
System name      TIUMEM1

Device security settings
UMMDISK resource name      GNORR.191
Type of minidisk sensitivity
Read password protection      AllOrSet Write
Mwrite password protection      Unused In HCPRWA GLBLDSK table      No
RACF universal access      RACF global access
RACF ID * access

Class      Profile
UMMDISK

Pri Audit concern
15 Minidisk not protected by RACF but by unencrypted CP minidisk passwords
***** Bottom of Data *****

```



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

(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            CPOWNERD
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

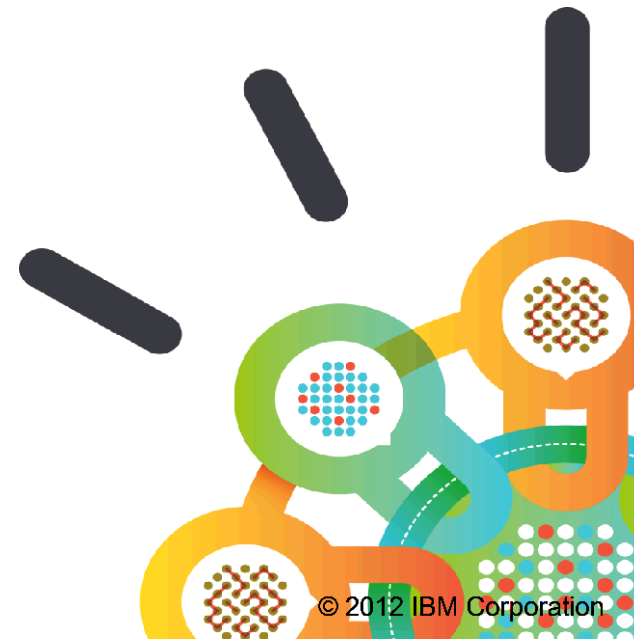
Class    Profile
VMDEV    **

User    Access  ACL id  When
_ IBMUSER  ALTER  IBMUSER

```



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 SYSTEM TERMINAL'
00011 punch 'FILEDEF CKRCMD TERMINAL'
00012 punch 'FILEDEF SYSIN DISK CKR1BTSI SYSIN *'
00013 punch 'FILEDEF CKRCARLA DISK ISPNUL 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

```
zSecure Manager for RACF - Setup - Run

Command ==> _____

Specify run options
Enter "/" to select option(s)
/ Use permanent work data sets (CKRCMD is always permanent)
- Delete permanent work data sets on exit
- Delete CKRCMD on exit (may contain readable passwords)
/ Allocate CKRCMD data set with RECFM=FB,LRECL=80
/ Allocate previous input files at startup
- Suppress warning messages when appropriate input files not selected
- Display of all status messages in sequence (degrades performance)
- Suppress call to RACF naming convention exit ICHCNX00
- Suppress use of RACF naming convention table ICHNCV00
- Suppress use of RACF range table ICHRRNG
- Touch RACF connect owner as little as possible

Suppress messages, enter numbers separated by commas
```

UI – Intermediate 'Action on command' setting

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

```

zSecure Manager for RACF - S      Press PF3 to accept
Command ==> _____
Action on command . . . 1 1. Queue 2. Execute 3. Not allowed
                        - Execute display commands (for option 1 only)
Confirmation . . . . 1 1. None 2. Deletes 3. Passwords 4. All
Command generation
Enter "/" to select option(s)
/ Overtyp e fields in panels
/ Change generated commands
/ Generate SETROPTS REFRESH commands
  / Issue prompt before generating SETROPTS REFRESH commands
Commands to generate
/ RACF commands
  
```

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 _____

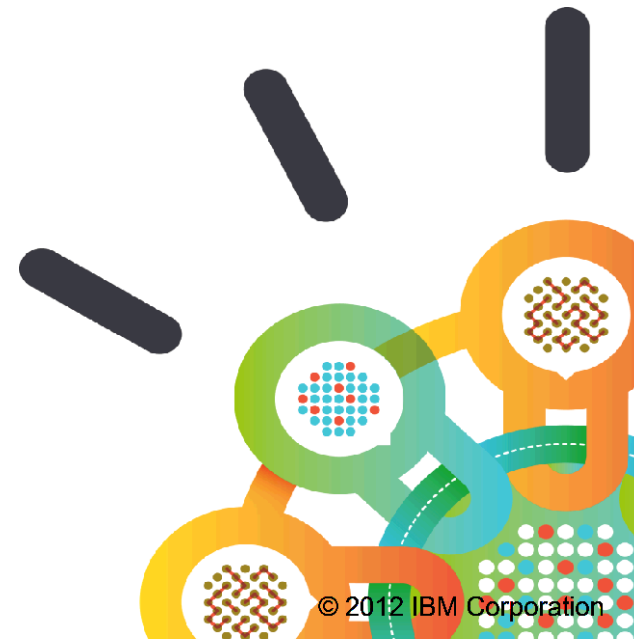
Installation data _____

_ 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
USAMDSET	JOIN	-	-	-	READ	_____	_____	18Jan2012	IBMUSER

Availability information



Availability

- Version 1.13.1 is available from October 26th 2012
 - 5655-T01 IBM Security zSecure Admin 1.13.1
 - 5655-T02 IBM Security zSecure Audit 1.13.1
 - 5655-T09 IBM Security zSecure Visual 1.13.1
 - 5655-T11 IBM Security zSecure Alert 1.13.1
 - 5655-T05 IBM Security zSecure CICS Toolkit 1.13.1
 - 5655-T07 IBM Security zSecure Command Verifier 1.13.1
 - 5655-T15 IBM Tivoli Compliance Insight Manager Enabler for z/OS 1.13.1

- Supported releases are z/OS 1.10 through z/OS 1.13

Availability

- Version 1.11.1 is available since June 15, 2012
 - 5655-T13 IBM Security zSecure Manager for RACF z/VM 1.11.1
- Supported releases are z/VM V5R4 through z/VM V6R2
 - zSecure 1.11.1 no longer provides service for z/VM V5R3



Qradar SIEM Integration

- Built- in with zSecure Audit 1.13.1
- PTF UA66091 for zSecure Audit 1.13.0



zSecure Solution Packages

- IBM Security zSecure Administration
 - IBM Security zSecure Admin
 - IBM Security zSecure Visual
- 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
- IBM Security zSecure Compliance and Administration
 - IBM Security zSecure Administration package
 - IBM Security zSecure Compliance and Auditing package



Reference information

- **zSecure information center**

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_1.13/welcome.html

- **zSecure forum**

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

- **Redbook**

- <http://www.redbooks.ibm.com/abstracts/sg247633.html?Open>

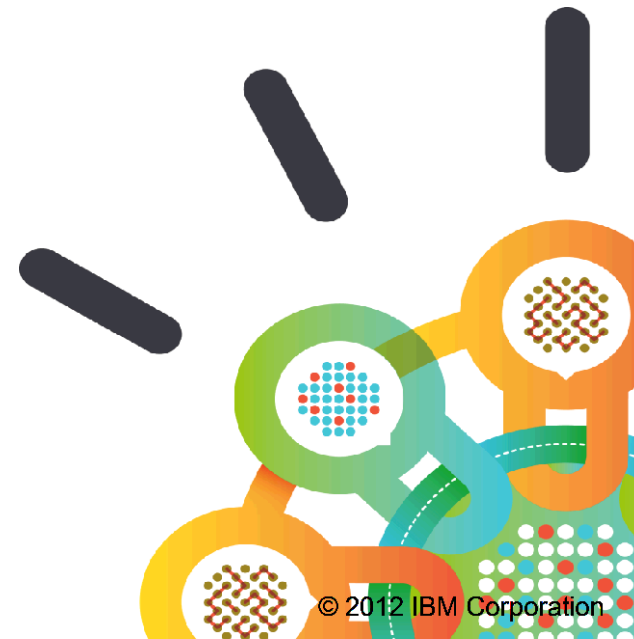
- **Enhancement requests**

http://www.ibm.com/developerworks/rfe/?BRAND_ID=90

- **Education**

http://www-304.ibm.com/jct03001c/services/learning/ites.wss/zz/en?pageType=tp_search_results_new&searchString=zsecure&noOfResultsPerPage=20&rowStart=0

Questions ?



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

© Copyright IBM Corporation 2012. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.