IBM Systems and Technology Group

RAA1

RACF (and z/OS) Security Update for z/OS V1R8 and Friends

Vanguard Security Expo
June, 2007

Walt Farrell, CISSP
z/OS Security Development
IBM Poughkeepsie
wfarrell@us.ibm.com

Trademarks

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

DB2*
e-business logo
IBM*
IBM eServer
IBM logo*
OS/390*
RACF*
z/OS*
Consul Products

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.
UNIX is a registered trademark of The Open Group in the United States and other countries.
SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

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

Notes:

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

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

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

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

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

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

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

Agenda

- **DFSMS Tape Security Enhancements**
- **RACF Support for DB2 Version 9**
- **IRRUT200 and IRRUT400 Enhancements**
- **Enhancements to the RACF Health Checks**
- **Virtual Key Rings**
- **Group Change Logging**
- **Password Phrases**
- **PKI Services Enhancements**

DFSMS Tape Security Enhancements

DFSMS: Tape Security Enhancements

- **Today for tape security, you can use:**
  - TAPEVOL profiles
  - DATASET profiles, with SETROPTS TAPEDSN
  - However, user can specify incorrect data set name unless you use:
    - TVTOC (tape volume table of contents) in TAPEVOL profiles to guarantee user specifies correct data set name
    - Or a tape management system that knows the right data set name
- **Some concerns:**
  - Management of TAPEVOL profiles can add administrative overhead
  - TVTOC processing limits the number of data sets on a tape
  - Users with access to some file based on the data set name may be able to access other files they should not have access to

DFSMS: Tape Security Enhancements

- **z/OS R8 will resolve those concerns, for systems with a compatible tape management system (such as DFSMSrmm)**
- **You can use new system-wide options to specify that:**
  - The system will automatically check security for tape data sets using the DATASET class, even with SETR NOTAPEDSN and with the TAPEVOL class inactive
  - Users must have access to the data on file 1 of a tape (by data set name) before accessing a subsequent file.
- **SYS1.PARMLIB(DEVSUPxx)**
  - TAPEAUTHDSN
  - TAPEAUTHF1
  - TAPEAUTHRC4, TAPEAUTHRC8

RACF Support for DB2 Version 9 (FASTAUTH Enhancements)

Roles and the Network Trusted Context

- **DB2 V9 introduces a new access control mechanism: The ROLE**
  - `CREATE ROLE TELLER`
    - 1 to 128 character value
  - `GRANT SELECT ON TABLE USER01.ABCD TO ROLE TELLER;`
  - Roles can only be used within a **TRUSTED CONTEXT**

Roles and the Network Trusted Context…

- **TRUSTED CONTEXT is a new DB2 V9 construct which allows the assignment of authorization information to a connection.**
- **Example: Assign the role TELLER to any job named MARKN which connects using the authID MARKN:**

```
CREATE TRUSTED CONTEXT CONTEXT_01
       BASED UPON CONNECTION USING SYSTEM AUTHID MARKN
       ATTRIBUTES (JOBNAME 'MARKN')
       DEFAULT ROLE TELLER
       ENABLE;
```

Network Trusted Context

- **Example: Assign the role TELLER to a connection established from IP address 9.12.20.152 and the auth ID SRVR001**

```
CREATE TRUSTED CONTEXT CONTEXT_02
       BASED UPON CONNECTION USING SYSTEM AUTHID SRVR001
       ATTRIBUTES (ADDRESS '9.12.20.152')
       DEFAULT ROLE TELLER
       ENABLE
```

Network Trusted Context…

- **When DB2's native authorization mechanisms are used, RACF is completely uninvolved in the access control decision**
- **When RACF is used to control access to DB2 objects…**
  - DB2 V9 passes the ROLE name to DSNXRXAC
  - DSNXRXAC passes the ROLE name to RACF on a REQUEST=FASTAUTH
  - Access can be allowed if the ROLE was specified on a PERMIT command

Changes to REQUEST=FASTAUTH

- **RACROUTE REQUEST=FASTAUTH has been enhanced to accept the specification of a CRITERIA**
  - CRITERIA= causes FASTAUTH to check a new conditional access list entry
  - There are two parts to the criteria specification:
    - The CRITERIA name
      - For DB2, the CRITERIA name is SQLROLE
    - The CRITERIA value
      - For DB2, this is the ROLE that is associated with the thread

Changes to REQUEST=FASTAUTH…

- **The new AUTHCHKS= parameter on REQUEST=FASTAUTH allows an application to tell FASTAUTH to use *only* the CRITERIA for an authorization request**
  - **AUTHCHKS=CRITONLY** causes FASTAUTH to ignore UACC and standard access list. Mandatory access checks are performed.
  - **AUTHCHKS=ALL** is the default

Changes to REQUEST=FASTAUTH…

- **Example: A REQUEST=FASTAUTH with a ROLE**

```
RACROUTE REQUEST=FASTAUTH,
        WORKA=RACROUTE_worka,
        REQSTOR=XAC,
        SUBSYS=XAPLGPAT,
        DECOUPL=YES,
        WKAREA=FAST_wkarea,
        ENTITYX=FAST_ENTX,
        CLASS=FAST_CLASS,
        ACEE=(R4),
        ACEEALET=(R5),
        ATTR=(R8),
        LOG=NOFAIL,
        MSGSUPP=NO,
        LOGSTR=LOGSTR,
        CRITERIA=FAST_CRITERIA_COUNT,
        AUTHCHKS=CRITONLY,
        RELEASE=7730,
        MF=(E,FASTD)
*       . . .
*       . . .
FAST_CRITERIA_COUNT   DC F'1'
                      DC CL8'SQLROLE '
                      DC F'6'
                      DC CL128'TELLER'
```

Changes to the PERMIT Command

- **CRITERIA are specified on the RACF PERMIT in the conditional access list**
  - `PERMIT DSND.SYSADM CL(DSNADM) ID(MARKN)`
    `WHEN(CRITERIA(SQLROLE(TELLER)))`

IRRUT200 and IRRUT400 Enhancements

RACF: IRRUT200 and IRRUT400 enhancements

Problem 1: When copying from primary into backup to resynchronize them you can lose updates:

- (1) IRRUT200 to copy from active primary to inactive backup;
- (2) some update happens (only to primary)
- (3) Use RVARY to activate the backup.

- **Solution: IRRUT200 now supports a new parameter, PARM=ACTIVATE**
  - If SYSRACF is an active primary, and SYSUT1 is the inactive backup, and PARM=ACTIVATE, then
  - IRRUT200 will issue an internal RVARY ACTIVE before it releases its database serialization.
  - Result: no updates can occur before the RVARY completes, and the backup and primary remain synchronized.

RACF: IRRUT200 and IRRUT400 enhancements

- **Problem 2: Database corruption will occur if**
  - You use IRRUT200 or IRRUT400 with input DD and output DD pointing to same data set
  - You use IRRUT200 or IRRUT400 to copy into an active RACF data set
- **Solution: Both utilities will now detect these conditions and terminate before performing the copy operation.**

- **Available as APAR OA14916 for z/OS R7.**

Enhancements to RACF's Health Checks

The RACF Health Checks

- **The RACF Health Checks examine key system resources and verify that:**
  - RACF's serialization requests are not altered by global resource serialization (GRS) resource name lists (RNLs)
    - RACF_GRS_RNL check
  - **Key system resources have a proper baseline set of protections**
    - RACF_SENSITIVE_RESOURCES check
- **With z/OS V1R8, the existing RACF checks are enhanced and seven new checks are added.**

What's New?

- **With z/OS V1R8, these checks are new:**
  - **RACF_IBMUSER_REVOKED**
    - Verifies that the user ID IBMUSER is revoked
    - Defaults: Severity(Medium), Interval (24:00)
  - **RACF_<class-name>_ACTIVE**
    - Verifies that the class <class-name> is active
      - Check is performed for FACILITY, OPERCMDS, TAPEVOL, TEMPDSN, TSOAUTH, UNIXPRIV
    - Defaults: Severity(Medium), Interval(24:00)

What's New? …

- **With z/OS V1R8, these checks have been modified:**
  - **The RACF_SENSITIVE_RESOURCES now:**
    - Reports on PARMLIB and LINKLIST datatsets
    - Reports on key sensitive general resources
  - **The RACF_GRS_RNL check honors the Health Checker "verbose" mode in addition to "debug" mode**
    - Running the RACF_GRS_RNL check in either verbose mode or debug mode causes it to list all of the ENQ names that it is validating.

RACF_FACILITY_ACTIVE Successful Execution Output

```
CHECK(IBMRACF,RACF_FACILITY_ACTIVE)
START TIME: 03/02/2006 14:50:57.305795
CHECK DATE: 20051111  CHECK SEVERITY: MEDIUM
CHECK PARM: FACILITY


IRRH228I The class FACILITY is active.

END TIME: 03/02/2006 14:50:57.314865  STATUS: SUCCESSFUL
```

RACF_UNIXPRIV_ACTIVE Exception Output

```
CHECK(IBMRACF,RACF_UNIXPRIV_ACTIVE)
START TIME: 03/02/2006 14:50:57.304859
CHECK DATE: 20051111  CHECK SEVERITY: MEDIUM
CHECK PARM: UNIXPRIV


* Medium Severity Exception *

IRRH229E The class UNIXPRIV is not active.

  Explanation:  The class is not active. IBM recommends that the
    security administrator at your installation activate this class and
    define in it the profiles to properly protect your system.

  System Action:  The check continues processing. There is no effect on
    the system.
```

RACF_SENSITIVE_RESOURCES New Output

Current Link List Dataset Report

S	Data Set Name	Vol	UACC	Warn	ID*	User
E	ASM.SASMMOD1	ZDR18				
E	ATC.V2R1M4.SATGBMOD	D94RF1				
E	RACF318.LINKLIB	D97107				
E	RACF318.MIGLIB	D97107				
	SYS1.CMDLIB	ZDR18	None	No	****	
	SYS1.CSSLIB	ZDR18	None	No	****	
	SYS1.DFQLLIB	ZDR18	None	No	****	
	SYS1.DGTLLIB	ZDR18	None	No	****	
	SYS1.LINKLIB	ZDR18	None	No	****	
	SYS1.MIGLIB	ZDR18	None	No	***	

RACF_SENSITIVE_RESOURCES New Output

Sensitive General Resources Report

S	Resource Name	Class	UACC	Warn	ID*	User
	BPX.DAEMON	FACILITY	None	No	****	
	BPX.FILEATTR.APF	FACILITY	None	No	****	
	BPX.SERVER	FACILITY	None	No	****	
	BPX.SUPERUSER	FACILITY	None	No	****	
	ICHBLP	FACILITY	None	No	****	
	IRR.PASSWORD.RESET	FACILITY				
	MVS.SET.PROG	OPERCMDS				
	MVS.SETPROG	OPERCMDS				
E	ACCT	TSOAUTH	Updt	No	****	
E	CONSOLE	TSOAUTH	None	Yes	****	
E	OPER	TSOAUTH	None	No	Updt	
E	PARMLIB	TSOAUTH	None	No	Read	
E	TESTAUTH	TSOAUTH	None	No	Read	
	SUPERUSER.FILESYS	UNIXPRIV				
	SUPERUSER.FILESYS.CHANGEPERMS	UNIXPRIV				
	SUPERUSER.FILESYS.CHOWN	UNIXPRIV				

Rollback

- **These checks have been rolled back to z/OS V1R6 with APAR OA16514**
  - V1R6 PTF: UA29221
  - V1R7 PTF: UA29222

References

- **Additional information:**
  - IBM Health Checker for z/OS User's Guide (SA22-7994)
  - z/OS Security Server (RACF) Messages and Code (SA22-7686)
  - "*An Apple a Day Keeps the PMRs Away*", and "*Check, Please*!", z/OS Hot Topics, August 2005, which can be found on the z/OS Hot Topics web site at: http://www.ibm.com/servers/eserver/zseries/zos/bkserv/hot_topics.html

Virtual Key Rings

RACF: Virtual Key Rings

- **Scenario:**
  - z/OS user wants to use FTP to an SSL-enabled FTP server
  - Today each such user must have a certificate key ring containing the certificate of the trusted certifying authority (CA) that signed the server's certificate.
- **Problem: Many users may want to use SSL-based client applications. All will need their own key rings, probably with identical contents, causing extra administration**
- **Solution: Virtual key rings**
  - RACF will treat all the certificates that belong to a user as a key ring, without the administrator having to physically create a ring
  - Especially valuable for the case of certificates "owned" by the CERTAUTH user

Group Change Logging

Overview: Problem and solution

- **z/OS LDAP currently supports the query and update of USER, GROUP, and group connection attributes using the SDBM back end to talk to RACF**
- **RACF currently supports LDAP change logging of updates to USER profiles**
- **Thus, there is a functional gap in RACF change logging with respect to the RACF functions supported by z/OS LDAP**
- **Solution – Support change logging of group and connection updates**

Overview: Problem and Solution …

- **Customer and other feedback for Password Enveloping function revealed a couple of deficiencies**
  - No indication in LISTUSER as to existence of password envelope
  - No change log entry created for a new password which is not enveloped
- **Solution – New line of LISTUSER output, and unconditional change logging of password updates**

Group Change Logging

- **New NOTIFY.LDAP.GROUP resource in RACFEVNT class results in change log entries for:**
  - Additions made using the ADDGROUP command
  - Modifications made using the ALTGROUP command
  - Deletions made using the DELGROUP command

Group Change Logging …

- **New NOTIFY.LDAP.CONNECT resource in RACFEVNT class results in change log entries for:**
  - Additions and modifications made using the CONNECT command
  - Deletions made using the REMOVE command
  - Establishment of the connection of a user to its default group by the ADDUSER command
  - Modifications to a user's connection information using the GROUP, UACC and AUTHORITY operands of the ALTUSER command

R_Proxyserv Callable Service (IRRSPY00)

- **Can be invoked by applications which perform their own profile updates (not using RACF commands) in order to get an LDAP change log entry created**
- **Extended to support group and connect "profiles"**
  - Internal-only change. No change to parameter list.
  - Some documentation tweaked to describe contents of profile name, which is not automatically a user anymore

Password Enveloping Enhancements

- **LISTUSER indicates presence of password envelope when:**
  - RACFEVNT class active and PASSWORD.ENVELOPE profile exists

  OR

  - User has a (residual) envelope
- **Documentation beefed up to describe how to "phase out" enveloping function**
  - Residual envelopes get cleaned out of the RACF database

Password Enveloping Enhancements …

```
USER=ACE   NAME=UNKNOWN   OWNER=WELLIE
CREATED=92.162
DEFAULT-GROUP=KINGS    PASSDATE=00.000 PASS- INTERVAL=N/A PHRASEDATE=N/A
PASSWORD ENVELOPED=NO
ATTRIBUTES=NONE
REVOKE DATE=NONE    RESUME DATE=NONE
LAST-ACCESS=06.044/12:26:08
CLASS AUTHORIZATIONS=NONE
NO-INSTALLATION-DATA
NO-MODEL-NAME
```

Password Enveloping Enhancements …

- **When NOTIFY.LDAP.USER defined, a password change always results in a change log entry**
  - When enveloped, existing behavior continues
    - "*ComeAndGetIt*" string in 'changes' attribute
  - When not enveloped
    - "*NoEnvelope*" string in 'changes' attribute
- **Password may not be enveloped because**
  - User not eligible for enveloping
  - Password contains invalid characters
  - Enveloping operation failed due to error

Password Phrases

RACF Password Phrases

- **RACF will allow you to specify a password phrase for a user:**
  - 14 to 100 characters in length
  - Mixed-case, including alphabetic, numeric, and a large selection of special characters including blanks
  - Basic syntax rules: user ID can not appear in phrase; must contain at least two alphabetic and at least two non-alphabetic characters; must not contain more than two consecutive identical characters.
- **Can provide better interoperability with other systems that allow longer passwords**
- **Can provide better security than 8-character passwords**
- **Requires changes in applications that support passwords and want to support phrases**
  - TSO/E, z/OS UNIX System Services, IMS, CICS, etc. will require changes
  - Changes will occur over time. Not in z/OS R8 for IBM applications.
- **Users can have both a password phrase and a password**
  - **Will probably need both until all applications they use support phrases**

Some externals you will see

- **PHRASE operand on ADDUSER/ALTUSER. NOPHRASE on ALTUSER**
- **ATTRIBUTES=PASSPHRASE on LISTUSER**
- **SETROPTS PASSWORD options which apply to phrases**
  - INTERVAL
  - REVOKE
  - HISTORY
  - MINCHANGE

Some externals you will see …

- **New RACROUTE REQUEST=VERIFY/X keywords**
  - PHRASE=
  - NEWPHRASE=
- **New Password Phrase exit – ICHPWX11**
- **YES/NO field in IRRDBU00 output indicates presence of password phrase for user**
- **New ICH408I message texts for failed phrases**
- **New event code qualifiers for RACINIT/JOBINIT SMF record**

PKI Services Enhancements

PKI Services: Multiple Certificate Authority (CA) Support

- **Today:**
  - You can run only one instance of PKI Services daemon on a z/OS image
  - That single PKI Services daemon can act as (operate as) only a single certificate authority
- **This makes it difficult to**
  - Operate a certificate authority hierarchy
  - Host multiple certificate authorities as a service bureau
- **z/OS R8: You can run multiple PKI Services daemons on one z/OS system**
  - Each can operate as a different CA to resolve the above difficulties

PKI Services: SCEP Support

- **Certificates are used by humans today, but increasingly also used by hardware (routers, VPN devices, etc.)**
- **Today, PKI Services accepts requests only via a web page**
  - Leads to much manual work to get certificates for devices
- **z/OS R8: PKI Services will accept requests via the Simple Certificate Enrollment Protocol (SCEP) directly from the devices, reducing the need for manual administrative actions**

z/OS V1R9 RACF Update

RACF V1R9

- Password phrase support
  - 9-14 character gap allowed
- Extend encryption for Kerberos
  - AES will be supported
- Java interfaces
  - Allow administration and querying of users and groups via API

RACF V1R9

- PKI Updates
  - Writable SAF Key rings – population of certificates programatically
  - 2 byte UTF8 character support in certificates
  - Additional certificate notification and query support

RACF for z/VM Update

What's in a Name?

- **RACF Security Server feature Function Level 530 (FL530) for z/VM V5.3**

- Mixed case passwords
  - SETROPTS command used to enable mixed case, and to define expanded password quality rules
- Password phrase support
  - 9-100 character authenticator with few character restrictions
  - Immediate support for LOGON, FTP, TELNET
  - Sample exit uses REXX for quality rules
  - Can force use of password phrases by deleting passwords
  - Existing SETROPTS PASSWORD options apply to phrases
    - HISTORY, REVOKE, INTERVAL, WARNING

RACF for z/VM 5.3 …

- Support for (new) z/VM LDAP server
  - Query, update RACF user and group profiles via SDBM backend
  - Clients (e.g.Linux) can authenticate to LDAP using RACF password
  - Remote authorization and auditing services
  - Logging of LDAP server events in SMF DATA file
- SMF Unload utility (RACFADU) updated
  - Support for LDAP server and client auditing
  - Output available in XML format

RACF for z/VM 5.3 …

- Support for (new) CP FOR command
  - Allows user to run a command under another user's authority
  - Requires LOGON BY (SURROGAT class) authority
- Support for new subcodes of DIAGNOSE X'88'
  - Allows a server to validate a client's password or phrase
    - Server must have VMCMD class authority
  - Can check for client LOGON BY authority to a target
- Various user-related improvements
  - NOPASSWORD users, NOEXPIRED keyword, improved audit of password changes, ALTUSER adds current password to history

Consul

Additional Tools to support RACF database administration and analysis

- zAdmin
  - ISPF-based interface for managing the RACF database
- zAudit
  - ISPF-based interface for analyzing the RACF database and monitoring mainframe security
- zAlert
  - Watches mainframe security events and alerts administrators of suspicious activity
- zLock
  - Allows for more granular permission settings around which administrators can perform which RACF commands

Questions ?