




IBM Systems and Technology Group

RACF Update

Session RTA1
Vanguard Security Expo
June, 2008

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

© 2008 IBM Corporation



IBM Systems and Technology Group

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*
- Consult 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 multiprocessing in the user's job stream, the I/O 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.

© 2008 IBM Corporation

2

IBM Systems and Technology Group 

Agenda

z/OS V1R8 RACF Update

- RACF Support for DB2 Version 9
- IRRUT200 and IRRUT400 Enhancements
- Enhancements to the RACF Health Checks
- Virtual Key Rings
- Group Change Logging
- Password Phrases
- Remote Authorization and Audit (EIM)
- PKI Services Enhancements


z/OS V1R9 RACF Update

- Password Phrase enhancement
- Kerberos AES support
- Java RACF User and Group administration interface
- Writable SAF Keyring support
- PKI Updates

z/OS V1R10 RACF Preview


RACF for z/VM Update

© 2008 IBM Corporation 3

IBM Systems and Technology Group 

**RACF Support for DB2 Version 9
(FASTAUTH Enhancements)**


© 2008 IBM Corporation 4

IBM Systems and Technology Group 

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**

© 2008 IBM Corporation 5

IBM Systems and Technology Group 

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;
```

© 2008 IBM Corporation 6

IBM Systems and Technology Group

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
```

© 2008 IBM Corporation 7

IBM Systems and Technology Group

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

© 2008 IBM Corporation 8

IBM Systems and Technology Group

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

© 2008 IBM Corporation 9

IBM Systems and Technology Group

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

© 2008 IBM Corporation 10

IBM Systems and Technology Group

Changes to REQUEST=FASTAUTH...

- Example: A REQUEST=FASTAUTH with a ROLE

```

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

```

© 2008 IBM Corporation 11

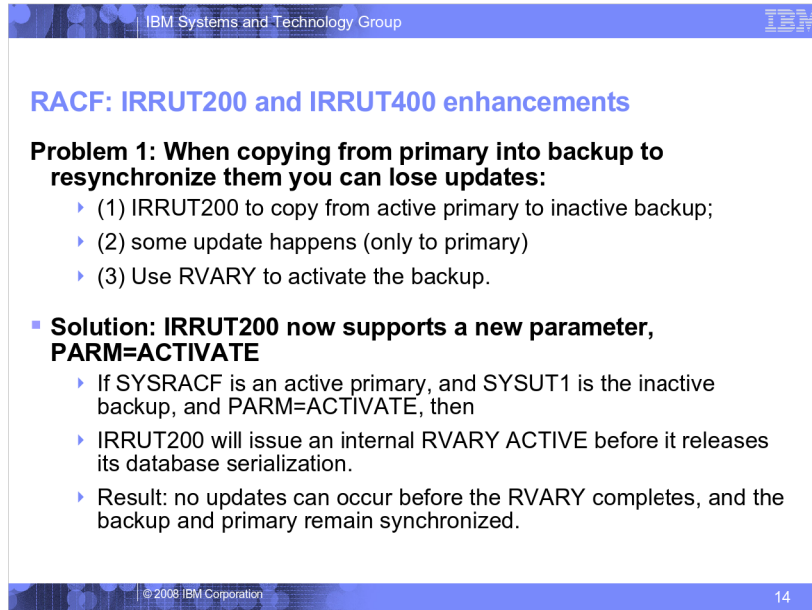
IBM Systems and Technology Group

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)))

© 2008 IBM Corporation 12



IBM Systems and Technology Group

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.**

© 2008 IBM Corporation 15

IBM Systems and Technology Group

Enhancements to RACF's Health Checks


© 2008 IBM Corporation 16

IBM Systems and Technology Group 

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.**

© 2008 IBM Corporation 17

IBM Systems and Technology Group 

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)

© 2008 IBM Corporation 18

IBM Systems and Technology Group

What's New? ...

- With z/OS V1R8, these checks have been modified:
 - The **RACF_SENSITIVE_RESOURCES** now:
 - Reports on PARMLIB and LINKLIST datasets
 - 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.

© 2008 IBM Corporation 19

IBM Systems and Technology Group

RACF_FACILITY_ACTIVE Successful Execution Output

```
CHECK(IBMRA CF,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
```

© 2008 IBM Corporation 20

IBM Systems and Technology Group

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.

© 2008 IBM Corporation 21

IBM Systems and Technology Group

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.DGTLIB	ZDR18	None	No	****	
SYS1.LINKLIB	ZDR18	None	No	****	
SYS1.MIGLIB	ZDR18	None	No	***	

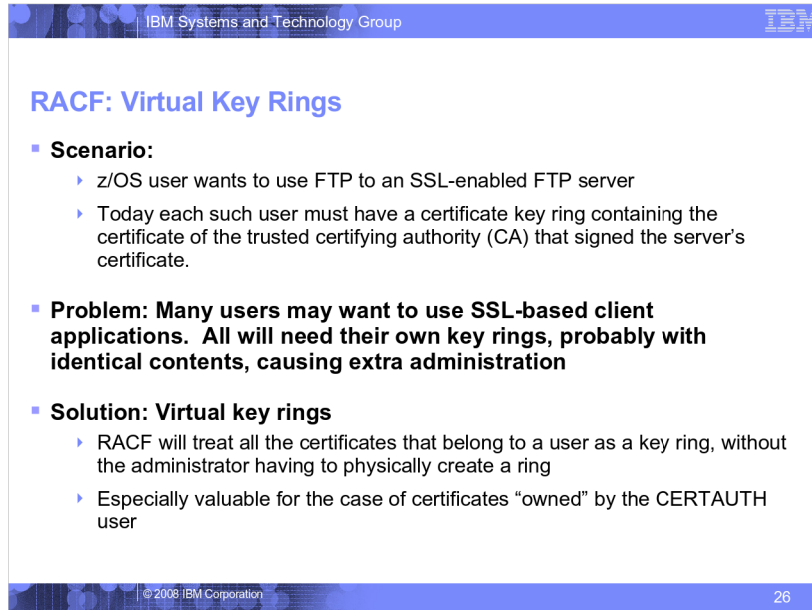
© 2008 IBM Corporation 22

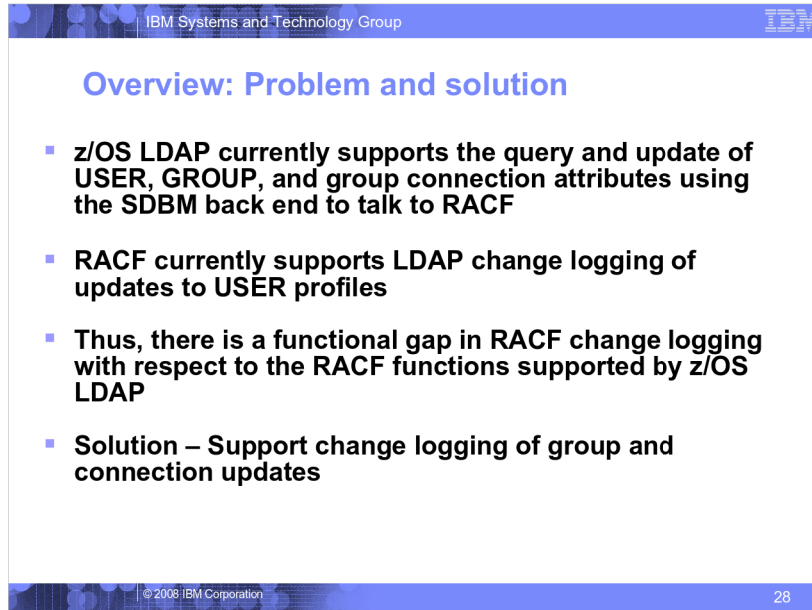
IBM Systems and Technology Group					
RACF_SENSITIVE_RESOURCES New Output					
Sensitive General Resources Report					
S	Resource Name	Class	UACC	Warn	ID* User
	BPX.DAEMON	FACILITY	None	No	****
	BPX.FILEATTR.APF	FACILITY	None	No	****
	BPX.SERVER	FACILITY	None	No	****
	BPX.SUPERUSER	FACILITY	None	No	****
	ICHLPL	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			


© 2008 IBM Corporation 23

IBM Systems and Technology Group					
Rollback					
<ul style="list-style-type: none"> ▪ These checks have been rolled back to z/OS V1R6 with APAR OA16514 <ul style="list-style-type: none"> • V1R6 PTF: UA29221 • V1R7 PTF: UA29222 					

© 2008 IBM Corporation 24






IBM Systems and Technology Group 

Overview: Problem and Solution ...

- **Customer and other feedback for Password Enveloping function revealed some 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**

© 2008 IBM Corporation 29

IBM Systems and Technology Group 

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

© 2008 IBM Corporation 30

IBM Systems and Technology Group

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

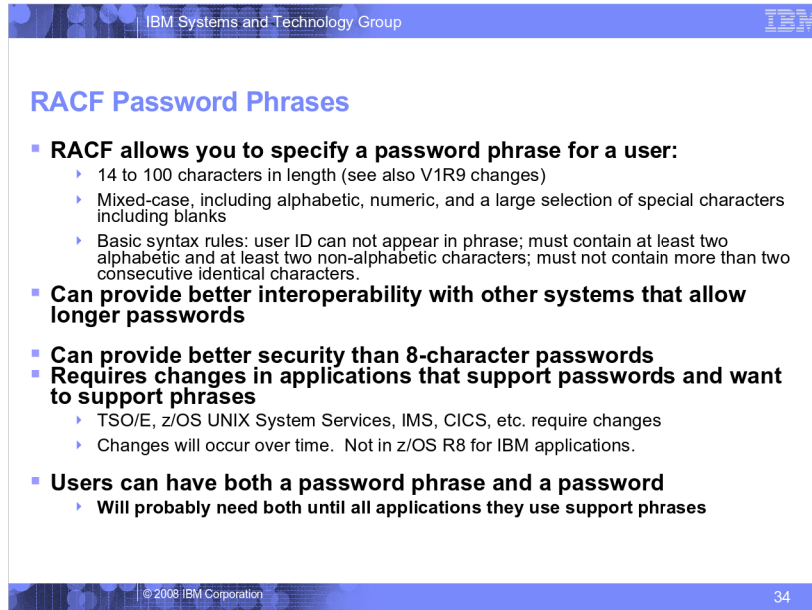
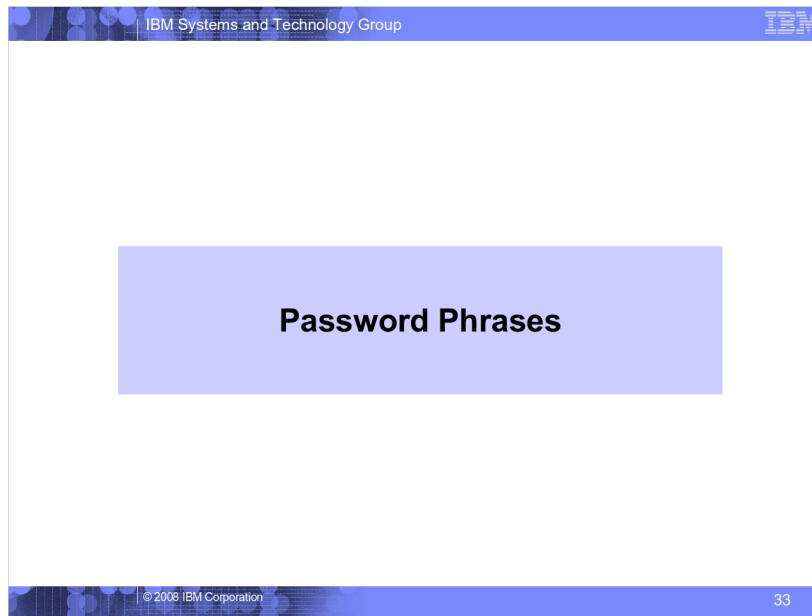
© 2008 IBM Corporation 31

IBM Systems and Technology Group

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
```

© 2008 IBM Corporation 32



IBM Systems and Technology Group

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

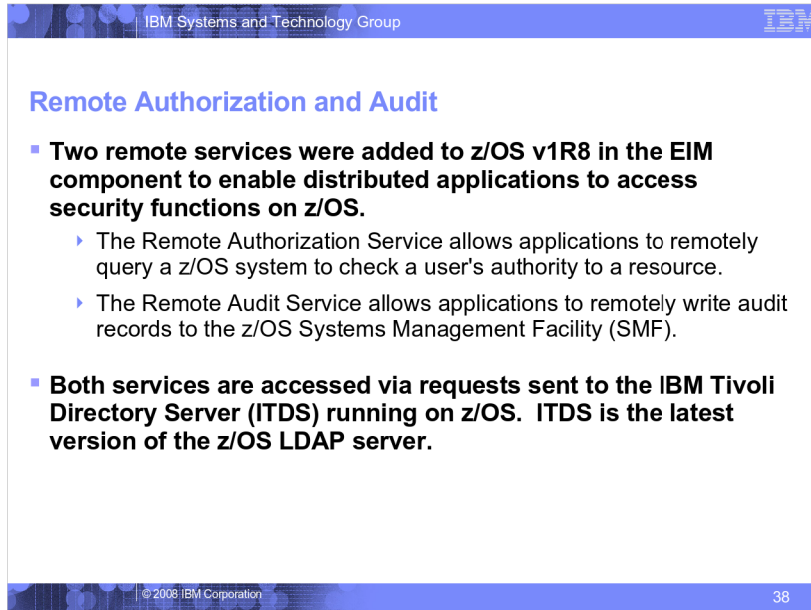
© 2008 IBM Corporation 35

IBM Systems and Technology Group

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**

© 2008 IBM Corporation 36



IBM Systems and Technology Group

Remote Authorization and Audit

- **The Remote Authorization service can be thought of as a remote interface to the RACROUTE REQUEST=AUTH service.**
- **The Remote Audit service can be thought of as a remote interface to the R_AUDITX SAF callable service.**

For more information, see:
z/OS Integrated Security Services Enterprise Identity Mapping (EIM) Guide and Reference

© 2008 IBM Corporation 39

IBM Systems and Technology Group

PKI Services Enhancements

© 2008 IBM Corporation 40

IBM Systems and Technology Group

PKI Services: Multiple Certificate Authority (CA) Support

- **Before z/OS V1R8:**
 - You could run only one instance of PKI Services daemon on a z/OS image
 - That single PKI Services daemon could act as (operate as) only a single certificate authority
- **This made it difficult to**
 - Operate a certificate authority hierarchy
 - Host multiple certificate authorities as a service bureau
- **z/OS V1R8: You can run multiple PKI Services daemons on one z/OS system**
 - Each can operate as a different CA to resolve the above difficulties

© 2008 IBM Corporation 41

IBM Systems and Technology Group

PKI Services: SCEP Support


- **Certificates are used by humans today, but increasingly also used by hardware (routers, VPN devices, etc.)**
- **Before z/OS V1R8, PKI Services accepted requests only via a web page**
 - Required too much manual work to get certificates for devices
- **z/OS V1R8: PKI Services can accept requests via the Simple Certificate Enrollment Protocol (SCEP) directly from the devices, reducing the need for manual administrative actions**

© 2008 IBM Corporation 42

IBM Systems and Technology Group 

z/OS V1R9 RACF Update

© 2008 IBM Corporation 43

IBM Systems and Technology Group 

Password Phrase Enhancement

© 2008 IBM Corporation 44

IBM Systems and Technology Group

Password Phrase Support Enhancements


- **With z/OS V1R8, password phrases could be from 14-100 characters in length. There was no support for a password or password phrase from 9 to 13 characters in length**
 - This presents an interoperability issue with some other platforms
- **With z/OS V1R9, password phrases from 9 to 13 characters are allowed only if an ICHPWX11 password phrase exit is coded which accepts the shorter phrase.**
 - If ICHPWX11 is not present at all, the minimum acceptable password phrase length remains 14.
- **A sample ICHPWX11 exit is provided which is coded to utilize the System REXX facility.**

© 2008 IBM Corporation 45

IBM Systems and Technology Group

Kerberos AES support

© 2008 IBM Corporation 46

IBM Systems and Technology Group 

Kerberos support


- **z/OS's Kerberos has been extended to support the AES encryption algorithm.**
 - z/OS Kerberos interoperability with other implementations improved.
- **These functions are designed to support RFC3962**
Advanced Encryption Standard (AES) Encryption for Kerberos 5

© 2008 IBM Corporation 47

IBM Systems and Technology Group 

**Java RACF user and group
administration interface**

© 2008 IBM Corporation 48

IBM Systems and Technology Group 

Java RACF User and Group administration interface


- **New Java interfaces**
 - Allow administration and querying of users, groups and user-group connection information via JAVA API calls.
 - These APIs internally call the z/OS LDAP (ISS or ITDS) server to perform the functions.
 - This makes these APIs callable from applications running on or off the z/OS platform.

© 2008 IBM Corporation 49

IBM Systems and Technology Group 

Writable SAF keyring and certificate support

© 2008 IBM Corporation 50

IBM Systems and Technology Group 

Writable SAF Keyring and Certificate support

- **R_datalib SAF callable services updated to allow programs to perform additional certificate functions.**
 - Keyrings may now be created and deleted
 - Certificates can be added and deleted to RACF
 - Certificates can be added and deleted from keyrings
- **Prior to this support, the only way to perform these functions was via the RACF RACDCERT TSO command.**

© 2008 IBM Corporation 51

IBM Systems and Technology Group 



PKI updates

© 2008 IBM Corporation 52

IBM Systems and Technology Group

PKI updates

- **PKI Updates**
 - ▶ Certificates containing 2-byte UTF-8 characters which can be mapped to code page 1047 characters are supported.
 - ▶ The use of SDBM credential for the LDAP administrator in PKI Services will be allowed.
 - ▶ The maximum limit of the certificate validity period will be changed from 3650 days (10 years) to 9999 days (approx. 27 years).
 - ▶ Automated certificate renewal will be designed to send renewal certificates via e-mail when the expiration dates for older certificates are approaching.
 - ▶ New e-mail notification for the PKI administrator will be provided for pending certificate requests.

© 2008 IBM Corporation 53

IBM Systems and Technology Group

Coming Soon

z/OS V1R10 RACF Preview

© 2008 IBM Corporation 54

IBM Systems and Technology Group

Planned for V1R10: Password Phrase Exploitation

- Password Phrase exploitation
 - TSO/E
 - z/OS UNIX rlogin, BPX1PWD, BPX1SEC, BPX1TLS
 - z/OS UNIX su & passwd commands
 - z/OS Kerberos
 - z/OS LDAP for z/OS SDBM backend
 - Password Phrase search
 - Password Phrase change logging
 - OpenSSH (IBM Ported Tools for z/OS)

© 2008 IBM Corporation 55

IBM Systems and Technology Group

Planned for V1R10: Password Reset Enhancements

- More granularity in allowing password reset
 - Can be scoped by OWNER or Group Tree
- Before V1R10: FACILITY profile IRR.PASSWORD.RESET allowed password resets for users without SPECIAL/AUDITOR/OPERATIONS or PROTECTED
 - READ authority: can set an expired password or resume user
 - UPDATE: can also set a non-expired password
 - CONTROL: can also reset password within MINCHANGE window

© 2008 IBM Corporation 56

IBM Systems and Technology Group

Planned for V1R10: Password Reset Enhancements ...

- V1R10: New FACILITY profiles:
 - IRR.PWRESET.OWNER.owner-of-user
 - Grants authority based on the user or group that owns the user
 - IRR.PWRESET.TREE.owner-of-group-tree
 - Grants authority based on group tree scope
 - That is, if “owner of group tree” owns the user being reset, or owns a group that owns the user, or owns a group that owns a group that ...
- Authorities to these work the same as for IRR.PASSWORD.RESET:
 - READ authority: can set an expired password or resume user
 - UPDATE: can also set a non-expired password
 - CONTROL: can also reset passwords within MINCHANGE window

© 2008 IBM Corporation 57

IBM Systems and Technology Group

Planned for V1R10: Custom Fields

- RACF will allow administrators to define new fields in USER and GROUP profiles
 - New fields can be used in:
 - RACF commands
 - RACF ISPF panels
 - LDAP SDBM
- Profiles in CFIELD class define the field names and allowable data format
- USER and GROUP profiles have a new CSDATA segment to hold the new fields
- Profiles in FIELD class determine who can view or modify the new data, as for other segments

© 2008 IBM Corporation 58

IBM Systems and Technology Group

Planned for V1R10: Custom Fields ...

- Example 1:
 - RDEFINE CFIELD USER.CSDATA.EMPSER UACC(NONE) +
CFDEF(TYPE(NUM) FIRST(NUMERIC) OTHER(NUMERIC) +
MAXLENGTH(8) MINVALUE(100000) MAXVALUE(99999999) +
HELP('EMPLOYEE SERIAL NUMBER, 6-8 DIGITS') +
LISTHEAD('EMPLOYEE SERIAL='))
 - ADDUSER U1 CSDATA(EMPSER(234567))

© 2008 IBM Corporation 59

IBM Systems and Technology Group

Planned for V1R10: Custom Fields ...

- Example 2:
 - RDEFINE CFIELD USER.CSDATA.ADDRESS UACC(NONE) +
CFDEF(TYPE(CHAR) MAXLENGTH(100) +
FIRST(ANY) OTHER(ANY) +
HELP('HOME ADDRESS, UP TO 100 CHARACTERS') +
MIXED(YES) +
LISTHEAD('HOME ADDRESS ='))
 - ALTUSER U1 CSDATA(+
ADDRESS('123 Main St., Home Town, NY, USA'))

© 2008 IBM Corporation 60

IBM Systems and Technology Group

Planned for V1R10: RACF Health Checks

- Customer-specified resource checks
 - Extends RACF Sensitive Resources checks
 - Allows specification of additional resources important to an installation
 - Uses profiles in GXFACILI class to specify the resources and checks to perform
- ICHAUTAB checks
 - IBM recommends not using ICHAUTAB (authorized caller table)
 - Improper use can compromise system security and integrity
 - Presence of entries in ICHAUTAB will trigger a medium exception
 - Presence of LPA entries in ICHAUTAB will trigger a severe exception

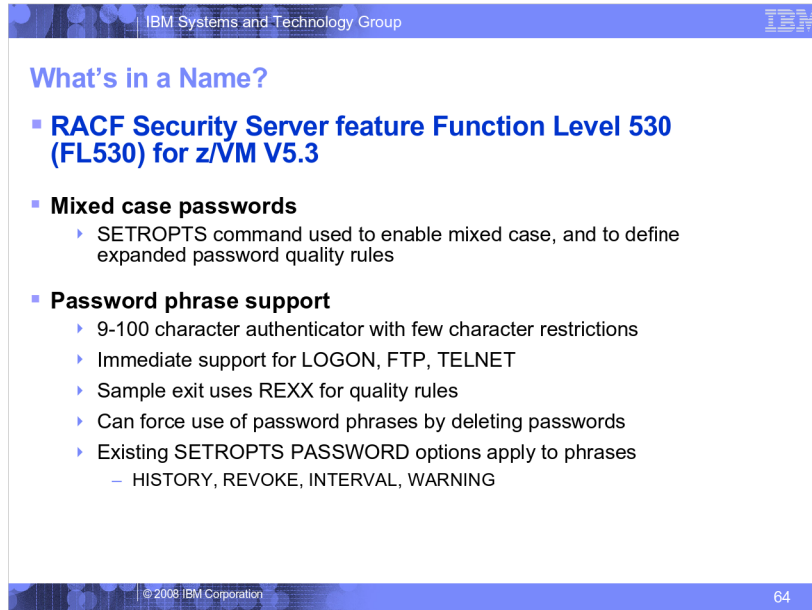
© 2008 IBM Corporation 61

IBM Systems and Technology Group

Planned for V1R10: Other Items

- RACDCERT – replace BSAFE with IBM Crypto Library in C (CLIC)
 - Allow 4096 bit RSA keys through software
- PKI services – additional Distinguished Name attribute types and additional UTF-8 character set support

© 2008 IBM Corporation 62



IBM Systems and Technology Group

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

© 2008 IBM Corporation 65

IBM Systems and Technology Group

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

© 2008 IBM Corporation 66