RACF® z/OS® V1R11 Update

Chicago RACF Users Group

28 October 2009

Mark Nelson, CISSP®, CSSLP™

z/OS® Security Server (RACF) Design and Development

IBM Poughkeepsie

markan@us.ibm.com

© 2009 IBM Corporation

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

Other company, product, or service names may be trademarks or service marks of others.

© 2009 IBM Corporation

Agenda

What's in z/OS V1R10
- Custom Fields
- Password Phrase Exploitation
- More Granularity in Allowing Password Reset
- Enhanced RACF Health Checks

What's new with z/OS V1R11 RACF
- Program Object Signature Verification
- Logon Statistics Suppression
- Identity Propagation
- R_admin extract for General Resource
- Change logging for General Resource
- Automatic assignment of UID and GID to users of Unix System Services
- Profile name in Authorization Exits
- IRRADU00 support for WAS and TKLM
- RACDCERT multi-byte character improvements
- PKI Private Key recovery
- PKI Web Pages
- PKI Support for SHA256 with RSA signature algorithm

3

© 2009 IBM Corporation

---

z/OS Version 1 Release 10 RACF Update

4

© 2009 IBM Corporation

z/OS V1R10: Password Phrase Exploitation

- **Password phrase exploitation**
  - ▸ TSO/E
  - ▸ z/OS UNIX® rlogin, BPX1PWD, BPX1SEC, BPX1TLS
  - ▸ z/OS UNIX su and passwd commands
  - ▸ z/OS Kerberos
  - ▸ z/OS LDAP for z/OS SDBM backend
  - ▸ OpenSSH (IBM Ported Tools for z/OS)

```
------------------------- TSO/E LOGON -------------------------


Enter LOGON parameters below:              RACF LOGON parameters:

Userid   ===> IBMUSER

Password ===> _

Procedure ===> RACFR1B                     Group Ident  ===>

Acct Nmbr ===>

Size     ===>

Perform  ===>

Command  ===>

Enter an 'S' before each option desired below:
 -New Password    -Nomail    -Nonotice   -Reconnect   -OIDcard

PF1/PF13 ==> Help    PF3/PF15 ==> Logoff    PA1 ==> Attention    PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field
```

5

z/OS V1R10: Password Reset Granularity

- **More granularity for Password Reset and LISTUSER**
  - ▸ Before V1R10: The FACILITY resource IRR.PASSWORD.RESET allowed password resets for users without the SPECIAL, OPERATIONS, AUDITOR, or PROTECTED attribute. Access to the IRR.LISTUSER resource allowed the listing of a USER profile base segment.

- **With V1R10, the authority to reset a password can be granted based on profile ownership or group-tree ownership using FACILITY class 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 ...

6

z/OS V1R10: Password Reset Granularity…

- **With V1R10, the authority to issue the LISTUSER command can be granted based on profile ownership or group-tree ownership using FACILITY class profiles:**
  - IRR.LU.OWNER.owner-of-user
    - Grants authority based on the user or group that owns the user
  - IRR.LU.TREE.owner-of-group-tree
    - Grants authority based on group tree scope

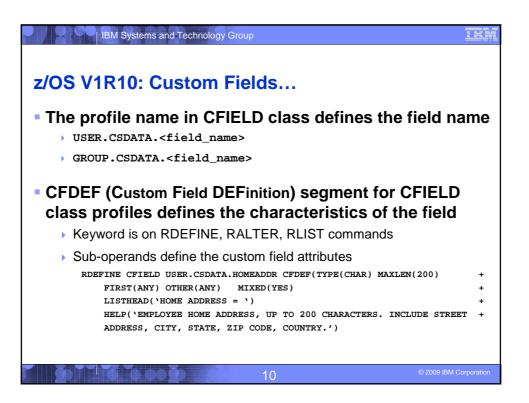- **Users can be excluded password reset or LISTUSER with "exclusion" profiles:**
  - IRR.PWRESET.EXCLUDE.*excluded-user*
  - IRR.LU.EXCLUDE.*excluded-user*

7

---

z/OS V1R10: Custom Fields

- **With Custom Fields you can create your own fields in the RACF database by defining profiles!**
  - No assembler programming required
  - No ICHEINTY, RACROUTE experience required!

- **You define the contents of the fields**
  - Field name (1-8 characters)
  - Field Type: Character, Numeric, Hexadecimal, Flag (Yes/No)
  - Heading for LISTUSER or LISTGRP command
  - Help text
  - Maximum field length
  - For character fields: Character restrictions for first and remaining characters, Mixed case or uppercase
  - For numeric fields: Minimum value, Maximum value

- **Other field customization can be performed in a field validation exit (IRRVAF01) which is under the control of the MVS dynamic exit facility**

8

---

z/OS V1R10: Custom Fields…

- **Custom fields for USER and GROUP profiles**
  - ▸ Field semantics (names and data formats) defined as profiles in the new CFIELD general resource class
  - ▸ New CSDATA segments in USER and GROUP profiles hold the data
  - ▸ FIELD class ("field level access") can be used to control access
  - ▸ Can be processed from
    - RACF commands
    - RACF ISPF panels
    - LDAP SDBM
    - R_admin
    - Database Unload

9

z/OS V1R10: Custom Fields…

- **The profile name in CFIELD class defines the field name**
  - ▸ `USER.CSDATA.<field_name>`
  - ▸ `GROUP.CSDATA.<field_name>`

- **CFDEF (Custom Field DEFinition) segment for CFIELD class profiles defines the characteristics of the field**
  - ▸ Keyword is on RDEFINE, RALTER, RLIST commands
  - ▸ Sub-operands define the custom field attributes

```
RDEFINE CFIELD USER.CSDATA.HOMEADDR CFDEF(TYPE(CHAR) MAXLEN(200)      +
    FIRST(ANY) OTHER(ANY)   MIXED(YES)                                +
    LISTHEAD('HOME ADDRESS = ')                                       +
    HELP('EMPLOYEE HOME ADDRESS, UP TO 200 CHARACTERS. INCLUDE STREET +
    ADDRESS, CITY, STATE, ZIP CODE, COUNTRY.')
```

10

z/OS V1R10: Custom Fields…

- **CSDATA (CuStom DATA) segment for USER and GROUP profiles**
  - ▸ Keyword is on ADDUSER, ALTUSER, LISTUSER, ADDGROUP ALTGROUP, LISTGRP commands
  - ▸ Sub-operands are YOUR custom fields!
    - – ALTUSER SHANNON CSDATA(HOMEADDR('14 Main Street, Anywhere, NY 12345, USA'))

- **The LISTUSER command shows**
  ```
  LU SHANNON NORACF CSDATA

   USER=SHANNON


   CSDATA INFORMATION
   ------------------
   HOME ADDRESS = 14 Main Street, Anywhere, NY 12345, USA


   READY
  ```

- **RACF panels can be used with Custom Fields**

---

z/OS V1R10: Custom Fields…

```
. . . . . . . . . . . . . . . . . . . . . . . . . . . . .
                  RACF - USER PROFILE SERVICES      ENTER REQUIRED FIELD

  SELECT ONE OF THE FOLLOWING:

        1     ADD         Add a user profile
        2     CHANGE      Change a user profile
        3     DELETE      Delete a user profile
        4     PASSWORD    Change your own password and related information
        5     AUDIT       Monitor user activity (Auditors only)


   D or 8    DISPLAY      Display profile contents
   S or 9    SEARCH       Search the RACF data base for profiles


  ENTER THE FOLLOWING INFORMATION:

    USER    ===> SHANNON     Userid


  OPTION ===> 2
   F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
   F7=UP        F8=DOWN      F9=SWAP      F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

z/OS V1R10: Custom Fields…

```
 .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .
                      RACF - CHANGE USER SHANNON

    OWNER              _____     Userid or group name
    USER NAME          _____
    DEFAULT GROUP      _____     Group name

    _   Change PASSWORD related information
    s   Add or Change OPTIONAL information

  TO ASSIGN A USER ATTRIBUTE, ENTER YES, TO CANCEL, ENTER NO

      ____   GROUP ACCESS       ____   SPECIAL
      ____   ADSP               ____   OPERATIONS
      ____   OIDCARD            ____   AUDITOR
      ____   NO-PASSWORD        ____   RESTRICTED

  CHANGE OR DELETE THE MODEL PROFILE USED FOR USER DATA SETS (OPTIONAL):

      NEW MODEL   _____
      DELETE      ____     YES if no model is to be used
  COMMAND ===>
   F1=HELP      F2=SPLIT     F3=END      F4=RETURN    F5=RFIND     F6=RCHANGE
   F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

z/OS V1R10: Custom Fields…

```
 .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .
                      RACF - CHANGE USER SHANNON
  COMMAND ===>

  To add or change the following information, enter any character.

    _  CLASS AUTHORITY                 _  KERB PARAMETERS
    _  INSTALLATION DATA               _  LDAP PROXY PARAMETERS
    _  SECURITY LEVEL or CATEGORIES    _  ENTERPRISE IDENTITY MAPPING
    _  SECURITY LABEL                  s  CSDATA PARAMETERS
    _  LOGON RESTRICTIONS
    _  NATIONAL LANGUAGES
    _  DFP PARAMETERS
    _  TSO PARAMETERS
    _  OPERPARM PARAMETERS
    _  CICS PARAMETERS
    _  WORK ATTRIBUTES
    _  OMVS PARAMETERS
    _  NETVIEW PARAMETERS
    _  DCE PARAMETERS
    _  OVM PARAMETERS
    _  LNOTES PARAMETERS
   F1=HELP      F2=SPLIT     F3=END      F4=RETURN    F5=RFIND     F6=RCHANGE
   F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

z/OS V1R10: Custom Fields…

```
. . . . . . . . . . . . . . . . . . . . . . . . .
                Set Custom Fields for  USER  SHANNON              ROW 1 TO 1 OF 1
COMMAND INPUT ===>                                          SCROLL ===> PAGE

Delete ALL CSDATA information  (NOCSDATA)  ___  YES or blanks.

Select one or more custom fields.  Use d to delete, h for help,
  u to undo changes made during this session, or x to set/edit a field.
 Hit ENTER to continue.
                                                  Value
SEL FieldName Description                         ----+----1----+----2-
  s  HOMEADDR  HOME ADDRESS                        14 Main Street, Anywh
****************************** Bottom of data ******************************




   F1=HELP      F2=SPLIT     F3=END      F4=RETURN   F5=RFIND    F6=RCHANGE

   F7=UP        F8=DOWN      F9=SWAP     F10=LEFT    F11=RIGHT   F12=RETRIEVE
```

---

z/OS V1R10: Custom Fields…

```
. . . . . . . . . . . . . . . . . . . . . . . . .
                RACF - CUSTOM KEYWORD DATA for SHANNON
COMMAND ===>                                           SCROLL ===> PAGE
Field Name:  HOMEADDR
Description:  HOME ADDRESS
14 Main Street, Anywhere, NY, 12528, USA_____
_____
_____




   (Enter changes.  Hit ENTER to save, PF3 to CANCEL)
   F1=HELP      F2=SPLIT     F3=END      F4=RETURN   F5=RFIND    F6=RCHANGE
   F7=UP        F8=DOWN      F9=SWAP     F10=LEFT    F11=RIGHT   F12=RETRIEVE
```

z/OS V1R10: Custom Fields…

```
   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .   .
 RACF HELP                    CUSTOM FIELD INFORMATION

  Field:  HOMEADDR

 EMPLOYEE HOME ADDRESS, UP TO 200 CHARACTERS. INCLUDE STREET ADDRESS, CITY, STATE,
 ZIP CODE, COUNTRY.




 The first character must be of type ANY.
 All other characters must be of type ANY.




 OPTION ===>
  F1=HELP       F2=SPLIT      F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE

  F7=UP         F8=DOWN       F9=SWAP      F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

---

z/OS V1R10: RACF Health Checks

- **RACF Health Check Enhancements:**
  - ▸ **ICHAUTAB checks:**
    - For over 20 years, IBM has recommended not using the RACF Authorized Caller Table (ICHAUTAB)
    - RACF introduces a new check to verify that ICHAUTAB is not being used
      - RACF_ICHAUTAB_NONLPA raises a SEV(MED) exception if a non-LPA resident ICHAUTAB is found
    - The existing RACF_SENSITIVE_RESOURCES raises a SEV(HIGH) exception if an LPA-resident ICHAUTAB is found

z/OS V1R10: RACF Health Checks…

- **The current RACF checks examine key elements of the z/OS infrastructure, but:**
  - ▸ The checks look at the resources IBM thinks are important
    - – Unless you wrote your own check you can't examine the protection of your data resources

- **With z/OS V1R10, you can check the protection of the resources you want simply by defining profiles and registering your check with the IBM Health Checker for z/OS**

---

z/OS V1R10: RACF Health Checks…

- **Defining your own resource check takes these three steps:**

  1. Defining a RACF profile in the new RACFHC general resource class. This profile contains the list of resources that you want to check

  2. Define a PARMLIB entry that defines your check using the IBM Health Checker for z/OS Dynamic Registration

  3. Activate your PARMLIB entry

z/OS V1R10: RACF Health Checks…

- **The RACFHC class contains profiles which have the resources you want to check. The RDEFINE command to add a profile is:**

```
RDEFINE RACFHC MY_RESOURCE_LIST
    ADDMEM(DATASET/PROD.VALUABLE.DATA/ZDR17B/NONE
        DATASET/SEC.FILING.FORMS//NONE
        RACFHC/MY_RESOURCE_LIST//NONE)
```

- **The ADDMEM field defines the resources that you want checked. The format is:**

```
className/resourceName/volume/maximumPublicAccess
```

  - `className` is any valid RACF class
  - `resourceName` is a resources name within the class
  - `Volume` is the volume serial for a DATASET resource, otherwise no value should be specified
  - `maximumPublicAccess` is the access level which if exceeded results in an exception. Valid values are NONE, READ, UPDATE, and CONTROL.
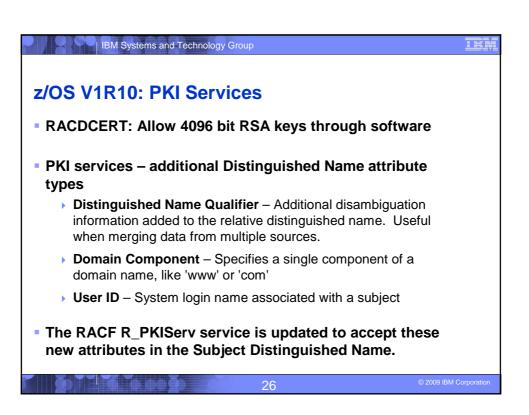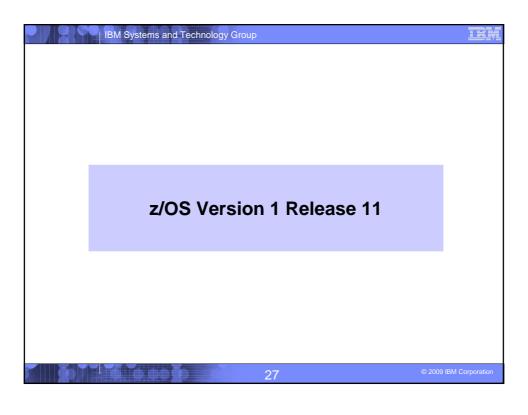
---

z/OS V1R10: RACF Health Checks…

- **In addition to defining resources in the ADDMEM value, you can specify one or more IBM-defined report sets. These report sets are:**

  ▸ IRR_APFLIST: APF data set list
  ▸ IRR_LINKLIST: Current link list data set list
  ▸ IRR_PARMLIB: Current PARMLIB data set list
  ▸ IRR_RACFDB: Data sets which comprise the RACF data base
  ▸ IRR_SYSREXX: System REXX data set
  ▸ IRR_ICHAUTAB: ICHAUTAB entries

- **Sample profile definition for a pre-defined set of resources**

```
RDEFINE RACFHC MY_SYSTEM_STUFF
    ADDMEM(DATASET/SYS1.SAMPLIB//READ
    IRR_APFLIST
    IRR_RACFDB)
```

z/OS V1R10: RACF Health Checks…

- A Health Checker PARMLIB statement is used to define your check, set its characteristics (such as the interval, severity), and associate the check with the RACFHC profile which contains the resources you want checked

```
ADD CHECK(USER01,MY_INSTALLATION_HEALTH_CHECK)
    CHECKROUTINE(IRRHCR00)
    MESSAGETABLE(IRRHCM00)
    ENTRYCODE(100)
    PARM('USER(USER01)  RESOURCELIST(MY_RESOURCE_LIST)')
    DATE(yyyymmdd)
    REASON('My sensitive resources')
    GLOBAL
    ACTIVE
    SEVERITY(HIGH)
    INTERVAL(08:00)
```

---

z/OS V1R10: RACF Health Checks…

- The final step is to activate your check. After adding it to a member (HZSPRMMN in this example) activate the PARMLIB entry using the MVS modify command for the Health Checker address space:

```
    F HC,ADD,PARMLIB=MN
```

- Your check is now registered with the IBM Health Checker for z/OS!

```
Display  Filter  View  Print  Options  Help
----------------------------------------------------------------------------
SDSF HEALTH CHECKER DISPLAY  RACFR1B              LINE 38-53 (92)
NP   NAME                         CheckOwner      State           Status
     MY_INSTALLATION_HEALTH_CHECK USER01          ACTIVE(ENABLED)  EXCEPT
     PDSE_SMSPDSE1                IBMPDSE         ACTIVE(ENABLED)  EXCEPT
     RACF_FACILITY_ACTIVE        IBMRACF         ACTIVE(ENABLED)  SUCCES
     RACF_GRS_RNL                IBMRACF         ACTIVE(DISABLED) ENV N/
```

---

z/OS V1R10: RACF Health Checks…

```
CHECK(USER01,MY_INSTALLATION_HEALTH_CHECK)
START TIME: 02/27/2008 16:16:22.678052
CHECK DATE: 20070425  CHECK SEVERITY: HIGH
CHECK PARM: USER(USER01)  RESOURCELIST(MY_RESOURCE_LIST)


                Resource List from MY_RESOURCE_LIST

S Resource Name                    Class    Vol    UACC Warn ID*  User
- ------------------------------ -------- ------ ---- ---- ---- ----
V PROD.VALUABLE.DATA               DATASET  ZDR17B
V SEC.FILING.FORMS                 DATASET
V PUBLIC.REPORTS                   DATASET  REGVOL
  MY_RESOURCE_LIST                 RACFHC          None No   ****

* High Severity Exception *

...
...
...
```

---

z/OS V1R10: PKI Services

- **RACDCERT: Allow 4096 bit RSA keys through software**

- **PKI services – additional Distinguished Name attribute types**
  - **Distinguished Name Qualifier** – Additional disambiguation information added to the relative distinguished name. Useful when merging data from multiple sources.
  - **Domain Component** – Specifies a single component of a domain name, like 'www' or 'com'
  - **User ID** – System login name associated with a subject

- **The RACF R_PKIServ service is updated to accept these new attributes in the Subject Distinguished Name.**

z/OS Version 1 Release 11

---

z/OS V1R11: Program Object Signature Verification

- **Allows the signing of program objects and the verification of the signature of program objects when the objects are loaded into storage**
  - ▸ BINDER: Creates signatures by calling RACF when the SIGN option has been specified
  - ▸ RACF: Stores the information (certificates, keys, and options) necessary for the signature generation and validation, calculates the signatures, performs the validations, and logs the results.
  - ▸ LOADER: Calls RACF when program objects are loaded

- **You can sign your own code and vendors can sign theirs**

---

z/OS V1R11: Program Object Signature Verification…

- **Why sign code?**
  - ▸ "Belts and suspenders" or "defense in depth": This support is intended to be used in conjunction with existing security mechanisms .
  - ▸ Digitally signing code can help increase the reliability and security of the system by adding an additional layer of controls on executable programs running on the system.
    - – Digitally signing code makes it possible to detect changes to programs due to tampering or corruption.
    - – Requiring that certain code be signed makes it easier to enforce change control procedures and protect against accidental changes to program code libraries. This helps avoid errors such as accidently placing 'test' code on a 'production' system.

29

© 2009 IBM Corporation

z/OS V1R11: Program Object Signature Verification…

- **RACF profiles are used to control program signing:**
  - ▸ Key ring associated with the user performing the signing
    - – Contains the information appropriate for program signing (private key, X.509 certificates (signing, CertAuth) which themselves must be appropriately signed
  - ▸ IRR.PROGRAM.SIGNING profile(s) in the FACILITY class
    - – Used to associate the key ring owner, key ring name, and message digest algorithm used in the signature generation and validation process.

30

© 2009 IBM Corporation

z/OS V1R11: Program Object Signature Verification…

- **RACF profiles are used to control program verification:**
  - IRR.PROGRAM.SIGNATURE.VERIFICATION profile in the FACILITY class
    - Used to associate the key ring owner and key ring name of the key ring which contains the signature verification key ring
  - Profiles in the PROGRAM class
    - Contains information options that specify the actions to be taken during verification process:
      - SIGREQUIRED: Is a signature required for this program? (YES,NO)
      - FAILLOAD: Under what conditions should the load fail? (ANYBAD, BADSIGONLY, NEVER)
      - SIGAUDIT: What should be logged? (ALL, SUCCESS, ANYBAD, BADSIGONLY, NONE)

31

© 2009 IBM Corporation

z/OS V1R11: Program Object Signature Verification…

- **Considerations:**
  - Only program objects (which must reside in in PDSEs) can be signed and verified.
    - Code in PDS or z/OS Unix System Services file system, or non Program Object code cannot be signed and verified. However, z/OS UNIX programs can 'link' to signed executables in PDSEs.
  - If a signed program is zapped (executable code changed), its signature is no longer valid.
  - IBM ships portions of the System SSL product as signed code.
  - Support is new for z/OS R11 and has been rolled back to z/OS R10.
  - Any installation or software provider can use these services to sign their own code.
  - Program objects are not encrypted

32

© 2009 IBM Corporation

z/OS V1R11: Logon Statistics Suppression

- **Allows you to specify which applications should only record on the first system access of a day**
    - ▸ Why? Reduced I/O and lower the impact of serialization on the RACF dataset.

- **APPL profiles are used to specify which applications are taking advantage of logon statistics suppression**
    - ▸ Specify "RACF-INITSTATS(DAILY)" anywhere in the APPLDATA
    - ▸ APPL class must be active and RACLISTed

33

© 2009 IBM Corporation

---

z/OS V1R11: Identity Propagation

- **Prior to z/OS V1R11, clients using distributed server applications which used a common server or application identity for transaction executing on z/OS would not be able to pass the identity of the end user to z/OS for logging**

- **With z/OS V1R11, applications can pass the distributed identity information abut the end user (distinguished name and realm) into z/OS where it will be used for logging**
    - ▸ Exploited by CICS TS 4.1

- **The distributed identity can be mapped to a RACF identity at:**
    - ▸ the distributed application server (as is often done today) or
    - ▸ the execution point on z/OS, using the new RACMAP support

```
RACMAP  [ID(mapped-to-userID)]
    MAP
        USERDIDFILTER(NAME('distributed-identity-username-filter'))
        REGISTRY(NAME('distributed-identity-registryname'))
        [WITHLABEL('label-name')]
  | DELMAP[(LABEL('label-name'))]
  | LISTMAP[(LABEL('label-name'))]
```

34

© 2009 IBM Corporation

---

z/OS V1R11: R_admin Enhancements

- **R_admin can now be used to extract information about general resources**
    - Extract specified profile - ADMN_XTR_RESOURCE (X'1F')
    - Extract next profile - ADMN_XTR_NEXT_RESOURCE (X'20')

- **Authorization required for problem state callers:**
    - At least READ access to the IRR.RADMIN.RLIST resource in the FACILITY class
    - Users are limited to seeing only the information that would be displayed by an RLIST command
        - For example , audit settings will be suppressed if caller does not have the AUDITOR attribute

- **Supervisor callers can request either, both, or no check**
    - Command authority enforced by default

z/OS V1R11: R_admin Enhancements…

- **R_admin SETROPTS option extraction (ADMN_XTR_SETR (X'16')) may now be called from problem state**

- **Authorization required for problem state caller:**
    - At least READ access to IRR.RADMIN.SETROPTS.LIST in the FACILITY class
    - Authority as enforced by the SETROPTS command
        - For example, audit settings will be suppressed if caller does not have the AUDITOR attribute

- **No changes required to existing programs other than to remove MODESET into supervisor state**

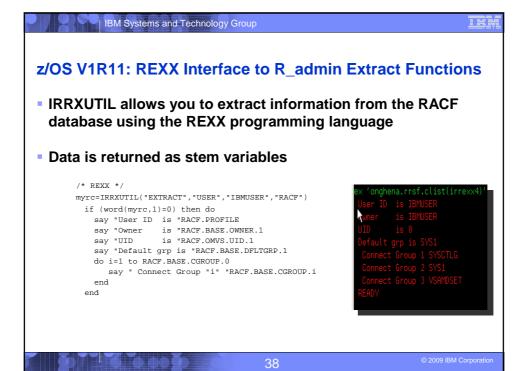## z/OS V1R11: LDAP Change Logging of General Resources

- **You can now tell RACF to create change log entries for changes to general resources by defining the profile NOTIFY.LDAP.*class-name* in the RACFEVNT class and activate the class**
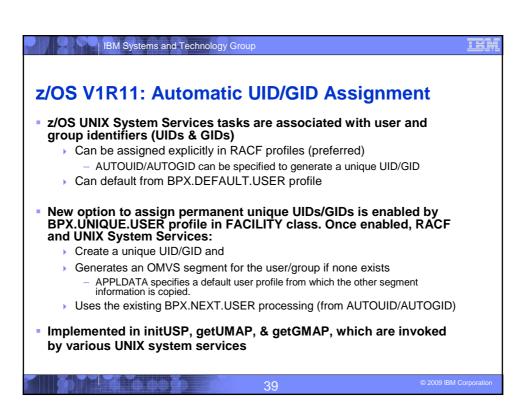
- **Events which are logged:**
  - Resource additions made using the **RDEFINE** command
  - Resource modifications made using the **RALTER** command
  - Changes to the resource's access list using the **PERMIT** command
  - Resource deletions made using the **RDELETE** command

- **ICHEINTY/RACROUTE applications can create their own change log entries using R_proxyserv (IRRSPY00)**

---

z/OS V1R11: REXX Interface to R_admin Extract Functions

- **IRRXUTIL allows you to extract information from the RACF database using the REXX programming language**

- **Data is returned as stem variables**

```
/* REXX */
myrc=IRRXUTIL("EXTRACT","USER","IBMUSER","RACF")
  if (word(myrc,1)=0) then do
    say "User ID  is "RACF.PROFILE
    say "Owner    is "RACF.BASE.OWNER.1
    say "UID      is "RACF.OMVS.UID.1
    say "Default grp is "RACF.BASE.DFLTGRP.1
    do i=1 to RACF.BASE.CGROUP.0
      say " Connect Group "i "RACF.BASE.CGROUP.i
    end
  end
```

```
ex 'onghena.rrsf.clist(irrexx4)'
User ID  is IBMUSER
Owner    is IBMUSER
UID      is 0
Default grp is SYS1
 Connect Group 1 SYSCTLG
 Connect Group 2 SYS1
 Connect Group 3 VSAMDSET
READY
```

z/OS V1R11: Automatic UID/GID Assignment

- **z/OS UNIX System Services tasks are associated with user and group identifiers (UIDs & GIDs)**
  - Can be assigned explicitly in RACF profiles (preferred)
    - AUTOUID/AUTOGID can be specified to generate a unique UID/GID
  - Can default from BPX.DEFAULT.USER profile

- **New option to assign permanent unique UIDs/GIDs is enabled by BPX.UNIQUE.USER profile in FACILITY class. Once enabled, RACF and UNIX System Services:**
  - Create a unique UID/GID and
  - Generates an OMVS segment for the user/group if none exists
    - APPLDATA specifies a default user profile from which the other segment information is copied.
  - Uses the existing BPX.NEXT.USER processing (from AUTOUID/AUTOGID)

- **Implemented in initUSP, getUMAP, & getGMAP, which are invoked by various UNIX system services**

---

z/OS V1R11: Profile Name in Authorization Exits

- **The RACROUTE REQUEST=AUTH (ICHRCX02) and REQUEST=FASTAUTH(ICHRFX02,ICHRFX04) exits have always received a pointer to the profile which was used in the access control decision**
  - Profile is one which allowed or denied the request
  - Can differ from the resource name (if a generic profile was matched)

- **With z/OS V1R11, the exits receive the name of the profile as well**
  - For REQUEST=FASTAUTH, if the profile name is generic, then the internal format of the profile name is returned
  - RACROUTE REQUEST=AUTH, the profile name is always in external format
  - A new service is provided to map the internal format of the profile name to the external format

z/OS V1R11: SMF Unload of WAS & TKLM SMF data

- **Support for z/OS SMF repository of audit data**
  - WebSphere Application Server (WAS) V7
  - Tivoli Key Lifecycle Manager (TKLM)

- **Both WAS and TKLM create SMF Type 83 records via the z/OS JAVA class interface to the R_auditx service**
  - Subtype 5: WebSphere
  - Subtype 6: TKLM

- **IRRADU00 unloads XML and traditional tabular-format output files of audit data**

- **LRECL of tabular IRRADU00 output is now 12288**
  - Will be adjusted automatically by IRRADU00

41　　　　　　　　　© 2009 IBM Corporation

---

z/OS V1R11: Digital Certificate Support

- **RACDCERT multi-byte character improvements**

  - Support (installation, retrieval and authentication) for certificates which contain characters which are outside the 1047 code page.
  - If a character does not map to code page 1047, the character will be represented by 6 characters in the format of U+nnnn, where nnnn is the Unicode code point of that character in hexadecimal format
  - When the certificate profile is created, the 6-character format will contribute to the profile name.
    - There is a risk of exceeding the profile name limit, which will prevent the creation of the certificate in RACF.

- **PKI Private Key recovery**

  - Prior to z/OS V1R11, PKI services did not generate private/public key pairs. In R11, key generation and key archival capabilities are being introduced. The certificate requestor will have the option to generate the public/private key pair themselves as in previous releases or have PKI Services generate the key pair.
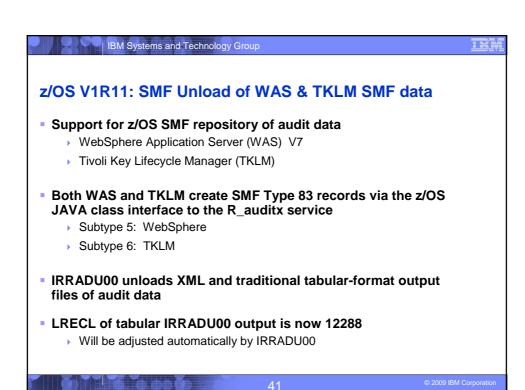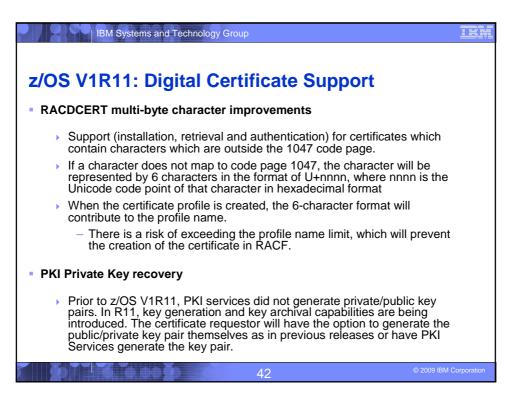
42　　　　　　　　　© 2009 IBM Corporation

z/OS V1R11: Digital Certificate Support

- **PKI Web Pages**
  - ▸ PKI services now provides Java server pages (JSPs) and an XML template file to create and customize the PKI Services Web application as an alternative to the existing REXX CGI support.

- **PKI Support for SHA256 with RSA signature algorithm**
  - ▸ PKI Services will support the "SHA256 with RSA encryption" signature algorithm for signing certificates, certificate and authority revocation lists (CRL/ARL), and OCSP responses

43

© 2009 IBM Corporation