# RACF V2R2 Preview and Goody Bag

*Julie Bergh*
*Ross Cooper, CISSP®*
*IBM Corporation*

*March 5th, 2015*
*Session: 16960*

#SHAREorg

SHARE is an independent volunteer-run information technology association that provides **education**, professional **networking** and industry **influence**.

# RACF V2R2 Preview

- **RACF Read Only Auditor** - New type of auditor that can look but not change settings.
- **Granular Digital Certificate Authority** - New more granular digital certificate authority checking option.
- **Unix Search Authority** - Allows an administrator to search/list UNIX files regardless of individual directory settings.
- **FSEXEC** – Restricting UNIX execute access
- **New and Updated RACF Heath Checks**
- **RACF Remote Sharing Enhancements:**
  - RRSF Dynamic Main Switch - Allows switching the RRSF main node
  - Unidirectional Connection - Deny In Bound support
  - RACF Remote Sharing Configuration Information API
- **RACF Password Enhancements:**
  - New Special Characters Support
  - Phrase Only Users
  - Expire without setting password
  - New Encryption Algorithm Option - **KDFAES**

# RACF V2R2 Preview

- This material is **preliminary**
- Work is in progress but not all designs/code are complete
- Some of what follows **will change!**
  - Some things might never appear, or appear (possibly much) later
  - Some things will be implemented differently as we go through Development
  - Some things will have different names and externals
  - Some things may be added

*** Statements regarding IBM future direction and intent are subject to change or withdrawal, and represent goals and objectives only.**

# RACF
# Read Only Auditor

# Read Only Auditor

- **User with the RACF AUDITOR Attribute:**
  - Can audit a RACF controlled system by viewing RACF profiles and SETROPTS settings.
  - Can **control** the logging of detected accesses to any RACF protected resources during RACF authorization checking and accesses to the RACF database.

- **User with the Read Only Auditor – ROAUDIT attribute:**
  - Can list RACF profiles and other security settings
  - Can NOT control logging settings
  - RACF list commands and utilities are updated to permit users with ROAUDIT the same ability to list information that would be allowed to users with AUDITOR.

- Allows installations to create users that can view system information but not alter any system controls.
  - Suitable for use by an external auditor who may need to verify the current security state of a system – allows that user to view system information but does not unintentionally grant the user the ability to change (or sabotage) system settings.

# Read Only Auditor

- **Enable Read Only Auditor attribute:**

  ```
  ALTUSER / ADDUSER USER1 ROAUDIT
  ```

- **Disable Read Only Auditor attribute:**

  ```
  ALUTUSER USER1 NOROAUDIT
  ```

- "Listing" commands (and related R_admin functions) are modified to test for the ACEEROA flag when determining the user's authority to list information about RACF profiles.
  - **Commands:** LISTDSD, LISTGRP, LISTUSER, RLIST, SETROPTS LIST, SEARCH
  - **z/OS UNIX:** ck_access
  - **Utilities:** DSMON, IRRUT100, IRRXUTI2
- ACEEROA (ROAUDIT) is distinct from the existing ACEEAUDT (AUDITOR) ACEE flag.
  - Both flags may be set (or unset) for the same user.
  - If both flags are set, the ACEEAUDT flag takes precedence in any authority checking.
    - Setting the ACEEROA flag on an existing user that already has the ACEEAUDT flag set will not remove that user's authority to RACF resources.

# Digital Certificate Granular Authority

# Digital Certificate Granular Authority

**Background:**

- Certificate administration in RACF:
  - **RACDCERT** commands
  - **R_DataLib** callable service
- Authorization to perform certificate administration:
  - **IRR.DIGTCERT.<function>** profiles in the **FACILITY** class control access to cert, ring – level of authority based on if the invoker wants to process his/her own, another's, or a CA/SITE certificate:
    - **READ** access to perform action on your own certificate / ring
    - **UPDATE** access to perform action on other's certificate / ring
    - **CONTROL** access to perform action on CERTAUTH / SITE certificate
  - **R_DataLib** authorization can also be controlled using ring-specific profile checking in the **RDATALIB** class
    - **<ring owner>.<ring name>.UPD**

# Granular Certificate Authority

New Granular Certificate Authority features in V2R2:

- New controls to protect certificates:
  - Access to certificates can be controlled by **RDATALIB** Profiles:
    **IRR.DIGTCERT.<cert owner>.<cert label>.LST/UPD.<function>**

- RACF **RACDCERT** can now check **RDATALIB** profiles:
  - Enabled by defining the **IRR.RACDCERT.GRANULAR** profile in the **RDATALIB** class

# UNIX Search Authority

# UNIX Search Authority

- **UNIX Security Administration:**
  - z/OS UNIX defines a set of **UNIXPRIV** class profiles to manage various UNIX privileges:

    **SUPERUSER.FILESYS.CHANGEPERMS** – Change file permissions
    **SUPERUSER.FILESYS.CHOWN** - Change file owners
  - These privileges lack the ability to read or search directories.
  - In order to search directories, the administrator must be granted one of:
    - Search authority to containing directories
    - RACF Auditor
    - **BPX.SUPERUSER** in **FACILITY** Class / UID 0
- **New V2R2 UNIX Search Authority:**
  - New function introduced in V2R2 will allow for directory read / search authorization to be granted via a new RACF profile:

    **SUPERUSER.FILESYS.DIRSRCH -** Allows a user to read and search all directories, without the authority to open other files.

# UNIX Search Authority

- Allowing z/OS UNIX users to search directories:
  - To allow z/OS UNIX users to read and search all file system directories, regardless of file permission bits or access lists, create a profile in the **UNIXPRIV** class protecting a resource called **SUPERUSER.FILESYS.DIRSRCH**. Then permit users and groups with at least READ access performing the following steps.

1. Define a profile in the **UNIXPRIV** class.

```
RDEFINE UNIXPRIV SUPERUSER.FILESYS.DIRSRCH UACC(NONE)
```

2. Add the user or group to the access list with at least READ access.

```
PERMIT SUPERUSER.FILESYS.DIRSRCH CLASS(UNIXPRIV) ID(USER01 GRPX)
       ACCESS(READ)
```

3. If the **UNIXPRIV** class is not already active, activate and RACLIST it.

```
SETROPTS CLASSACT(UNIXPRIV) RACLIST(UNIXPRIV)
```

4. If the **UNIXPRIV** class is already active and RACLISTed, refresh it.

```
SETROPTS RACLIST(UNIXPRIV) REFRESH
```

You have now given directory search permission to the specified users and groups.

# FSEXEC
# Restricting UNIX execute access

# Restricting UNIX execute access

- It may be desirable to mark a z/OS File System as non-executable:
  - Prevent unintentional execution of files in a shared file system such as /tmp
- **New FSEXEC Class :**
  - Prevent users from executing any file in a z/OS File System (zFS) file system or Temporary File System (TFS).
  - Can allow selected users and groups to remain eligible for execute access.
  - Supports an improved audit posture by enabling the RACF administrator to demonstrate a single point of control for restricting execute access to one or more file systems that might contain authorized code, or code of unknown origin.
- **Notes:**
  - When a file system is protected by an FSEXEC profile with UACC(NONE), only users and groups with UPDATE access authority or higher are eligible for execute file access. Eligible users are then subject to the usual authorization checking, which includes checking for superuser authority, ownership, permission bits, access control lists (ACLs), and UNIXPRIV authorities.
  - When a file system is protected by an FSEXEC profile and a user has insufficient access authority to it, RACF denies file execution access regardless of other user authorizations. Superuser or auditor privilege does not override FSEXEC denial of access.

# FSEXEC - Restricting UNIX execute access

Access to execute files in a UNIX file system may be controlled by defining profiles in the new FSEXEC class.

1) Define a profile in the FSEXEC class to protect each the file system. The profile name is the FILESYSTEM name specified on the MOUNT statement. Since profiles in the FSEXEC class are case sensitive, ensure the profile name on the RDEFINE command matches the letter case of the name on the MOUNT statement.

```
RDEFINE FSEXEC /tmp UACC(NONE)
```

2) If multiple file systems are have similar names, you can define a generic profile name to protect multiple file systems. Before you define a generic profile in the FSEXEC class, enable generics for the class, as follows.

```
SETROPTS GENERIC(FSEXEC)
RDEFINE FSEXEC OMVS.ZFS.ADMIN.** UACC(NONE)
```

3) For selected users and groups who require execute access, authorize with them UPDATE access.

```
PERMIT OMVS.ZFS.ADMIN.** CLASS(FSEXEC) ID(USER019 GROUPADM) ACCESS(UPDATE)
```

4) Activate your profile changes in the FSEXEC class, as follows. If the FSEXEC class is not already active, activate and RACLIST

```
SETROPTS CLASSACT(FSEXEC) RACLIST(FSEXEC)
```

5) If the FSEXEC class is already active and RACLISTed, refresh it.

```
SETROPTS RACLIST(FSEXEC) REFRESH
```

# RACF Health Checks

# New and Updated RACF Health Checks

- RACF is introducing four new health checks
  - **RACF_CSFKEYS_ACTIVE**
  - **RACF_CSFSERV_ACTIVE**
  - **RACF_PASSWORD_CONTROLS**
  - **RACF_ENCRYPTION_ALGORITHM**

- RACF is updating the **RACF_SENSITIVE_RESOURCE** to:
  - Report on the protection status of ICSF TKDS, PKDS, and CKDS data sets
  - Report on the protection status of the RACF remote sharing (RRSF) work data sets
  - Report on the protection status of additional z/OS UNIX resources

# New and Updated RACF Health Checks

- **RACF_CSFKEYS_ACTIVE** and **RACF_CSFSERV_ACTIVE** raise an exception if the class is inactive

```
CHECK(IBMRACF,RACF_CSFKEYS_ACTIVE)
SYSPLEX:    LOCAL     SYSTEM: RACFR22
START TIME: 03/05/2014 16:45:04.542092
CHECK DATE: 20140106  CHECK SEVERITY: MEDIUM
CHECK PARM: CSFKEYS


* Medium Severity Exception *

IRRH229E The class CSFKEYS is not active.

  Explanation:  The class is not active. IBM recommends that the
    security administrator evaluate the need for this class, define
    profiles in it as appropriate, and activate the class.

. . .
. . .

  Automation:  None.

  Check Reason:  IBM recommends activating this class

END TIME: 03/05/2014 16:45:04.606623  STATUS: EXCEPTION-MED
```

# New and Updated RACF Health Checks

- **RACF_SENSITIVE_RESOURCES** is updated to examine the ICSF CKDS, PKDS, and TKDS VSAM data sets

```
CHECK(IBMRACF,RACF_SENSITIVE_RESOURCES)
SYSPLEX:    LOCAL     SYSTEM: RACFR22
START TIME: 03/05/2014 17:52:23.177975
CHECK DATE: 20120106  CHECK SEVERITY: HIGH
. . .
. . .
. . .


                          ICSF Dataset Report

S Data Set Name                              Vol    UACC Warn ID*  User
- ------------------------------------------ ------ ---- ---- ---- ----
  RACFDRVR.ICSF.PKDS                        D94001 None No   ****
  RACFDRVR.ICSF.CKDS                        D94001 None No   ****
  RACFDRVR.ICSF.TKDS                        D94001 None No   ****

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

# New and Updated RACF Health Checks

- **Notes on these Checks:**
  - Clients who are not using ICSF may chose to make the ICSF checks INACTIVE using a HZSPRMxx PARMLIB statement.
  - **RACF_CSFSERV_ACTIVE**, **RACF_CSFKEYS_ACTIVE**, and the ICSF CKDS, PKDS, and TKDS update to **RACF_SENSITIVE_RESOURCES** is being shipped on releases V1.12, V1.13, and V2.1 with APAR OA44696.

# New and Updated RACF Health Checks

- **RACF_PASSWORD_CONTROLS** examines basic password controls
- Clients can modify the IBM recommendation with a health check parameter

```
CHECK(IBMRACF,RACF_PASSWORD_CONTROLS)
SYSPLEX:    LOCAL     SYSTEM: RACFR22
START TIME: 03/05/2014 16:45:04.494234
CHECK DATE: 20140118  CHECK SEVERITY: MEDIUM

                        RACF Password Controls

S Control                                          Value Target
- ------------------------------------------------ ----- ------
E Mixed case passwords are allowed                  NO   YES
  Number of consecutive unsuccessful logon attempts  3     3

* Medium Severity Exception *

IRRH283E The RACF_PASSWORD_CONTROLS check found an exception
with one or more password control settings.
. . .
. . .
  Automation:  None.

  Check Reason:  Password control recommendations should be used.

END TIME: 03/05/2014 16:45:04.603476  STATUS: EXCEPTION-MED
```

# New and Updated RACF Health Checks

- **RACF_ENCRYPTION_ALGORITHM** examines the return code from the RACF encryption exit (ICHDEX01) exit for authentication and raises an exception:
  - V1R12, V1R13 & V2R1 - Anything other than DES is in use
  - V2R2 – Anything other than KDFAES is in use
- **ICHDEX01** communicates the desired encryption with a return code:
  - 00: Installation-defined
  - 04: Masking
  - 08: DES
  - 12: Installation-defined
  - 16: DES then masking
- V1R12, V1R13 & V2R1 - The lack of **ICHDEX01** currently requests DES then the RACF “masking” algorithm and is considered an exception.

# New and Updated RACF Health Checks

- The **RACF_ENCRYPTION_ALGORITHM** check reports on the use of encryption for authentication since the last IPL

```
CHECK(IBMRACF,RACF_ENCRYPTION_ALGORITHM)

START TIME: 01/31/2014 09:44:29.892717
CHECK DATE: 20140131  CHECK SEVERITY: HIGH

IRRH287I  ICHDEX01 is in use on this system.

              ICHDEX01 Return Codes

Installation Mask    DES      Installation  DES then   Other
Only         Only    Only     Only          Mask
(RC=00)      (RC=04) (RC=08)  (RC=12)       (RC=16)
------------ ------- -------  ------------- ---------  --------
NO           NO      YES      NO            YES        NO


IRRH289E ICHDEX01 indicates an encryption algorithm other than DES is in use.

END TIME: 01/31/2014 09:44:29.893680  STATUS: EXCEPTION-HIGH
```

# New and Updated RACF Health Checks

- **Notes on RACF_PASSWORD_CONTROLS and RACF_ENCRYPTION_ALGORITHM:**
  - These checks are being shipped on releases V1.12, V1.13, and V2.1 with an APAR OA45608.

# New and Updated RACF Health Checks

- **RACF_SENSITIVE_RESOURCES** is updated to examine the RRSF input and output data sets

```
CHECK(IBMRACF,RACF_SENSITIVE_RESOURCES)
SYSPLEX:    LOCAL     SYSTEM: RACFR22
START TIME: 03/05/2014 17:52:23.177975
CHECK DATE: 20120106  CHECK SEVERITY: HIGH
. . .
. . .
. . .


                         RRSF Dataset Report

S Data Set Name                                Vol    UACC Warn ID*  User
- ------------------------------------------- ------ ---- ---- ---- ----
  SYS1.MVSX.INMSG                             D94001 None No   ****
  SYS1.MVSX.MVSA.INMSG                        D94001 None No   ****
  SYS1.MVSX.MVSA.OUTMSG                       D94001 None No   ****
  SYS1.MVSX.MVSB.INMSG                        D94001 None No   ****
  SYS1.MVSX.MVSB.OUTMSG                       D94001 None No   ****
. . .
. . .
. . .
```

# New and Updated RACF Health Checks

- The **RACF_SENSITIVE_RESOURCES** check is updated to check on these z/OS UNIX resources:
  - **FACILITY class:**
    - BPX.POE
    - BPX.JOBNAME
    - BPX.FILEATTR.SHARELIB
    - BPX.SMF
    - BPX.STOR.SWAP
    - BPX.UNLIMITED.OUTPUT
  - **UNIXPRIV class:**
    - SUPERUSER.FILESYS.QUIESCE
    - SUPERUSER.FILESYS.PFSCTL
    - SUPERUSER.FILESYS.VREGISTER
    - SUPERUSER.IPC.RMID
    - SUPERUSER.SETPRIORITY
  - **SURROGAT class:**
    - BPX.SRV.<userid>

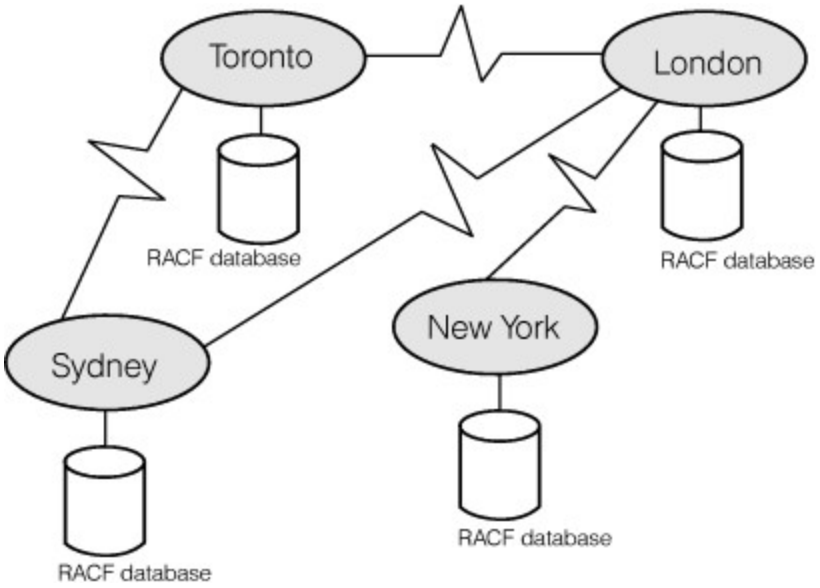
# RRSF
# RACF Remote Sharing Enhancements

# RRSF Enhancements

- **RRSF Unidirectional Nodes**
  - Ability to define a remote RRSF node which is not allowed to make updates
- **RRSF Dynamic Main Node Switch**
  - Ability to switch the RRSF Main Node
- **RRSF Configuration Information API**
  - Retrieve RRSF network configuration information programatically

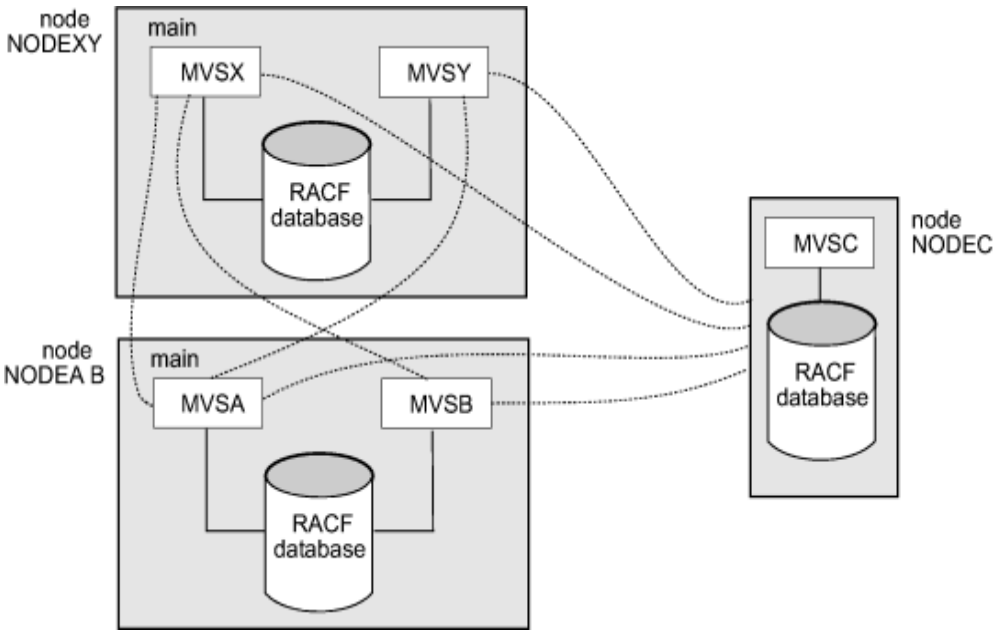
# Overview – The RRSF network

- Consists of **nodes**
  - *Local node: The one I'm logged on to at the moment*
  - *Remote nodes (all the others)*
  - *Local node can run in "local mode", where there are no remote nodes*
- The **TARGET** operator command is used to define, modify, and delete, and list nodes, as well as to de/activate them
- **TARGET** commands are contained within the RACF parameter library, and are executed automatically when the RACF subsystem starts
- The RACF parameter library member is specified in your started procedure JCL
- RACF parameter library members can be "chained together" using the SET INCLUDE(xx) command



# Overview – Multi-System Node (MSN)

- A set of systems sharing a RACF database (can be in a SYSPLEX, or simply on shared DASD)
- Managed with the TARGET command by specifying both NODE and SYSNAME
- All Single System Nodes (SSNs) send requests only to the MAIN system of a MSN
- All peer systems of an MSN send requests only to SSNs, and to the MAIN systems of remote MSNs
- Peer systems do not speak with each other, and non-MAIN systems do not speak with non-MAIN systems of remote MSNs



# RRSF
# Dynamic Main Switch

# Problem: Changing the MAIN system for a MultiSystem Node is, shall we say, complicated

1) Drop TSO/E and JES on the original local main system.
2) On the original local main system, issue the RACF STOP command to stop the RACF subsystem.
3) Make connections dormant:
    1) On the local system that is to be the new main, issue a TARGET DORMANT command for its local connection. Also issue TARGET DORMANT commands to make all connections with remote nodes dormant.
    2) On each remote node, issue TARGET DORMANT commands for the original and new main systems. Do not perform step 7 until the INMSG files for the original and new main systems on each remote node have drained.

    Issue TARGET LIST commands to verify that the INMSG data sets on the local node have been drained before you go on to the next step.
4) If the workspace data sets for the original main system and the new main system are not on shared DASD with a shared catalog, copy the workspace data sets for the original main system to DASD accessible to the new main system, using the same workspace data set names.
5) On the new main system, issue a TARGET MAIN command to make it the main system. If you have not specified the prefixes for the workspace data sets and the LU names for the member systems consistently in the TARGET commands that defined the local multisystem node, this step will fail.
6) Issue the same TARGET MAIN command that you issued in step 5 on each nonmain system on the local multisystem node. Issue this command on the original main system only if it is to remain in the multisystem node.
7) Issue TARGET LIST commands to verify that the INMSG data sets on the remote nodes have been drained before you perform this step. On each remote system (that is, all remote systems of all remote nodes), issue the same TARGET MAIN command that you issued in step 5.
8) On the new main system, issue TARGET OPERATIVE commands to make the connection with itself and all connections with remote nodes operative.
9) On each remote system (that is, all remote systems of all remote nodes), issue TARGET OPERATIVE commands for the original main (if it is to remain in the multisystem node) and new main systems.
10) Update the TARGET commands in the RACF parameter libraries for all systems on all nodes in the RRSF network to reflect the new main system. If you fail to update the RACF parameter library for a system, the next time that system has its RACF subsystem restarted or is IPLed, the original TARGET commands will be issued, and requests and returned output will accumulate in the wrong OUTMSG workspace data set. However, RACF will issue appropriate error messages and prevent communications.
11) If the original main system is still part of the multisystem node, (and assuming that you have updated its RACF parameter library as discussed in step 10) restart the RACF subsystem, TSO/E and JES on the original main system.

# Wouldn't it be nice if instead:

- **From any (uplevel) system in the MSN, issue:**

```
TARGET NODE(this-msn) SYSNAME(new-MAIN) NEWMAIN

IRRM102I SYSTEM new-main IS NOW THE MAIN SYSTEM IN
LOCAL NODE msn-name.
```

- **Optionally harden the change in your RACF parameter library member**
  - if you expect re-IPLs before switching back, or if the change is intended to be long term.

# And if I'm not in a sysplex (sharing with RESERVE/RELEASE), I'd even be happy with:

1) **From the old MAIN system issue:**

```
TARGET NODE(this-msn) SYSNAME(new-MAIN) NEWMAIN
IRRM098I DRAINING SYSTEM OF INBOUND WORK. DO NOT
INITIATE THE MAIN SWITCH ON THE NEW MAIN SYSTEM UNTIL
MESSAGE IRRM099I IS ISSUED.
IRRM099I ALL INBOUND WORK HAS COMPLETED. IT IS NOW SAFE
TO INITIATE THE MAIN SWITCH ON THE NEW MAIN SYSTEM.
```

2) **From the new MAIN system, issue:**

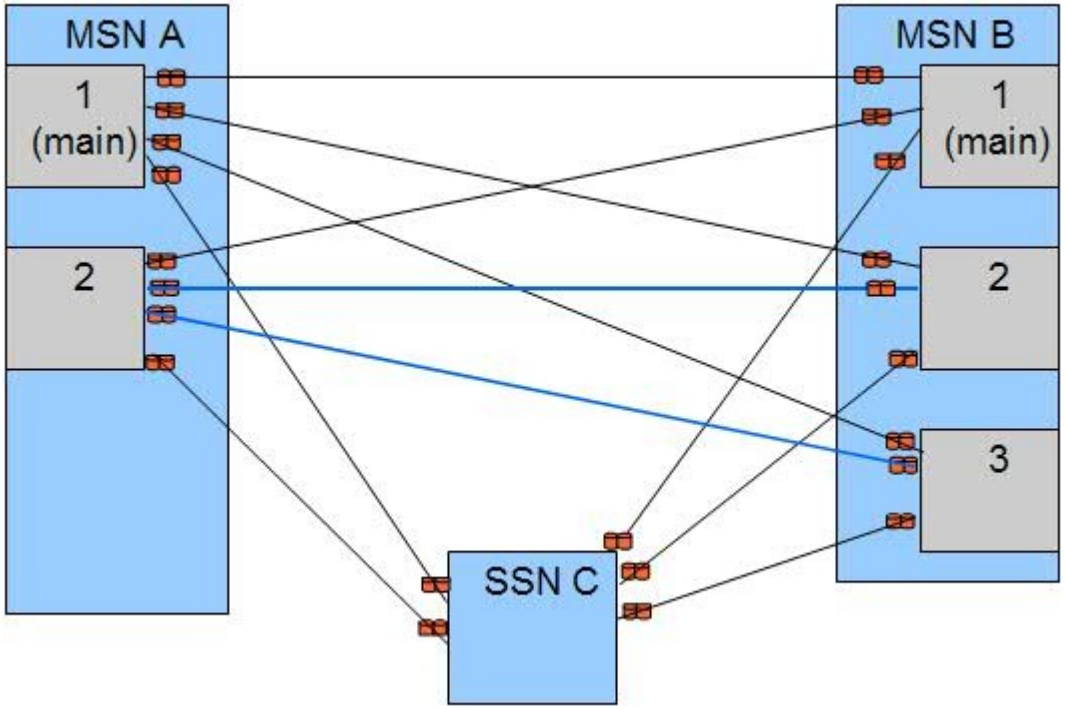
```
TARGET NODE(this-msn) SYSNAME(new-MAIN) NEWMAIN
IRRM102I SYSTEM new-main IS NOW THE MAIN SYSTEM IN
LOCAL NODE msn-name.
```

3) **From the remaining peer systems, issue:**

```
TARGET NODE(this-msn) SYSNAME(new-MAIN) NEWMAIN
```

4) **Optionally harden the change in parmlib.**

# We're changing the model to this:




New SET **FULLRRSFCOMM** enablement options causes TARGET DORMANT and TARGET OPERATIVE to allocate workspace files and establish network connections between remote non-MAIN systems (which currently remain in DEFINED state).

# RACF Remote Sharing Configuration Information API

# R_admin/IRRXUTIL enhancement

- **Active RRSF configuration information can be retrieved with a new R_Admin (IRRSEQ00) function**
  - Function code X'21' - ADMN_XTR_RRSF
  - Output mapping ADMN_XTRSF_MAP
- **The IRRXUTIL REXX interface is likewise enhanced**
  - myrc=IRRXUTIL("EXTRACT","_RRSFEXTR","_RRSFEXTR", "RACF","")
- **Can be useful to report on the active configuration and even for automation**
  - (Note that SYSREXX added console interfaces in V2R1)

# R_admin/IRRXUTIL enhancement

- **Type of information returned:**
  - Subsystem operator command prefix
  - SET AUTODIRECT, AUTOAPPL, AUTOPWD, PWSYNC settings
  - SET FULLRRSFCOMM setting
  - Array of RRSF nodes/systems, where each entry contains the configuration information for that node/system
    - Active state
    - VSAM file names/statistics
    - Protocol listener status for local node
    - Protocol information, including AT-TLS information for TCP
    - Description
  - Index to local node(/system) in array

# RACF Remote Sharing Unidirectional Connections

# RRSF Unidirectional Connections

- **Sometimes sharing is bad:**
  - It is impossible to prevent a privileged user on a test system from escalating his privilege on a production system when they are connected using RRSF. The honor system applies.
- **You can't tell me what to do:**
  - Any RRSF node can define another RRSF node such that inbound requests from that node are to be denied

- Protect against accidental or malicious damage to your production system
- Demonstrate to an auditor your compliance with your security policy, regardless of the configuration established on the remote node

# Defining the Connection

- Use a new TARGET command keyword when defining a remote node

```
TARGET NODE(THATNODE) DENYINBOUND
```

- When the remote node is a multisystem node:

```
TARGET NODE(THATNODE) SYSNAME(*) DENYINBOUND
```

- To change your mind, use **NODENYINBOUND**

- DENYINBOUND is ignored if specified for the LOCAL node

# Indication that your updates are not welcome

- **DENYINBOUND** setting is exchanged during handshaking as a connection is established
- A new message indicates that work is not being accepted from your system

```
IRRI082I (<) ATTENTION: PARTNER NODE IS NOT ACCEPTING INBOUND WORK
       FROM THIS NODE.
IRRI027I (<) RACF COMMUNICATION WITH TCP NODE NODE1 SYSNAME SYS1 HAS
       BEEN SUCCESSFULLY ESTABLISHED USING CIPHER ALGORITHM 35
       TLS_RSA_WITH_AES_256_CBC_SHA.
```

- It is possible for both sides to deny each other. This might still have some value in that OUTPUT/NOTIFY requests can be sent across the connection

# And if I send updates anyway?

- Requests from the remote system will be denied with a message indicating that inbound work is not accepted
  - For RACLINK DEFINE (Note RACLINK APPROVE is OK)

```
IRRP023I RACLINK could not be completed for user IBMUSER
because node NODE1 is not accepting inbound work.
```

  - For directed command (AT/ONLYAT) or automatically directed work

```
IRRT035I Node NODE1 is not accepting work from NODE2.
```

  - A down level system will get rejected, though the message may not be as obvious
- A counter of rejected work from that system will be maintained, and displayed by TARGET LIST
- The counter can be reset with:

```
TARGET NODE(x) SYSNAME(Y) RESETDENYINBOUNDCOUNT
```

# Indication by TARGET LIST

- On the **denied** system:

```
IRRM010I (<) RSWL SUBSYSTEM PROPERTIES OF REMOTE RRSF NODE NODE1
             SYSNAME SYS1 (MAIN):
   STATE       - OPERATIVE ACTIVE
   DESCRIPTION - <NOT SPECIFIED>
   PROTOCOL    - TCP
                 HOST ADDRESS     - ALPS4092.POK.IBM.COM
                 IP ADDRESS       - 9.57.1.93
                 LISTENER PORT    - 18136
                 AT-TLS POLICY:
                   RULE_NAME      - RRSF-CLIENT
                   CIPHER ALG     - 35 TLS_RSA_WITH_AES_256_CBC_SHA
                   CLIENT AUTH    - REQUIRED
   THIS NODE IS NOT ACCEPTING INBOUND WORK
   TIME OF LAST TRANSMISSION TO   - 16:56:50 JAN 23, 2014
...
```

# Indication by TARGET LIST

- On the **denying** system:

```
IRRM010I (<) RSWJ SUBSYSTEM PROPERTIES OF REMOTE RRSF NODE NODE2
             SYSNAME SYS3 (MAIN):
   STATE        - OPERATIVE ACTIVE
   DESCRIPTION  - <NOT SPECIFIED>
   PROTOCOL     - TCP
                  HOST ADDRESS      - ALPS4220.POK.IBM.COM
                  IP ADDRESS        - 9.57.1.221
                  LISTENER PORT     - 18136
                  AT-TLS POLICY:
                    RULE_NAME       - RRSF-CLIENT
                    CIPHER ALG      - 35 TLS_RSA_WITH_AES_256_CBC_SHA
                    CLIENT AUTH     - REQUIRED
   INBOUND WORK IS NOT ACCEPTED FROM THIS NODE
         NUMBER OF REQUESTS DENIED FROM THIS SYSTEM: 4
   TIME OF LAST TRANSMISSION TO    - 17:22:07 JAN 23, 2014
```

# RACF Password Enhancements

# RACF Password Enhancements

- **RACF Password Special Characters**
  - Additional characters now supported for passwords
- **Password Phrase only users**
  - Ability to have a password phrase without a password
- **Expire a password without setting a new password**
  - Ability to expire a password without having to set a new password
- **New Password Encryption option**
  - Optionally encrypt / hash the password and password phrase using a new more modern algorithm

# RACF Password Special Characters

# RACF Password Special character support

- **Support 14 additional characters**
  - Currently, there are 65 possible password characters if mixed-case is in effect
    - 65**8 = 318,644,812,890,625 possible 8-char passwords
  - With the additional 14 characters
    - 79**8 =1,517,108,809,906,561

# RACF Password Special character support

| Symbol | Hexadecimal value* |
|---|---|
| . | 4B |
| < | 4C |
| + | 4E |
| \| | 4F |
| & | 50 |
| ! | 5A |
| * | 5C |
| - | 60 |
| % | 6C |
| _ | 6D |
| > | 6E |
| ? | 6F |
| : | 7A |
| = | 7E |

# Usage & Invocation

- **Enable special characters with:**

  SETROPTS PASSWORD(SPECIALCHARS)

- **Confirm this with SETROPTS LIST:**

```
PASSWORD PROCESSING OPTIONS:
  THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS KDFAES
  PASSWORD CHANGE INTERVAL IS  60 DAYS.
  PASSWORD MINIMUM CHANGE INTERVAL IS   3 DAYS.
  MIXED CASE PASSWORD SUPPORT IS IN EFFECT
  SPECIAL CHARACTERS ARE ALLOWED.
  10 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
  AFTER   5 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
      A USERID WILL BE REVOKED.
  PASSWORD EXPIRATION WARNING LEVEL IS  15 DAYS.
  INSTALLATION PASSWORD SYNTAX RULES:
    RULE 1  LENGTH(8)     xxxxxxxx
   LEGEND:
    A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL *-
ANYTHING
    c-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL $-NATIONAL s-
SPECIAL
    x-MIXED ALL
```

# Usage & Invocation

- **Disable special characters with:**
  - SETROPTS PASSWORD(NOSPECIALCHARS)
  - Confirm this with SETROPTS LIST

    PASSWORD PROCESSING OPTIONS:

    ...

    SPECIAL CHARACTERS ARE NOT ALLOWED.

    ...
- **If the user has special characters in his password when the function is disabled:**
  - The user will always be able to logon with it and change their password (at logon or using the PASSWORD command) on that system

# Password Phrase Only Users

# Usage & Invocation

- Uses existing **NOPASSWORD** keyword of **ADDUSER/ALTUSER**
- It is simply allowed now in cases where it previously wasn't
  - While specifying **PHRASE()**
  - When a phrase exists in the user profile
- Displayed by LISTUSER using existing attributes

```
USER=PHRONLY   NAME=UNKNOWN   OWNER=IBMUSER
CREATED=14.206
DEFAULT-GROUP=SYS1      PASSDATE=N/A     PASS-
INTERVAL= 30 PHRASEDATE=00.000
ATTRIBUTES=NOPASSWORD PASSPHRASE
```

- FLAG7 field in USER profile can now have both bit 0 (no password) and bit 2 (has password phrase) on

# Expire Password
# without setting a password

# Expire a password and phrase without changing it

- Uses existing **EXPIRED** keyword of **ALTUSER**
- When specified without **PASSWORD** and **PHRASE**, sets the changed-dates to 0, thus expiring the password
  - Previously, **EXPIRED** was ignored in this situation
- **Before:**

```
USER=GRONK  NAME=UNKNOWN  OWNER=IBMUSER   CREATED=14.206
DEFAULT-GROUP=SYS1     PASSDATE=14.206 PASS-INTERVAL= 30
PHRASEDATE=14.206
ATTRIBUTES=PASSPHRASE
```

- **Command:**

```
ALTUSER GRONK EXPIRED
```

- **After:**

```
USER=GRONK  NAME=UNKNOWN  OWNER=IBMUSER   CREATED=14.206
 DDEFAULT-GROUP=SYS1     PASSDATE=00.000 PASS-INTERVAL= 30
PHRASEDATE=00.000
 ATTRIBUTES=PASSPHRASE
```

# V2R2 Only Password Enhancements

# V2R2 Only Password Enhancements

- **RACF_ENCRYPTION_ALGORITHM Health Check:**
  - Raises an exception if KDFAES is not active
- **Default Passwords:**
  - Removal of Default Group as Default password:
    - ADDUSER will not assign a default password
    - ALTUSER and PASSWORD can not set a default password
- **RACLINK DEFINE:**
  - Support password phrases
- **ICHDEX01 Password Processing exit:**
  - Not needed unless implementing your own password encryption
  - Absence of ICHDEX01 will default to DES only

# New Password Encryption Algorithm

# New Password Encryption Algorithm Option

- **RACF and Passwords:**
  - Passwords and Password phrases are encrypted / hashed before being stored in the RACF database.
- **DES Algorithm:**
  - Password / Phrase is run though a Key Derivation Function to generate a DES key. The DES key is used to encrypt the USERID.
  - Encrypted password hash can not be decrypted.
  - Passwords are validated by performing the password encryption algorithm on the user provided password and comparing to the encrypted password in the RACF database.
- **Offline database attack:**
  - All password databases should be protected against unauthorized access.
  - An attacker with access to an offline password database may attempt to recover passwords by systematically encrypting a large number of passwords and comparing to the encrypted values in the database.

# New Password Encryption Algorithm

- **Start with:**
  - DES hash for passwords – Maintains upward compatibility
  - Clear-text password phrase
- **Append random text (salt)**
- **Iteratively hash (SHA256) this text a (large) number of times to derive an AES key**
  - This step is intentionally slowing down the encryption process!
- **Encrypt the RACF user ID with the AES key**
- **Results:**
  - 16-byte hash which must be stored with the salt and other information. This no longer fits in PASSWORD field. Extension fields are defined to contain the extra information.

# Enabling the New Algorithm

- **Enable the new algorithm:**

```
SETROPTS PASSWORD(ALGORITHM(KDFAES))
```

  - No ICHDEX01 exit required to enable it!
- **Confirm this with SETROPTS LIST:**

```
PASSWORD PROCESSING OPTIONS:
  THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS KDFAES
  PASSWORD CHANGE INTERVAL IS  60 DAYS.
  PASSWORD MINIMUM CHANGE INTERVAL IS   3 DAYS.
  MIXED CASE PASSWORD SUPPORT IS IN EFFECT
  SPECIAL CHARACTERS ARE ALLOWED.
  10 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
  AFTER   5 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
      A USERID WILL BE REVOKED.
  PASSWORD EXPIRATION WARNING LEVEL IS  15 DAYS.
  INSTALLATION PASSWORD SYNTAX RULES:
    RULE 1  LENGTH(8)     xxxxxxxx
   LEGEND:
    A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL *-
ANYTHING
    c-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL $-NATIONAL s-
SPECIAL
    x-MIXED ALL
```

# Disabling the New Algorithm

- **Enable the new algorithm:**

```
SETROPTS PASSWORD(ALGORITHM(NOALGORITHM))
```

- **Confirm this with SETROPTS LIST:**

```
PASSWORD PROCESSING OPTIONS:
  THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS LEGACY
  PASSWORD CHANGE INTERVAL IS  60 DAYS.
  PASSWORD MINIMUM CHANGE INTERVAL IS   3 DAYS.
  MIXED CASE PASSWORD SUPPORT IS IN EFFECT
  SPECIAL CHARACTERS ARE ALLOWED.
  10 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
  AFTER   5 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
      A USERID WILL BE REVOKED.
  PASSWORD EXPIRATION WARNING LEVEL IS  15 DAYS.
  INSTALLATION PASSWORD SYNTAX RULES:
    RULE 1  LENGTH(8)     xxxxxxxx
   LEGEND:
    A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL *-
ANYTHING
    c-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL $-NATIONAL s-
SPECIAL
    x-MIXED ALL
```

# Transitioning to the new Algorithm

- **KDFAES Active:**
  - New passwords will be encrypted under the active algorithm
  - Existing passwords will be evaluated regardless of their format (except for masking)
  - Same for history, which can contain entries for different formats

- **Nothing gets automatically converted to the new format:**
  - Conversion mechanism is provided:
    - Works only when existing algorithm is **DES**

      (Will otherwise create an unusable password and history)

# Converting Passwords to KDFAES

- Passwords and password history which are **DES** format can be converted directly to **KDFAES**.
- When current algorithm is **KDFAES**:

```
ALTUSER USER1 PWCONVERT
```

  - Converts any legacy passwords and password history entries to KDFAES format
  - **Note:** Password phrases are not converted

- When current algorithm is **NOALGORITHM**:

```
ALTUSER USER1 PWCONVERT
```

  - This indicates that all password history entries and password phrase history entries in **KDFAES** format should be deleted.

# Password History Cleanup

- When the **SETROPTS PASSWORD(HISTORY(n))** value is changed password history entries can be stranded and never be reused.
- Previously the the RACF website provided a utility to clean these old password history values: **CUTPWHIS**

- New password history cleanup method:

```
ALTUSER USER1 PWCLEAN
```

- The new password convert option, **PWCONVERT**, will also perform a **PWCLEAN**

# DBUNLOAD Password Updates

- **DBUNLOAD now displays user password fields:**
  - You can demonstrate to an auditor that passwords and password phrases are encrypted under the new algorithm with the help of new fields created by the IRRDBU00 utility.
  - A sample query is included.
- **Fields:**
  - **USBD_PWD_ALG** - Algorithm used to protect password. Values include “LEGACY”, “KDFAES”, and “NOPASSWORD”.
  - **USBD_LEG_PWDHIST_CT** - Number of legacy password history entries
  - **USBD_XPW_PWDHIST_CT** - Number of non-legacy (e.g. KDFAES) password history entries
  - **USBD_PHR_ALG** - Algorithm used to protect password phrase. Values include “LEGACY”, “KDFAES”, and “NOPHRASE”.
  - **USBD_LEG_PHRHIST_CT** - Number of legacy password phrase history entries
  - **USBD_XPW_PHRHIST_CT** - Number of non-legacy (e.g. KDFAES) password phrase history entries

# RACF Goody Bag

- **Provide some information RACF related items**
- RACF main page
  - http://www-03.ibm.com/systems/z/os/zos/features/racf/
- RACF main page
  - http://www-03.ibm.com/systems/z/os/zos/features/racf/index.html
- RACF what's new – talks briefly about new items. Examples, like information provide in this presentation
  - http://www-03.ibm.com/systems/z/os/zos/features/racf/whatsnew.html
- RACF z/VM
  - http://www-03.ibm.com/systems/z/os/zos/features/racf/vm.html

# z/OS Health Checker Quick Background

- The objective of IBM Health Checker for z/OS is to identify potential problems before they impact your availability or, in worst cases, cause outages. It checks the current active z/OS and sysplex settings and definitions for a system and compares the values to those suggested by IBM or defined by you. It is not meant to be a diagnostic or monitoring tool, but rather a continuously running preventative that finds potential problems. IBM Health Checker for z/OS produces output in the form of detailed messages to let you know of both potential problems and suggested actions to take. Note that these messages do not mean that IBM Health Checker for z/OS has found problems that you need to report to IBM! IBM Health Checker for z/OS output messages simply inform you of potential problems so that you can take action on your installation.
- There are several parts to IBM Health Checker for z/OS:
- The **framework** of the IBM Health Checker for z/OS is the interface that allows you to run and manage checks. The framework is a common and open architecture, supporting check development by IBM, independent software vendors (ISVs), and users.
- Individual **checks** look for component, element, or product specific z/OS settings and definitions, checking for potential problems. The specific component or element owns, delivers, and supports the checks.
- Checks can be either **local**, and run in the IBM Health Checker for z/OS address space, or **remote**, and run in the caller's address space. So far, most IBM checks are local.

# z/OS Health Checker Quick Background

- A check is actually a program or routine that identifies potential problems before they impact your availability or, in worst cases, cause outages. A check is owned, delivered, and supported by the component, element, or product that writes it.
- Checks are separate from the IBM Health Checker for z/OS framework. A check might analyze a configuration in the following ways:
- Changes in settings or configuration values that occur dynamically over the life of an IPL. Checks that look for changes in these values should run periodically to keep the installation aware of changes.
- Threshold levels approaching the upper limits, especially those that might occur gradually or insidiously.
- Single points of failure in a configuration.
- Unhealthy combinations of configurations or values that an installation might not think to check.

# RACF Goody Bag

- **Provide some information RACF related items**
- RACF reporting  RACFICE2 - Security Analysis using RACF Unload Utilities and DFSORT'S ICETOOL by Mark Nelson
  - RACF introduced the RACFICE reports in 'SYS1.SAMPLIB(IRRICE)'. RACFICE used DFSORT's ICETOOL to create a set of 30+ reports based on the output of the RACF Database Unload Utility (IRRDBU00) and the RACF SMF Unload Utility (IRRADU00).
  - Contains reports on the RACF DB as well as violation reporting, etc.
- z/OS migration Guides  - contain information on Security changes for the various releaseses.  Example, the z/OS 1.12 migration guide talked about TRUSTED started tasks having access to resources and not just datasets
  - http://www-03.ibm.com/systems/z/os/zos/library/bkserv/zos_migration_manuals.html
- z/OS release information  - talks about RACF as well as other security updates for that release
  - http://www-03.ibm.com/systems/z/os/zos/
- Resources – to be continued

# RACF Goody Bag

- **Resources**
  - Presentations on RACF and z/OS Security
    - IBMers are often presenting RACF and other security-related topics at conferences. These are the presentation materials from some of our most popular sessions. Samples include:
      - Crypto
      - z/OS Security Server (aka. RACF)
      - Auditing
      - LDAP
      - Communication Server
  - RACF User Groups –
    - http://www-03.ibm.com/systems/z/os/zos/features/racf/ugroups.html
  - RACF on the Road - IBMers are recognized experts on RACF and are often in the field presenting RACF and related security topics
    - http://www-03.ibm.com/systems/z/os/zos/features/racf/road.html

# RACF Goody Bag

- **Resources**
  - Library – contains link to manuals as well as some redbooks
    - http://www-03.ibm.com/systems/z/os/zos/features/racf/library/library.html
  - Education – Current course offerings
    - http://www-03.ibm.com/systems/z/os/zos/features/racf/classes.html
  - History of RACF
    - http://www-03.ibm.com/systems/z/os/zos/features/racf/racfhist.html
  - RACF-L – information on how to sign up for RACF-L - Customers and IBM participants may also discuss RACF on the RACF-L discussion list. RACF-L is not operated or sponsored by IBM, but is run by the University of Georgia.
    - http://www-03.ibm.com/systems/z/os/zos/features/racf/links/racf-l.html

# RACF Goody Bag

- **Downloads**
  - **http://www-03.ibm.com/systems/z/os/zos/features/racf/**
    - **Disclaimers - The software is provided "as-is", and IBM disclaims all warranties, express or implied, including but not limited to implied warranties of merchantibility or fitness for a particular purpose.**
    -
- BPXCHECK - a REXX program which reports on RACF settings related to the assignment of z/OS UNIX UIDs and GIDs (for example, AIM stage, BPX.DEFAULT.USER, BPX.NEXT.USER, BPX.UNIQUE.USER, SHARED.IDS, etc).
- CDT2DYN - a utility to help change installation-defined RACF classes into dynamic classes.
- CUTPWHIS – OBSOLETE
- DBSYNC - a utility which compares two RACF databases and creates the commands to make them similar. Can also assist in merging RACF databases from different systems.
-

# RACF Goody Bag

- **Downloads**
- DBU2MSXL - a set of scripts which loads the output of the RACF Database Unload Utility (IRRDBU00) into Microsoft® Excel spreadsheet.
- DBU2MSAC - a set of scripts which loads the output of the RACF Database Unload Utility (IRRDBU00) into Microsoft Access.
- IRRHFSU - a utility which unloads the UNIX System Services Hierarchical File System file security information in a manner compatible with with IRRDBU00.
- IRRXUTIL, a set of sample REXX programs which illustrate the power of IRRXUTIL, the new REXX interface to the R_admin callable service. IRRXUTIL allows you to extract profile and SETROPTS information from the RACF database using the REXX programming language.
- LISTCDT, a tool which analyzes and reports on your RACF Class Descriptor Table (CDT)

# RACF Goody Bag

- **Resources**
  - z/OS Statement of Integrity
    - http://www-03.ibm.com/systems/z/os/zos/features/racf/zos_integrity_statement.html
  - First issued in 1973, IBM's MVS System Integrity Statement, and subsequent statements for OS/390 and z/OS, has stood for over three decades as a symbol of IBM's confidence in and commitment to the z/OS operating system. IBM reaffirms its commitment to z/OS System Integrity.
  -

# RACF Goody Bag

- **Resources**
  - z/OS Statement of Integrity
  - IBM's commitment includes design and development practices intended to prevent unauthorized application programs, subsystems, and users from bypassing z/OS security – that is, to prevent them from gaining access, circumventing, disabling, altering, or obtaining control of key z/OS system processes and resources unless allowed by the installation. Specifically, z/OS "System Integrity" is defined as the inability of any program not authorized by a mechanism under the installation's control to circumvent or disable store or fetch protection, access a resource protected by the z/OS Security Server (RACF), or obtain control in an authorized state; that is, in supervisor state, with a protection key less than eight (8), or Authorized Program Facility (APF) authorized. In the event that an IBM System Integrity problem is reported, IBM will always take action to resolve it.
  - IBM's long-term commitment to System Integrity is unique in the industry, and forms the basis of z/OS' industry leadership in system security. z/OS is designed to help you protect your system, data, transactions, and applications from accidental or malicious modification. This is one of the many reasons IBM System z remains the industry's premier data server for mission-critical workloads.

# RACF Goody Bag

- **Resources**
  - 
  - Performance
    - http://www-03.ibm.com/systems/z/os/zos/features/racf/racfperf.html
  - UNIX Systems Services
    - http://www-03.ibm.com/systems/z/os/zos/features/racf/secureoe.html
  - Frequently Asked Questions
    - http://www-03.ibm.com/systems/z/os/zos/features/racf/faqs.html
    - 
  - Security Portal - The z Systems Security Portal is intended to help you stay current with security and system integrity fixes by providing current patch data and now also provides Associated Common Vulnerability Scoring System (CVSS) V2 ratings for new APARs.
    - http://www-03.ibm.com/systems/z/solutions/security_subintegrity.html
    - 

# z/OS Health Checker - RACF

# Heath Check RACF_AIM_STAGE

- The RACF_AIM_STAGE check examines the RACF database application identity mapping (AIM) to see whether it is at AIM stage 3, which is recommended. Your system programmer can convert your RACF database to AIM stage 3 using the IRRIRA00 conversion utility.

- **Reason for check:**
- AIM stage 3 allows RACF to more efficiently handle authentication and authorization requests from applications such as z/OS UNIX and is required to use some RACF function. You should assign a unique UNIX UID for each user and a unique GID for each group that needs access to z/OS UNIX functions and resources. Assigning unique IDs rather than shared IDs improves overall security and increases user accountability. However, if you have a large number of users without OMVS segments who need access to z/OS UNIX services, such as FTP, you might choose not to assign UNIX identities in advance of their need to use the services. In these cases, when your RACF database has been converted to AIM stage 3, you can enable RACF to automatically assign unique UNIX UIDs and GIDs at the time they are needed.

# z/OS Health Checker Checks

| NAME | CheckOwner | State | Status | Result |
|---|---|---|---|---|
| RACF_AIM_STAGE | IBMRACF | ACTIVE(ENABLED) | EXCEPTION-MEDIUM | 8 |
| RACF_FACILITY_ACTIVE | IBMRACF | ACTIVE(ENABLED) | SUCCESSFUL | 0 |
| RACF_GRS_RNL | IBMRACF | ACTIVE(ENABLED) | SUCCESSFUL | 0 |
| RACF_IBMUSER_REVOKED | IBMRACF | ACTIVE(ENABLED) | EXCEPTION-MEDIUM | 8 |
| RACF_ICHAUTAB_NONLPA | IBMRACF | ACTIVE(ENABLED) | SUCCESSFUL | 0 |
| RACF_OPERCMDS_ACTIVE | IBMRACF | ACTIVE(ENABLED) | SUCCESSFUL | 0 |
| RACF_SENSITIVE_RESOURCES | IBMRACF | ACTIVE(ENABLED) | EXCEPTION-HIGH | 12 |
| RACF_TAPEVOL_ACTIVE | IBMRACF | ACTIVE(ENABLED) | EXCEPTION-MEDIUM | 8 |
| RACF_TEMPDSN_ACTIVE | IBMRACF | ACTIVE(ENABLED) | EXCEPTION-MEDIUM | 8 |
| RACF_TSOAUTH_ACTIVE | IBMRACF | ACTIVE(ENABLED) | SUCCESSFUL | 0 |
| RACF_UNIX_ID | IBMRACF | ACTIVE(ENABLED) | EXCEPTION-MEDIUM | 8 |
| RACF_UNIXPRIV_ACTIVE | IBMRACF | ACTIVE(ENABLED) | EXCEPTION-MEDIUM | 8 |
| ZOSMIGV2R1_DEFAULT_UNIX_ID | IBMRACF | INACTIVE(ENABLED) | INACTIVE | 0 |

# z/OS Health Checker Checks

| NAME | Severity | SevCode | WTOType | ModifiedBy |
|---|---|---|---|---|
| RACF_AIM_STAGE | MEDIUM | 8 | EVENTUAL | |
| RACF_FACILITY_ACTIVE | MEDIUM | 8 | EVENTUAL | |
| RACF_GRS_RNL | HIGH | 12 | CRITICAL | |
| RACF_IBMUSER_REVOKED | MEDIUM | 8 | EVENTUAL | |
| RACF_ICHAUTAB_NONLPA | MEDIUM | 8 | EVENTUAL | |
| RACF_OPERCMDS_ACTIVE | MEDIUM | 8 | EVENTUAL | |
| RACF_SENSITIVE_RESOURCES | HIGH | 12 | CRITICAL | |
| RACF_TAPEVOL_ACTIVE | MEDIUM | 8 | EVENTUAL | |
| RACF_TEMPDSN_ACTIVE | MEDIUM | 8 | EVENTUAL | |
| RACF_TSOAUTH_ACTIVE | MEDIUM | 8 | EVENTUAL | |
| RACF_UNIX_ID | MEDIUM | 8 | EVENTUAL | |
| RACF_UNIXPRIV_ACTIVE | MEDIUM | 8 | EVENTUAL | |
| ZOSMIGV2R1_DEFAULT_UNIX_ID | LOW | 4 | INFO | |

# z/OS Health Checker Checks

| NAME | Reason |
|---|---|
| RACF_AIM_STAGE | AIM Stage 3 is suggested. |
| RACF_FACILITY_ACTIVE | IBM recommends activating this class |
| RACF_GRS_RNL | None of the RACF ENQ names should be in RNLs. |
| RACF_IBMUSER_REVOKED | IBMUSER should be revoked. |
| RACF_ICHAUTAB_NONLPA | ICHAUTAB entries must be protected. |
| RACF_OPERCMDS_ACTIVE | IBM recommends activating this class |
| RACF_SENSITIVE_RESOURCES | Sensitive resources should be protected. |
| RACF_TAPEVOL_ACTIVE | IBM recommends activating this class |
| RACF_TEMPDSN_ACTIVE | IBM recommends activating this class |
| RACF_TSOAUTH_ACTIVE | IBM recommends activating this class |
| RACF_UNIX_ID | Unique UNIX identities are recommended. |
| RACF_UNIXPRIV_ACTIVE | IBM recommends activating this class |
| ZOSMIGV2R1_DEFAULT_UNIX_ID | Migration check for BPX.DEFAULT.USER removal. |

# Health Checks: RACF_AIM_STAGE (OK)

```
  Display  Filter  View  Print  Options  Search  Help
 -------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY RACF_AIM_STAGE               LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                          SCROLL ===> HALF
********************************* TOP OF DATA ***********************************
CHECK(IBMRACF,RACF_AIM_STAGE)
START TIME: 05/11/2012 14:36:29.892717
CHECK DATE: 20110101  CHECK SEVERITY: MEDIUM

IRRH500I The RACF database is at the suggested stage of application
identity mapping (AIM). The database is at AIM stage 03.

END TIME: 05/11/2012 14:36:29.893680  STATUS: SUCCESSFUL
******************************** BOTTOM OF DATA ********************************
```

# Health Checks: RACF_AIM_STAGE (Exception)

```
CHECK(IBMRACF,RACF_AIM_STAGE)
START TIME: 10/02/2013 19:20:50.635255
CHECK DATE: 20110101  CHECK SEVERITY: MEDIUM

* Medium Severity Exception *

IRRH501E The RACF database is not at the suggested stage of application
identity mapping (AIM). The database is at AIM stage 00.

  Explanation:  The RACF_AIM_STAGE check has determined that the RACF
    database is not at the suggested stage of application identity
    mapping (AIM). Your system programmer can convert your RACF database
    using the IRRIRA00 conversion utility. See z/OS Security Server RACF
    System  Programmer's Guide for information about running the
    IRRIRA00 conversion utility.

    Stage 3 of application identity mapping allows RACF to more
    efficiently handle authentication and authorization requests from
    applications such as z/OS UNIX and is required to use some RACF
    function. You should assign a unique UNIX UID for each user and a
    unique GID for each group that needs access to z/OS UNIX functions
    and resources. Assigning unique IDs rather than shared IDs improves
```

# Health Checks: RACF_AIM_STAGE (Exception)

overall security and increases user accountability. However, if you have a large number of users without OMVS segments who need access to z/OS UNIX services, such as FTP, you might choose not to assign UNIX identities in advance of their need to use the services. In these cases, when your RACF database has been converted to AIM stage 3, you can enable RACF to automatically assign unique UNIX UIDs and GIDs at the time they are needed. See z/OS Security Server RACF Security Administrator's Guide for information about enabling RACF for automatic assignment of unique UNIX identities.

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

Operator Response: Report this problem to the system security administrator.

System Programmer Response: If you want to use RACF function such as support for automatically assigning unique UNIX UIDs and GIDs at the time that they are needed, run the IRRIRA00 utility to advance the RACF database to application identity mapping stage 3. For details about using the IRRIRA00 utility, see z/OS Security Server RACF System Programmer's Guide.

# Heath Check RACF Classes

- Each of the following checks are made to see if the following RACF classes are active

- RACF_FACILITY_ACTIVE
- RACF_OPERCMDS_ACTIVE
- RACF_TAPEVOL_ACTIVE
- RACF_TEMPDSN_ACTIVE
- RACF_TSOAUTH_ACTIVE
- RACF_UNIXPRIV_ACTIVE

- **Reason for check:**
- An effective RACF implementation requires that the baseline group of RACF general resource classes listed above be active.

# Heath Check RACF_FACILTY_ACTIVE

```
CHECK(IBMRACF,RACF_FACILITY_ACTIVE)
START TIME: 10/02/2013 19:20:50.636493
CHECK DATE: 20051111  CHECK SEVERITY: MEDIUM
CHECK PARM: FACILITY


IRRH228I The class FACILITY is active.
```

# Heath Check RACF_OPERCMDS_ACTIVE

```
CHECK(IBMRACF,RACF_OPERCMDS_ACTIVE)
START TIME: 10/02/2013 19:20:50.636545
CHECK DATE: 20051111  CHECK SEVERITY: MEDIUM
CHECK PARM: OPERCMDS

IRRH228I The class OPERCMDS is active.
```

# Heath Check RACF_TAPEVOL_ACTIVE

```
CHECK(IBMRACF,RACF_TAPEVOL_ACTIVE)
START TIME: 10/02/2013 19:20:50.636204
CHECK DATE: 20051111  CHECK SEVERITY: MEDIUM
CHECK PARM: TAPEVOL


* Medium Severity Exception *

IRRH229E The class TAPEVOL is not active.

  Explanation:  The class is not active. IBM recommends that the
    security administrator evaluate the need for this class, define
    profiles in it as appropriate, and activate the class.

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

  Operator Response:  Report this problem to the system security
    administrator and the system auditor.
```

# Heath Check RACF_TEMPDSN_ACTIVE

```
CHECK(IBMRACF,RACF_TEMPDSN_ACTIVE)
START TIME: 10/02/2013 19:20:50.637580
CHECK DATE: 20051111  CHECK SEVERITY: MEDIUM
CHECK PARM: TEMPDSN


* Medium Severity Exception *

IRRH229E The class TEMPDSN is not active.

  Explanation:  The class is not active. IBM recommends that the
    security administrator evaluate the need for this class, define
    profiles in it as appropriate, and activate the class.

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

  Operator Response:  Report this problem to the system security
    administrator and the system auditor.
```

# Heath Check RACF_TSOAUTH_ACTIVE

```
CHECK(IBMRACF,RACF_TSOAUTH_ACTIVE)
START TIME: 10/02/2013 19:20:50.637524
CHECK DATE: 20051111  CHECK SEVERITY: MEDIUM
CHECK PARM: TSOAUTH

IRRH228I The class TSOAUTH is active.
```

# Heath Check RACF_UNIXPRIV_ACTIVE

```
CHECK(IBMRACF,RACF_UNIXPRIV_ACTIVE)
START TIME: 10/02/2013 19:20:50.636060
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 evaluate the need for this class, define
    profiles in it as appropriate, and activate the class.

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

  Operator Response:  Report this problem to the system security
    administrator and the system auditor.
```

# Heath Check RACF_GRS_RNL

- Check evaluates whether the RACF ENQ names are in either the installation system exclusion resource name list (SERNL) or the system inclusion resource name list (SIRNL).
- During its normal course of processing, RACF performs numerous serialization requests using the Global Resource Serialization (GRS) RESERVE, ENQ, and DEQ services. These serialization requests allow RACF to ensure that changes to the RACF database and RACF control blocks are done in a consistent manner, maintaining the integrity of RACF data.

- **Reason for check:**
- Installations that convert RACF SYSTEM ENQs to SYSTEM ENQs can corrupt the RACF data base and experience outages.

# Heath Check RACF_GRS_RNL

```
CHECK(IBMRACF,RACF_GRS_RNL)
START TIME: 10/02/2013 19:20:50.638135
CHECK DATE: 20040703  CHECK SEVERITY: HIGH

                          RACF_GRS_RNL Report

S Major    Minor                 Type  QName    Rname              Type
- -------- -------------------- ----- -------- ---------------- ----

IRRH203I No RACF ENQ names were found in the GRS Resource Name List.
```

# Heath Check RACF_IBMUSER_REVOKED

- Check looks to see if the IBMUSER user ID is still active.

- **Reason for check:**
- The IBMUSER user ID is intended for use only during the initial installation process. After installation, the IBMUSER user ID should be revoked so that it cannot be used by unauthorized users.

# Heath Check RACF_IBMUSER_REVOKED

```
CHECK(IBMRACF,RACF_IBMUSER_REVOKED)
START TIME: 10/02/2013 19:20:50.637729
CHECK DATE: 20051111  CHECK SEVERITY: MEDIUM

* Medium Severity Exception *

IRRH225E The user ID IBMUSER is not revoked.

  Explanation:  The user ID IBMUSER has not been revoked. IBM recommends
    revoking IBMUSER.

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

  Operator Response:  Report this problem to the system security
    administrator and the system auditor.

  System Programmer Response:  Revoke IBMUSER.

  Problem Determination:  See the RACF Auditor's Guide and the RACF
    System Programmer's Guide.
```

# Heath Check RACF_ICHAUTHAB_NONLPA

- The RACF_ICHAUTAB_NONLPA check examines the RACF Authorized Caller Table (ICHAUTAB) and reports if there are any non-LPA entries in it. The output format is similar to the report format for the ICHAUTAB Report in RACF_SENSITIVE_RESOURCES, with the exception that LPA-resident modules are not listed.

- **Reason for check:**
- IBM recommends that installations have no entries in the ICHAUTAB table.

# Heath Check RACF_ICHAUTHAB_NONLPA

```
CHECK(IBMRACF,RACF_ICHAUTAB_NONLPA)
START TIME: 10/02/2013 19:20:50.635676
CHECK DATE: 20070411  CHECK SEVERITY: MEDIUM

                          ICHAUTAB Non-LPA Report

S Module   REQUEST= REQUEST= Location
           VERIFY   LIST
- -------- -------- -------- --------

IRRH239I There are no ICHAUTAB programs on this system.
```

# Heath Check RACF_SENSITIVE_RESOURCES

- The RACF_SENSITIVE_RESOURCES check examines the security characteristics of several system-critical data sets and general resources other than data sets. The output of this check is a list of exceptions flagged.
- For each of these, the check examines:
- For system-critical data sets, that the data set exists on the expected volume. If the data set does not exist on the volume, a V (volume exception) is placed in the Status (S) column.
- That the resource has baseline protection. For example, APF data sets can have a general access as high as READ, while the data sets which comprise the RACF data base must have a general access of NONE.
- **Reason for check:**
- The system is critically exposed if these resources are not properly protected.

# Heath Check RACF_SENSITIVE_RESOURCES

```
CHECK(IBMRACF,RACF_SENSITIVE_RESOURCES)
START TIME: 10/02/2013 19:20:50.637942
CHECK DATE: 20040703  CHECK SEVERITY: HIGH

                                APF Dataset Report

S Data Set Name                                    Vol    UACC Warn ID*  User
- ----------------------------------------------- ------ ---- ---- ---- ----
E ADB710.SADBLINK                                  VTUT8A
E ADB720.SADBLINK                                  VTUT9A
V ALLSTAR.PROD.LOAD                                VPWK01
V ANF.SANFLOAD                                     VTMVSC
V AOP.SAOPLOAD                                     VTMVSC
E APM110.SFBIAUTH                                  VTAPMA
E ASN710.SASNALNK                                  VTD71A
E ASN710.SASNLLNK                                  VTD71A
E ATH220.SATHLOAD                                  VTATHC
E ATH310.SATHLOAD                                  VTATHD
  BJT.V2R3M0.SBJTLOAD                              VPWK05 Read No   ****
E BJT.V3R1M0.SBJTLOAD                              VPWK06 Altr No   ****
E BJT.V3R1M0.SBJTLPA                               VPWK06 Altr No   ****
  CAN390.BASE.RKANMOD                              VPCANA Read No   ****
```

# Heath Check RACF_SENSITIVE_RESOURCES

RACF Dataset Report

| S | Data Set Name | Vol | UACC | Warn | ID* | User |
|---|---|---|---|---|---|---|
| E | SYS1.RACFPRM1 | VPWK04 | Read | No | **** | |
| E | SYS1.RACFBCK1 | VPWK05 | Read | No | **** | |

PARMLIB Dataset Report

| S | Data Set Name | Vol | UACC | Warn | ID* | User |
|---|---|---|---|---|---|---|
| E | LVL0.PARMLIB | VTLVL0 | | | | |
| E | SVTSC.PARMLIB | VTMVSG | | | | |
| | SYS1.PARMLIB | VIMVSB | None | No | None | |
| | VENDOR.PARMLIB | VPMVSD | Read | No | **** | |

# Heath Check RACF_SENSITIVE_RESOURCES

Current Link List Dataset Report

| S | Data Set Name | Vol | UACC | Warn | ID* | User |
|---|---|---|---|---|---|---|
| E | ADB710.SADBLINK | VTUT8A | | | | |
| | CAN390.S0W1.RKANMOD | VPCANA | Read | No | **** | |
| | CAN390.TKANMOD | VTCANA | Read | No | **** | |
| E | CBC.SCCNCMP | VTMVSC | | | | |
| E | CBC.SCLBDLL | VTMVSC | | | | |
| E | CBC.SCLBDLL2 | VTMVSC | | | | |
| E | CEE.SCEERUN | VTMVSC | | | | |
| E | CEE.SCEERUN2 | VTMVSC | | | | |
| E | CICSTS22.CICS.SDFHLINK | VTTS2A | | | | |
| E | CICSTS22.CPSM.SEYULINK | VTTS2A | | | | |
| E | CKR.V210.SCKRLOAD | VPWK09 | Altr | No | **** | |
| E | CKR.V210.SC4RLNK | VPWK08 | Altr | No | **** | |
| E | CSF.SCSFMOD0 | VTMVSC | | | | |
| E | DCF140.DCFLOAD | VTDCFA | | | | |
| E | DIT130.SDITMOD1 | VTDITA | | | | |

# Heath Check RACF_SENSITIVE_RESOURCES

System Rexx Dataset Report

| S | Data Set Name | Vol | UACC | Warn | ID* | User |
|---|---|---|---|---|---|---|
| | SYS1.SAXREXEC | VTMVSC | Read | No | **** | |
| | VENDOR.REXXLIB | VPWK09 | Read | No | **** | |

Sensitive General Resources Report

| S | Resource Name | Class | UACC | Warn | ID* | User |
|---|---|---|---|---|---|---|
| | BPX.DAEMON | FACILITY | None | No | **** | |
| E | BPX.FILEATTR.APF | FACILITY | None | No | Read | |
| | BPX.FILEATTR.PROGCTL | FACILITY | None | No | **** | |
| | BPX.SERVER | FACILITY | None | No | **** | |
| | BPX.SUPERUSER | FACILITY | None | No | **** | |
| | ICHBLP | FACILITY | | | | |
| | IRR.PASSWORD.RESET | FACILITY | None | No | **** | |
| E | MVS.SET.PROG | OPERCMDS | Ctrl | No | **** | |
| E | MVS.SETPROG | OPERCMDS | Ctrl | No | **** | |
| | ACCT | TSOAUTH | None | No | **** | |
| | CONSOLE | TSOAUTH | None | No | **** | |
| | OPER | TSOAUTH | None | No | **** | |

# Heath Check RACF_SENSITIVE_RESOURCES

```
* High Severity Exception *

IRRH204E The RACF_SENSITIVE_RESOURCES check has found one or
more potential errors in the security controls on this system.

  Explanation:  The RACF security configuration check has found one or
    more potential errors with the system protection mechanisms.

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

  Operator Response:  Report this problem to the system security
    administrator and the system auditor.

  System Programmer Response:  Examine the report that was produced by
    the RACF check. Any data set which has an "E" in the "S" (Status)
    column has excessive authority allowed to the data set. That
    authority may come from a universal access (UACC) or ID(*) access
    list entry which is too permissive, or if the profile is in WARNING
    mode. If there is no profile, then PROTECTALL(FAIL) is not in
    effect. Any data set which has a "V" in the "S" (Status) field is
    not on the indicated volume. Remove these data sets from the list or
    allocate the data sets on the volume. If this is not an SMS data
```

# Heath Check RACF_SENSITIVE_RESOURCES

set, it may have been migrated. Any data set which has an "M" in the "S" (Status) field has been migrated. Any data set which has a "U" in the "S" (Status) field has not been checked, because the dataset was in use by another user.

The CSV_APF_EXISTS check provides additional analysis of the non-RACF aspects of your APF list.

If the "S" field contains an "E" or is blank, then blanks in the UACC, WARN, and ID(*) columns indicate that there is no RACF profile protecting the data set. Data sets which do not have a RACF profile are flagged as exceptions, unless SETROPTS PROTECTALL(FAIL) is in effect for the system.

If a valid user ID was specified as a parameter to the check, that user's authority to the data set is checked. If the user has an excessive authority to the data set, that is indicated in the USER column. For example, if the user has ALTER authority to an APF-authorized data set, the USER column contains ">Read" to indicate that the user has more than READ authority to the data set.

# Heath Check RACF_SENSITIVE_RESOURCES

```
Problem Determination:  See the RACF System Programmer's Guide and the
  RACF Auditor's Guide for information on the proper controls for your
  system.

Source:
  RACF System Programmer's Guide
  RACF Auditor's Guide

Reference Documentation:
  RACF System Programmer's Guide
  RACF Auditor's Guide

Automation:  None.

Check Reason:  Sensitive resources should be protected.
```

# Health Checks: New and Updated Checks

- **RACF is planning on shipping these new checks in z/OS V2.1:**
  - RACF_AIM_STAGE
  - RACF_UNIX_ID
  - RACF_CERTIFICATE_EXPIRATION
- **RACF_AIM_STAGE and RACF_UNIX_ID are intended to assist you in migrating from BPX.DEFAULT.USER, which, as announced, is being withdrawn with z/OS V2.1**
  - These two checks rolled back to z/OS V1.12 and z/OS V1.13 with OA37164
- **Automatic start for the Health Checker address space at IPL time**

# Health Checks: RACF_AIM_STAGE

- **The RACF_AIM_STAGE Health Check examines your application identity mapping (AIM) setting and flags as an exception if you are at a stage less than stage 3.**
  - Stage 0: No AIM support; only mapping profiles are used
  - Stage 1: Mapping profiles are used; alternate index created and managed, but not used
  - Stage 2: Alternate index create, managed, and used; mapping profiles maintained.
  - Stage 3: Only alternate index maintained and used. Mapping profiles deleted.
- **Moving from each stage requires the execution of the IRRIRA00 utility.**
- **AIM stage 2 or stage 3 is needed for certain RACF functions**

# Health Checks: RACF_AIM_STAGE

- z/OS V1R13 is the last release that supports default UNIX identities implemented using the BPX.DEFAULT.USER profile in the FACILITY class. To replace this function you can do one of the following:
- Use the replacement BPX.UNIQUE.USER profile function provided in z/OS R11 to enable RACF to automatically generate unique UIDs and GIDs.
- Define OMVS segments for all users and groups who require UNIX services. The RACF_UNIX_ID check detects whether RACF is enabled to perform the best practice of automatically assigning unique UNIX identities when users without OMVS segments access the system to use UNIX services. This determination is based on whether the BPX.UNIQUE.USER and BPX.DEFAULT.USER profiles are defined in the FACILITY class.

- **Reason for check:**
- IBM recommends that a unique UNIX UID be assigned to each user and that a unique GID be assigned to each group that needs access to z/OS UNIX functions and resources. Assigning unique identities, rather than shared identities, improves overall security and increases user accountability.

# Health Checks: RACF_UNIX_ID

- **The RACF_UNIX_ID Health Check determines whether RACF will automatically assign unique z/OS UNIX System Services identities when users without OMVS segments use certain UNIX services**
  - If you are not relying on RACF to assign UIDs and GIDs, the check informs you that you must continue to assign z/OS UNIX identities
  - If you are relying on the BPX.DEFAULT.USER support, the check issues an exception
  - If you are relying on the BPX.UNIQUE.USER support, the check will verify requirements and indicate if any exceptions are found
    - FACILITY class profile BPX.UNIQUE.USER must exist
    - RACF database must be at Application Identity Mapping (AIM) stage 3
    - UNIXPRIV class profile SHARED.IDS must be defined
    - UNIXPRIV class must be active and RACLISTed
    - FACILITY class profile BPX.NEXT.USER must be defined and its APPLDATA field must contain valid ID values or ranges

# Health Checks: RACF_UNIX_ID (OK)

# Health Checks: RACF_UNIX_ID (OK)

```
********************************* TOP OF DATA **********************************
CHECK(IBMRACF,RACF_UNIX_ID)
START TIME: 05/18/2012 14:12:18.914396
CHECK DATE: 20110101  CHECK SEVERITY: MEDIUM

IRRH502I RACF attempts to assign unique UNIX IDs when users or groups
that do not have OMVS segments use certain z/OS UNIX services.

Requirements for this support:

S Requirement
- -----------------------------------------------------------------
  FACILITY class profile BPX.UNIQUE.USER is defined
  RACF database is at the required AIM stage:
    AIM stage = 03
  UNIXPRIV class profile SHARED.IDS is defined
  UNIXPRIV class is active
  UNIXPRIV class is RACLISTed
  FACILITY class profile BPX.NEXT.USER is defined
  BPX.NEXT.USER profile APPLDATA is specified (not verified):
    APPLDATA = 1000/100

IRRH506I The RACF UNIX identity check has detected no exceptions.

END TIME: 05/18/2012 14:12:18.921241  STATUS: SUCCESSFUL
```

# Health Checks: RACF_UNIX_ID (Exception)

```
   Display  Filter  View  Print  Options  Search  Help
 ------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY RACF_UNIX_ID                  LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                            SCROLL ===> HALF
******************************** TOP OF DATA ********************************
CHECK(IBMRACF,RACF_UNIX_ID)
START TIME: 05/17/2012 16:45:01.400010
CHECK DATE: 20110101  CHECK SEVERITY: MEDIUM

IRRH502I RACF attempts to assign unique UNIX IDs when users or groups
that do not have OMVS segments use certain z/OS UNIX services.

Requirements for this support:

S Requirement
- ---------------------------------------------------------------------
  FACILITY class profile BPX.UNIQUE.USER is defined
E RACF database is not at the required AIM stage:
    AIM stage = 00
E UNIXPRIV class profile SHARED.IDS is not defined
E UNIXPRIV class is not active
E UNIXPRIV class is not RACLISTed
E FACILITY class profile BPX.NEXT.USER is not defined

* Medium Severity Exception *

IRRH503E RACF cannot assign unique UNIX IDs when users or groups that
do not have OMVS segments use certain z/OS UNIX services. One or more
requirements are not satisfied.

  Explanation:  The RACF UNIX identity check has determined that you
    want RACF to assign unique UNIX IDs when users or groups without
    OMVS segments use certain z/OS UNIX services. However, RACF is not
    able to assign unique UNIX identities for z/OS UNIX services because
    one or more of the following requirements are not satisfied:
```

# Health Checks: RACF_UNIX_ID (Exception)

```
********************************* TOP OF DATA ***********************************
CHECK(IBMRACF,RACF_UNIX_ID)
START TIME: 05/18/2012 14:22:52.066301
CHECK DATE: 20110101  CHECK SEVERITY: MEDIUM

* Medium Severity Exception *

IRRH505E The BPX.DEFAULT.USER profile in the FACILITY class
indicates that you want RACF to assign shared default UNIX
IDs when users or groups that do not have OMVS segments use
certain z/OS UNIX services.

  Explanation:  The RACF UNIX identity check has found the
    BPX.DEFAULT.USER profile in the FACILITY class. The presence of this
    profile indicates an intent to have RACF assign shared default UNIX
    UIDs and GIDs when users without OMVS segments access the system to
    use certain UNIX services.
  Reference Documentation:
    z/OS Security Server RACF Security Administrator's Guide

  Automation:  None.

  Check Reason:  Unique UNIX identities are recommended.

END TIME: 05/18/2012 14:22:52.067783  STATUS: EXCEPTION-MED
```

# Health Checks: RACF_CERTIFICATE_EXPIRATION

- **The RACF_CERTIFICATE_EXPIRATION health check finds the certificates in the RACF database expired or about to expire**
  - Expiration window is an installation-defined value with a default of 60 days.
  - Valid expiration window values are 0-366 days
- **For each certificate, the check displays:**
  - The certificate “owner” ('SITE', 'CERTAUTH', or 'ID(*user_id*)')
  - The certificate label
  - The end date
  - The trust status
  - The number of rings to which the certificate is connected
- **The check only flags as exceptions those certificates which are TRUSTED.**

# Health Checks: RACF_CERTIFICATE_EXPIRATION (OK)

```
CHECK(IBMRACF,RACF_CERTIFICATE_EXPIRATION)
START TIME: 01/23/2012 08:10:01.603497
CHECK DATE: 20111010  CHECK SEVERITY: MEDIUM



                  Certificates Expiring in 60 Days



S Cert Owner   Certificate Label                End Date   Trust Rings
- ------------ -------------------------------- ---------- ----- -----



IRRH277I No exceptions are detected. Expired certificates that are not
trusted or are associated with only a virtual key ring are not
exceptions.



END TIME: 01/23/2012 08:10:01.643285  STATUS: SUCCESSFUL
```

# Health Checks: RACF_CERTIFICATE_EXPIRATION (Exception)

```
CHECK(IBMRACF,RACF_CERTIFICATE_EXPIRATION)
START TIME: 02/28/2013 09:23:37.747549
CHECK DATE: 20111010  CHECK SEVERITY: MEDIUM

                  Certificates Expiring within 60 Days

S Cert Owner    Certificate Label                 End Date   Trust Rings
- ------------ -------------------------------- ---------- ----- -----
E CERTAUTH      VERISIGN CLASS 1 INDIVIDUAL      2008-05-12 Yes     0
E ID(MARKN)     MARK-001                         2012-11-11 Yes     0
E ID(MARKN)     MARK0001                         2012-11-05 Yes     0
  ID(CERTAUTH) START_OFF_M001__END_OFF_M001      2012-01-25 No      0
  ID(MARKN)     START_OFF_M001__END_OFF_M001      2012-01-25 No      0
  ID(SITE)      START_OFF_M001__END_OFF_M001      2012-01-25 No      0
  CERTAUTH      START_OFF_M365__END_OFF_M001      2012-01-25 No      0
  ID(CERTAUTH) START_OFF_M365__END_OFF_M001      2012-01-25 No      0
  CERTAUTH      ICP-Brasil CA                     2011-11-30 No      0
  CERTAUTH      MICROSOFT ROOT AUTHORITY - 01     2002-12-31 No      0
  CERTAUTH      VERISIGN CLASS 3 PUBLIC           2004-01-07 No      0
  CERTAUTH      VERISIGN CLASS 2 PUBLIC           2004-01-06 No      0

* Medium Severity Exception *

IRRH276E One or more certificates expired or are expiring within
the warning period.

  Explanation:  The RACF_CERTIFICATE_EXPIRATION check found one or more
    certificates that expired or are expiring within the warning period.
```

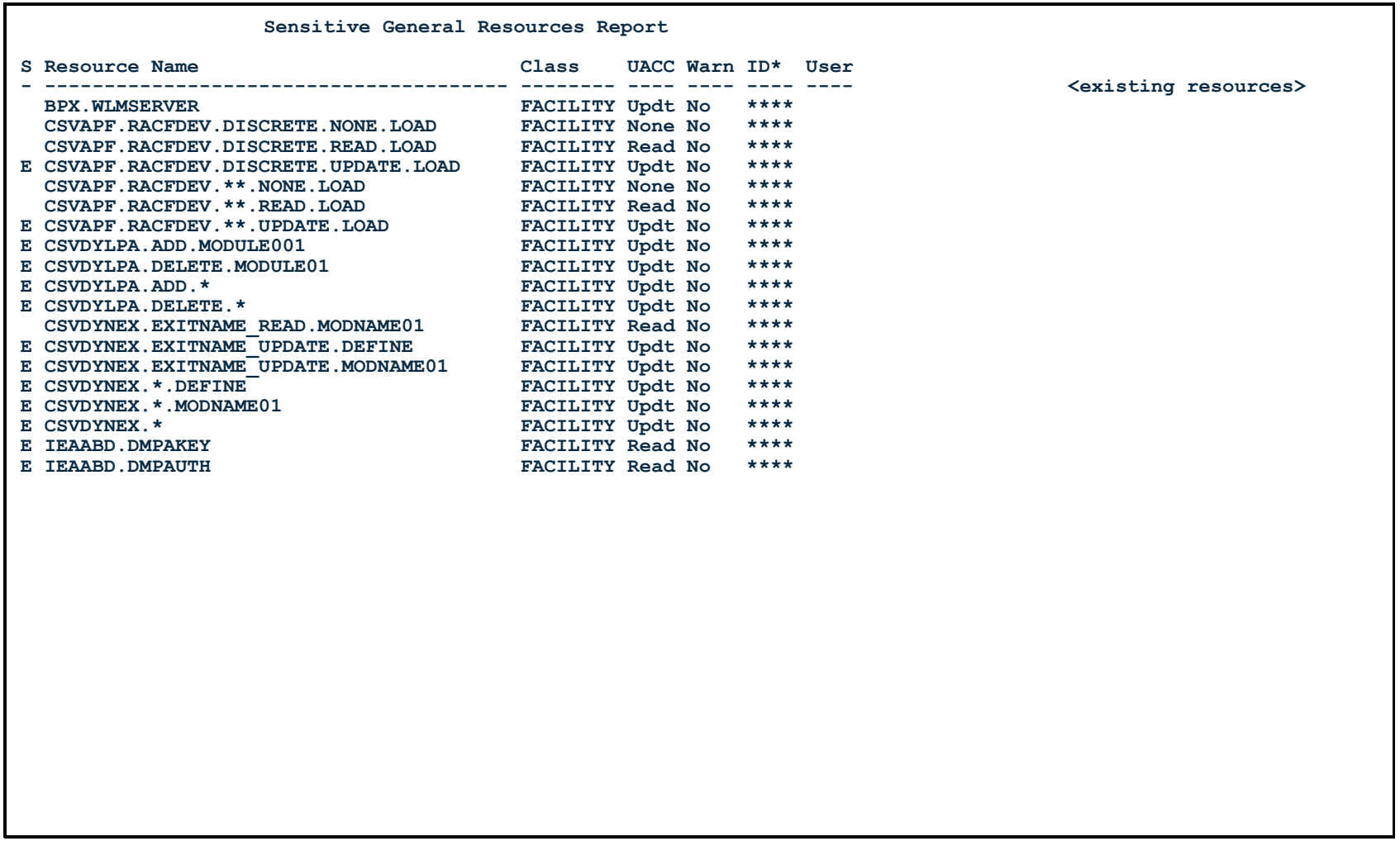
# Health Checks: RACF_CERTIFICATE_EXPIRATION (Exception)

```
  The RACF_CERTIFICATE_EXPIRATION check lists each certificate that
  has an ending date prior to the current date or that has an ending
  date that is prior to the current date adjusted by the warning
  period that the installation has specified as a parameter to the
  RACF_CERTIFICATE_EXPIRATION check. If a parameter is not specified,
  a default warning period of 60 days is used.

  Only certificates that are marked as trusted result in exceptions.
  These certificates have an "E" in the "S" (Status) column. The trust
  status of the certificate is shown in the "Trust" column. The number
  of key rings to which the certificate is connected (other than the
  virtual key ring) is shown in the "Rings" column.

  Use the RACDCERT LIST command to list complete information about any
  certificate. The RACDCERT command syntax is:

          RACDCERT CERTAUTH     LIST(LABEL('label-name'))
                                 or
          RACDCERT SITE         LIST(LABEL('label-name'))
                                 or
          RACDCERT ID(user-id)  LIST(LABEL('label-name'))


  See z/OS Security Server RACF Security Administrator's Guide and the
  z/OS Security Server RACF Command Language Reference for more
  information about digital certificates.

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

# Health Checks: RACF_SENSITIVE_RESOURCES

- **The RACF_SENSITIVE_RESOURCES check has been updated to check these new "static" resources names:**
  - BPX.DEBUG/FACILITY
  - BPX.WLMSERVER/FACILITY
  - IEAABD.DMPAKEY/FACILITY
  - MVS.SLIP/OPERCMDS
  - SUPERUSER.PROCESS.GETPSENT/UNIXPRIV
  - SUPERUSER.PROCESS.KILL/UNIXPRIV
  - SUPERUSER.PROCESS.PTRACE/UNIXPRIV

# Health Checks: RACF_SENSITIVE_RESOURCES



Sensitive General Resources Report

| S | Resource Name | Class | UACC | Warn | ID* | User | |
|---|---|---|---|---|---|---|---|
| - | ---------- | -------- | ---- | ---- | ---- | ---- | <existing resources> |
| | BPX.WLMSERVER | FACILITY | Updt | No | **** | | |
| | CSVAPF.RACFDEV.DISCRETE.NONE.LOAD | FACILITY | None | No | **** | | |
| | CSVAPF.RACFDEV.DISCRETE.READ.LOAD | FACILITY | Read | No | **** | | |
| E | CSVAPF.RACFDEV.DISCRETE.UPDATE.LOAD | FACILITY | Updt | No | **** | | |
| | CSVAPF.RACFDEV.**.NONE.LOAD | FACILITY | None | No | **** | | |
| | CSVAPF.RACFDEV.**.READ.LOAD | FACILITY | Read | No | **** | | |
| E | CSVAPF.RACFDEV.**.UPDATE.LOAD | FACILITY | Updt | No | **** | | |
| E | CSVDYLPA.ADD.MODULE001 | FACILITY | Updt | No | **** | | |
| E | CSVDYLPA.DELETE.MODULE01 | FACILITY | Updt | No | **** | | |
| E | CSVDYLPA.ADD.* | FACILITY | Updt | No | **** | | |
| E | CSVDYLPA.DELETE.* | FACILITY | Updt | No | **** | | |
| | CSVDYNEX.EXITNAME_READ.MODNAME01 | FACILITY | Read | No | **** | | |
| E | CSVDYNEX.EXITNAME_UPDATE.DEFINE | FACILITY | Updt | No | **** | | |
| E | CSVDYNEX.EXITNAME_UPDATE.MODNAME01 | FACILITY | Updt | No | **** | | |
| E | CSVDYNEX.*.DEFINE | FACILITY | Updt | No | **** | | |
| E | CSVDYNEX.*.MODNAME01 | FACILITY | Updt | No | **** | | |
| E | CSVDYNEX.* | FACILITY | Updt | No | **** | | |
| E | IEAABD.DMPAKEY | FACILITY | Read | No | **** | | |
| E | IEAABD.DMPAUTH | FACILITY | Read | No | **** | | |

# Health Checks: ZOSMIGV1R13_DEFAULT_UNIX_ID

- This check determines whether a client is relying on RACF to assign default z/OS UNIX identities for users without OMVS segments who are accessing UNIX services. IBM recommends that a unique UNIX UID be assigned to each user and that a unique GID be assigned to each group that needs access to z/OS UNIX functions and resources.
- Starting with z/OS V1R13, support for the default UNIX identity, implemented using the BPX.DEFAULT.USER profile in the FACILITY class, is no longer available, so a migration action may be required if you are using it. The need for a migration action is based on whether the BPX.UNIQUE.USER and BPX.DEFAULT.USER profiles are defined in the FACILITY class.

# Health Checks: ZOSMIGV1R13_DEFAULT_UNIX_ID

```
   Display  Filter  View  Print  Options  Search  Help
 -------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY ZOSMIGV2R1_DEFAULT_UNIX_ID    LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                           SCROLL ===> HALF
********************************* TOP OF DATA ***********************************
CHECK(IBMRACF,ZOSMIGV2R1_DEFAULT_UNIX_ID)
START TIME: 05/11/2012 14:38:04.920543
CHECK DATE: 20110101  CHECK SEVERITY: LOW

IRRH504I RACF is not enabled to assign UNIX IDs when users or groups
that do not have OMVS segments use certain z/OS UNIX services. If you
choose not to define UNIX IDs for each user of UNIX functions, you can
enable RACF to automatically generate unique UNIX UIDs and GIDs for you.

END TIME: 05/11/2012 14:38:04.921996  STATUS: SUCCESSFUL
******************************** BOTTOM OF DATA *********************************
```

- **This is a migration check!**
  - Note the name: ZOSMIGV2R1.....This check is to prepare you to identify issues when you migrate to z/OS V2.1
  - Shipped INACTIVE;  you activate when you start your V2.1 migration planning

# RACF Goody Bag

- **Resources**
  - 
  - More to come .....
  - 
  - Other ideas .....
  - 
    - 

# Questions?

# Thank You