RACF, VSAM and the Path to an Encrypted RACF Database

Mark Nelson, CISSP®, CSSLP®

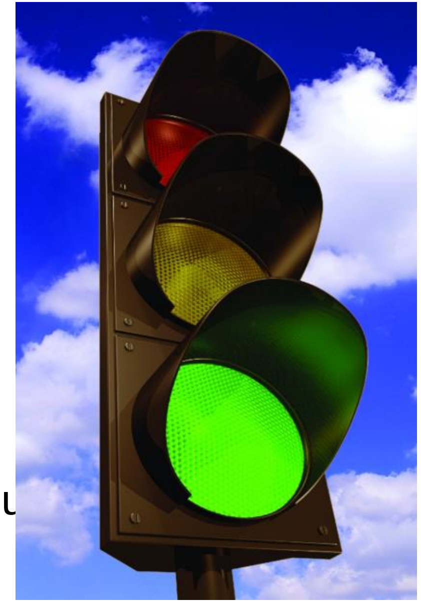
z/OS Security Server (RACF®) Design and Development
markan@us.ibm.com
IBM® Poughkeepsie

14 October 2021

RACF DB Statement of Direction

Encrypted VSAM data set support in RACF

> “IBM intends to enhance pervasive encryption through RACF support for the use of an encrypted VSAM data set as its data base in specific configurations.”



For V2R5, the “specific configuration” is:

- Non-shared (may be on a device marked as shared)
- Single RACF data set
  - May have both a primary and a backup RACF data set
- Running in application identity mapping (AIM stage 3)
- That is free from internal errors (IRRUT200 and IRRDBU00 run withou error)
- Non-SMS managed (which means not encrypted)
- Not in RACF sysplex communications mode or RACF data sharing mode

Why VSAM?

- **RACF's use of VSAM:**
  - Enables future data set encryption
    - Modifications are required to support encryption early in the IPL
  - Allows the use of a VSAM data set in a manner which integrates well with RACF's existing serialization
  - Is consistent with RACF's current database architecture
    - Converting RACF relative byte addresses to VSAM record numbers is
  - Provides the ability to utilize existing diagnostics
  - Leverages standard z/OS skills
  - Leverages current and future I/O infrastructure improvements

Changes with a RACF VSAM Data Set

- **No change to the RACF programming interfaces (RACROUTE, ICHEINTY, RACF Callable Services, IRRXUTIL, RACF commands)**

- **No changes to the RACF serialization structure (major names of SYSZRACF, SYSZRACn)**
    - But there is a new SYSVSAM ENQ.

- **Applications which read the RACF data base directly *__may__* have actions to take to support VSAM**
    - Disclosed at the vendor disclosure meeting in April 2020 and September 2020 and through ICN 1775 (18 August, 2020)

Migrating to a RACF VSAM DATA SET

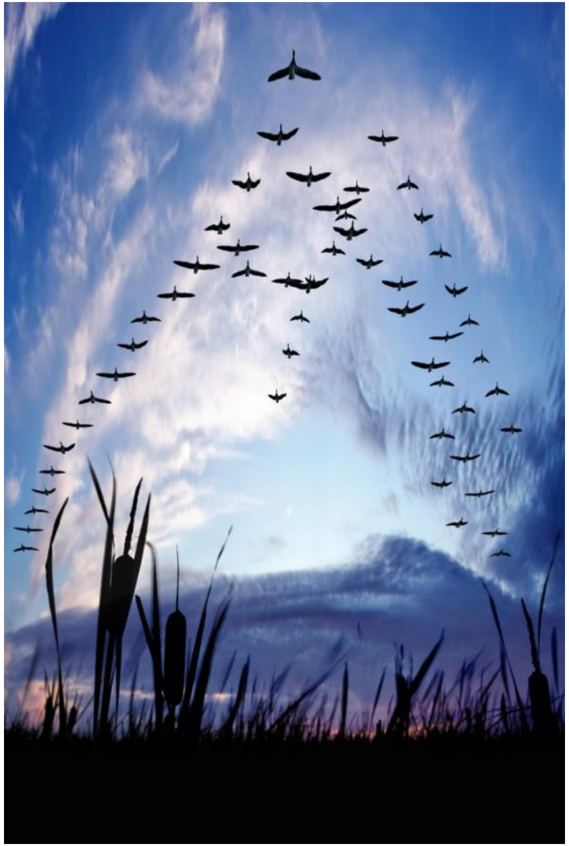
Recommended Migration Path

- **Migration risk can be minimized by:**
  - Migrating your backup data set to VSAM
  - Running with the VSAM backup data set for a period of time
  - Using RVARY SWITCH and RVARY ACTIVATE to make your VSAM data set your primary and your non-VSAM your backup data set
  - Running with the RACF VSAM primary data set and non-VSAM backup
  - Migrating your backup data set to VSAM

Migrating to a RACF VSAM Data Set…

- **There are two migration paths to a RACF data set:**
  - A. With an IPL
  - B. Without an IPL

- **Migrating With an IPL (During a quiesced time with few/no RACF data base updates):**
  1. Create VSAM data set to be the backup RACF VSAM data set
  2. Prepare a new ICHRDSNT or IRRPRMxx member which points to the new VSAM backup data set
  3. Use IRRUT200/IRRUT400 to copy into the new VSAM backup RACF data set
  4. IPL with the new ICHRDSNT or IRRPRMxx PARMLIB



Migrating to a RACF VSAM Data Set…

- **Migrating without an IPL:**
    1. Create a VSAM data set to be the new RACF VSAM backup data set
    2. Inactivate the current backup data set
    3. Copy the primary RACF data set to the VSAM data set using IRRUT200, PARM=RENAMEACTIVATE(archive-dsn)

IRRUT200: RENAMEACTIVATE

- **With z/OS V2R5, IRRUT200 introduces PARM=RENAMEACTIVATE(*dsn*) which:**
  - Renames the current inactive backup data set to *dsn*
    - We call this the “archive” data set
  - Renames the SYSUT1 data set to the *inactive backup data set name*
  - Copies the SYSRACF data set to the inactive backup data set
  - Activates the backup data set

- **Used in the migration from a non-VSAM RACF data set to a VSAM RACF data set**

- **RENAMEACTIVATE** can be used with both non-VSAM and VSAM data sets

Migrating to a RACF VSAM Data Set…

- **Note that there are three data sets involved in the IRRUT200 PARM=RENAMEACTIVATE(*dsn*) processing:**
  - The live primary RACF data set (SYSRACF)
  - The inactivated backup data set (specified in the DSNT/PARMLIB)
  - The target of the copy operation data set (SYSUT1)
- **PARM=RENAMEACTIVATE performs these steps:**
  - Renames the current inactive backup RACF data to *dsn.* We call this the “archive” data set
  - Renames the SYSUT1 data set to RACF backup data set name
  - Copies the live primary RACF data set (SYSRACF) to the RACF backup data set name
  - RVARY ACTIVEs the backup RACF data set

Migrating to a RACF VSAM Data Set…

- **IRRUT200 PARM=RENAMEACTIVATE(*dsn*) requires that:**
  - The primary RACF data set (SYSRACF), the SYSUT1 data set (VSAM data set), and the ”archive” data set (dsn) must be covered by a generic data set profile
    - If not, the utility terminates with a return code of 12 and no processing is performed.

- **If an error occurs during the copy part of the process (which is after the renaming) , IRRUT200 renames the data sets back to the original names**

Example: Migrating the Backup Data Set

- **Starting point:**
  - **Primary RACF Data Set:** RACF.PRIM
  - **Backup: RACF Data Set:** RACF.BACK
  - **VSAM Data Set:** RACF.BACK.VSAM
  - **Target Name for Existing Backup Data Set:** RACF.BACK.OLD

- **IRRUT200 JCL:**

```
//IRRUT200 EXEC PGM=IRRUT200,
//         PARM=RENAMEACTIVATE('RACF.BACK.OLD')
//SYSPRINT DD  SYSOUT=*
//SYSRACF  DD  DISP=SHR,DSN=RACF.PRIM
//SYSUT1   DD  DISP=SHR,DSN=RACF.BACK.VSAM
//SYSUT2   DD  SYSOUT=*
//SYSIN    DD  *
 INDEX FORMAT
 MAP ALL
 END
/*
```

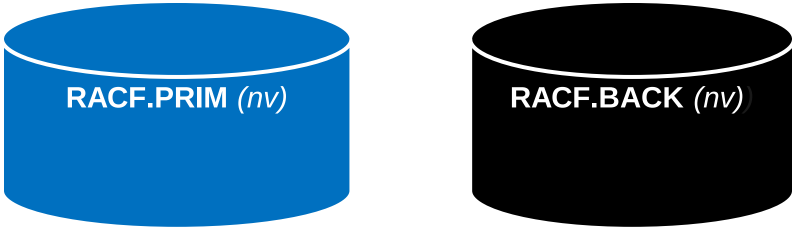
Migration Starting Point

ICHRDSNT/PARMLIB

- **P:RACF.PRIM(nv)**
- **B:RACF.BACK(nv)**

Active Primary

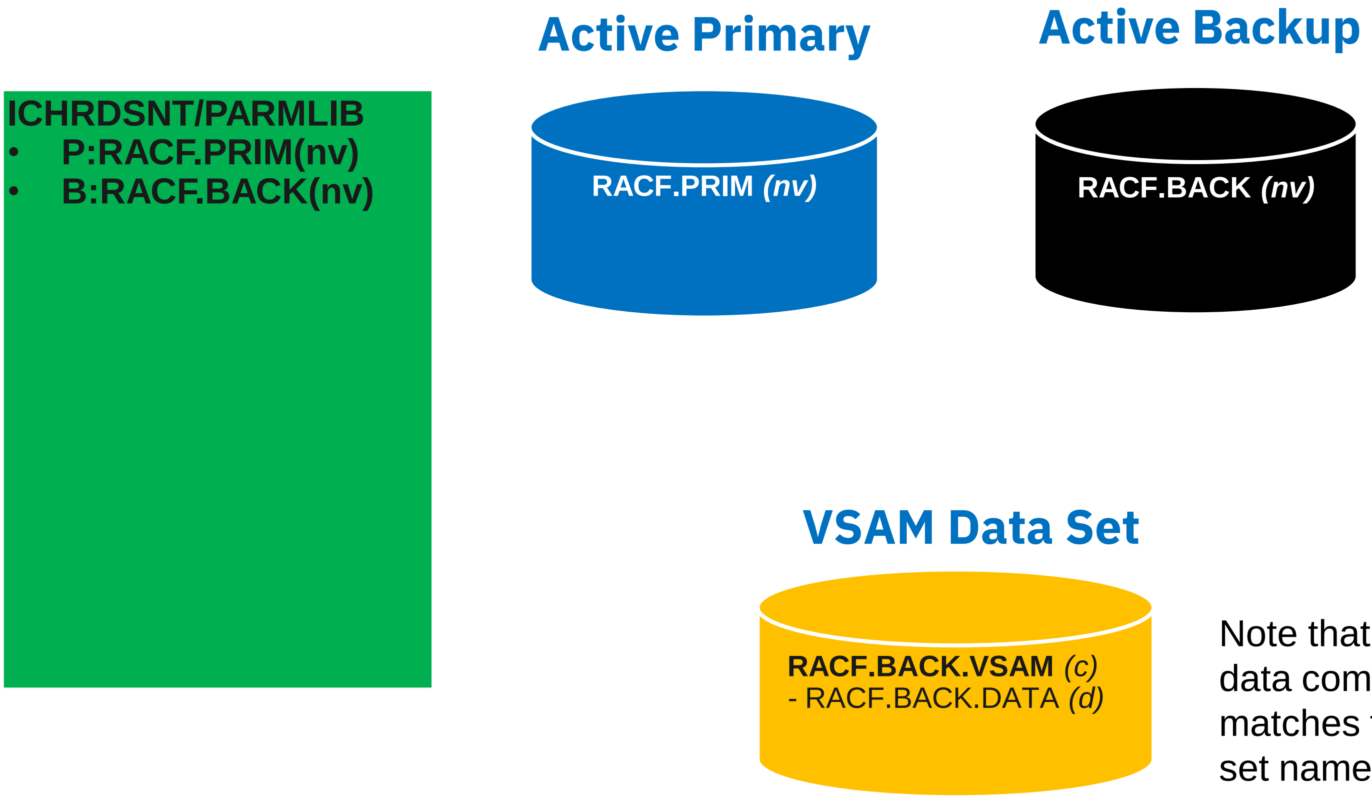
Active Backup



RACF.PRIM *(nv)*

RACF.BACK *(nv)*

Step 1: Create a VSAM Data Set



ICHRDSNT/PARMLIB

- P:RACF.PRIM(nv)
- B:RACF.BACK(nv)

Active Primary

RACF.PRIM *(nv)*

Active Backup

RACF.BACK *(nv)*

VSAM Data Set

RACF.BACK.VSAM *(c)*
- RACF.BACK.DATA *(d)*

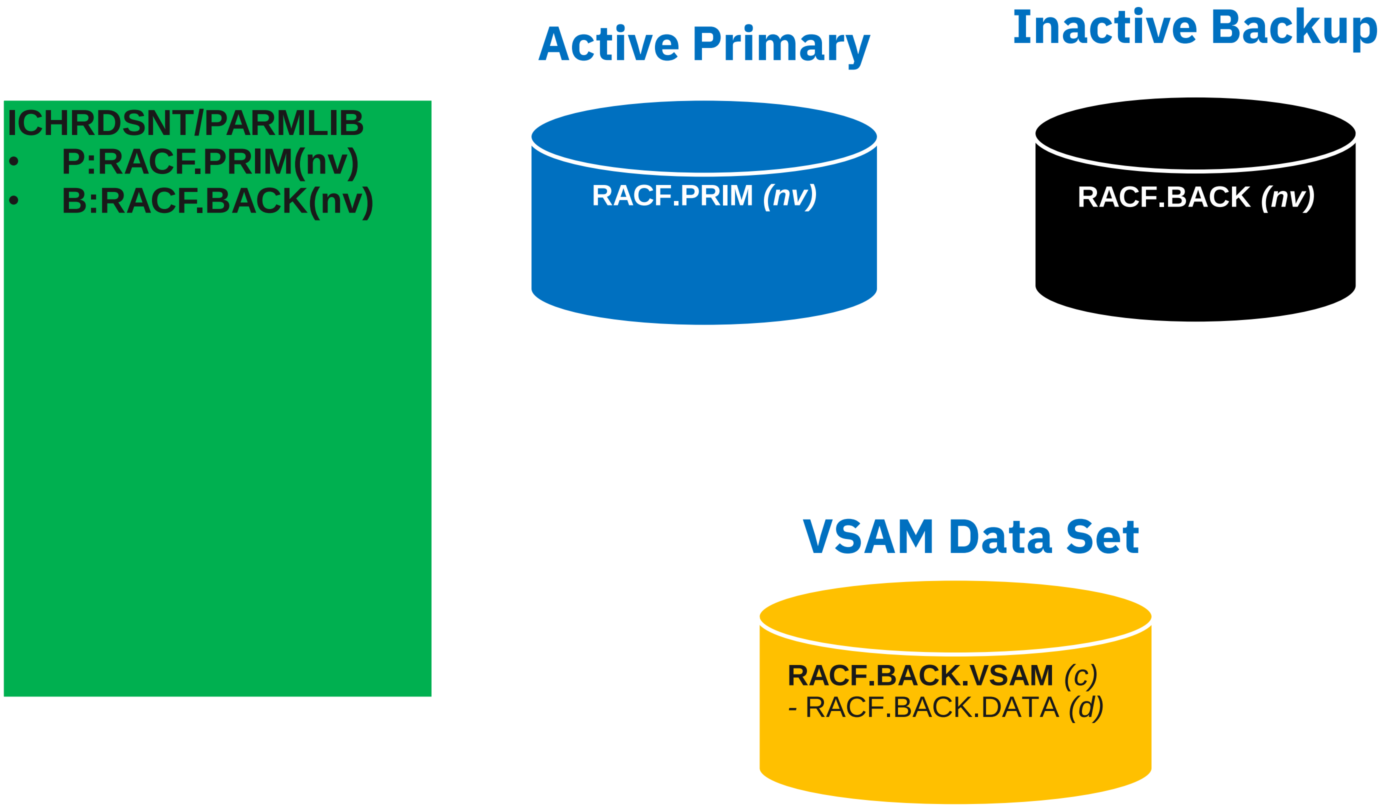
Note that the selected data component name matches the backup data set name

Step 1: Create a VSAM Data Set

- **RACF VSAM Data Set Creation using IDCAMS JCL:**

```
//DEFVSAM JOB ,'DEFINE VSAM RACF DS',
// MSGLEVEL=(1,1),TYPRUN=HOLD
//IDCAMS EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
DEFINE CLUSTER (NAME('RACF.BACK.VSAM’)
   LINEAR
   NONSPANNED
   ERASE
   REUSE
   SHAREOPTIONS(3,3)
   VOLUMES(TEMP02))
DATA (
   NAME('RACF.BACK.DATA’)
   CISZ(4096)
   CYLINDERS(8 0)
   FREESPACE(0 0))   )
/*
```

Step 2: RVARY INACT the Backup Data Set



ICHRDSNT/PARMLIB

- **P:RACF.PRIM(nv)**
- **B:RACF.BACK(nv)**

Active Primary

RACF.PRIM *(nv)*

Inactive Backup

RACF.BACK *(nv)*

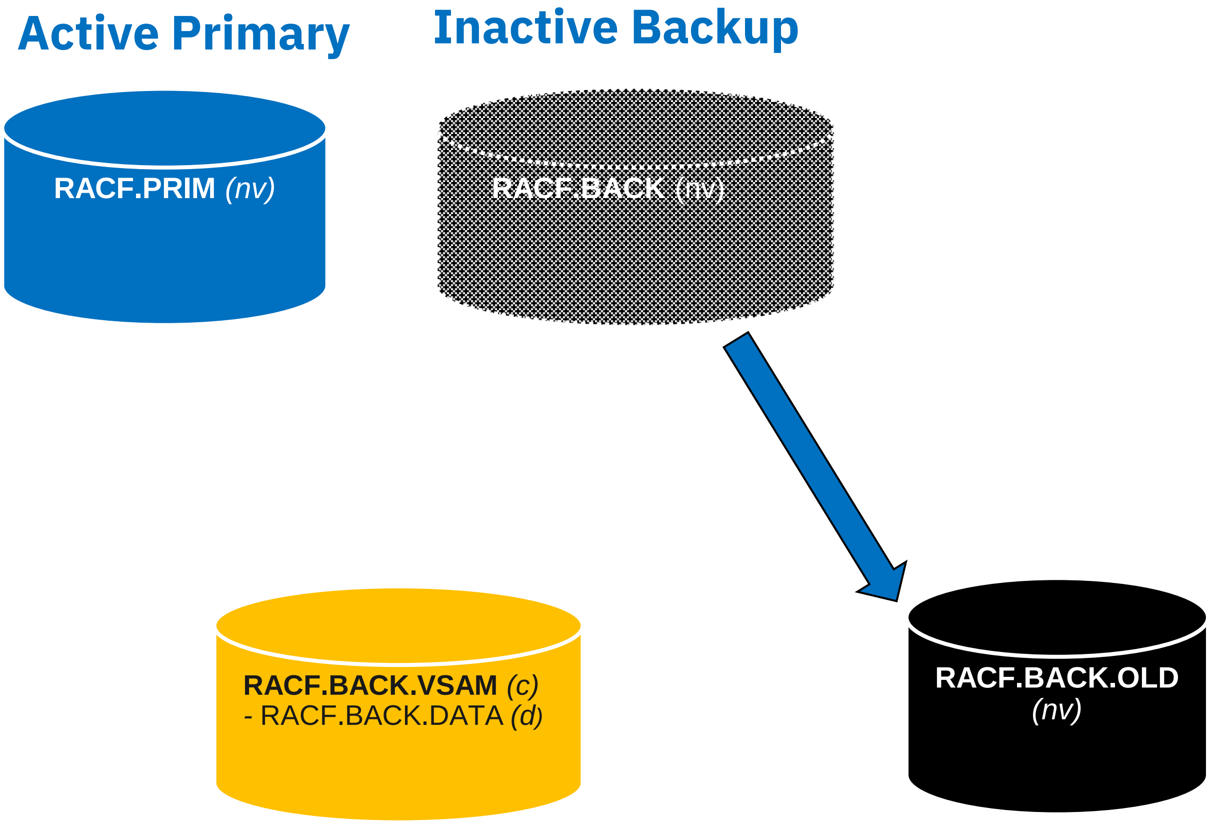
VSAM Data Set

RACF.BACK.VSAM *(c)*
- RACF.BACK.DATA *(d)*

Step 3: RENAMEACTIVATE - First Rename

ICHRDSNT/PARMLIB

- **P:RACF.PRIM(nv)**
- **B:RACF.BACK(nv)**



Active Primary

Inactive Backup

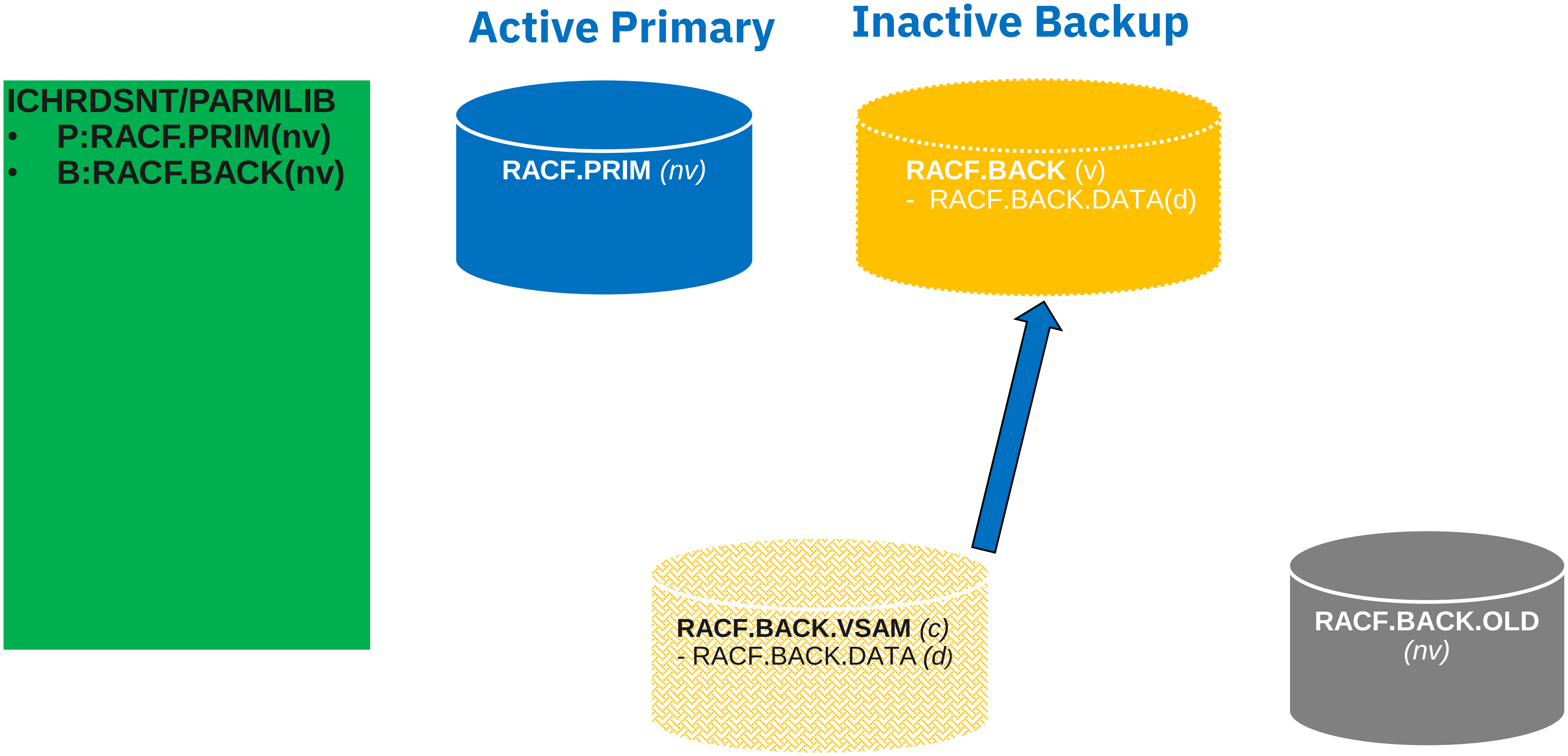
RACF.PRIM *(nv)*

RACF.BACK *(nv)*

RACF.BACK.VSAM *(c)*
- RACF.BACK.DATA *(d)*

RACF.BACK.OLD
(nv)

RENAMEACTIVATE - Second Rename



ICHRDSNT/PARMLIB

- **P:RACF.PRIM(nv)**
- **B:RACF.BACK(nv)**

Active Primary

RACF.PRIM *(nv)*

Inactive Backup

RACF.BACK (v)
- RACF.BACK.DATA(d)

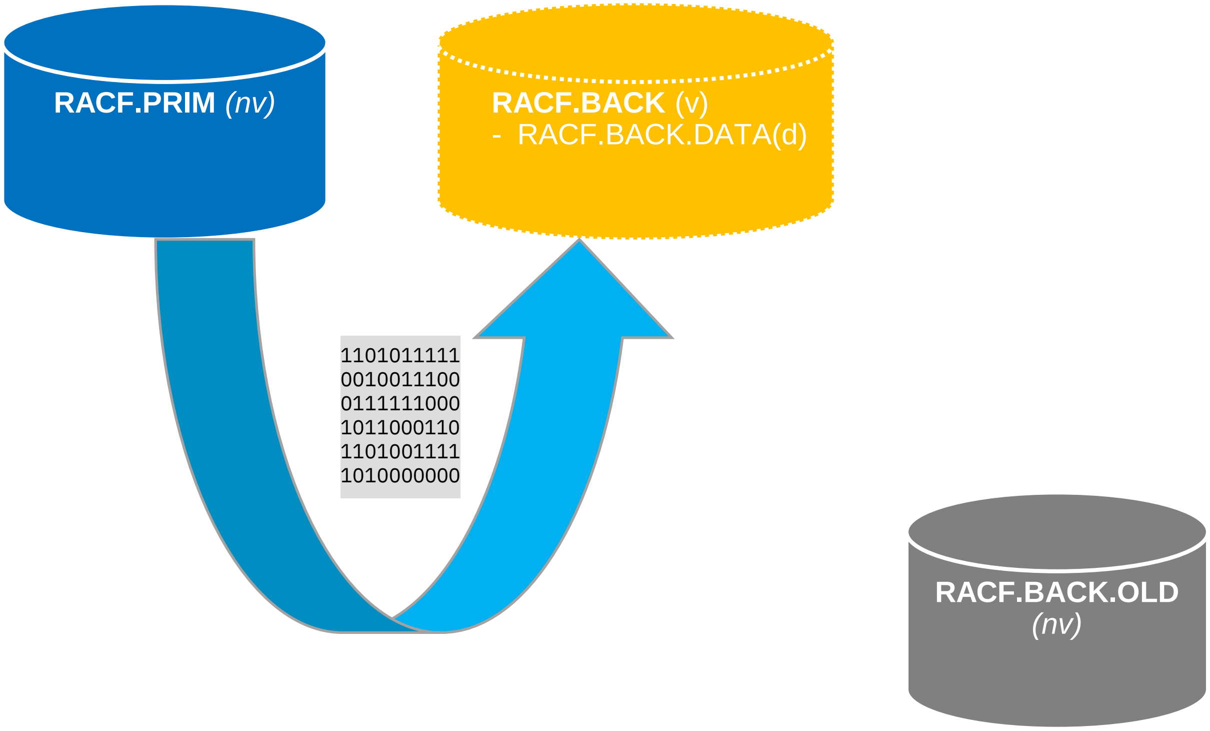
RACF.BACK.VSAM *(c)*
- RACF.BACK.DATA *(d)*

RACF.BACK.OLD
(nv)

RENAMEACTIVATE: Copy Process

ICHRDSNT/PARMLIB

- **P:RACF.PRIM(nv)**
- **B:RACF.BACK(nv)**



Active Primary

Inactive Backup

RACF.PRIM *(nv)*

RACF.BACK (v)
- RACF.BACK.DATA(d)

1101011111
0010011100
0111111000
1011000110
1101001111
1010000000

RACF.BACK.OLD
(nv)

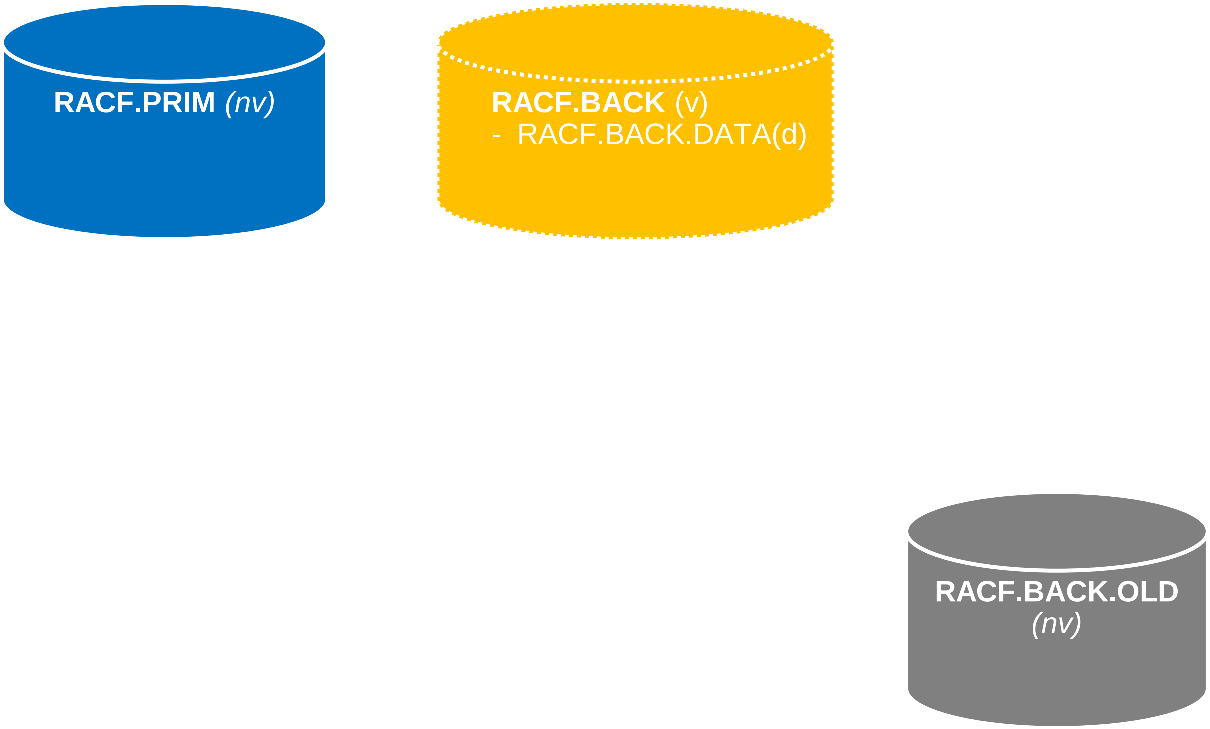
RENAMEACTIVATE: ACTIVATE

ICHRDSNT/PARMLIB

- **P:RACF.PRIM(nv)**
- **B:RACF.BACK(nv)**

Active Primary

Active Backup



RACF.PRIM *(nv)*

RACF.BACK (v)
- RACF.BACK.DATA(d)

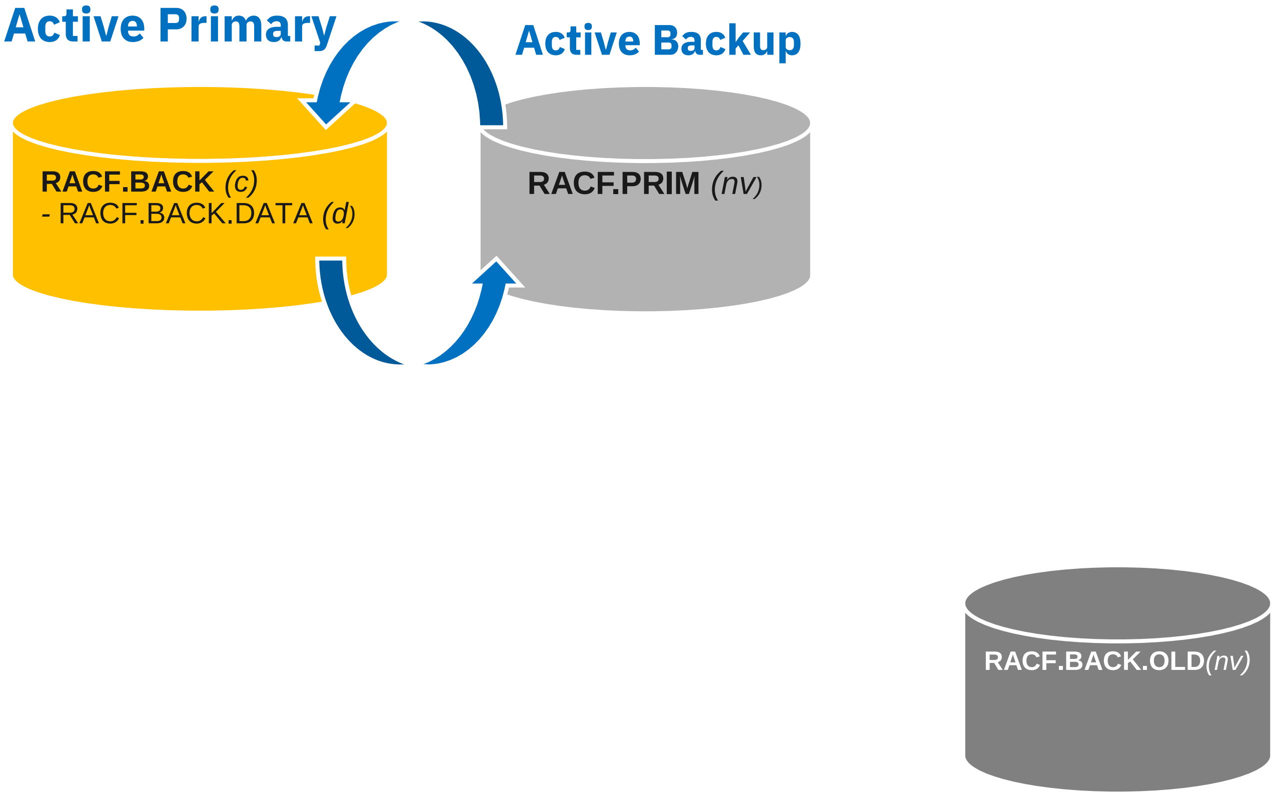
RACF.BACK.OLD
(nv)

Later – Issue RVARY SWITCH and ACTIVATE

ICHRDSNT/PARMLIB

- **P: RACF.BACK(v)**
- **B: RACF.PRIM(nv)**

Don’t forget to update ICHRDSNT or PARMLIB!



Active Primary

Active Backup

RACF.BACK *(c)*
- RACF.BACK.DATA *(d)*

RACF.PRIM *(nv)*

RACF.BACK.OLD*(nv)*

Miscellaneous RACF Utility JCL Changes

- **The RACF manager requires additional storage. CodeREGION=0K or REGION=0M on RACF utilities JCL**

- **When a RACF VSAM data set is being used there is an additional ENQ being issued**
  - (Major Name: SYSVSAM, Minor Name: <racf_dsn_name>||<catalog name>)
  - Code DISP=SHR for VSAM RACF data base names on RACF utility JCL

IRRUT200’s Use of IEBGENER

- **IRRUT200 now uses IDCAMS REPRO instead of IEBGENER to copy the RACF data sets, which results in a change in IRRUT200 messages:**

  - **IEBGENER**

```
DATA SET UTILITY –

PROCESSING ENDED AT EOD
IRR62065I - IEBGENER copied SYSRACF to the work dataset SYSUT1, IEBGENER RC=0000
```

  - **IDCAMS REPRO**

```
IRR62005I - IDCAMS REPRO copied SYSRACF to the work data set SYSUT1
```

RACF, VSAM and the Path to an Encrypted RACF Database

Mark Nelson, CISSP®, CSSLP®

z/OS Security Server (RACF®) Design and Development
markan@us.ibm.com
IBM® Poughkeepsie

14 October 2021