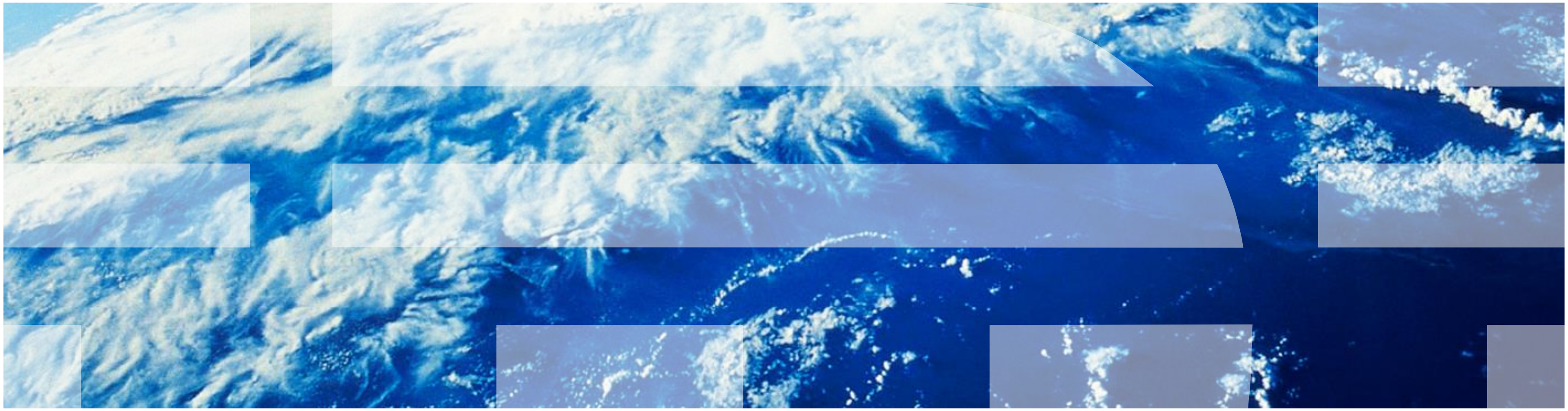
NY/Tampa/Raleigh/Dallas RACF® Users Group - Five Minute Madness

15 May 2019

IBM®
590 Madison Avenue
New York, NY



Current “Five Minute Madness” Sessions

- Allocating RACF Data Sets with IRRUT200
- MFA 2.0 Announcement
  - https://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/3/897/ENUS219-003/index.html&lang=en&request_locale=en
- SETROPTS enhancement to Audit System Sensitive Resources
- David had Something to Say

Allocating RACF Data Sets with IRRUT200

Allocating RACF Data Sets IRRADU00

- **Consider the following IRRUT200 invocation:**

```
//VERIFY    JOB
//STEP      EXEC PGM=IRRUT200
//SYSRACF   DD DSN=SYS1.RACF,DISP=SHR
//SYSUT1    DD UNIT=SYSALLDA,SPACE=(CYL,10,,CONTIG),DSN=PROD.RACF.BACKUP,
//          DCB=(LRECL=4096,RECFM=F,DSORG=PSU)
//SYSUT2    DD SYSOUT=A
//SYSPRINT  DD SYSOUT=A
//SYSIN     DD *
INDEX
MAP
/*
```

- **Allocation is for the RACF data set to be a sequential, single extent, unblocked, unmoveable, fixed length 4096 data set**

- **But will it be?**

Allocating RACF Datasets with IRRUT200…

- **IRRUT200 invokes the IEBGENER utility to perform the copy operation**

- **Installations which use IBM's DFSORT can choose to automatically use DFSORT's ICEGENER for its higher performance characteristics**

- **The DFSORT OUTSEC controls whether DFSORT uses *automatic* secondary allocation for output data sets that are temporary or new.**
  - If OUTSEC is enabled then data sets which are allocated during the IRRUT200 job step may end up in multiple extents which can cause an I/O error and a S500 abend when the data set is used as an online RACF data base or as input to the other RACF utilities

- ***OUTSEC is the installation default***
  - … which can be changed by the installation

Allocating RACF Datasets with IRRUT200…

- **DFSORT provides a way to override this installation default by using the DFSPARM DD statement to specify “OPTION NOOUTSEC”**

```
//VERIFY   JOB
//STEP     EXEC PGM=IRRUT200
//SYSRACF  DD DSN=SYS1.RACF,DISP=SHR
//SYSUT1   DD UNIT=SYSALLDA,SPACE=(CYL,10,,CONTIG),DSN=PROD.RACF.BACKUP,
//         DCB=(LRECL=4096,RECFM=F,DSORG=PSU)
//SYSUT2   DD SYSOUT=A
//SYSPRINT DD SYSOUT=A
//DFSPARM  DD *
 OPTION NOOUTSEC
/*
//SYSIN    DD *
INDEX
MAP
```

- **Net:** If you:
  - Allocate a RACF data set in IRRUT200 and
  - Use that data set as input to any process which expects a valid RACF data set and
  - Have ICEGENER configured as a replacement for IEBGENER and
  - Have OUTSEC set as the DFSORT default
  - Then, add the //DFSPARM DD * statement to set OPTION NOOOUTSEC for the execution of IRRUT200

- **See OA56715(DOC APAR) for the complete details**

MFA 2.0

IBM Z MFA Supported Token Types:

- RSA SecurID hard and soft tokens
- IBM TouchToken app for Time-based One-Time Passwords (TOTPs)
- PassTicket support and application-level granularity
- Smart card certificate-based authentication (one of the supported types is Personal Identity Verification/Common Access Card (PIV/CAC))
- Generic RADIUS support
- One-Time Passcodes generated by the IBM Security Access Manager (ISAM) pick-up OTP capability
- Tokens sent via SMS or email from IBM Cloud™ Identity Verify
- SafeNet RADIUS support
- RSA SecurID RADIUS support
- Generic TOTP support
- Yubico Yubikey tokens capable of generating One-Time Passcodes (OTP) using Yubico's OTP algorithm

IBM Z MFA 2.0 Also Supports:

- The ability to run multiple instances of the Multi-Factor Authentication Web Services started task in a sysplex.
- The ability to configure Multi-Factor Authentication to operate in a strict PCI-compliant mode.
- Integration through an SAF API that enables Express® Logon Facility to work with Multi-Factor Authentication.
- Compound authentication, which allows the specification of more than one authentication factor in the authentication process.
- Compound in-band authentication, which requires the user to supply a RACF credential (password or passphrase) in conjunction with a valid MFA credential.
- Integration with ISAM where once the user has authenticated to ISAM, the user is presented with a One-Time Passcode (OTP). The user then enters the OTP into z/OS application authentication dialogs instead of their RACF password or passphrase. IBM Z MFA then validates the provided credential with SAM to determine whether to allow or deny the user access.
- Enhanced security in the Out-of-Band preauthentication web dialogs by requiring the user to provide their policy name prior to entering their user name and credentials for the specified policy. As an aid for ease-of-use, the web address of the web server and policy name can be bookmarked by the user's web browser.
- RACF Identity Tokens (JSON Web Tokens support) where a set of authentication API calls can be linked together to appear as a single authentication transaction.
- Self-service password or passphrase change for both MFA users and non-MFA users.

NY/Tampa/Raleigh/Dallas RACF® Users Group - Five Minute Madness

15 May 2019

IBM®
590 Madison Avenue
New York, NY