ACF2 vs RACF

Eamonn McGrath
BMC Mainframe Services

November 2020
Session 1AL

ACF2 vs RACF

What this presentation isn't meant to be:

- A tool to assist in converting between the two ESMs
- A model for choosing between either ESM
- Aimed at a higher level than beginner
- An exercise in "Death by Powerpoint" ☺

ACF2 vs RACF

What this presentation is hoping to be:

- A review of the basic concepts of mainframe security (briefly)
- To hopefully increase your knowledge of either of the mainframe security managers
- Entertaining and fun ☺

ACF2 vs RACF

Who am I?

- RACF and ACF2 security consultant
- 20 years in this field

ACF2 vs RACF

Who am I?

When not performing my “day Job” I can usually be found:

Or

ACF2 vs RACF

Who am I?

These days It’s more likely this:

ACF2 vs RACF

- Two ESMs (External Security Managers)
- One underlying Operating System

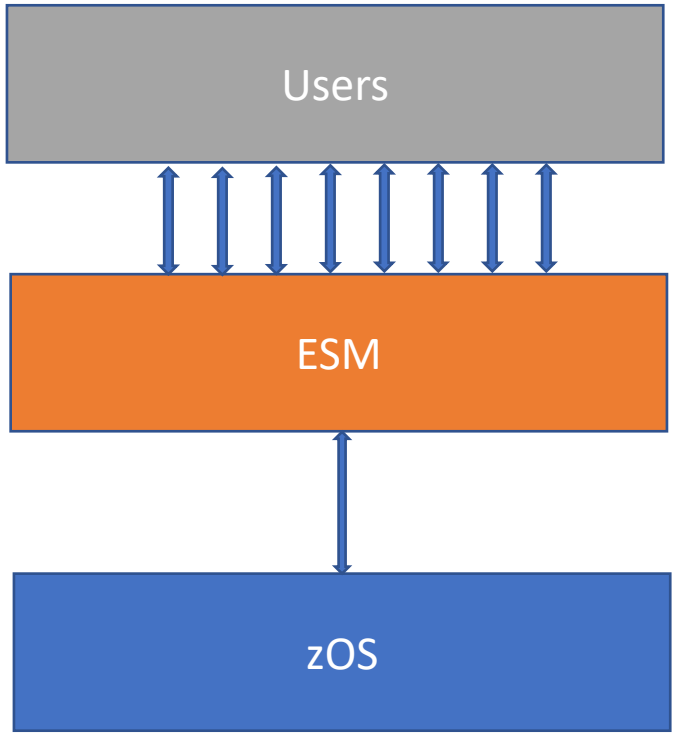
"THE SAME BUT DIFFERENT"

"It's not a competition"

ACF2 vs RACF

What is an ESM and why do we need one?

- Sits on top of zOS
- Takes the pressure off of zOS for access requests



ACF2 vs RACF

RACF and ACF2 a (very) brief history

- RACF
  - **R**esource **A**ccess **C**ontrol **F**acility
  - Released 1976 by IBM
  - Largest market share
- ACF2
  - **A**ccess **C**ontrol **F**acility **2**
  - Released 1978 by SKK and acquired by CA in 1987
  - Second largest market share

There is also CA's Top Secret Services. The third ESM for zOS.

(But we are not mentioning that one 'cos it's Top Secret. Shhhh..)

ACF2 vs RACF

What is the same?

- Both use SAF
- Both have security databases
- Both write SMF
- Both protect data as defined

ACF2 vs RACF

Now The FUN stuff

What's different:

First major difference is "out of the box" ACF2 denies access unless there is an access rule to grant it whilst RACF generally grants access unless a profile exists to restrict the it*.

*Kind of

ACF2 vs RACF

Database(s)

RACF

- 1 primary and 1 backup Database
- Contains everything
- Can be split into several datasets to reduce contention / storage issues
- Synchronously updated between primary and backup

ACF2

- 3 primary and 3 alternate databases
- LOGONID – Contains all logonids
- RULES – Contains all rulesets
- INFOSTG (Info Storage) – Contains all the rest that ACF2 needs to function
- Not synchronously updated

ACF2 vs RACF

Started Tasks & Start-up

RACF

- RACF STC does not need to operate for RACF to run normally
- Part of the operating system SMP/e
- Default userid IBMUSER must be present, if it is deleted it is recreated at IPL with enhanced privileges

ACF2

- ACF2 STC must be active for ACF2 to run normally
- If ACF2 STC is not running a WTOR will be produced for every security call
- Needs to be installed and set into the zOS environment
- ACFUSER logonid does not need to be present and can be deleted once the system is set up and a secure alternative created

ACF2 vs RACF

RACF -> ACF2 comparison table #1

RACF

- Userid
- Dataset Profile
- General Resource Profile

ACF2

- Logonid
- Dataset Rule
- Resource Rule

ACF2 vs RACF

Modes

RACF

- NOPROTECTALL
- PROTECTALL

ACF2

- QUIET
- LOG
- WARN
- RULE
- ABORT

ACF2 vs RACF

Global Settings

RACF

- SETROPTS

ACF2

- GSO

ACF2 vs RACF

Dataset Rules & Profiles

RACF

- 44 characters in length (including qualifier separators)
- 1st qualifier must be an existing user or group
- Access can be via Userid, Group or Universal (UACC, ID(*))
- Single RACF profile protects a dataset

ACF2

- 8 character max $KEY
- 4K limit – NEXTKEY allows for chaining rules that exceed 4K
- Reads through all rules to check if one grants (or denies) access to the requesting user
- Must be decompiled to update and recompiled to take effect

ACF2 vs RACF

Dataset & Rule Profiles

RACF

- Access is compounding (higher access inherits all previous levels of access)

ACF2

- Access is individual (each level of access is unique and does not inherit access from lower levels)

ACF2 vs RACF

RACF -> ACF2 comparison table #2 (access levels)

RACF

- NONE
- READ
- UPDATE
- CONTROL
- ALTER
- EXECUTE

ACF2

- DENY
- READ
- WRITE
- ALLOCATE
- EXECUTE

ACF2 vs RACF

General Resource & Rule Profiles

RACF

- Length determined in the CDT when class defined (1 to 246 characters including qualifier separators)
- Access can be via Userid, Group or Universal (UACC, ID(*))
- Single RACF profile protects a resource

ACF2

- 40 character max $KEY (unqualified)
- 4K limit – NEXTKEY allows for chaining rules that exceed 4K
- Reads through all rules to check if one grants (or denies) access to the requesting user
- Must be decompiled to update and recompiled to take effect

ACF2 vs RACF

Users

RACF

- Userid max length 8 characters
- Must be connected to at least one group (default group)

Example:

USERID – IBMUSER

Default Group – SYS1

Owner - IBMUSER

ACF2

- Logonid max length 8 characters
- Must have a valid UID string assigned (24 characters max length and must contain the logonid)
- UID string allows ACF2 to group users

Example:

LOGONID – TSGEMC

UiD string – TSGITSUSECTSGEMC

ACF2 vs RACF

Users - Attributes

RACF

- SPECIAL
- OPERATIONS
- AUDITOR
- ROAUDIT
- PRIVILEGED (STCs Only)
- TRUSTED (STCs Only)
- PROTECTED

ACF2

- SECURITY
- NON-CNCL
- AUDIT
- READALL
- STC
- RESTRICT

ACF2 vs RACF

Special Thanks To:

Ciara O’Connor

Thanks To:

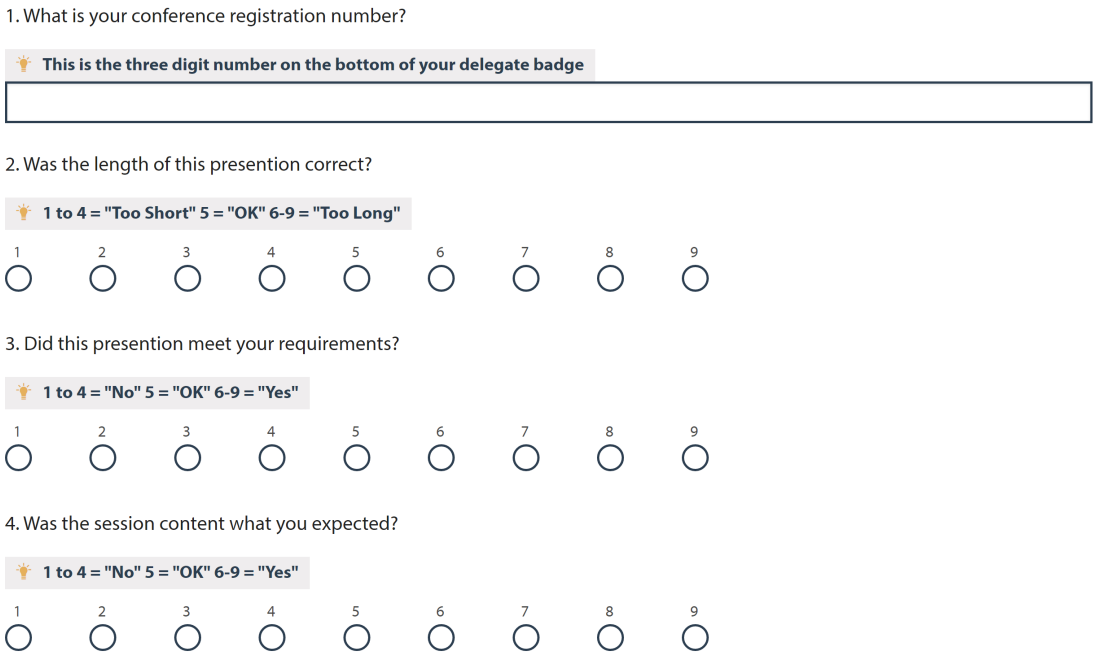
Carla Flores, Julie Bergh and Reg Harbeck

ACF2 vs RACF

Questions?

Please submit your session feedback!

- Do it online at http://conferences.gse.org.uk/2020/feedback/1AL
- This session is 1AL


1. What is your conference registration number?

This is the three digit number on the bottom of your delegate badge

2. Was the length of this presention correct?

1 to 4 = "Too Short" 5 = "OK" 6-9 = "Too Long"

1 2 3 4 5 6 7 8 9

3. Did this presention meet your requirements?

1 to 4 = "No" 5 = "OK" 6-9 = "Yes"

1 2 3 4 5 6 7 8 9

4. Was the session content what you expected?

1 to 4 = "No" 5 = "OK" 6-9 = "Yes"

1 2 3 4 5 6 7 8 9

GSE UK Conference 2020 Charity

- The GSE UK Region team hope that you find this presentation and others that follow useful and help to expand your knowledge of z Systems.
- Please consider showing your appreciation by kindly donating a small sum to our charity this year, NHS Charities Together. Follow the link below or scan the QR Code:

http://uk.virginmoneygiving.com/GuideShareEuropeUKRegion

NHS CHARITIES TOGETHER