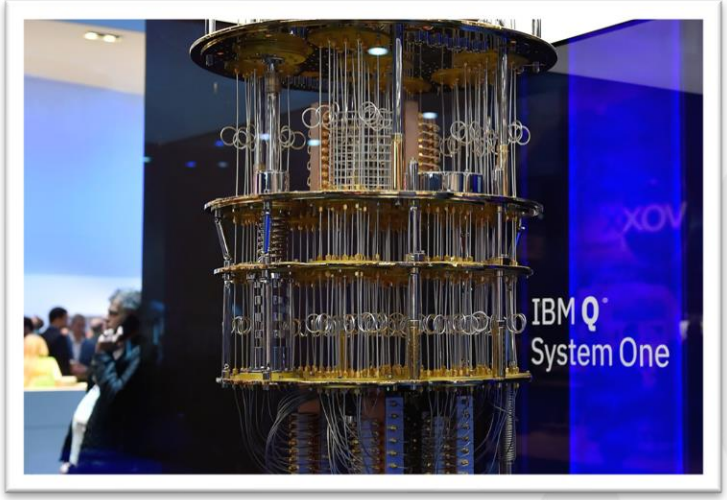
IBM® z/OS® Security Server RACF® Update Summer 2023 Edition

Ross Cooper, CISSP®
IBM z/OS Security Server (RACF) Design and Development
August, 2023



IBM Poughkeepsie Lab

RACF Update Agenda

SHARE
EDUCATE • NETWORK • INFLUENCE

z/OS 3.1 Only

- APPLAUDIT Enhancements
- Custom Field Information in ACEE

z/OS 2.5 – Continuous Delivery:

- Identity Token Enhancements **(NEW in July)**
- Passphrase Interval
- Support for the IBM Z Security and Compliance Center
- Center for Internet Security (CIS) IBM z/OS V2R5 with RACF Benchmark
- Encrypted RACF VSAM data set as RACF database
- Ability to Disable Additional logon attempts for a RACF-SPECIAL user after exceeding the SETROPTS PASSWORD(REVOKE(nnn)) value
- Sharing RACF data base with RACF on z/VM

APPLAUDIT ENHANCEMENTS

Logging Application Logons

- Which users are successfully logging on to your z/OS applications?
- z/OS Applications call RACROUTE REQ=VERIFY to authenticate a user and create a security environment (ACEE).
- RACROUTE REQ=VERIFY can create SMF type 80 event code 1 (JOBINIT) records.
- Applications control logging with the RACROUTE **LOG=** keyword.
  - **LOG=NONE** – Requests are not logged
  - **LOG=ALL** – All successes and failures are logged
  - **LOG=ASIS** – All failures are logged and some successes are logged:
    - A successful RACROUTE REQUEST=VERIFY is logged under the following conditions:
      - SETROPTS AUDIT(USER) is active and a user's password or password phrase is changed
      - Authentication using a PassTicket
      - Authentication of an IBM Multi-Factor Authentication user using a password or password phrase.
      - APPLAUDIT is in effect for the application

Existing APPLAUDIT Overview

- APPLAUDIT is an existing setting that enables logging of successful logons when:
  - The application has:
    - **LOG=ASIS** is specified or defaulted
    - **APPL=<application-name>** is specified
    - Not specified **SESSION=OMVSSRV** (UNIX applications)
  - The installation has:
    - **APPLAUDIT** enabled: `SETROPTS APPLAUDIT`
    - Audited successful access to **APPL** (GLOBALAUDIT or AUDIT) class profile associated with **<application-name>:** `RALTER APPL profile-name GLOBALAUDIT(ALL)`
    - **Activated** and **RACLISTed APPL** class: `SETROPTS CLASSACT(APPL) RACLIST(APPL)`

- **Notes:**
  - RACF documentation prior to z/OS 3.1 documents that APPLAUDIT only applies to APPC applications, but it works with any application that fulfils the above requirements.
  - The APPL class profiles are also used to protect applications. See Protecting Applications in the Security Administrator's Guide.
  - **TSO:** Use VERIFYAPPL(ON) in IKJTSOxx for TSO to specify an APPL to RACROUTE.

APPLAUDIT – SMF Type 80 Format

- **SMF Type 80 Event Code 1 (“JOBINIT”)** records log the logon to and logoff from an application.
- **Example RACF SMF Unload:**

Type	Qualifier	Time	Date		APPLAUDIT		APPL Name
JOBINIT	RACINITI	17:26:17	2023-01-04	…	YES	…	MYAPPL
JOBINIT	RACINITD	17:26:20	2023-01-04	…	YES	…	MYAPPL

- **APPL class access records:**
  - Profile logging also results in an SMF 80 Event Code 2 (“ACCESS”) record for successful access to the APPL profile at logon.
  - This check is bypassed when a VLF cache match is found for the user in the IRRACEE VLF class, so the ACCESS record will not always accompany the RACINITI/RACINITD records.

APPLAUDIT Enhancements

SHARE
EDUCATE • NETWORK • INFLUENCE

1. **Documentation:**
   - RACF 3.1 pubs documentation of APPLAUDIT is updated to indicate that it applies to all z/OS applications that meet the requirements (not just APPC applications).
2. **Testing:**
   - Formally tested APPLAUDIT with non-APPC applications on all supported releases
3. **APPLAUDIT Support for UNIX Applications:**
   - APPLAUDIT is extended to optionally enable auditing successful logons to UNIX applications (SESSION=OMVSSRV).
   - **Note:** Applications that use initACEE to authenticate users, look like UNIX applications (SESSION=OMVSSRV).

APPLAUDIT for UNIX Applications

- **APPLAUDIT** is optionally enabled for UNIX applications:
  - New **OPTAUDIT** class is added to contain logging-related compatibility switches.
    - Documentation is provided in the Auditor's Guide to suggest allowing auditors to create, manage, and delete profiles in the OPTAUDIT class.
  - Enable logging successful logons to UNIX applications:
    1. Activate the OPTAUDIT class:

       ```
       SETR CLASSACT(OPTAUDIT)
       ```

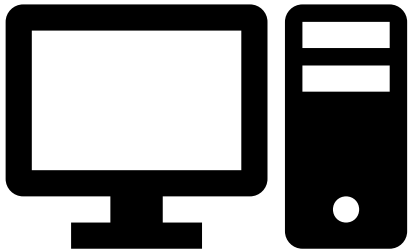
    2. Create the new switch profile in the new OPTAUDIT class:

       ```
       RDEFINE OPTAUDIT APPLAUDIT.FOR.UNIX
       ```

    3. RACLIST (or REFRESH) the OPTAUDIT class:

       ```
       SETR RACLIST(OPTAUDIT)
       ```

    - When a user successfully logs onto a UNIX application (SESSION=OMVSSRV) and all other APPLAUDIT requirements are met, an SMF 80 record will be cut.



APPLAUDIT Other Externals

- **RACF Subsystem:**
  - Required to extend APPLAUDIT to UNIX applications.
  - Listens for RACLIST REFRESHs of the OPTAUDIT class via ENF 62
  - ENF 62 listener status message is displayed on the console during subsystem initialization:

```
IRRC093I (<) RSWJ SUBSYSTEM ENF 62 LISTENER IS ESTABLISHED.
```

- **New RCVTAAUX bit in RCVT:**
  - Indicates that SETROPTS APPLAUDIT is extended to UNIX applications:
  - On when APPLAUDIT.FOR.UNIX exists and OPTAUDIT class is RACLIST REFRESHed

- **SMF 80 Logoff records (RACROUTE REQ=DELETE of ACEE):**
  - With this new support, the DELETE audit record also includes the application name which was used to create the ACEE.

CUSTOM FIELD INFORMATION IN ACEE

Custom Fields Overview

- Custom fields are fields within the RACF database that an installation can customize to store security information in RACF profiles:
  - Users, Groups
  - Data Sets and General Resources (starting in V2.4)

- The names and attributes of custom fields can be tailored.
- Once a custom field is defined, use RACF commands, such as the **ALTUSER, ALTGROUP, ALTDSD** and **RALTER** to add data to a custom field in a profile.
- Custom Fields are defined in the **CSDATA** segment of the **CFIELD** class.

Custom Fields Example

Define a new USER class field for the employee Serial Number called EMPSER:

```
RDEFINE CFIELD USER.CSDATA.EMPSER UACC(NONE)
     CFDEF(TYPE(NUM) FIRST(NUMERIC) OTHER(NUMERIC) MAXLENGTH(8)
          MINVALUE(100000) MAXVALUE(99999999)
          HELP('EMPLOYEE SERIAL NUMBER, 6 - 8 DIGITS') LISTHEAD('EMPLOYEE SERIAL='))
```

Activate the CFIELD class:

```
SETR CLASSACT(CFIELD)
```

Update RACF command dynamic parse:

```
IRRDPI00 UPDATE
```

Use the custom field to assign a user a Serial Number:

```
ALTUSER COOP CSDATA(EMPSER(123456))
```

List the custom field:

```
LISTUSER COOP CSDATA NORACF
USER=COOP
CSDATA INFORMATION
-----------------------------------------
EMPLOYEE SERIAL= 123456
```

Custom Fields in ACEE

SHARE
EDUCATE • NETWORK • INFLUENCE

- **ACEEs and Authentication:**
  - During user authentication, RACF reads certain fields from the user profile in the RACF database and builds a security environment (ACEE)
  - The ACEE is used by RACF to satisfy authorization and auditing requests

- **Custom Fields in the ACEE:**
  - Starting with z/OS V3R1, you can direct RACF to place custom field information from a user profile into the ACEE for retrieval by the R_GetInfo (IRRSGI00) callable service.

- **New ACEE(YES|NO) on CFIELD definition:**
  - `RDEFINE CFIELD USER.CSDATA.EMPSER UACC(NONE) CFDEF(TYPE(NUM) FIRST(NUMERIC) OTHER(NUMERIC)MAXLENGTH(8) MINVALUE(100000) MAXVALUE(99999999)` **`ACEE(YES)`**
    `HELP('SERIAL NUMBER, 6 - 8 DIGITS')LISTHEAD('EMPLOYEE SERIAL=‘))`
- **Refresh dynamic parse:** `IRRDPI00 UPDATE`
- **Add custom field to user:** `ADDUSER JOE CSDATA(EMPSER(123456))`
- **Now JOE’s EMPSER can be retrieved using the R_GetInfo service.**

Custom Fields in ACEE – R_GetInfo

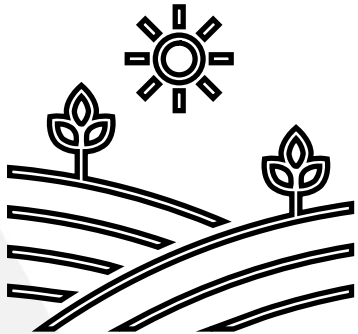
- **R_GetInfo -** New Function Code 3 **-** Get CSDATA from ACEE

- **Authorization:**
  - FLAC – Field Level Access Checking – Granted via profiles in FIELD class
    - Determines which fields (including custom fields) the caller can view or modify
  - Authorized callers can optionally skip FLAC
  - Authorized callers can provide an ACEE_ptr to extract CSDATA from.

- **Invocation:**

CALL IRRSGI00 (

…
Num_parms, - New Value: 16 for function code X'0003'
…
Function_code, - New value: X'0003'- Get CSDATA from ACEE
Option, - Single / All fields? NOFLAC*? (supervisor state only)
…
Result_entries, - For FC 3 - CSDATA fields return area
CSDATA_keyword_name, - **New:** Field to retrieve or null for all
ACEE_ptr) - **New:** ACEE address



IDENTITY TOKEN ENHANCEMENTS

Identity Token Support

Identity Token:

- An Identity Token is used to assert user claims which can be trusted by the consumer of the token.
- RACF use adheres to the JSON Web Token (JWT) IETF specifications: RFC 7519

RACROUTE Support for Identity Tokens:

- RACROUTE authentication processing can generate and validate Identity Tokens (IDT).
  - **Generation -** Applications can request that an IDT be returned from RACROUTE.
  - **Validation -** Applications can supply an IDT to authenticate a user instead of other credentials.

IDT Configuration:

- The security administrator can create profiles in the IDTDATA class:
  - Configure how certain fields in an IDT are generated and validated

Identity Token Use cases

Linking Multiple Authentication API Calls:

- In some cases, user authentication requires multiple steps:
  - **Expired Password / Invalid New Password / MFA Expired PIN …**
- **Problem:**
  - MFA credentials are one time use.
  - When multiple authentication calls are required, an already consumed MFA token will fail.
- **Solution:**
  - The Identity Token can be used to link authentication status information between multiple authentication API calls without replaying the MFA credentials.

Replaying Proof of Authentication:

- Some applications authenticate a user and “replay” that authentication multiple times.
- **Problem:**
  - Some applications cache the user provided credential and replay it back again later.
  - For users with one time use MFA tokens, this does not work.
- **Solution:**
  - The Identity Token support allows applications to authenticate a user and receive proof of that authentication which can be supplied back to RACROUTE in place of other credentials like a password.
  - Signed JWTs can be returned to an end user for later use by the application.

Identity Token Format

A JSON Web Token (JWT) is used to assert claims between multiple parties. They are often used to prove a user has been authenticated.

- **JWT RFC7519:** https://tools.ietf.org/html/rfc7519
- **Used by common authentication protocols:** OpenID Connect, Oauth2

JWT:

- **Header (JOSE):**
  - **{“alg” : “HS256” or “none”}** – Signature Algorithm: **HS256** = HMAC with **SHA-256**, none = unsecured
- **Body Claims – (JWS Payload):**
  - **{“jti” : “cb05…”,** – JWT Unique identifier
  - **“iss” : “saf”,** – Issuer name – Entity that created the JWT
  - **“sub” : “USER01”,** – Subject (the authenticated user)
  - **“aud” : “CICSLP8”,** – Audience – Target consumer of the JWT
  - **“exp” : 1486744112,** – Expiration time - (Seconds since 1970 - Expired tokens should be rejected)
  - **“iat”: 1486740112,** – Issued at – The time at which the JWT was issued.
  - **“amr”:[”mfa-comp”,”saf-pwd”]}** – Authentication Method References - Indicates how the subject was authenticated
- **Signature (JWS)** – Encoded in binary
  - 389A21CD32108C3483DA

Identity Token New Use Cases

RACF JWT Support Limitations:

- **JWT generation:** Only with RACROUTE REQ=VERIFY,ENVIR=CREATE with authentication credentials supplied. Protected User IDs not supported.
- **JWT validation:** Only with RACROUTE REQ=VERIFY,ENVIR=CREATE when target user's authenticators match the JWT "amr" claims. Protected User IDs not supported.

New Requested Use Cases:

1. **Generate IDT from ACEE:**
   - Some applications have use cases where their APIs are called "downstream" by other applications with the ACEE security environment already established.
   - Requesting the ability to generate a JWT for a user ID that has ACEE security environment established (protected users included)
     - Do not wish to call RACROUTE REQ=VERIFY,ENVIR=CREATE
2. **Authenticate user with JWT created from ACEE (including protected users):**
   - JWT passed securely to the target application interface, which will in turn call RACROUTE REQ=VERIFY,ENVIR=CREATE (which is not supported for protected users today.)

Identity Token Enhancements

z/OS 3.1 base and 2.4/2.5 via PTFs
APARs RACF - OA63462, SAF - OA63463

Generation of IDTs From an Existing ACEE Security Environment:

- This new support introduces the capability for applications to use the initACEE callable service to generate an IDT from an ACEE.
- The returned IDT can be used to authenticate the user using the existing IDT support in RACROUTE REQEST=VERIFY.
- The new initACEE function can generate an IDT for a protected user without traditional authentication mechanisms.

Authentication of User with IDT Generated from an ACEE:

- This new support introduces the capability for RACROUTE REQEST=VERIFY to authenticate a user with an IDT which was generated from an ACEE.
- With this new support a user with the protected attribute can optionally be authenticated with an IDT.

Identity Token – New initACEE Function

The initACEE SAF/RACF callable service provides an interface for identity related functions:

1. Creating and managing RACF security contexts through the z/OS UNIX System Services pthread_security_np service, __login service, or by other MVS server address spaces that do not use z/OS UNIX services.
2. Registering and deregistering certificates through the z/OS UNIX System Services __security service.
3. Querying a certificate to determine if it is associated with a user ID.
4. Generating an Identity Token (IDT) from an ACEE security environment.

Identity Token – New initACEE Function

New initACEE Function Code:

X'07' – GENIDT - Generate an IDT from ACEE

Authorization: Only supports supervisor state callers.

Parameters:

IDTA – (Input/Output):

- The name of a fullword containing the address of an Identity Token Area for the generation of an Identity Token for the specified ACEE.
- Same format as IDTA for RACROUTE VERIFY - IDTA parameter details described in RACROUTE Macro Reference Appendix G.
- Mapped by SAF macro IRRPIDTA.

ACEE2_ptr – Input:

- Point to existing ACEE. (Or picks up from TCB/ASCB)

ACEE2_ALET – Input:

- ALET qualifier for ACEE2_ptr.

APPL_ID – Input (Required):

- Target application for Identity Token.
- May be different than APPL from the ACEE

Other parameters: All other parameters are not supported for GENIDT function code

Identity Token - initACEE SMF Records

initACEE SMF Record Type 80 Event Code 67 – New relocate 449:

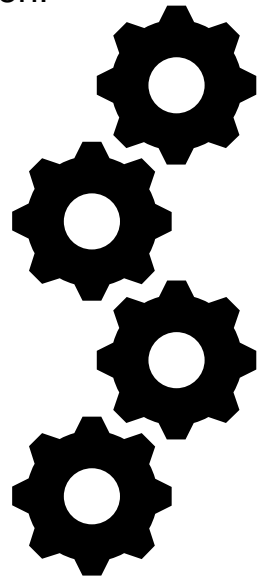
Format of the InitACEE record extension (event code 67)					
Field Name	Type	Len	Start	End	Comments
INTA_USER_NAME	Char	20	282	301	The name associated with the user ID.
…	…	…	…	…	…
INTA_CERT_FGRPRNT	Char	64	4496	4559	Certificate SHA64 fingerprint in printable hex
INTA_IDT_USER	Char	8	4561	4568	User ID from specified ACEE for generate IDT function
INTA_APPL	Char	8	4570	4577	Application name specified to initACEE for generate IDT function
INTA_IDT_BUILD_RSNC	Char	8	4579	4586	IDT Build Reason Code
INTA_SERVICE_CODE	Char	8	4588	4595	Failing Service Identifier
INTA_SERVICE_RC	Char	8	4597	4604	Failing Service Return Code
INTA_SERVICE_RSNC	Char	8	4606	4613	Failing Service Reason Code

New Event Code Qualifiers:

- **SUCCSIDT (11)** Successful IDT generated from ACEE.
- **FAILIDT (12)** Failed attempting to generate IDT from ACEE.

Identity Token – New Configuration

IDTDATA profile and IDTPARMS segment is used to hold IDT generation/validation configuration.



New IDTPARMS keyword for RDEFINE/RALTER:

```
[ IDTPARMS(
      [ SIGTOKEN(pkcs11-token-name) ]
      [ SIGSEQNUM(pkcs11-sequence-number) ]
      [ SIGCAT(pkcs11-category) ]
      [ SIGALG( HS256 | HS384 | HS512) ]
      [ ANYAPPL( YES | NO ) ]
      [ IDTTIMEOUT(timeout-minutes) ]
      [ PROTALLOWED ( YES | NO ) ]
) ]
...
```

PROTALLOWED (YES | NO)

Specifies whether an Identity Token (IDT) validated with this profile can be used to authenticate a protected user.

Identity Token - Other Externals

- **PROTALLOWED Keyword:**
  - RACF Templates - New field IDTPARMS segment: IDTPROTA
  - R_Admin support: IDTPROTA
  - DBUnload support: GRIDTP_PROTECTED_ALLOWED

- **RACROUTE REQ=VERIFY,ENVIR=CREATE,IDTA=<idta>:**
  - When PROTALLOWED(YES) for matching IDTDATA profile, then IDTA can be used to authenticate a protected user
  - SMF 80 Event code 1 (JOBINIT) record now indicates when a protected user is authenticated with an IDT.

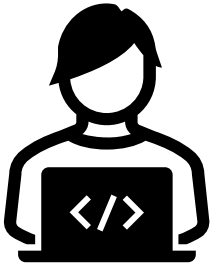
PASSWORD PHRASE INTERVAL

Password Interval Current Processing

SHARE
EDUCATE • NETWORK • INFLUENCE

RACF Password Change Interval:

- Defines the interval that users must change their password *or password phrase*
- Range: 1-254 days
- A system default can be specified
  - `SETROPTS PASSWORD(INTERVAL(<days>))`
- A user default can be specified
  - `PASSWORD USER(<user>) INTERVAL(<days>)`
  - `PASSWORD USER(<user>) NOINTERVAL`
- RACF uses the shorter of the system level and user specific interval as a user's effective password interval



Q: Is the 254-day limit appropriate for password phrases?

- Clients are requesting a longer RACF password phrase interval to match other platforms.
- NIST Special Publication 800-63B:
  - "Do not require that memorized secrets be changed arbitrarily (e.g., periodically) unless there is a user request or evidence of authenticator compromise."

PassPhrase Change Interval

SHARE
EDUCATE • NETWORK • INFLUENCE

- **z/OS 3.1 and 2.5 PTFs:**
  - **RACF APAR OA61951 (PTF UJ90043)**
  - **SAF APAR OA61952 (PTF UJ90042)**

- **Password Phrase Interval:**
  - RACF provides a new separate password phrase specific change interval which can be different than the existing password interval and supports much longer values.

- The password phrase interval can be set at:
  - The system level with the SETROPTS command
  - The user level with the PASSWORD/PHRASE command.

System PassPhrase Interval

Set System Password Phrase Interval:

```
SETROPTS PASSWORD(PHRASEINT(365))
```

- **Range:** 0-65,534 days (179 years)
- **Default value:** 0 - (Password phrase interval is not in effect)
- **Authorization:** Must have the RACF SPECIAL attribute
- **Details:**
  - A PHRASEINT value of zero indicates that the system does not have a phrase interval set and, in this case, the existing password interval controls the change interval for both passwords and password phrases.
  - When PHRASEINT is set to a non-zero value, it overrides the existing system level password interval control for password phrases.

System PassPhrase Interval…

Set System Password Interval to 90 days and Password Phrase Interval to 365 days:

```
SETROPTS PASSWORD(INTERVAL(90) PHRASEINT(365))
SETR LIST…
PASSWORD CHANGE INTERVAL IS 90 DAYS.
PASSWORD PHRASE CHANGE INTERVAL IS   365 DAYS.
```

Set System Password Interval to 30 days and Password Phrase Interval to zero (not in effect):

```
SETROPTS PASSWORD(INTERVAL(30) PHRASEINT(0))
SETR LIST…
PASSWORD CHANGE INTERVAL IS 30 DAYS.
PASSWORD CHANGE INTERVAL IS IN EFFECT FOR PASSWORD PHRASES.
```

User PassPhrase Interval

Set User Specific Password Phrase Interval:

```
PASSWORD USER(RACFU01) PHRASEINT(356)
```

- **Range:** 0-65,534 days (179 years)
- **Default:** 0 (User does not have a password phrase interval set)
- **Authorization:** SPECIAL or GROUP SPECIAL (Users can not set their own PHRASEINT)
- **Details:**
  - A PHRASEINT value of 0 indicates that the user does not have a phrase interval set. In this case, when the system level password phrase interval has a non-zero value it is used as the effective password phrase change interval and otherwise the existing password interval is used instead.
  - When the user's PHRASEINT is set to a non-zero value, it is used as the effective password phrase change interval and it overrides the system level password phrase interval control and system level password interval control.

User PassPhrase Interval…

Set User Level Password Phrase Interval to 365:

```
PASSWORD USER(RACFU01) INTERVAL(30) PHRASEINT(365)
LISTUSER RACFU01…
PASS-INTERVAL=30
PHRASE-INTERVAL=00365
```

Set User Level Password Phrase Interval to Never Expire:

```
PASSWORD USER(RACFU01) NOINTERVAL NOPHRASEINT
LISTUSER RACFU01…
PASS-INTERVAL=N/A
PHRASE-INTERVAL=N/A
```

Set User Level Password Phrase Interval to Zero (not in Effect):

```
PASSWORD USER(RACFU01) INTERVAL(30) PHRASEINT(0)
LISTUSER RACFU01…
PASS-INTERVAL=30
```

* (Password phrase interval line not listed when zero)

PassPhrase Interval – SMF

SMF Record Type 80:

- Data Type 6 command related data is updated to support the new PHRASEINT keyword of the SETROPTS and PASSWORD/PHRASE commands.
  - **SETROPTS command** - Update relocate to hold the new phrase interval
  - **PASSWORD/PHRASE commands** - Update relocate to hold the phrase interval
    - ‘FFFF’x in new field means NOPHRASEINT

SMF Record Type 81:

- The RACF SMF record type 81 RACF initialization record is updated to add a new field for the password phrase interval.
  - **RACF Initialization** – New field to hold new phrase interval setting

PassPhrase Interval – RRSF

Command direction Considerations:

- PASSWORD PHRASEINT(nnn) and NOPHRASEINT will not work on a remote node without this support.
- SETR PASSWORD(PHRASEINT(nnn)) will not work on a system that does not have this support

Handshaking Considerations:

- Update node def block to include 2-byte phrase interval for handshake (reuse reserved space)
- Lower-level system will ignore the new phrase interval field and not issue a message
- Up level systems will compare the phrase interval field. When not equal, issue message

```
IRRI007I ATTENTION: LOCAL NODE localnode HAS A DIFFERENT
SETROPTS PASSWORD(option) THAN PARTNER NODE partnernode.
```

PassPhrase Interval – Other

R_Admin Callable Service:

- Updated to support the new PHRASEINT keyword of the PASSWORD/PHRASE commands.
- Updated to support the new PHRASEINT keyword of the SETROPTS command.

DBUNLOAD – RACF Database Unload Utility:

- Unloads the new base segment user field for phrase interval
- DB2 samples are updated: RACDBUTB & RACDBULD

PassPhrase Interval – Health Checker

RACF_PASSWORD_CONTROLS

- The RACF_PASSWORD_CONTROLS health check examines the client's RACF password control settings and raises an exception when recommended settings are not being used.
- Using the IBM supplied default Health Check parameter values, an exception would be raised if either:
  - RACF is not enabled for mixed-case passwords.
  - The invalid password revocation count is greater than three (3).
  - The maximum days a password/passphrase is valid is greater than 90.
  - The installation is using phrase intervals and the maximum days a password phrase is valid is greater than 365. (New for z/OS 3.1)
  - The INITSTATS function is not in effect.

PassPhrase Interval – Health Checker

The output of RACF_PASSWORD_CONTROLS when no exception is raised:

```
CHECK(IBMRACF,RACF_PASSWORD_CONTROLS)
SYSPLEX:    LOCAL     SYSTEM: RACFR31
START TIME: 11/05/2022 11:03:51.323496
CHECK DATE: 20220118 CHECK SEVERITY: MEDIUM
CHECK PARM: REVOKE(3),MIXEDCASE(YES),INTERVAL(90),PHRASEINT(365), INITSTATS(YES)

                          RACF Password Controls

S Control                                                 Value Target
- ------------------------------------------------------ ----- ------
  Mixed case passwords are allowed                       YES   YES
  INITSTATS in effect                                    YES   YES
  Maximum number of consecutive failed logon attempts    003   003
  Maximum days before a password/phrase expires          030   090
  Maximum days before a phrase expires                   00365 00365

IRRH284I No exceptions are detected.

END TIME: 11/05/2022 11:03:51.324034 STATUS: SUCCESSFUL
```

Effective Interval Examples

System and User Password and Phrase Change Interval Settings				Effective Password and Phrase Interval	
SETROPTS Password Interval	**User Password Interval**	**SETROPTS Phrase Interval**	**User Phrase Interval**	**Effective Password Interval**	**Effective Phrase Interval**
90	30	0	0	30	30
30	90	0	0	30	30
90	90	365	0	90	365
90	90	0	365	90	365
90	90	365	200	90	200
90	90	365	500	90	500

SUPPORT FOR THE IBM Z SECURITY AND COMPLIANCE CENTER

RACF SMF 1154 Subtype 83

- **Applications can request that participating z/OS applications cut security related SMF records:**
  - Request comes from a zOSMF REST API (such the IBM Z Security and Compliance Center)
  - RACF will create an SMF 1154 Subtype 83 record which contains compliance information.

- RACF SMF Records are documented in RACF Macros and Interfaces

RACF SMF 1154 Subtype 83 Contents

SMF Record Section	Contents
RACFSMRY: RACF Summary information (SETROPTS, etc.)	RACF ACTIVE/INACTIVE, definition of IBMUSER, SAUDIT,CMDVIOL, OPERAUDIT, MIXEDCASE, password rules, password exit status, password interval, password history, maximum failed password attempts, user inactivity, default RVARY passwords, password encryption algorithm, CATDSNS, ERASE, ACEECHK, BATCHALLRACF…
RACFCRIT: Critical RACF general resources	UACC, ID(*), WARNING AUDIT, GAUDIT information for critical RACF general resources (e.g. BPX.SUPERUSER)
RACFAPFL: Critical data set	UACC, ID(*), WARNING information for APF, RACF, LINKLIST, RRSF and PARMLIB data sets.
RACFACTL: Programs defined in the RACF Authorized Callers Table (Non-recommended options)	Module name and module location (LPA, not in LPA).

RACF
VSAM DATABASE

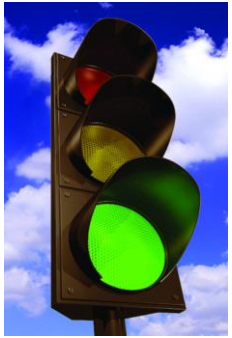
RACF VSAM Data Set Support

V2.5 VSAM RACF DB Support:

- RACF V2.5 has support for using a VSAM dataset as the RACF database

Base z/OS V2.5 restrictions

- Non-shared (may be on a device marked as shared)
- Non-split RACF data set
- Non-SMS managed (which means not encrypted)
- Not in RACF sysplex communications mode or RACF data sharing mode
- All systems sharing the RACF DB must be at z/OS V2.5
- Not defined in MSTRJCL
- Running in application identity mapping (AIM stage 3)
- That is free from internal errors (IRRUT200 and IRRDBU00 run without error)



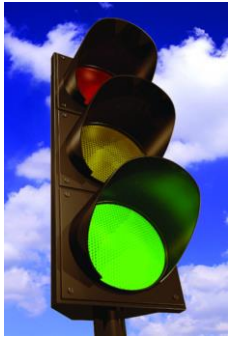
Encrypted VSAM Data Set Support in RACF

Encrypted RACF DB:

- 3.1 base and V2.5 APAR OA62267 allows an encrypted DB and removes several restrictions

Base z/OS V2.5 restrictions, removed with APAR OA62267

- ~~Non-shared (may be on a device marked as shared)~~
- ~~Non-split RACF data set~~
- ~~Non-SMS managed (which means not encrypted)~~
- ~~Not in RACF sysplex communications mode or RACF data sharing mode~~
- All systems sharing the RACF DB must be at z/OS V2.5
- Not defined in MSTRJCL
- Running in application identity mapping (AIM stage 3)
- That is free from internal errors (IRRUT200 and IRRDBU00 run without error)



RACF APAR OA62267:

- PTF UJ08531, available 8 June 2022

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)

DISABLING ADDITIONAL LOGON ATTEMPTS FOR RACF SPECIAL USERS

SPECIAL User Excessive Password Prompt

- **SETROPTS PASSWORD(REVOKE(nnn))**
  - Establishes the maximum number of incorrect authentication attempts before a user is revoked.

- **When an incorrect logon attempt exceeds the REVOKE limit:**
  - Non-SPECIAL users are revoked immediately
  - For users with the SPECIAL attribute a message to the console asks the operator if the user should be revoked or allow an additional attempt

- **ICH301I MAXIMUM PASSWORD ATTEMPTS BY SPECIAL USER *userid* [AT TERMINAL *terminalid*.]**
  - **ICH302D REPLY Y TO ALLOW ANOTHER ATTEMPT OR N TO REVOKE USERID *userid*.**
    - Y – Allows the attempt to logon and does not revoke the user
    - N – Revokes the user

SPECIAL User Excessive Password Prompt Disablement

- **With OA63091 (z/OS 2.3, 2.4 and 2.5) you can disable additional logon attempts for a RACF SPECIAL user once the SETROPTS PASSWORD(REVOKE(nnn)) value has been exceeded**
  - The disablement can be enabled on an application-by-application basis

- **Enabled with the definition of an XFACILIT class discrete profile of the name:**
  - **`IRR.DENY.SPECIAL.USER.ADDITIONAL.PASSWORD.ATTEMPTS.APPL.appl-name`**
  - The appl-name must match the APPL= value on the RACROUTE REQUEST=VERIFY.
  - If no appl-name was specified on the REQUEST=VERIFY, then it defaults to the same derivation method as used in PassTicket application name derivation.
    - Documented in the RACF Security Administrator's Guide
  - This is a profile existence check only. No profile attributes (UACC, access list, etc.) are considered.
- **Caution:** Enabling this support will cause RACF special users to be revoked when the revoke limit is reached. Ensure there is a way to resume a special user from the console without needing to logon.

SHARING A RACF DB WITH Z/VM

Sharing a z/OS RACF DB with z/VM

- **Starting with z/VM 7.3, RACF z/OS and RACF z/VM will not be able to share the RACF database.**
  - Attempts to IPL z/OS with a z/VM 7.3 RACF database will fail and the operator will be prompted for a different RACF database.
  - This change comes with APAR OA62875.
  - For details, see: https://www.vm.ibm.com/zvm730/announce.html

HOMEWORK

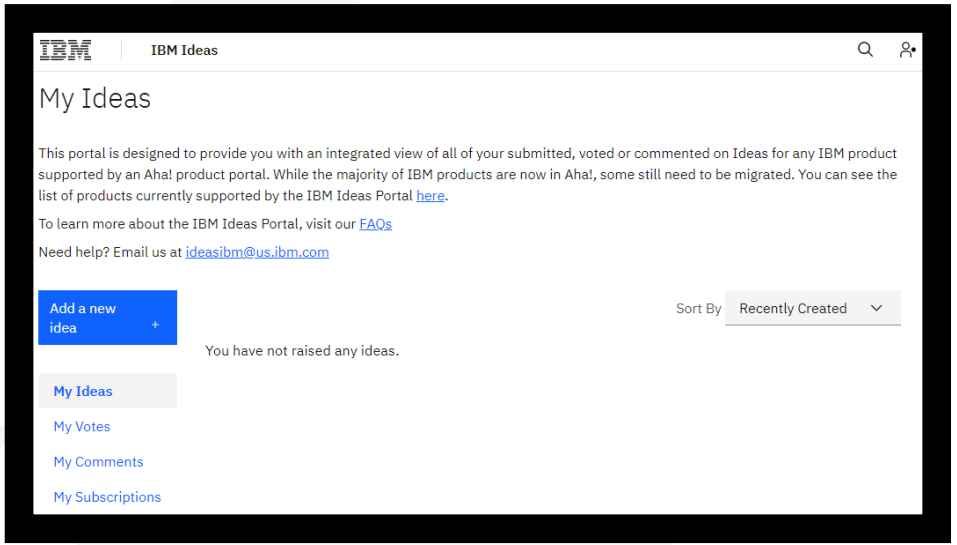
Homework – Start implementing these NOW

- **KDFAES**
  - Strong protection for passwords and phrases in the RACF database
  - Mitigate an offline password database attack
  - Available for 10 years
- **Enhanced PassTickets**
  - Huge upgrade in security over legacy PassTickets
  - Available for 3 years
- **RACF Health Checks**
  - Automatic validation of security settings against recommendations
  - Highly configurable
  - Continuous monitoring
- **MFA – Multi-factor authentication**
  - Industry standard for strong protection of authentication

IDEAS

IBM Ideas

- **Requirements should be submitted to IBM Ideas:**
  - Reviewed by the design and development teams
  - Facilitates a dialog between clients and IBM
  - **Ideas Link:** https://ideas.ibm.com



IBM® z/OS® Security Server RACF® Update Summer 2023 Edition

Ross Cooper, CISSP®
IBM z/OS Security Server (RACF) Design and Development
August, 2023

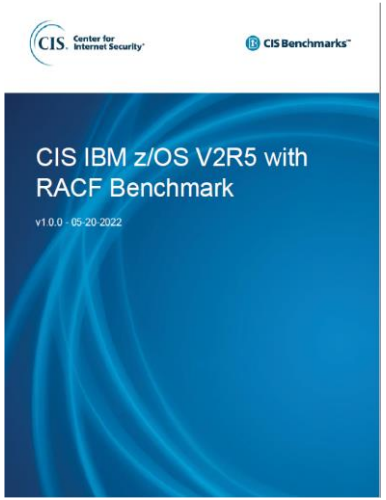
BACKUP

CENTER FOR INTERNET SECURITY (CIS) IBM Z/OS V2R5 WITH RACF BENCHMARK

CIS Benchmark for z/OS

- **The Center for Internet Security, Inc. (CIS®):**
  - Community-driven not-for-profit organization responsible for the CIS Controls® and CIS Benchmarks™, best practices for securing IT systems and data.

- **The z/OS V2R5 with RACF Benchmark:**
  - Contains 219 recommendations across 9 domains
    1. Identification and Authentication
    2. Authorization and Access Control Management
    3. Logging and Auditing
    4. System Resilience
    5. Storage Management
    6. Networking
    7. Cryptography and Encryption
    8. Job Management
    9. UNIX System Services



- https://www.cisecurity.org/benchmark/ibm_z
  - Provide contact information, link e-mailed