RACF ® Update for z/OS® 3.2

NY/Tampa/Dallas/Raleigh/Chicago RACF Users Group
19 November, 2025

Mark Nelson, RACF Development, CISSP®, CSSLP®, markan@us.ibm.com
Bruce Wells, RACF Development, brwells@us.ibm.com

RACF Update: What Did we Cover Before?

11 June, 2025

- **z/OS® 3.2 items**
  - RACF Support for Digital Certificates with multiple subject alt names
  - Granular data set encryption support for basic and large format data sets

- **Continuous Delivery**
  - Common Criteria Evaluation
  - Validated Boot
  - KEYSMSTR Class Enhancements
  - Stronger Encryption for Enveloped for Passwords/Password Phrases
  - Logging Supervisor State or Key 0 Opens of VSAM data sets

15 May 2024

- SPECIAL user password revocation prompt suppression
- Support for AES as the password-based encryption algorithm for PKCS#12 packages in both RACF and PKI Services
- RVARY password protection
- https://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/nyrug_2024_05_15_racf_update.pdf

RACF Update: What did we Cover Before...

11 October, 2023

- z/OS 3.1 Only
  - APPLAUDIT Enhancements
  - Custom Field Information in ACEE
- Continuous Delivery
  - Identity Token Enhancements
  - 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 SE PASSWORD(REVOKE(nnn)) value
  - Sharing RACF data base with RACF on z/VM
  - https://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/nyrug_2023_10_11_RACF_Update_3.1.pdf

More z/OS 3.2 Enhancements

RACF Update: What are we Covering Today?

- **User Quarantine/Containment**
- **OPERCMDS Authorization for RVARY**
- **Virtual Storage Constraint Relief (VSCR)**
- **Identity Token (IDT) Enhancement**
- **Supervisor State or Key Zero VSAM Opens**
- **New CIS Benchmark® for z/OS and RACF**
- **New function APAR: OA67750**

New Function APAR OA67750: Bypass Built in PassPhrase Rules

- **The built-in password phrase syntax rules may now be bypassed by:**
  - Defining a profile named PHRASE.BYPASS.BUILTIN.SYNTAX.RULES in the new OPTRACF class
  - and activating and RACLISTing the OPTRACF class

- **All of the following rules are bypassed (note the length rules are not included):**
  - Must not contain the user ID (as sequential uppercase or sequential lowercase characters)
  - Must contain at least 2 alphabetic characters (A - Z, a - z)
  - Must contain at least 2 non-alphabetic characters (numerics, punctuation, or special characters)
  - Must not contain more than 2 consecutive characters that are identical

New Function APAR OA67750: Bypass Built in PassPhrase Rules

- **SETROPTS LIST is updated to help you sort things out:**

```
PASSWORD PROCESSING OPTIONS:
  THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS KDFAES
  PASSWORD CHANGE INTERVAL IS 30 DAYS.
  PASSWORD CHANGE INTERVAL IS IN EFFECT FOR PASSWORD PHRASES.
  PASSWORD MINIMUM CHANGE INTERVAL IS 0 DAYS.
  MIXED CASE PASSWORD SUPPORT IS NOT IN EFFECT
  SPECIAL CHARACTERS ARE ALLOWED.
  NO PASSWORD HISTORY BEING MAINTAINED.
  USERIDS NOT BEING AUTOMATICALLY REVOKED.
  NO PASSWORD EXPIRATION WARNING MESSAGES WILL BE ISSUED.
  NO INSTALLATION PASSWORD SYNTAX RULES ARE PRESENT.
  NEW PHRASE EXIT ICHPWX11 IS [NOT] ACTIVE
  BUILT-IN PHRASE SYNTAX RULES ARE [NOT] BEING BYPASSED
```

New Function APAR OA67750: Bypass Built in PassPhrase Rules

- **The Github sample new phrase exit will be updated to allow selective enforcement of the bypassed rules**
  - https://github.com/IBM/IBM-Z-zOS/tree/main/zOS-RACF/Downloads/RexxPwExit

- **z/OS 3.2 PTF available now**
- **z/OS 3.1 PTF available early next week**

- **See https://www.ibm.com/support/pages/apar/OA67750 for more information**

Statement of Direction

Anomaly Detection, Notification, Quarantine:

IBM® plans to provide a software solution that introduces **cyber anomaly detection and notification** for the z/OS® platform to mitigate the potential risk of malicious software. IBM plans to provide **the option of quarantine functionality** that further extends existing remediation options. It is the intent for these combined functions, per NIST guidelines, to be used by the client to **satisfy compliance regulations** requiring anti-malware coverage for z/OS. This intent includes standards such as the Payment Card Industry Data Security Standard (PCI DSS) version 4.0.

10 September 2024 Announcement: IBM Threat Detection for z/OS 1.1 delivers AI-driven discovery of anomalies that could be indicative of a cyberattack

Link: https://www.ibm.com/docs/en/announcements/threat-detection-zos-11-delivers-ai-driven-discovery-anomalies-that-could-be-indicative-cyberattack

User Quarantine - Objective

REVOKE Attribute

- The **REVOKE** attribute can be used to prevent a user from successfully authenticating to z/OS applications.
- In many cases, *revoking a user with an active session does not remove their ability to continue to use RACF protected resources* from the application.
- **Exceptions:**
  - RACF does issue an ENF signal when a user is revoked, and some applications listen for the ENF signal and subsequently prevent the user from performing further actions.
  - Some applications have a way for a user's active session to be cancelled. Like the console command for TSO: C U=USERID
  - Applications perform third-party authorization checks

User Quarantine Objective

- Provide a way for a RACF administrator to prevent a user with an active security context from continuing to access RACF protected resources.

User Quarantine - ALTUSER

Quarantining a User

- Starting in z/OS 3.2, the **ALTUSER** command can be used to contain a user ID, which revokes the user ID and denies access to any RACF protected resources, even for currently active security contexts.

Syntax

```
ALTUSER userid
…
[ REVOKE [(date)] | NOREVOKE |
  CONTAIN | NOCONTAIN |
  NEVERCONTAIN | ALLOWCONTAIN ]
```

User Quarantine – ALTUSER Keywords

CONTAIN

Specifies that RACF is to prevent the user from accessing the system and immediately fail the user's subsequent access requests, even for currently active sessions.
If a RESUME date exists for this user, it is removed if CONTAIN is specified for the user.
This option also sets the REVOKE attribute in the user profile.

NOCONTAIN

Specifies that RACF is to allow access requests for the user in an active session to function normally.
The NOCONTAIN operand removes the user from the user containment list and removes the CONTAIN attribute from the user profile. NOCONTAIN has no effect on the REVOKE setting. To remove the REVOKE setting for a user, you must specify RESUME.

NEVERCONTAIN

Specifies that the user cannot be contained.
If the user is contained when this attribute is set, the user remains contained. In this case, it is necessary to enter a separate ALTUSER command with the NOCONTAIN option to remove the user from containment.

ALLOWCONTAIN

Removes the NEVERCONTAIN attribute from the user.

RESUME

Keyword is unchanged, but will fail if CONTAIN is already set for user. In this case, NOCONTAIN must be specified on the same command or on a previous command to process the RESUME keyword.

Note: *All containment keywords are mutually exclusive with the REVOKE keyword.*

User Quarantine - ADDUSER

Deleting a Contained User

- Does not remove it from the containment list, so that any active sessions for that user do not gain the ability to access RACF protected resources.

ADDUSER NOCONTAIN

- The ADDUSER command has the NOCONTAIN keyword to be able to add back a user that is currently contained.

Syntax:

```
ADDUSER userid
…
   [NOCONTAIN]
```

NOCONTAIN

If specified for a user ID that exists in the user containment list, the NOCONTAIN operand causes the user ID to be removed from the containment list, and thus removed from quarantine.

Usage note: The NOCONTAIN keyword is needed when the user ID that is being defined through ADDUSER was deleted after previously being placed in the containment list. NOCONTAIN removes the ID from that list and allows it to be defined again as a user that is able to access the system, based on the usual defined authorities.

User Quarantine – Authorization

User Quarantine Authorization

The ability to perform User Quarantine can be authorized by RACF SPECIAL or access to profiles in the FACILITY class.

- **SPECIAL** Authority required to use containment keywords - OR –

- **FACILITY** class profile **IRR.CONTAIN.USER**
  - **READ** – Allows use of CONTAIN keyword (ALTUSER or ADDUSER)
  - **UPDATE** – Allows use of CONTAIN, NOCONTAIN, NEVERCONTAIN and ALLOWCONTAIN keywords

User Quarantine – LISTUSER

LISTUSER for a Contained User:

- The LISTUSER command will now show CONTAIN status as a user attribute.

```
USER=ERIC  NAME=UNKNOWN  OWNER=IBMUSER   CREATED=23.237
DEFAULT-GROUP=SYS1     PASSDATE=N/A    PASS-INTERVAL=N/A PHRASEDATE=N/A
ATTRIBUTES=REVOKED CONTAINED GRPACC ATTRIBUTES=PROTECTED
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=UNKNOWN
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
…
```

User Quarantine – SETROPTS

Active Containment list

- The active containment list has the users CONTAINed since last IPL.
- Previously CONTAINed users are REVOKEd so they cannot initiate sessions, so they do not need to be in the active containment list.

SETROPTS Lists the Active Containment List

- SETROPTS lists the users in the active user containment list.
- Does not list all users with the CONTAIN attribute since that would require reading all user profiles.

SETROPTS LIST Examples

- **When No users contained:**

```
CONTAINED USERS: THERE ARE NO CONTAINED USERS
```

- **When some users contained:**

```
CONTAINED USERS:
  FRED     RACFUSR1 RACFUSR2
```

User Quarantine – Delivery

RACF User Quarantine support has been shipped back to z/OS 3.2 and 3.1:

- **Base support shipped via APARs:**
  - OA67286 (RACF 3.1 & 3.2)
  - OA67288 (SAF 3.1)

- **z/OS 2.5 has coexistence support for a shared DB that maintains containment settings when FLAG4 is updated**
  - OA67786 (RACF 2.5)

OPERCMDS Authorization for RVARY

- **OPERCMDS resources can be used to authorize the use of RVARY without requiring a console prompt in most cases.**
  - However, RVARY passwords should be established for exceptions when in failsoft mode.

- **READ access to the following OPERCMDS resources enables the use of the RVARY command:**
  - IRR.RVARY.STATUS when the ACTIVE or INACTIVE keyword is used
  - IRR.RVARY.SWITCH when the SWITCH, DATASHARE, or NODATASHARE keyword is used.

RACF Constraint Relief

- **DIAGxx PARMLIB CBLOC VIRTUAL31(IHAACEE3PTY)**
  - Directs RACF to allocate third-party ACEEs into 31-bit memory, providing 24-bit virtual storage constraint relief (VSCR)
  - Requires that clients verify that no AMODE(24) applications or exits reference the ACEE3PTY field in an ACEE.

- **RACF Address Space Reusable ASID**
  - The RACF subsystem address space now uses REUSASID=YES on its internal start so that the ASID is reused when the address space is terminated.
  - Clients should change any manual or automated start of the RACF subsystem to also specify REUSASID=YES.

IDT - New in 3.2 and OA65299

Starting with OA65299 (RACF) and OA66783 (SAF) for z/OS 3.1

- Add support to generate and validate RACF identity tokens (IDTs)with RSA signatures using secure ICSF CCA key labels
- Add support to generate and validate RACF IDTs with HMAC signatures using clear and secure ICSF CCA key labels

Value

- More secure and streamlined key distribution for RSA keys via digital certificates
- Option for CCA HMAC keys provides more flexibility and opportunity to use CCA secure HMAC keys in installations that do not have a crypto co-processor in EP11 mode.

IDT – New IDTPARMS Keywords

[IDTPARMS(

[SIGTOKEN(*pkcs11-token-name*) | NOSIGTOKEN]

[SIGSEQNUM(*pkcs11-sequence-number*) | NOSIGSEQ]

[SIGCAT(pkcs11-category) | NOSIGCAT]

[SIGLABELPRIMARY(*primary-label*)]

[SIGKIDPRIMARY(*primary-kid*)]

[SIGALG(HS256 | HS384 | HS512 |

RS245 | RS384 | RS512) | NOSIGALG]

[ANYAPPL(YES | NO)]

[IDTTIMEOUT(*timeout-minutes*)]

[PROTALLOWED (YES | NO)]

)

NOIDTPARMS]

Location of the signing key (PKCS#11 TKDS HMAC key)
Note: Does not support RSA

Location of the signing key (CCA CKDS RSA or HMAC key)

Key Identifier (KID) of SIGLABELPRIMARY

Signature algorithm to use

Whether IDTs can be used by other applications

Validity interval of a token

Whether IDT can authenticate a protected ID

Logging of Supervisor State or Key 0 VSAM OPENs

- **As documented in *z/OS DFSMS Using Data Sets:***
  - "VSAM OPEN routines bypass RACF security checking if the program issuing OPEN is in supervisor state or protection key 0".
    - No RACF call means access is allowed and no possibility for an SMF 80 record

- **APARs OA66738 and OA67032 allow you become aware of the places in which SAF check is being bypassed**

- **These APARs cause a REQUEST=AUTH to be performed against the resource STGADMIN.IGG.AUTO.BYPASS.LOG for READ authority in the FACILITY to write a log record**
  - Only successes are logged on authorization check (LOG=NOFAIL)
    - No log record is written if access is not allowed
  - The LOGSTR contains the data set name
    - `SAF CHECK BYPASSED FOR VSAM OPEN. PROGRAM NAME=<program name (8 char)>, JOB STEP=<job step name (8 char)>, DSN=<data set name (44 char)>`
  - Specifying AUDIT(SUCCESS) or AUDIT(ALL) causes the records to be written

Prevention of Supervisor State or Key 0 VSAM OPENs…

- **The installation on z/OS 3.1 (and earlier releases) of APARs OA66738 and OA67032 and the definition of a profile covering the resource STGADMIN.IGG.AUTO.BYPASS.LOG in the FACILITY class *will not affect the applications ability to OPEN the VSAM data set***
- **In 3.2 the *default behavior* for VSAM OPEN which the program issuing the OPEN is in supervisor state or protection key 0 is to no longer bypass the SAF check and the related RACF security check.**
- **If user has at least READ access authority to the resource STGADMIN.IGG.AUTO.BYPASS.ALLOW in the FACILITY class, the supervisor state or protection key 0 program will bypass the SAF check.**

z/OS Common Criteria

- **z/OS 2.5 has:**
  - **Completed the Common Criteria evaluation for version 4.3 of the Operating System Protection Profile (OSPP) and placed on the National Information Assurance Partnership (NIAP) Product Compliant List (PCL) (21 October, 2024)**
  - **Completed the Common Criteria Evaluation at an EAL4+ level of trust (29 September, 2025)**
  - **Details here:** https://www.commoncriteriaportal.org/products/index.cfm

Agenzia per la Cybersicurezza Nazionale

OCSI
Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) ve.3.1 rel. 5

Certificato n. *(Certificate No.)*	08/2024
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/ATS/05/2023/RC, v 1.0.
Decorrenza *(Date of 1st Issue)*	21 ottobre 2024
Nome e Versione del Prodotto *(Product Name and Version)*	IBM z/OS Version 2 Release 5
Sviluppatore *(Developer)*	IBM Corporation
Tipo di Prodotto *(Type of Product)*	Sistema Operativo
Conformità a PP *(PP Conformance)*	Protection Profile for General Purpose Operating Systems v.4.3
Funzionalità di sicurezza *(Conformance of Functionality)*	Funzionalità conformi a PP, CC Parte 2 estesa

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR *(CCRA recognition for components up to EAL2 and ALC_FLR only)*

Riconoscimento SOGIS MRA per componenti fino a EAL4 *(SOGIS MRA recognition for components up to EAL4)*

Roma, 21 ottobre 2024

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

Agenzia per la Cybersicurezza Nazionale

OCSI
Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) ve.3.1 rel. 5

Certificato n. *(Certificate No.)*	07/2025
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/ATS/07/2024/RC, v 1.0.
Decorrenza *(Date of 1st Issue)*	29 settembre 2025
Nome e Versione del Prodotto *(Product Name and Version)*	IBM z/OS Version 2 Release 5
Sviluppatore *(Developer)*	IBM Corporation
Tipo di Prodotto *(Type of Product)*	Sistema Operativo
Livello di Garanzia *(Assurance Level)*	EAL4+ (ALC_FLR.3) conforme a CC Parte 3
Conformità a PP *(PP Conformance)*	Nessuna
Funzionalità di sicurezza *(Conformance of Functionality)*	TDS specifico per il prodotto, conforme CC Parte 2 estesa

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR *(CCRA recognition for components up to EAL2 and ALC_FLR only)*

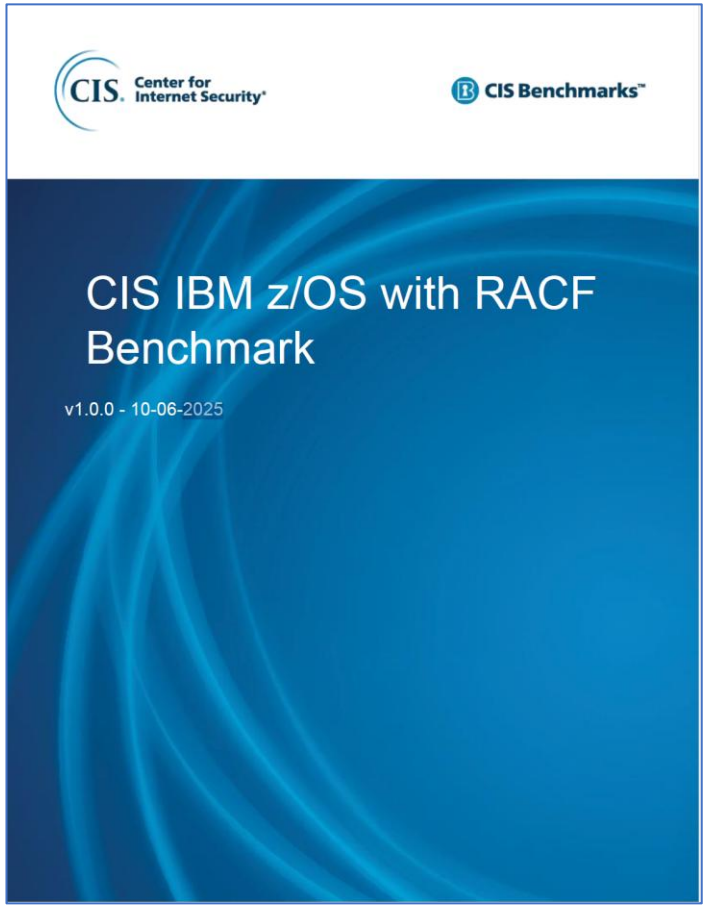
Riconoscimento SOGIS MRA per componenti fino a EAL4 *(SOGIS MRA recognition for components up to EAL4)*

Roma, 29 settembre 2025

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)
[ORIGINAL SIGNED]

CIS Benchmark

- **New version delivered in October, 2025:**
  - Not tied to a specific z/OS release (which is the reason for the reset to v1.0.0)
  - Document size increased by 200 pages:
    - Harmonized and consistent recommendation format
    - 20 new recommendations
  - Updated references to the CIS Critical Security Controls
    - The controls are mapped to well know standards (PCI DSS v4.0, DORA, SOC2)
  - https://www.cisecurity.org/cis-benchmarks



RACF ® Update for z/OS® 3.2

NY/Tampa/Dallas/Raleigh/Chicago RACF Users Group
19 November, 2025

Mark Nelson, RACF Development, CISSP®, CSSLP®, markan@us.ibm.com
Bruce Wells, RACF Development, brwells@us.ibm.com