z/OS 3.2 IBM Education Assistant

Solution Name: RACF User Quarantine

Solution Element(s): z/OS Security Server RACF

July 2025

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

- See URL http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Objectives (slide 1 of 2)

The Task:	Immediately removing RACF privilege of a user in an active session.
The Challenge:	In the current environment revoking RACF privilege of a user will only keep that user from initiating another session. Any sessions that have already authenticated will still be allowed access to RACF resources. There needs to be a way for the active users to be quarantined so that they are refused access, even from active sessions .
The Objective:	Provide a way for an administrator to quarantine active users.
The Solution:	Extend z/OS Security Server RACF to contain a user, such that future authorization requests from that user are denied.

Objectives (slide 2 of 2)

Background

If it is determined that a user needs to be denied access to the system it can be given the REVOKE attribute. This will keep the user from obtaining a new security context and using it to access resources. This, however, does not restrict users that already have security contexts and they will have normal access until their session ends.

Hence, the objective: provide a way for an administrator to keep a user with a way to keep a user with an active security context from continuing to access RACF resources.

Overview

- Who (Audience)
  - Security Administrators architecting protection of system resources
  - RACF Administrators managing user access
- What (Solution)
  - RACF updates to implement immediate revocation of access by a user Wow (Benefit / Value, Need Addressed)
  - Issue: Users are currently revoked for new session initiation, but active sessions still provide access to system resources
  - Benefit: Users will have no ability to access RACF-protected resources via containment aware services, even in active sessions

Usage & Invocation – ALTUSER Command (slide 1 of 16)

The ALTUSER command will now be able to cause revocation of access in all sessions, which includes active sessions

Syntax

```
>> ALTUSER  --->

>-------------------------------------------------------------->
 |--- REVOKE(date) | NOREVOKE | CONTAIN | NOCONTAIN
      | NEVERCONTAIN | ALLOWCONTAIN                    ---|
```

Usage & Invocation – ALTUSER Command (slide 2 of 16)

Syntax

CONTAIN – Behaves the same as the REVOKE keyword without a date and in addition causes all future access requests to fail in active sessions. If a RESUME date exists for this user, it will be removed.

NOCONTAIN – Will allow access requests from active sessions to function normally. The NOCONTAIN option does not resume the user ID. To resume a user with CONTAIN status, the RESUME keyword must be specified as well.

NEVERCONTAIN – Will disallow a user from being contained. If a user is contained when this attribute is set, the user will remain contained. A separate ALU command can be issued with NOCONTAIN to remove containment of this user.

ALLOWCONTAIN – Will remove the NEVERCONTAIN attribute from a user

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

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

Authorization

SPECIAL Authority required to use these keywords OR

FACILITY class profile IRR.CONTAIN.USER

READ – Allows use of CONTAIN keyword

UPDATE – Allows use of CONTAIN, NOCONTAIN, NEVERCONTAIN and ALLOWCONTAIN keywords

ICH21005I NOT AUTHORIZED TO SPECIFY *operand*, OPERAND IGNORED

Usage & Invocation – ALTUSER Command (slide 3 of 16)

New Messages

ICH21024I CANNOT RESUME USER *userid* WITH CONTAIN ATTRIBUTE

Explanation: The user being altered has the CONTAIN attribute. NOCONTAIN must be specified to allow RESUME

System action: RESUME is not processed for this user and the command continues

USER response: Specify NOCONTAIN and try again

Module: ICHCCU00

ICH21025I CANNOT CONTAIN USER *userid* WITH NEVERCONTAIN ATTRIBUTE

Explanation: The user being altered has the NEVERCONTAIN attribute. NEVERCONTAIN must be removed to allow CONTAIN to be specified

System action: CONTAIN is not processed for this user and the command continues

USER response: Specify ALLOWCONTAIN and try again

Module: ICHCCU00

ICH21026I USER *userid* NOT UPDATED IN CONTAINMENT LIST

Explanation: The user being altered has been updated in the database, but the in-storage containment list has not been updated

System action: The command continues

USER response: Contact the Security Administrator to determine why the list update failed. Possible reasons are a full containment list or the RACF address space not being available.

Module: ICHCCU00

ICH21005I NOT AUTHORIZED TO SPECIFY CONTAIN/NOCONTAIN/NEVERCONTAIN/ALLOWCONTAIN, OPERAND IGNORED.

(New keyword insert)

Explanation: The invoker of the command does not have authority to the keyword being specified

System action: The command terminates

USER response: Get authority to the keyword

Module: ICHCCU00

Usage & Invocation – List Processing (slide 4 of 16)

New Message

IRR423I LIST *listname* **FULL.** *entryname* **NOT ADDED.**

Explanation: Adding an entry to a list has failed because the maximum number of entries has been reached.

For example, when adding to USERQ, the list of contained users, the user's profile has been updated, but the userid has not been added to the active list of users with CONTAIN status because the list contains 100 users. That user's active sessions will still have normal access.

System action: The list is unchanged

USER response: Contact Security Administrator

Operator Response: Contact Security Administrator

RACF Security Administrator response: Determine why so many entries are on the referenced list and remediate the cause. Then redrive the action that failed to update the list previously.

For example, for USERQ, determine why so many users are being contained and remediate the cause. Update users that should not be contained by setting NOCONTAIN in their RACF profiles, which will free up space in the active list of contained users. Then issue ALTUSER with CONTAIN for the original, failing user to add them to the list.

Descriptor code:
4
- **System Status**

Routing Codes:
9
- **System Security**
- The message gives information about security checking, for example, a request for a password.

Usage & Invocation – ADDUSER Command (slide 5 of 16)

The ADDUSER command will now allow a non-existent user to be removed from the active containment list so that it can be added to the database. This is needed when a contained user is deleted and needs to be added again during the lifetime of an IPL.

Syntax

```
>> ADDUSER  --->

>-------------------------------------------------------->
 |--- NOCONTAIN ---|
```

Usage & Invocation – ADDUSER Command (slide 6 of 16)

Syntax

NOCONTAIN – Will remove a non-existant user from the containment list to allow it to be added to the database again.

Authorization

SPECIAL Authority required to use the NOCONTAIN keyword OR
FACILITY class profile IRR.CONTAIN.USER
UPDATE – Allows use of NOCONTAIN keyword

ICH01028I COMMAND ENDED, NOT AUTHORIZED TO SPECIFY NOCONTAIN

Usage & Invocation – ADDUSER Command (slide 7 of 16)

New Messages

ICH01026I *userid* is contained. User not added.

Explanation: The user being added has the CONTAIN attribute. NOCONTAIN must be specified to remove the user from the containment list

System action: The user is not added

USER response: Specify NOCONTAIN and try again

Module: ICHCAU00

ICH01027I *userid* not updated in containment list.

Explanation: The user being added failed removal from the in-storage containment list.

System action: The user is not removed

USER response: Contact the Security Administrator to determine why the list update failed. A possible reason is the RACF address space is not available.

Module: ICHCAU00

ICH01028I COMMAND ENDED, NOT AUTHORIZED TO SPECIFY NOCONTAIN

Explanation: You do not have sufficient authority to specify the NOCONTAIN keyword.

System action: The command terminates

USER response: Obtain authority to specify NOCONTAIN and try again

Module: ICHCAU00

Usage & Invocation – ENF Signals (slide 8 of 16)

New ENF Signals

- ENF 71
  - Qualifiers currently being used for commands and REQUEST=VERIFY
  - IRRPENF2 New Qualifiers (Offset ‘0C’X)
    - IRR_ENF2Q_CONTAIN (02)
    - IRR_ENF2Q_NOCONTAIN (01)
- ALTUSER & ADDUSER
  - Issues ENF71 for CONTAIN/NOCONTAIN
  - Issues ENF71 for REVOKE when CONTAIN specified

Usage & Invocation – RACF DB (slide 9 of 16)

Database updates

- FLAG4 field in User profile
  - Bit0 still denotes revocation
  - Bit1 denotes CONTAIN attribute
  - Bit2 denotes NEVERCONTAIN attribute

DBUNLOAD updates

User basic data record (0200)

Field Name	Type	Position		Comments
		Start	End	
USBD_CONTAIN	Char	650	653	Is the user CONTAINed? Valid Values include "Yes" and "No".
USBD_NEVERCONTAIN	Char	655	658	Is the user disallowed the CONTAIN attribute? Valid Values include "Yes" and "No".

Usage & Invocation LISTUSER Command (slide 10 of 16)

The LISTUSER command will now show CONTAIN status

This example shows a user that was CONTAINed prior to NEVERCONTAIN being set

Output

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

Usage & Invocation – SETROPTS Command (slide 11 of 16)

- SETROPTS will return the list of users in the active user containment list.
  - List has users CONTAINed since last IPL
    - Previously CONTAINed users are REVOKEd so cannot initiate sessions
  - Will not return all users with attribute since it would require read of all users in DB to check setting

  - New output line:

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

Usage & Invocation – User Lookup (slide 12 of 16)

- RCVT will have bit RCVTCONT set if there are users in the containment list
- SMF 80 record for found contained user
  - New event code 92
  - New RELOCATE 68 (Security Event)
    - Contains user affected by the event and calling routine when failure occurred
    - Qualifier 0 is for containment
    - Intended to have additional qualifiers
    - Security Event Record Extension

Field name	Type	Length	Position		Comments
			Start	End	
SECE_USERID	Char	8	282	289	USERID associated with the event
SECE_MODULE	Char	8	291	298	The module associated with the event

  - New version of ICH408I secondary message

```
VIEW       RACFTEST.SAFID.SMFUNLD(ERIC) - 01.00            Columns 00001 00072
000054 SECEVENT CONTAIND 09:38:37 2024-09-12 IM13 NO   NO   NO   FRED     SYS1
000055 SECEVENT CONTAIND 09:38:46 2024-09-12 IM13 NO   NO   NO   FRED     SYS1
000056 SECEVENT CONTAIND 09:38:59 2024-09-12 IM13 NO   NO   NO   FRED     SYS1
```

```
VIEW       RACFTEST.SAFID.SMFUNLD(ERIC) - 01.00            Columns 00282 00353
000054 FRED     ICHRFC00
000055 FRED     ICHCRV00
000056 FRED     IRRENV00
```

```
RACFR31   ICH408I USER(FRED     ) GROUP(SYS1     ) NAME(####################)
SECURITY EVENT(CONTAIND) USER(FRED     ) MODULE(IRRENV00)
RACFR31   ICH408I USER(FRED     ) GROUP(SYS1     ) NAME(####################)
SECURITY EVENT(CONTAIND) USER(FRED     ) MODULE(ICHCRV00)
RACFR31   ICH408I USER(FRED     ) GROUP(SYS1     ) NAME(####################)
SECURITY EVENT(CONTAIND) USER(FRED     ) MODULE(ICHRFC00)
```

Usage & Invocation – User Lookup (slide 13 of 16)

Contained User Lookup Points

- RACROUTE
  - REQUEST=AUTH
  - REQUEST=FASTAUTH
- RACHECK
- FRACHECK
- RACF Callable Services
  - CK_ACCESS
- RACF Command Envelope
- RACDCERT
- RVARY
- RACLINK
- RACMAP
- RACPRIV
- RACPRMCK

Usage & Invocation- RACROUTE (slide 14 of 16)

New RACROUTE Return Code (SAF RC, RACF RC, RSN) 8,8,xx

- ‘CC’x - RACROUTE request failed, invoking user has CONTAIN attribute (Contained Caller)
- ‘CD’x - RACROUTE request failed, passed user has CONTAIN attribute (Contained Delegate)

- REQUEST=AUTH
- REQUEST=FASTAUTH
- Additional services will have consistent RCs across RACROUTE calls as they adopt enforcing containment

Usage & Invocation – CK_ACCESS (slide 15 of 16)

New Reason Code ‘CC’x

- Request failed, invoking user has CONTAIN attribute (Contained Caller)

- Will be consistent across all SAF callable services as they enforce containment

Usage & Invocation – New/Reused Messages (slide 16 of 16)

- RACF Envelope
  IRRV023I You are not authorized to issue this command.
- RACDCERT (existing msg)
  - IRRD101I You are not authorized to issue the RACDCERT command
- RACLINK
  - IRRS009I You are not authorized to issue the RACLINK command.
- RACMAP (existing msg)
  - IRRW201I You are not authorized to issue the RACMAP command.
- RACPRIV (existing msg)
  - IRRW002I You are not authorized to issue the RACPRIV command.
- RACPRMCK
  - IRRY306I You are not authorized to issue the RACPRMCK command.
- RVARY
  - ICH15033I YOU ARE NOT AUTHORIZED TO ISSUE THE RVARY COMMAND

Interactions & Dependencies

- Software Dependencies
  - None.
- Hardware Dependencies
  - None.
- Exploiters
  - N/A

Upgrade & Coexistence Considerations

Systems sharing the RACF database will not allow new sessions to be created after CONTAIN is set since REVOKE is also set in the user's profile, but active sessions will be unaffected until the ENF signal is processed or CONTAIN is specified on the sharing system

Downlevel sharing systems will not acknowledge the setting of CONTAIN but will still acknowledge REVOKE, which is set when CONTAIN is specified

Installation & Configuration

- Are any APARs or PTFs needed for enablement? OA67286 OA67288 (function available on z/OS 3.1)
- What jobs need to be run? No new jobs are required.
- What hardware configuration is required? No special configuration is required.
- What PARMLIB statements or members are needed? No new members are needed.
- Are any other system programmer procedures required? No.
- Are there any planning considerations? No.
- Are any special web deliverables needed? No.
- Does installation change any system defaults? No.

Summary

- RACF now provides the ability to contain a user which in effect quarantines them, stopping them from accessing RACF resources from active sessions.
  - Allows administrators to immediately revoke privilege of a user to protect the system

Appendix

IBM Publications

Security Server RACF Callable Services

- CK_ACCESS new reason code
- R_Admin new user profile fields

Security Server RACF Command Language Reference

- ADDUSER command updates
- ALTUSER command updates
- LISTUSER output updates
- SETROPTS LIST output

Security Server RACF Data Areas

- RCVT and IRRPENF2 update

Security Server RACOUTE Macros Reference

- New return codes for REQUEST=AUTH, REQUEST=FASTAUTH and FRACHECK

Security Server RACF Messages and Codes

- New messages and ABEND code

Security Server RACF Security Administrator's Guide

- Section describing containment

Security Server RACF Auditor’s Guide

- DSMON updates

z/OS MVS Programming: Authorized Assembler Services Guide

- ENF 71 qualifiers