

z/OS 3.2 IBM Education Assistant

Solution Name: zSecure 3.2 (Admin/Audit/Adapters/CICS Tk/Cmd Verifier/Alert), zSCC 1.3

Solution Element(s): 5655-ABB 5655-ABC 5655-ABA 5655-ABD 5655-ABE 5655-ABG 5655-CC1

July 2025



Agenda

- Trademarks
- Objectives
- Overview
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Multi-Factor Authentication administration
- zSecure Admin Web UI
- Support for RACF enhancements
- Compliance standards
- IBM Threat Detection for z/OS
- Ideas
- Installation & Configuration
- Summary

Trademarks

- See url <http://www.ibm.com/legal/copytrade.shtml> for a list of trademarks.
- Additional Trademarks:
 - Center for Internet Security, CIS, and CIS Benchmark are trademarks of the Center for Internet Security (an independent nonprofit organization)
 - ACF2 is a trademark of Broadcom

Objectives

Describe new function in zSecure 3.2 and Z Security and Compliance Center 1.3

- Currency for z/OS Security Server (and other z/OS elements)
- Extended support for Multi-Factor Authentication administration
- Additional developments in the zSecure Admin web user interface
- Advances in compliance checking
- and more

Notes:

- zSecure 3.2 is **required** for support of z/OS 3.2 (but can also run on z/OS 2.5)
- zSCC 1.3 includes all of zSecure Audit 3.2.
- zSecure CICS Toolkit does not run on the z/OS platform directly.

Overview

- Who (Audience)
 - Systems programmers, Security administrators, Auditors, Compliance Assessors
- What (Solution)
 - Makes security administration, security compliance, and security compliance checking easier
- Wow (Benefit / Value, Need Addressed)
 - Provides easy interface for RACF administration and reporting
 - Reduces need for green screen skills by allowing web browser interaction
 - Reduces time spent on compliance checking through automation and built-in knowledge

Interactions & Dependencies

- Software Dependencies
 - Runs on any currently supported z/OS release
 - The zSecure portfolio and zSCC are priced software products
 - Besides the solution elements, there are some solution packages that contain several of them:
<https://community.ibm.com/community/user/security/blogs/jeroen-tigelman/2019/12/01/ibm-security-zsecure-administration-auditing-and-c>
- Hardware Dependencies
 - None, except as possibly implied by z/OS releases in support
 - Report engine: better performance on z15 and above

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level:
No, runs on any currently supported z/OS release
- As zSecure Command Verifier parses RACF commands in order to determine their conformance to policy, it requires updates whenever new commands or keywords are introduced. When z/OS Security Server puts such updates into the service stream, the required PTFs are usually linked via ++IF REQ.
- A new report engine load module **CKR8Z15** is included, while CKR4Z196 is dropped. If you give PROGRAM-controlled access, this might require updates. The option to use a 31-bit report engine has been removed from SE.0.
- There is **no zSecure Visual 3.2** (5655-ABF, the “Windows UI”).
End of marketing was announced in December 2024, with the replacement product being zSecure Admin (5655-ABB), which introduced a Web UI in October 2024.
Solution packages that included it no longer do, and the solution package with only Admin and Visual (5655-ABH, “Administration”) is no longer there.

Multi-Factor Authentication administration enhancements

MFA administration in zSecure Admin – ISPF UI (1)

On the detail display of RA.U (RACF administration – User), I(insert)

[ZSECURE-I-571](#)

The screenshot shows two ISPF panels. The main panel is titled "zSecure USER MFAUSER overview" and displays various user configuration options. A secondary panel, titled "zSecure - Insert factor", is overlaid on the main panel, listing 18 different MFA factor types with their descriptions.

Main Panel (zSecure USER MFAUSER overview):

- Command ==> Users like MFAUSER
- Line 39 of 75
- Scroll==> CSR
- 20 Mar 2025 16:16
- Security level: DASD administrator OPERATIONS No
- Categories list: Global audit set/list AUDITOR No
- Global audit list: ROAUDIT No
- Class authority
- Safeguards:
 - Ignore UACC/Glob/* RESTRICTED No
 - Log all user actions UAUDIT No
- MFA factor name: Act MFAactive
- MFA policy name
- Linked node.user Type Stat Pwd Defin
- Digital certificate labels: Digital
- *ZSECURE

Pop-up Panel (zSecure - Insert factor):

| Number | Factor Type | Description |
|--------|---------------------|------------------------------|
| 1 | AZFCERT1 | PIV/CAC or X.509 Certificate |
| 2 | AZFCKCTC | MFA Check CTC |
| 3 | AZFCKCTC TVT6081 | MFA Check CTC |
| 4 | AZFFALBK | User Driven Fallback |
| 5 | AZFLDAP1 | LDAP |
| 6 | AZFLDAP1 #VARIANT1 | LDAP |
| 7 | AZFLDAP1 #VARIANT2 | LDAP |
| 8 | AZFMETAS | CKCTC PolicyAuth protection |
| 9 | AZFPASS1 | Password or Passphrase |
| 10 | AZFPPTK1 | PassTicket |
| 11 | AZFRADP1 | Generic RADIUS |
| 12 | AZFRADP1 FORSANDERG | Generic RADIUS |
| 13 | AZFSFNP1 | SafeNet RADIUS |
| 14 | AZFSIDP1 | RSA SecurID ACEv5 UDP |
| 15 | AZFSIDP3 | RSA SecurID Auth API (HTTPS) |
| 16 | AZFSIDR1 | RSA SecurID RADIUS |
| 17 | AZFTOTP1 | TOTP |

MFA administration in zSecure Admin – ISPF UI (2)

The configuration panel depends on the factor chosen.

In this example, overrides can be specified to the default AZFEXEC configuration.

Menu Options Info Commands Setup

Insert TOTP factor

Command ==> _____

User ID : MFAUSER
Factor name : AZFTOTP1
Registration state : Not open

Set options below and press Enter to open factor for registration
- Make factor active

Set AZFTOTP1 parameters
Digest Algorithm : (SHA1, SHA256, SHA384, or SHA512)
Token Code Length : (6, 7, or 8 digits)
Token Period : (15, 30, or 60 seconds)
Skew Window : (1-10 intervals)

*ZSECURE
MA + d

zSecure - Confirm command

Command ==> _____

Ticket ID
Description More _____

Confirm or edit the following command
altuser MFAUSER mfa(factor(AZFTOTP1) active tags(REGSTATE:OPEN ALG:SHA384 NUMDIGITS:6 PERIOD:60 WINDOW:2))

Command execution . 1 1. QUEUE RACF command
2. QUEUE CKGRACF command (allows use of Reason)
3. ASK administrator to execute CKGRACF command
4. REQUEST CKGRACF command for later execution
5. WITHDRAW CKGRACF command

Reason
*ZSECURE
MA + d

MFA administration in zSecure Admin – ISPF UI (3)

After executing, the S(elect) and D(elete) actions are also available

```
zSecure USER MFAUSER overview                               Line 39 of 81
Command ==> _                                         Scroll==> CSR
Users like MFAUSER                                     20 Mar 2025 16:32

Security level                                         DASD administrator OPERATIONS No
Categories list                                       Global audit set/list AUDITOR No
                                                       Global audit list ROAUDIT No
                                                       Class authority

Safeguards
Ignore UACC/Glob/* RESTRICTED No
Log all user actions UAUDIT No

MFA factor name      Act MFAactive
AZFTOTP1           Yes 20Mar2025
MFA factor          Tag
AZFTOTP1            REGSTATE
AZFTOTP1            ALG
AZFTOTP1            NUMDIGITS
AZFTOTP1            PERIOD
AZFTOTP1            WINDOW

MFA policy name

Linked node.user   Type    Stat Pwd  Defined (GMT)     Approved (GMT) Creator
*ZSECURE

MA + d                                         02/015
```

OPEN will become PROVISIONED by registering, that is, by going to <https://hostname:6789/AZFTOTP1/GenericStart>, logging on with userid and password, and loading the QR code presented into a One Time Password generator such as IBM Verify or Google Authenticator. Afterwards R(e-register) will also be available, to go back to OPEN.

MFA administration in zSecure Admin – Web UI

- In the Web UI it looks like this (subject to further adjustments):

The image displays two screenshots of the zSecure Admin – Web UI interface for managing Multi-Factor Authentication (MFA).

Left Screenshot: Shows the "Manage Multi-Factor Authentication" page for user CRMBRL1. It lists "Configured factors" with the following data:

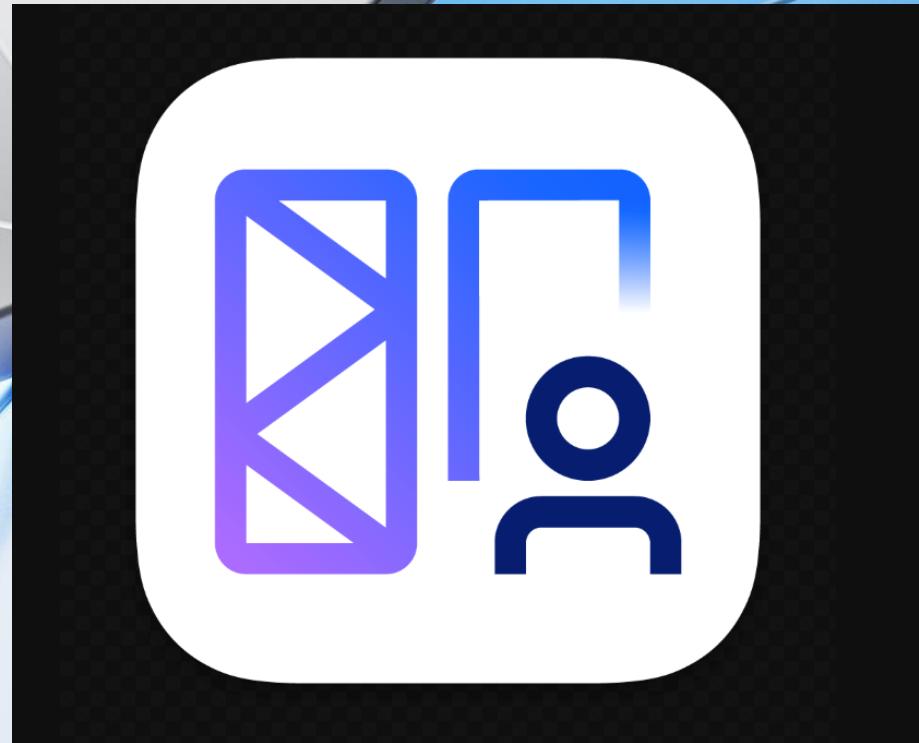
| Factor | Status | FactorActiveDate | Registration state |
|----------|--------|------------------|--------------------|
| AZFRADP1 | No | | |
| AZFTOTP1 | No | | OPEN |
| AZFLDAP1 | No | | |
| AZFYUBI1 | No | | CONFIRMED |
| AZFCERT1 | No | | OPEN |
| AZFPASS1 | No | | |

Right Screenshot: Shows the "Edit Factor" dialog for factor AZFTOTP1. The dialog fields are:

- Registration State:** OPEN
- Status:** Off (toggle switch)
- Digest Algorithm:** SHA256
- Skew window interval (1 - 10):** 6
- Token Code Length (digit):** 8
- Token Period (seconds):** 60

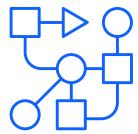
Buttons at the bottom of the dialog include "Cancel" and "Submit".

zSecure Admin Web UI



New icon

Feature highlights



Simplified management

A web-based zSecure plugin for z/OSMF to administer, control and customize certain security tasks

Based on customer feedback, the new zSecure Admin GUI addresses a need to simplify RACF administration and provide a more user-friendly environment for experienced and new RACF admins.



Secure administration¹⁴

Establishes secure connection directly with RACF via z/OSMF and verifies user credentials



Pre-built role management

Access to functions is based on customizable roles with pre-built roles for helpdesk, admins etc.



Modern design

Based on IBM Carbon, the design language of the interface is easy to grasp and use

Web user interface – selection results (1)

ZSS-1133

Redesigned for better user experience; before:

The screenshot shows a web-based user interface for IBM Security zSecure. The top navigation bar includes links for 'IBM Security zSecure', 'RACF', 'User', and 'User Selection Results'. Below the navigation is a search bar with placeholder text 'Press Enter to search'. The main content area is titled 'User selection results' and displays a table of user data. The table has 18 columns: User, Name, DfltGrp, Complex, Owner, Restricted, Revoked, Inactive, Protected, Special, Operator, Auditor, ROAudit, GroupSOA, CIAuth, HasCert, and PassExp. The 'Add user/segment' button is located at the top right of the table. The table contains 13 rows of data, each representing a user entry. At the bottom of the page, there are pagination controls for 'Items per page' (set to 20), '1-20 of 25 items', and '1 of 2 pages'.

| User | Name | DfltGrp | Complex | Owner | Restricted | Revoked | Inactive | Protected | Special | Operator | Auditor | ROAudit | GroupSOA | CIAuth | HasCert | PassExp |
|----------|----------------------|---------|----------|-------|------------|---------|----------|-----------|---------|----------|---------|---------|----------|--------|---------|---------|
| TEST# | USER FOR WZ1103055 2 | CRMQA | S8017NOD | CRMQA | - | Revoked | - | Protected | - | - | - | - | - | - | - | - |
| TESTER | | CRMB | SPL87NOD | CRMB | - | - | - | Protected | - | - | - | - | - | - | - | - |
| TESTJDBC | JUDITH RUIJTER | CRMB | SPL87NOD | CRMB | - | Revoked | - | - | - | - | - | - | - | - | - | PassExp |
| TESTMR1 | | CRMB | SPL87NOD | SYS1 | - | - | - | - | - | - | - | - | - | - | - | PassExp |
| TESTPP1 | TEST USER | CRMB | S8017NOD | SYS1 | - | - | - | Protected | - | - | Auditor | - | - | - | - | - |
| TESTSI13 | | CRMB | SPL87NOD | CRMB | - | - | - | - | - | - | - | - | - | - | - | PassExp |
| TESTUID1 | TEST 4 TESTUID1 | CRMQA | SPL87NOD | CRMQA | - | - | - | Protected | - | - | - | - | - | CIAuth | - | - |
| TESTUID1 | TEST 4 TESTUID1 | CRMQA | S8017NOD | CRMQA | - | - | - | Protected | - | - | - | - | - | CIAuth | - | - |
| TESTU1 | TEST 4 TESTU1 | CRMQA | SPL87NOD | CRMQA | - | - | - | Protected | - | - | - | - | - | CIAuth | - | - |
| TESTU1 | TEST 4 TESTU1 | CRMQA | S8017NOD | CRMQA | - | - | - | Protected | - | - | - | - | - | CIAuth | - | - |
| TESTU2 | TEST 4 TESTU2 | CRMQA | SPL87NOD | CRMQA | - | - | - | - | - | - | - | - | - | CIAuth | - | PassExp |
| TESTU2 | TEST 4 TESTU2 | CRMQA | S8017NOD | CRMQA | - | - | Inactive | - | - | - | - | - | - | CIAuth | - | PassExp |
| TEST001 | | CRMB | SPL87NOD | CRMB | - | - | - | - | - | - | - | - | - | - | - | - |

Web user interface – selection results (2)

Redesigned for better user experience; after:

The screenshot shows a modern web-based application interface for managing user selection results. The top navigation bar includes links for 'IBM Security zSecure', 'RACF', 'User', and 'User Selection Results'. Below the navigation is a search bar and a 'User selection results' section titled 'All users'. The main content area is a table with various columns representing user attributes like 'User', 'Complex', 'Name', 'DfltGrp', 'Owner', and many security-related fields such as 'Revoked', 'Inactive', 'Protected', 'Contained', 'Special', 'Operator', 'ROAudit', 'Nevercontain', 'GroupSOA', 'CIAuth', 'HasCert', 'PassExp', 'PhrExp', 'MFA', 'MFAFallback', and 'vMFA'. The table lists numerous user entries, each with a unique identifier (e.g., \$SSLIMIT, \$SSTEST1, #, ##, ###, #####, #####, ######, #######, ########, #########, irrcerta, irrmulti, irrsitec, AA1, ACFSTCID, ADM@ACL, ADM@SRV, AEISA) and specific details like 'CRMQA' as the complex and 'SYSTEST' as the owner. At the bottom of the table, there are pagination controls for 'Items per page' (set to 20), a total count of '1–20 of 6915 items', and '346 pages'.

Web user interface – line commands (1)

Redesigning for better user experience; before:

User password/phrase

Specify password/phrase action for User ID **TESTER**

Page 1 User password/phrase Page 2 Multi-system options

| | | |
|--|-----------|-------------------------------------|
| Userid | TESTER | Name |
| Last use date | 14Sep2015 | Last use time |
| Password changed | | Phrase changed |
| Revoked | No | Revoke inactive |
| Revoke date | | Resume date |
| Has a password | - | Has a phrase |
| Protected | No | |
| Installation data | | |
| Select password or phrase: <small>(1)</small> | | |
| <input checked="" type="radio"/> Password <input type="radio"/> Phrase <input type="radio"/> Protected | | |
| Select action: <small>(1)</small> | | |
| <input type="radio"/> No change <input type="radio"/> Remove <input checked="" type="radio"/> Specify new value <input type="radio"/> Set to default <input type="radio"/> Set to previous <input type="radio"/> Set to random | | |
| Options: <small>(1)</small> | | |
| <input checked="" type="radio"/> Default expiry <input type="radio"/> Expiry <input type="radio"/> No Expire | | |
| <input type="button" value="Cancel"/> | | <input type="button" value="Next"/> |

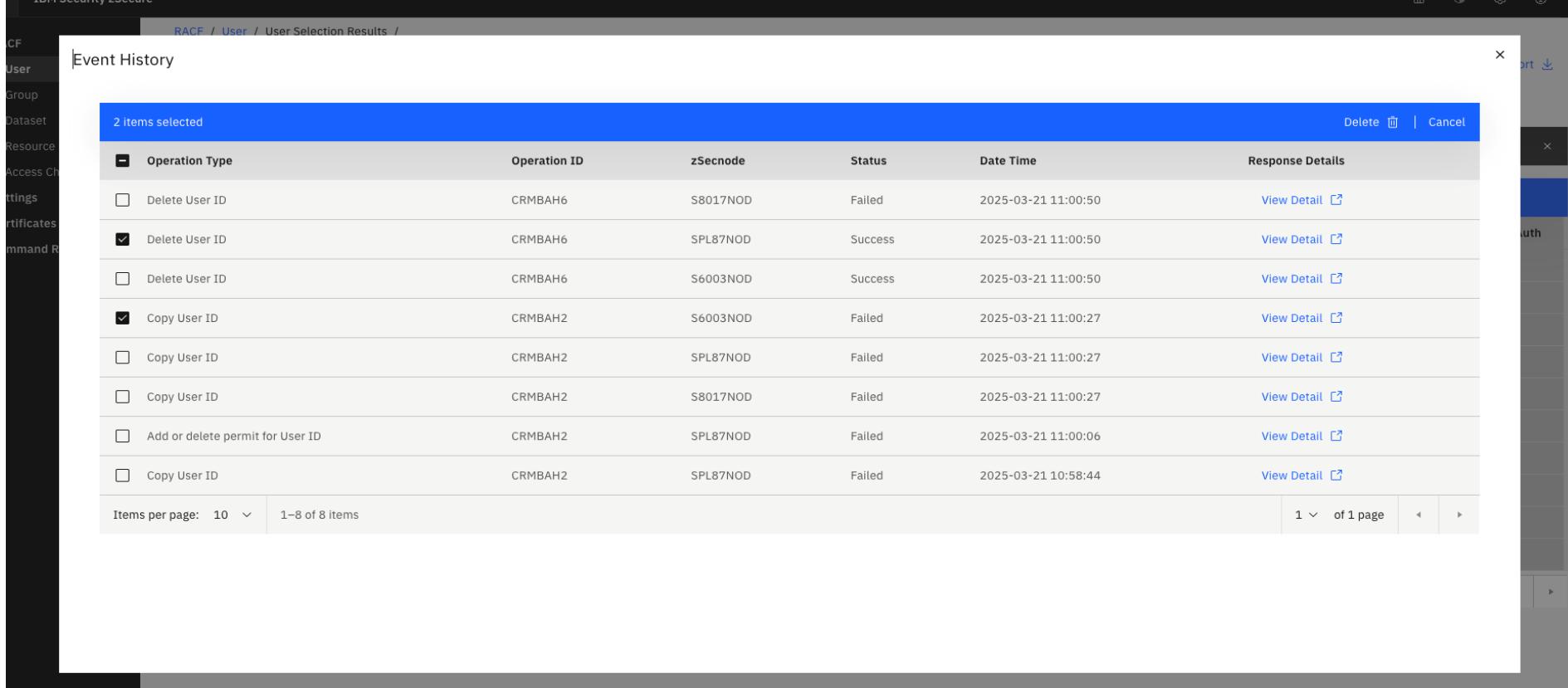
Web user interface – line commands (2)

Redesigning for better user experience; after:

The screenshot shows a modernized web interface for password management. The title bar reads '\$SSLIMIT' and the main heading is 'Manage password or phrase'. A sub-instruction below says 'Create a new password, edit an existing password or remove a password for the user.' On the left, there's a sidebar with a list of users ('Revolution', 'HasCert', etc.) and a 'Revoke' button. The main content area has three tabs: 'Manage Password' (selected), 'Generate ticket ID', and 'Select systems'. Under 'Manage Password', there are sections for 'Authentication type' (radio buttons for 'Password', 'Phrase', and 'Protected', with 'Password' selected), 'Password creation method' (dropdown 'Specify new value'), 'Expiry duration' (dropdown 'Default expiry'), and fields for 'New Password*' and 'Repeat Password*'. Below these are 'CKGRACF command actions' with checkboxes for 'Ignore history', 'Bypass exits', 'Bypass rules', and 'Resume user id after password creation' (which is checked). At the bottom are 'Cancel', 'Back', and a large blue 'Next' button.

Web user interface – history tab

History is now persistent across sessions, and adds detail such as target ID:



The screenshot shows a web-based interface for managing RACF users. The left sidebar includes options like CF, User, Group, Dataset, Resource, Access Changes, Certificates, and Command Run. The main navigation bar is at the top: RACF / User / User Selection Results. Below it, a sub-menu shows 'Event History'.

The central area displays a table titled 'Event History' with the message '2 items selected'. The table has columns: Operation Type, Operation ID, zSecnode, Status, Date Time, and Response Details. The data is as follows:

| Operation Type | Operation ID | zSecnode | Status | Date Time | Response Details |
|---|--------------|----------|---------|---------------------|-----------------------------|
| <input type="checkbox"/> Delete User ID | CRMBAH6 | S8017NOD | Failed | 2025-03-21 11:00:50 | View Detail |
| <input checked="" type="checkbox"/> Delete User ID | CRMBAH6 | SPL87NOD | Success | 2025-03-21 11:00:50 | View Detail |
| <input type="checkbox"/> Delete User ID | CRMBAH6 | S6003NOD | Success | 2025-03-21 11:00:50 | View Detail |
| <input checked="" type="checkbox"/> Copy User ID | CRMBAH2 | S6003NOD | Failed | 2025-03-21 11:00:27 | View Detail |
| <input type="checkbox"/> Copy User ID | CRMBAH2 | SPL87NOD | Failed | 2025-03-21 11:00:27 | View Detail |
| <input type="checkbox"/> Copy User ID | CRMBAH2 | S8017NOD | Failed | 2025-03-21 11:00:27 | View Detail |
| <input type="checkbox"/> Add or delete permit for User ID | CRMBAH2 | SPL87NOD | Failed | 2025-03-21 11:00:06 | View Detail |
| <input type="checkbox"/> Copy User ID | CRMBAH2 | SPL87NOD | Failed | 2025-03-21 10:58:44 | View Detail |

At the bottom, there are pagination controls: 'Items per page: 10' dropdown, '1–8 of 8 items' text, '1 of 1 page' text, and navigation arrows.

It is possible to delete some or all entries.

Support for RACF enhancements

Data Set Encryption (1)

DFSMS provides Tape Data Set Access Method Encryption
RACF provides support for setting a granular encryption policy
zSecure provides support for easy administration of RACF.

New RACF template field ENCTYPES available in CARLa, with alias ENCRYPTTYPES (the RACF command keyword).

Shown in RA.D (RACF administration – DATASET) in the DFP segment.

Overtype, COPY, RECREATE, MERGE support in zSecure Admin.

SMF: keyword formatted in RACF command in zSecure Audit (and Adapters/zSCC).

zSecure Command Verifier: C4R.DATASET.DFP.ENCRYPTTYPES.*profile* policy profiles to control keyword use

Back-ported to z/OS 2.5 and 3.1. Already available.

zSecure PTF numbers included in RACF presentation.

zSecure technote: <https://www.ibm.com/support/pages/node/7182342>

Data Set Encryption (2)

In the ISPF UI, the field value is shown as a string (on both display levels):

| zSecure DATASET DFP segments | | | | |
|--------------------------------------|----------|----------|---------------------|---------|
| Command ==> | Complex | ResOwner | Enc types policy | DataKey |
| like CRMQ.ENCTYPES.** | DCEIMGJB | CRMQ | EXTAPE EXPDSE EXSEQ | |
| Data set profile | | | | |
| CRMQ.ENCTYPES.EXTAPE.EXPDSE.EXSEQ.** | DCEIMGJB | CRMQ | EXTAPE EXPDSE INSEQ | |
| CRMQ.ENCTYPES.EXTAPE.EXPDSE.INSEQ.** | DCEIMGJB | CRMQ | EXTAPE EXPDSE NOSEQ | |
| CRMQ.ENCTYPES.EXTAPE.EXPDSE.NOSEQ.** | DCEIMGJB | CRMQ | EXTAPE EXPDSE NOSEQ | |
| CRMQ.ENCTYPES.EXTAPE.INPDSE.EXSEQ.** | DCEIMGJB | CRMQ | EXTAPE INPDSE EXSEQ | |

"encryptTape encryptPDSE encryptSEQ" (within quotes), where *encrypt* is either IN, EX, or NO:

- IN – Include the data set type for encryption.
- EX – Exclude the data set type from encryption.
- NO – When determining encryption eligibility, ENCTYPES is not considered for this data set type. This is the default behavior.

And in the UI selection is done like this:

| zSecure - Data set - Segment selection | | | | | | |
|--|------|------|----------------------------|-------|---------|-------|
| DATASET DFP segment selection | | | | | | |
| - DFP Resource owner | : | : | (resource owner or filter) | | | |
| - Encryption policies | Tape | : | Include | = | Exclude | = |
| | (or) | PDSE | Include | = | Exclude | = |
| | (or) | Seq. | Include | = | Exclude | = |
| | | | None | (Y/N) | None | (Y/N) |
| | | | None | (Y/N) | None | (Y/N) |
| — Key label | | | | | | |

Data Set Encryption

In the Web UI, the field is shown like this:

The screenshot shows the 'Dataset selection results' page in the RACF Web UI. The table lists datasets with their profiles, complex names, resource owners, data keys, and various policy settings. A specific row for dataset 'CRMBMK1.TEST1.ENCIN.**' is highlighted with a red box, and its detailed view is shown in a modal window below.

| Profile | Complex | ResOwner | DataKey | Name for HLQ | Instdata for HLQ | TAPE policy | PDSE policy | SEQ policy |
|---|---------|----------|-----------------|--------------|------------------|-------------|-------------|------------|
| CRMBMK1.TEST1.ENCIN.** | PLEX1 | CRMBMK1 | NEWCKDSKEYLABEL | | | Encrypt | Encrypt | Encrypt |
| CRMBMK1.TEST2.ENCIN.** | PLEX1 | CRMBMK1 | NEWCKDSKEYLABEL | | | Encrypt | Encrypt | Encrypt |
| CRMBMK1.TEST4.ENCALLEX.** | PLEX1 | | | | | No encrypt | No encrypt | No encrypt |
| CRMBMK2.TEST1.ENCIN.** | PLEX1 | CRMBMK1 | NEWCKDSKEYLABEL | | | Encrypt | Encrypt | Encrypt |
| CRMBMK2.TEST2.ENCIN.** | PLEX1 | CRMBMK1 | NEWCKDSKEYLABEL | | | Encrypt | Encrypt | Encrypt |
| CRMBMK2.TEST4.ENCALLEX.** | PLEX1 | | | | | No encrypt | No encrypt | No encrypt |
| CRMBPH1.ENCRYPA.** | PLEX1 | | | | | Encrypt | No policy | No policy |

Dataset detail
Dataset CRMBMK1.TEST1.ENCIN.** overview

Complex: PLEX1
Data set profile: CRMBMK1.TEST1.ENCIN.**

Encryption policy section

TAPE policy: Encrypt
PDSE policy: Encrypt
SEQ policy: Encrypt

Extend JWT support (“IDT3”) (1/2)

RACF provides support for additional Identity Tokens

zSecure provides support for easy administration of RACF.

New RACF template fields IDTLABP and IDTKIDP available in CARLa, with aliases SIGLABELPRIMARY and SIGKIDPRIMARY (the RACF command keywords).

Shown in RA.R (RACF administration – RESOURCE) in the IDTPARMS segment.

Overtype, COPY, RECREATE, MERGE support in zSecure Admin.

SMF: formatted in RACF command in zSecure Audit (and Adapters/zSCC).

SMF: new CARLa fields IDT_SIGNATURE_EVALUATOR, KEY_IDENTIFIER, and SIGNATURE_ALGORITHM for data in new relocate section 443 (SMF 80-1).

zSecure Command Verifier recognizes the keywords.

Back-ported to 3.1. zSecure APARs: OA67545 (HCKR310) OA67546 (HC4R310)

| zSecure FMID | zSecure PTF | RACF FMID | RACF PTF |
|---------------------|--------------------|------------------|-----------------|
| HCKR310 | UJ96690 | HRF77EO | UJ96699 |
| HC4R310 | UJ96691 | HRF77EO | UJ96699 |

Extend JWT support (“IDT3”) (2/2)

In the Web UI, the support looks like this:

The screenshot shows two pages from the IBM Security zSecure Web UI. The top page is titled "Resource selection results" and displays a table of RACF profiles. The bottom page is titled "Resource detail" and shows the configuration for a specific profile.

Resource selection results

| Location: | All | Complex | SigToken | Seqnum | Cat | SigAlg | AnyAppl | PrA | TimeOut | Primary ID token signing label | Primary ID token key identifier |
|-----------|-------------------------------|---------|-----------------------|--------|-----|--------|---------|-----|----------|--------------------------------|---------------------------------|
| IDTDATA | C4RQA00.TEST.IDTPARMS.SEGMENT | PLEX1 | MADALINA.@TOKEN | | | Yes | No | 5 | | | |
| IDTDATA | JWT.*.CRMBMZ1.SAF | PLEX1 | MADALINA.TEST.\$TOKEN | 1111 | | HS384 | Yes | No | 5 | | |
| IDTDATA | JWT.*.CRMBRL1.SAF | PLEX1 | | | | Yes | No | 5 | | | |
| IDTDATA | JWT.APPL01.CRMBPH1.SAF | PLEX1 | | | | Yes | No | 5 | LABEL111 | KID111 | |
| IDTDATA | JWT.APPL01.CRMBVK1.SAF | PLEX1 | | | | Yes | No | 5 | | | |
| IDTDATA | JWT.APPL01.CRMBVK2.SAF | PLEX1 | 100 | | | Yes | No | 5 | LAB100 | | |
| IDTDATA | JWT.APPL01.CRMBVK3.SAF | PLEX1 | | | | Yes | No | 5 | LAB100 | | |
| IDTDATA | JWT.APPL01.CRMBVK4.SAF | PLEX1 | | | | Yes | No | 5 | LAB100 | KID200 | |
| IDTDATA | JWT.APPL01.CRMBVK5.SAF | PLEX1 | | | | Yes | No | 5 | LAB100 | KID200 | |
| IDTDATA | JWT.APPL01.CRMBVK6.SAF | PLEX1 | | | | | | | | | |
| IDTDATA | JWT.APPL01.CRMBVK7.SAF | | | | | | | | | | |
| IDTDATA | JWT.APPL02.CRMBPH1.SAF | | | | | | | | | | |
| IDTDATA | JWT.APPL03.CRMBPH1.SAF | | | | | | | | | | |
| IDTDATA | JWT.APPL04.CRMBPH1.SAF | | | | | | | | | | |
| IDTDATA | JWT.APPL05.CRMBPH1.SAF | | | | | | | | | | |
| IDTDATA | JWT.APPL10.CRMBPH1.SAF | | | | | | | | | | |
| IDTDATA | JWT.APPL11.CRMBPH1.SAF | | | | | | | | | | |
| IDTDATA | JWT.APPL12.CRMBPH1.SAF | | | | | | | | | | |
| IDTDATA | JWT.APPL13.CRMBPH1.SAF | | | | | | | | | | |

Resource detail

Profile name: JWT.APPL01.CRMBVK5.SAF
Class: IDTDATA
Complex: PLEX1
Signing token name:
Signing token sequence number:
Signing token category:
ID token signing algorithm: NOSIGALG
 HS256
 HS384
 HS512
 RS256
 RS384
 RS512
ID token for any application: YES
ID token for protected user: NO
ID token timeout minutes: 5
Primary ID token key ident: KID200

Submit changes

RACF User Quarantine (CONTAIN) (1)

RACF provides support for quarantining a user

zSecure provides support for easy administration of RACF.

RACF user IDs can be CONTAINED (stronger than revoke).

Keywords CONTAIN, NOCONTAIN, NEVERCONTAIN, ALLOWCONTAIN.

Flags shown in RA.U (RACF administration – USER), etc., zSecure CICS Toolkit, and CKGRACF output.

COPY/RECREATE/MERGE will copy NEVERCONTAIN but not CONTAINED.

RA.U Password command extended with ALTUSER RESUME NOCONTAIN.

SMF formats keywords, and supports CONTAIN event, with details.

Alerts for CONTAIN event and setting NEVERCONTAIN property (zSecure Alert)

zSecure Command Verifier supports the keywords

RACF User Quarantine (CONTAIN) (2)

In the ISPF UI, the flags are shown like this:

zSecure USER overview

| User | Complex | Name | DfltGrp | Owner | RIRPC | SOARFC | g |
|---------|---------|----------------|---------|-------|-------|--------|---|
| U192701 | UNL1 | L0001927 USER1 | CRMB | CRMB | R | C | |
| U192702 | UNL1 | L0001927 USER2 | CRMB | CRMB | R | C | |
| U192703 | UNL1 | L0001927 USER3 | CRMB | CRMB | R | C | |
| U192704 | UNL1 | L0001927 USER4 | CRMB | CRMB | R | C | |
| U192705 | UNL1 | L0001927 USER5 | CRMB | CRMB | R | C | |
| U192706 | UNL1 | L0001927 USER6 | CRMB | CRMB | R | C | |

A

B

zSecure - RACF - User Attributes

| Specify groups of criteria that the userids must meet: | | | | |
|--|---------------|-------------|--------------|--------------------|
| Systemwide and group authorizations | | | | |
| OR | Special | Operations | Auditor | R0-auditor |
| | Group-special | Group-oper | Group-audit | Class auth |
| | Nevercontain | | | |
| Logon status | | | | |
| OR | Revoked | Inactive | Protected | Passw expired |
| | Revoked group | Certificate | Pass phrase | Phrase expired |
| | When day/time | ID mapping | Passw legacy | Phrase legacy |
| | MFA | MFA active | MFA fallback | Password |
| | Contained | | | |
| User properties | | | | |
| OR | Has RACLINK | Restricted | User audited | Mixed case pwd |
| CKGRACF features | | | | |
| OR | Queued cmds | Schedules | Userdata | MultiAuthority |
| Connect authority . | | | | |
| | | 1. Use | 2. Create | 3. Connect 4. Join |

RACF User Quarantine (CONTAIN) (3)

User detail display:

| zSecure USER overview | | | | | | | |
|------------------------------------|--------------------|---|-----|----|------|----------|-----------|
| Command ==> | Users like U19270* | | | | | | |
| <u>Identification of U192702</u> | | | | | | | |
| User name | L0001927 USER2 | | | | | | |
| Installation data | UNL1 | | | | | | |
| Owner | CRM WERKNEMERS | | | | | | |
| User's default group | CRM WERKNEMERS | | | | | | |
| Group | Auth | R | SOA | AG | Uacc | Revokedt | Resumendt |
| CRMB | USE | | | | NONE | | |
| <u>System access</u> | | | | | | | |
| Revoked (may be by date) | Yes | | | | | | |
| Contained | Yes | | | | | | |
| Inactive, revoked or pending | No | | | | | | |
| Days of week user can logon | SMTWTFS | | | | | | |
| Time of day user can logon | | | | | | | |
| Date user will be revoked | | | | | | | |
| Date user will be resumed | | | | | | | |
| <u>Statistics</u> | | | | | | | |
| Creation date | 12Jun25 | | | | | | |
| Last RACINIT current connects | | | | | | | |
| User's last use date | 12Jun25 | | | | | | |
| User's last use time | | | | | | | |
| <u>Passphrase</u> | | | | | | | |
| Has a password | Yes | | | | | | |
| Expired password | Yes | | | | | | |
| Password chg date in effect | | | | | | | |
| Password expiration date | 12Jun25 | | | | | | |
| Old passwords present # | 0 | | | | | | |
| Has a password envelope | | | | | | | |
| Password LEGACY encrypted | Yes | | | | | | |
| Old passwords LEGACY enc. # | | | | | | | |
| Password interval | 90 | | | | | | |
| Password interval in effect | 90 | | | | | | |
| <u>Authentication status</u> | | | | | | | |
| Mixed case password in effect | No | | | | | | |
| Failed pwd/phrase attempts # | | | | | | | |
| Nopwd and nophrase | PROTECTED | | | | | | |
| <u>Multi Factor Authentication</u> | | | | | | | |
| Any effective MFA factor | No | | | | | | |
| Fallback to pwd if MFA down | | | | | | | |
| z/VM MFA logon | No | | | | | | |
| z/VM MFA fallback | | | | | | | |
| <u>Mandatory Access Control</u> | | | | | | | |
| Security label | | | | | | | |
| Security level | | | | | | | |
| Categories list | | | | | | | |
| <u>Privileges</u> | | | | | | | |
| Security admin | SPECIAL No | | | | | | |
| DASD administrator | OPERATIONS No | | | | | | |
| Global audit set/list | AUDITOR No | | | | | | |
| Global audit list | ROAUDIT No | | | | | | |
| Nevercontain | No | | | | | | |
| <u>Safeguards</u> | | | | | | | |
| Ignore UACC/Glob/* RESTRICTED | No | | | | | | |
| Log all user actions | UAUDIT No | | | | | | |

RACF User Quarantine (CONTAIN) (4)

Web UI USER overview:

RACF / User / User Selection Results /

User selection results

All users

Location: All ▾

Press Enter to search

| User | DfltGrp | Owner | Revoked | Inactive | Restricted | Protected | Contained | Special | Operator | Auditor | ROAudit | Nevercontain | GroupSt |
|--------------------------|---------|---------|---------|----------|------------|-----------|-----------|---------|----------|---------|---------|--------------|---------|
| CRMBLU40 | CRMB | CRMBLU1 | - | - | - | Protected | - | - | - | - | - | Nevercontain | - |
| CRMBMB1 | CRMB | CRMB | - | - | - | - | - | Special | - | Auditor | - | Nevercontain | - |
| CRMBMK3 | CRMB | CRMB | - | - | - | - | - | Special | - | Auditor | - | Nevercontain | - |
| CRMBMK5 | CRMB | CRMB | - | - | - | - | - | Special | - | Auditor | - | Nevercontain | - |
| CRMBMK6 | CRMB | CRMB | Revoked | - | - | - | Contained | Special | - | Auditor | - | Nevercontain | - |
| CRMBRL2 | CRMB | CRMB | - | - | - | - | - | Special | - | Auditor | - | Nevercontain | - |
| CRMBRT3 | CRMB | CRMB | - | - | - | - | - | - | - | Auditor | - | Nevercontain | - |
| CRMBRT4 | CRMB | CRMB | Revoked | - | - | - | Contained | Special | Operator | Auditor | - | Nevercontain | - |
| CRMBVK2 | CRMB | CRMB | Revoked | - | - | - | Contained | Special | Operator | - | ROAudit | Nevercontain | - |

Items per page: 20 ▾ 1–9 of 9 items 1 ▾ of 1 page ▶ ▷

RACF User Quarantine (CONTAIN) (5)

Web UI selection:

Other Fields

| Attributes | | | | | | | |
|--|---------------------------|--|-------------------------------------|------------------------------------|---|--|--------------------------------------|
| System wide and group authorizations ① | | | | | | | |
| Logical operator | | Attributes | | | | | |
| <input checked="" type="radio"/> OR | <input type="radio"/> AND | <input type="checkbox"/> Special | <input type="checkbox"/> Operations | <input type="checkbox"/> Auditor | <input type="checkbox"/> RO-auditor | <input type="checkbox"/> Group-special | <input type="checkbox"/> Group-oper |
| | | <input type="checkbox"/> Nevercontain | | | | | |
| Logon status ① | | | | | | | |
| Logical operator | | Attributes | | | | | |
| <input checked="" type="radio"/> OR | <input type="radio"/> AND | <input type="checkbox"/> Revoked | <input type="checkbox"/> Inactive | <input type="checkbox"/> Protected | <input type="checkbox"/> Password expired | <input type="checkbox"/> Revoked group | <input type="checkbox"/> Certificate |
| | | <input type="checkbox"/> Phrase expired | | | | | |
| | | <input type="checkbox"/> When day/time | | | | | |
| | | <input type="checkbox"/> ID mapping | | | | | |
| | | <input type="checkbox"/> Password legacy | | | | | |
| | | <input type="checkbox"/> Phrase legacy | | | | | |
| | | <input type="checkbox"/> Contained | | | | | |
| | | | | | | <input type="checkbox"/> MFA | <input type="checkbox"/> Pass phrase |
| | | | | | | <input type="checkbox"/> MFA active | |
| System access | | | | | | | |
| Revoked (may be by date) ① | | Contained ① | | Inactive, revoked or pending ① | | Time of day user can logon ① | |
| NO | | NO | | NO | | XX | |
| Date user will be revoked① | | Date user will be resumed① | | | | HHMM:HHMM | |
| Privileges | | | | | | | |
| Security admin SPECIAL ① | | DASD administrator OPERATIONS ① | | Global audit set/list AUDITOR ① | | Global audit list ROAUDIT ① | |
| YES | | NO | | YES | | NO | |
| Nevercontain ① | | Class authority ① | | | | | |
| YES | | | | | | | |

RACF User Quarantine (CONTAIN) (6)

In order to RESUME a user, CONTAIN cannot remain set.

The screenshot shows the RACF User Selection dialog with the following details:

- User selection:** All users, Location: All.
- User:** CRMBAH1 (selected).
- Action:** Manage Password.
- Authentication type:** Password (radio button selected).
- Password creation method:** Specify new value.
- Expiry duration:** Default expiry.
- CKGRACF command actions:**
 - Ignore history
 - Bypass exits
 - Bypass rules
 - Resume user id after password creation
 - Remove contain (circled in red)
- Buttons:** Cancel, Back, Next (highlighted in blue), and Close.

RACF User Quarantine (CONTAIN) (7)

Updated zSecure CICS Toolkit screen (display only):

```
Termid = 1701           IBM zSecure CICS Toolkit           Date = 2025/174
Userid = CRMBPH1        LISTUSER = CRMBPH2             Time = 14:04:25

Name = ##### Owner = CRMBPH1 Password = ??????? Cre = 25168
Dfltgrp = CRMB Authority = Uacc = NONE Classcnt = 0000
Special = N Operations = N Auditor = N Restr = N Grpacc = N Adsp = N
Protected = Y Uaudit = N Revoke = N Revokedt = ***** Resumedt = *****
Contained = N Nevercontain = Y PhrInt = 00000
Lastacc = 25168/14:10:34 Passdate = 00000 Passint = 090 PwTry = 00 Secl = ***
SMTWTFS From Till Pwdgen = 255 Pwdcnt = 000 NumCtgy = 0000 NumGrp = 0001
YYYYYYYY 0000 0000 Model =

-----+---1---+---2---+---3-Installation data-5---+---6---+---7---+---+
| <===
-----+---1---+---2---+---3---+---4---+---5---+---6---+---7---+---+
PF1=Toggle 3=Chgopts 5=Ctgy 6=Segments 7=Groups 11=Search CLEAR=Main menu
```

RACDCERT multiple altnames

RACF provides support for multiple altnames in certificates
zSecure provides support for easy administration of RACF.

RACDCERT GENCERT adds keywords like ADOMAIN in addition to DOMAIN, etc.

RA.5 (RACF administration – certificates) will be updated to allow multiple altnames to be specified and generate the right RACF commands.

SMF data for these new specifications will be formatted appropriately.

====

New keyword PBE on RACDCERT EXPORT

to specify whether the new algorithm is needed when the export format is either PKCS12DER or PKCS12B64. The only acceptable values for this keyword are AES and TDES.

RA.5 line command EX updated

SMF command support

RACF CSDATA fields in RA.x selection and overview displays

Custom data support

The SE.6 Instdata option allowed defining substrings from installation data to display with the various profile displays.

This now becomes a Custom data option where you can add custom data fields to those profile displays.

- Underlying, there have been substantial updates to the engine support for DEFINE statements, where the target can more often be another DEFINE.

SE.6 extended custom data fields customization

```
Menu          Options      Info       Commands     Setup
zSecure - Setup - Custom data           Row 1 to 5 of 5
Command ==> _____                         Scroll ==> CSR
Select( S ) the class you want to maintain customer defined fields for

Class      Description
USER       RACF user customer defined fields
GROUP      RACF group customer defined fields
DATASET    RACF dataset customer defined fields
RESOURCE   RACF general resource customer defined fields
LOGONID    ACF2 LID customer defined fields
***** Bottom of data *****
```

- Put an S in front of USER

SE.6 - Add fields to USER display

| Menu | Options | Info | Commands | Setup | |
|---|-----------------------------|-----------------------|----------|----------------------------|-----------------|
| | | | | | Row 1 to 1 of 1 |
| Command ==> _ | | | | | Scroll ==> CSR |
| | | | | | |
| User output layout definitions | | | | | |
| | Overview display output | | | Detail display output | |
| | Concise print output | | | Detail print output | |
| | Concise narrow print output | | | Detail narrow print output | |
| | Additional connect output | | | | |
| User customer defined fields definition (D (delete), E (edit), I (insert customer field), N (new field)) | | | | | |
| | Field name | Default output header | | Pos Len Format | |
| | | | | | |
| | ***** Bottom of data ***** | | | | |

- Put an **I** below **Field name** to add a field definition

SE.6 - Adding custom fields

- Put an S in front of EMPSER

| Menu | Options | Info | Commands | Setup |
|--|------------|-----------------------|----------|--------------------|
| zSecure - Setup - Custom data | | | | Row 15 to 28 of 33 |
| Command ==> <u> </u> | | | | Scroll ==> CSR |
| Select(S) a User customer defined field to add | | | | |
| <hr/> | | | | |
| Category | Field name | Default output header | Len | Format |
| USER | DC1 | DC1 | 3 | NUM |
| USER | DC2 | DC2 | 3 | NUM |
| USER | DEPT | DEPT | 76 | CHAR |
| USER | EMAIL | EMAIL | 64 | CHAR |
| USER | EMPSER | EMPSER | 9 | NUM |
| USER | GSM | GSM | 12 | CHAR |
| USER | PIVSIG | PIVSIG | 64 | CHAR |
| USER | QUOT1 | QUOT1 | 76 | CHAR |
| USER | QUOT2 | QUOT2 | 12 | CHAR |
| USER | QUOT3 | QUOT3 | 12 | CHAR |
| USER | QUOT4 | QUOT4 | 12 | CHAR |
| USER | TOOL1 | TOOL1 | 5 | CHAR |
| USER | TOOL2 | TOOL2 | 4 | CHAR |
| USER | USRADR | USRADR | 76 | CHAR |

Press **PF3** when done adding fields

SE.6 - Adding custom fields to USER display layouts (1)

```
Menu          Options      Info       Commands    Setup
                                         zSecure - Setup - Custom data
                                         Row 1 to 1 of 1
Command ==> _____
                                         Scroll ==> CSR

User output layout definitions
- Overview display output           - Detail display output
- Concise print output             - Detail print output
- Concise narrow print output      - Detail narrow print output
- Additional connect output

User customer defined fields definition
( D (delete), E (edit), I (insert customer field), N (new field))

Field name      Default output header      Pos Len Format
- EMPSER        EMPSER                  CSD   9 NUM
***** Bottom of data *****
```

Put a / before Overview display output and Detail display output

SE.6 - Adding custom fields to USER display layouts (2)

```
Menu          Options        Info      Commands     Setup
                                         zSecure - Setup - Custom data           Row 1 to 1 of 1
Command ==> _____                         Scroll ==> CSR
Select( S ) fields to add to the User Overview display output layout
_____
Class      Field name      Default output header      Len Format
User       EMPSER          EMPSER                   9   NUM
***** Bottom of data *****

```

Put an **S** before the EMPSER field

SE.6 overview and detail for USER layout

```
Menu Options Info Commands Setup
zSecure - Setup - Custom data Row 1 to 1 of 1
Command ===> Scroll ===> CSR
User Overview display output layout definition
( I (insert field), D (delete), E (edit), M (move), A (after), B (before))
Overview display output
Field name Header Len Output modifiers
EMPSER EMPSER 9 NUM
***** Bottom of data *****
Menu Options Info Commands Setup
zSecure - Setup - Custom data Row 1 to 1 of 1
Command ===> Scroll ===> CSR
User Detail display output layout definition
( I (insert field), D Add newline E Add prefix header M (move), A (after), B (before))
Detail display output
N Field name P Header Len Output modifiers
/ EMPSER / EMPSER 9 NUM
***** Bottom of data *****
```

RA.U overview and detail enriched

```
zSecure USER CRMBRL1 overview Line 1 of 1
Command ==> Scroll==> CSR
Users like CRMBRL1
    User      ClAut Link #Cert #Maps PEPEM AG Pri   Home directory
    CRMBRL1      0      1       3      1 P P M      10 EMPSER /home/CRMBRL1
***** Bottom of Data *****
```

```
zSecure USER CRMBRL1 overview Line 1 of 201
Command ==> Scroll==> CSR
Users like CRMBRL1
7 Jul 2025 23:45

Identification of CRMBRL1 NMPIPL87
User name RONALD VAN DER LAAN
User name EMPSER 50294788
Owner CRMB
User's default group CRMB Group custom data
Group      Auth      R SOA AG Uacc      Revokedt      Resumedt
#TEST2      USE      SOA      NONE
CRMB      USE      SOA      NONE
DEPT
TEST
```

Compliance standards

Compliance standards - ISPF

In the ISPF UI, standards can be found under AU.R (Rule-based audit)

```
zSecure - Audit - Evaluate  
Command ==> _____  
  
Specify evaluation standards to run:  
/ z/os RACF/ACF2/TSS STIG           / z/os Products STIGs  
/ z/os RACF/ACF2 PCI-DSS             / z/os RACF CIS Benchmark  
/ z/os Db2 CIS Benchmark             _ z/os zSecure extra
```

The most important ones are the Security Technical Implementation Guides and Center for Internet Security benchmarks.

Current STIG levels are 9.4 (z/OS) and variable 6.x/7.x (Products).

Current CIS levels are 1.1 (RACF) and 1.0 (Db2).

Coverage for RACF is 90% or more (and increasing), ACF2 close behind.

Every quarter a STIG update is released (usually a few weeks after the Defense Information Systems Agency publishes their newest releases).

The Db2 CIS Benchmark requires a zSCC entitlement.

New Db2 report types

Underlying report types **DB2_CONTEXT** and **DB2_ROLE**:

- Objects with their authids from Db2 SYSCONTEXT, SYSCONTEXTAUTHIDS, and SYSCTXTRUSTATTRS, resp. objects from Db2 SYSROLES
- Sample CARLa members CKCDQDZ and CKCDQDI
- These require a zSCC entitlement
- Not added to the UI yet

DB2_CONTEXT

Record and detail level displays:

| DB2 context display | | | | | | | | | | | | | | | Scroll==> |
|----------------------------|-----------|------------|----------------|--------|-----|-----|-----|-----|---------|---------|-----------------|-----------------|-----------------|---------|-------------------|
| Complex | System | DB2I Count | | | | | | | | | | | | | 13 Jul 2025 23:45 |
| NMPIPL87 | ZS14 | DBD1 | 15 | | | | | | | | | | | | |
| DB2I Trusted context | SysAuthid | O Definer | D Default role | Dflt | sec | lab | Ena | AlP | Encrypt | Encrypt | created | Created | Altered | Remarks | |
| DBD1 CRMBCTX1 | CRMBJK1 | L CRMBJK2 | CRMBROLE | | | | Yes | No | No | | 6Feb2025 07:34 | 6Feb2025 07:34 | | | |
| DBD1 DB2CTXGR | DB2 | CRMBJK2 | | | | | Yes | No | No | HIGH | 13Feb2025 09:11 | 13Feb2025 09:11 | 13Feb2025 09:11 | | |
| DBD1 TRUSTCN1 | AUTHID1 | L CRMBJK2 | ROLE1 | | | | Yes | No | No | | 5Feb2025 12:10 | 5Feb2025 12:10 | | | |
| DBD1 TRUSTCN2 | AUTHID2 | L CRMBJK2 | ROLE2 | | | | Yes | No | No | | 5Feb2025 12:10 | 5Feb2025 12:10 | | | |
| DBD1 TRUSTCN3 | AUTHID3 | L CRMBJK2 | ROLE3 | | | | No | No | No | | 5Feb2025 12:10 | 5Feb2025 12:10 | | | |
| DBD1 TRUSTCN4 | AUTHID4 | CRMBJK2 | ROLE4 | | | | Yes | No | No | HIGH | 5Feb2025 12:10 | 5Feb2025 12:10 | 5Feb2025 12:10 | | |
| DBD1 TRUSTCN5 | AUTHID5 | L CRMBJK2 | CRMBROLE | LABEL5 | | | Yes | No | No | | 5Feb2025 12:10 | 5Feb2025 12:10 | 5Feb2025 12:10 | | |
| DBD1 TRUSTCN6 | AUTHID6 | L CRMBROLE | L ROLE1 | | | | Yes | No | No | | 6Feb2025 07:39 | 6Feb2025 07:39 | | | |
| DBD1 TRUSTCN7 | AUTHID7 | CRMBJK2 | | | | | Yes | No | No | | 12Feb2025 14:56 | 12Feb2025 14:56 | | | |
| DBD1 TRUSTCN88 | AUTHID88 | CRMBJK2 | | | | | Yes | No | No | HIGH | 7May2025 11:14 | 7May2025 11:14 | 7May2025 11:35 | | |
| DBD1 TRUSTCN89 | AUTHID89 | CRMBJK2 | | | | | Yes | No | No | HIGH | 7May2025 11:12 | 7May2025 11:12 | 7May2025 11:12 | | |
| DBD1 TRUSTCN8 | AUTHID8 | CRMBJK2 | | | | | Yes | No | No | HIGH | 7May2025 11:10 | 7May2025 11:10 | 7May2025 11:10 | | |
| DBD1 TRUSTCN9 | AUTHID9 | CRMBJK2 | | | | | Yes | No | No | | 7May2025 11:10 | 7May2025 11:10 | 7May2025 11:10 | | |
| DBD1 TRUSTCNA | AUTHIDA | CRMBJK2 | | | | | Yes | No | No | | 7May2025 11:12 | 7May2025 11:12 | 7May2025 11:12 | | |
| DBD1 TRUSTCNB | AUTHIDB | CRMBJK2 | | | | | Yes | No | No | | 7May2025 11:14 | 7May2025 11:14 | 7May2025 11:14 | | |
| ***** Bottom of Data ***** | | | | | | | | | | | | | | | |

| DB2 context display | | | | | | | | | | | | | | | Line 1 of 21 | | | | | |
|----------------------------|--------|------------|------------------|-----------|--|--|---------------------|------------------|----------|---------------------|----------|-----------|--|---------|-------------------|-----------|-----|-------------|--|--|
| Complex | System | DB2I Count | | | | | | | | | | | | | Scroll==> CSR | | | | | |
| | | | | | | | | | | | | | | | 13 Jul 2025 23:45 | | | | | |
| AUTHID | AAu | AUTHID | Role | | | | Authid | Seclabel | | Authid | creation | timestamp | | Authid | creation | timestamp | DB2 | Authid List | | |
| &CRMBJK5 | Yes | ROLE2 | | LABEL88 | | | 7 May | 2025 11:35:13.00 | | 2025-05-07-11.35.13 | | | | CRMBJK5 | | | | | | |
| &CRMBJK4 | Yes | ROLE2 | | | | | 7 May | 2025 11:35:13.00 | | 2025-05-07-11.35.13 | | | | CRMBJK4 | | | | | | |
| &CRMBJK3 | Yes | ROLE2 | | | | | 7 May | 2025 11:35:13.00 | | 2025-05-07-11.35.13 | | | | CRMBJK3 | | | | | | |
| &SYSPROG | Yes | ROLE2 | | | | | 7 May | 2025 11:35:13.00 | | 2025-05-07-11.35.13 | | | | CRMBNAI | CRMBSRU | CRMBJK99 | | | | |
| &DB2CTX | Yes | ROLE3 | | | | | 7 May | 2025 11:14:33.00 | | 2025-05-07-11.14.33 | | | | CRMBJKA | CRMBJKB | | | | | |
| IP address | | IP address | creation | timestamp | | | IP address | | creation | timestamp | DB2 | | | | | | | | | |
| 9.88.7.4 | | 7 May | 2025 11:14:33.00 | | | | 2025-05-07-11.14.33 | | | | | | | | | | | | | |
| 9.88.7.5 | | 7 May | 2025 11:14:33.00 | | | | 2025-05-07-11.14.33 | | | | | | | | | | | | | |
| 9.88.7.6 | | 7 May | 2025 11:14:33.00 | | | | 2025-05-07-11.14.33 | | | | | | | | | | | | | |
| Jobname | | Jobname | creation | timestamp | | | Jobname | | creation | timestamp | DB2 | | | | | | | | | |
| SERVAUTH | | SERVAUTH | creation | timestamp | | | SERVAUTH | | creation | timestamp | DB2 | | | | | | | | | |
| SERVCN6M | | 7 May | 2025 11:14:33.00 | | | | 2025-05-07-11.14.33 | | | | | | | | | | | | | |
| SERVCN6L | | 7 May | 2025 11:14:33.00 | | | | 2025-05-07-11.14.33 | | | | | | | | | | | | | |
| SERVCN6K | | 7 May | 2025 11:14:33.00 | | | | 2025-05-07-11.14.33 | | | | | | | | | | | | | |
| ***** Bottom of Data ***** | | | | | | | | | | | | | | | | | | | | |

DB2_ROLE

Record and detail level displays:

| DB2 roles display | | | | | |
|---------------------------|---|--|--|--|--|
| Command ==> | System DB2I Count ZS14 DBD1 7 | | | | |
| Role | Complex Created System CRMBROLE NMPIPL87 12Jan2024 ZS14 ROLE1 NMPIPL87 5Feb2025 ZS14 ROLE2 NMPIPL87 5Feb2025 ZS14 ROLE3 NMPIPL87 5Feb2025 ZS14 ROLE4 NMPIPL87 5Feb2025 ZS14 ROLE5 NMPIPL87 5Feb2025 ZS14 ROLEMC1 NMPIPL87 23May2025 ZS14 | | | | |
| | ***** Bottom of Data ***** | | | | |
| Command ==> | DB2 roles display | | | | |
| DB2 object | DB2 ssid system complex ver DBD1 ZS14 NMPIPL87 | | | | |
| Role | Role name ROLE4 | | | | |
| Role attributes | Authid of role definer CRMBJK2 | | | | |
| Definer type (L for role) | | | | | |
| Remarks | | | | | |
| Statistics | | | | | |
| Creation timestamp | 5Feb2025 11:57 | | | | |
| Release created | Db2 13 | | | | |
| | ***** Bottom of Data ***** | | | | |

Compliance standards – zSCC dashboard

IBM Z Security and Compliance Center provides a compliance dashboard.

Profiles [View docs](#)

A profile is a collection of related controls. After you gather the configuration information of your resources and prepare your systems for scanning, you can create profiles to define the list of controls that you'd like to validate against.

Filters: [Clear filter](#)

| Environment Type | Profile family | Category |
|------------------|----------------|----------|
| z/OS | CIS | All |

Search: Create [+](#)

| Name | Description | Type | Controls |
|--------------------|---------------------------------------|------------|----------|
| Db2_zos_CIS_1.0.0 | CIS IBM Db2 for z/OS Benchmark | Predefined | 319 |
| RACF_zos_CIS_1.0.0 | CIS benchmark IBM z/OS V2R5 with RACF | Predefined | |
| RACF_zos_CIS_1.1.0 | CIS benchmark IBM z/OS V2R5 with RACF | | |

September 10, 2024 4:16 PM

Items per page: 50 | 1–3 of 3 items [Download report](#)

Controls [①](#)

319 Total controls

Failures

Severity: Critical, High, Medium, Low

Drift over time

From: 08/10/2024 To: 09/10/2024

Drift (0-400)

Date (Sep 10, 2024)

[Control view](#) [Resource view](#)

IBM Z Security and Compliance Center

IBM Z Security and Compliance Center 1.3

This product is to some extent built on zSecure Audit 3.2 infrastructure.
The STIG and CIS standard evaluations are “sent over” to the dashboard.

In addition to the FMIDs provided from ShopZ, container images are provided to install under RedHat OpenShift or zCX.

The product follows a “continuous delivery” model.

zSCC – March 2025 update

Custom Goals for Independent Software Vendors and Users

- ISVs can now define their own subtypes for SMF 1154 (z/OS compliance evidence) and surface evidence in zSCC through the Common Data Provider component, and create goals associated to their subtype for z/OS based environments. Creating new goals support is also provided for existing users of zSCC (privileged users).

IBM Concert integration

- An automated OSCAL feed of zSCC compliance evaluation results is sent to IBM Concert

IBM Threat Detection for z/OS

IBM Threat Detection for z/OS (5698-CA1)

SMF 83-8 is the “anomaly detected” record from TDz.

The z/OS Compliance Integration Manager [3.2] component of zSCC 1.3 now writes SMF 83-8 recording activity into SMF 1154-97 records.

This recording activity is shown in the EV(ents) menu (zSecure Audit/zSCC).

Ideas

CL/SuperSession SMF support

CL/Supersession writes multiple events into a single SMF record, that with current CARLa support cannot really be extracted.

[ZAUDIT-I-263](#)

zSecure Audit (and Adapters/zSCC) adds support to process these SMF records (“creating multiple records from a single record”).

Add appropriate selection capabilities in the UI. Menu option EV.A.S.

- Back-ported to zSecure 3.1. Available. PTF UJ97479.

Technote <https://supportcontent.ibm.com/support/pages/zsecure-audit-31-added-smf-record-support-zsecure-carla-ibm-clsupersession>

Display Command Audit Trail in zSecure Admin

zSecure Command Verifier puts audit data into updated RACF profiles.

This information is stored in USRDATA fields, but zSecure Admin does not format the data in a readable fashion.

This \$C4R-data will now be formatted in the same format as it would be shown with LISTUSER etc.

[ZSECURE-I-53](#)
[ZSECURE-I-60](#)
[ZSECURE-I-132](#)
[ZSECURE-I-236](#)
[ZSECURE-I-425](#)

```
zSecure USER CRMBPH4 overview
Command ----> Line 78 of 105
Users like CRMBPH4          Scroll----> CSR
                               13 Jul 2025 19:32

UsrNm   Flg UsrData
- Profile: Created on 23.271/13:28 by CRMBPH1
- Segment: NETVIEW Added on 23.271/13:28 by CRMBPH1
- Segment: OMVS Added on 23.271/13:28 by CRMBPH1
- Segment: TSO Added on 23.271/13:28 by CRMBPH1
- Attrib: SPEC Added on 23.271/13:28 by CRMBPH1;Removed on 23.271/13:29 by
- Attrib: OPER Added on 23.271/13:28 by CRMBPH1;Removed on 23.271/13:29 by
- Attrib: AUDITOR Added on 23.271/13:28 by CRMBPH1;Removed on 23.271/13:29 by
- Attrib: PASSWRD Added on 23.271/13:28 by CRMBPH1
- Attrib: INSTDA Added on 23.271/13:28 by CRMBPH1
- Attrib: CAT Added on 23.271/13:28 by CRMBPH1
- Attrib: OWNER Added on 23.271/13:28 by CRMBPH1
- Attrib: DFLTGRP Added on 23.271/13:28 by CRMBPH1
- Attrib: NAME Added on 23.271/13:28 by CRMBPH1
```

Old layout:

```
UsrNm   Flg UsrData
- SC4RSBAS 00 A,23271/1328,CRMBPH1,00
- SC4RSNET 00 A,23271/1328,CRMBPH1,00
- SC4RSOMV 00 A,23271/1328,CRMBPH1,00
- SC4RSTSO 00 A,23271/1328,CRMBPH1,00
- SC4RASPC 00 A,23271/1328,CRMBPH1,00:D,23271/1329,CRMBPH1,00
- SC4RAOPR 00 A,23271/1328,CRMBPH1,00:D,23271/1329,CRMBPH1,00
- SC4RAAUD 00 A,23271/1328,CRMBPH1,00:D,23271/1329,CRMBPH1,00
- SC4RAPSW 00 A,23271/1328,CRMBPH1,00
- SC4RAINS 00 A,23271/1328,CRMBPH1,00
- SC4RACAT 00 A,23271/1328,CRMBPH1,00
- SC4RAOWN 00 A,23271/1328,CRMBPH1,00
- SC4RADFL 00 A,23271/1328,CRMBPH1,00
- SC4RANAM 00 A,23271/1328,CRMBPH1,00
```

Other Ideas

[ZSECURE-I-272](#) Access Monitor: select on Profile Owner for DATASET/RESOURCE

[ZSECURE-I-567](#) Show complete installation data for connections and subgroups in RA.U/G

[ZAUDIT-I-388](#) Explain impact of message CKR1403

[ZSECURE-I-581](#) Option to select on physical UNIX attributes as opposed to effective ones in RE.U.F

[ZSECURE-I-579](#) Resource Copy panel for wide screen (62x160)

[ZAUDIT-I-328](#) Lookup of DB2 fields to RACF

[ZALERT-I-93](#) Alert on buffer pool resources (BPO) under ACF2 option for Db2.

Also alert on granting Db2 admin privileges.

Subject: Alert: SYSADM Authority granted by CRMBRT1

Alert: SYSADM Authority granted by CRMBRT1
ACF2 for Db2 command used to grant SYSADM Authority

| | |
|---------------|---------------------------|
| Alert id | 2618 |
| Date and time | 20Mar2025 21:15:36.79 |
| Type | SYS |
| DB2ID | RENB |
| Rule entry | UID(CRMB CRMBRT2) PREVENT |
| Rule entry | UID(CRMB CRMBRT4) LOG |
| Rule entry | UID(CRMB CRMBRT5) ALLOW |
| User | CRMBRT1 RENE VAN T TE Z |
| Job name | CRMBRT1 |
| System id | ZS49 |

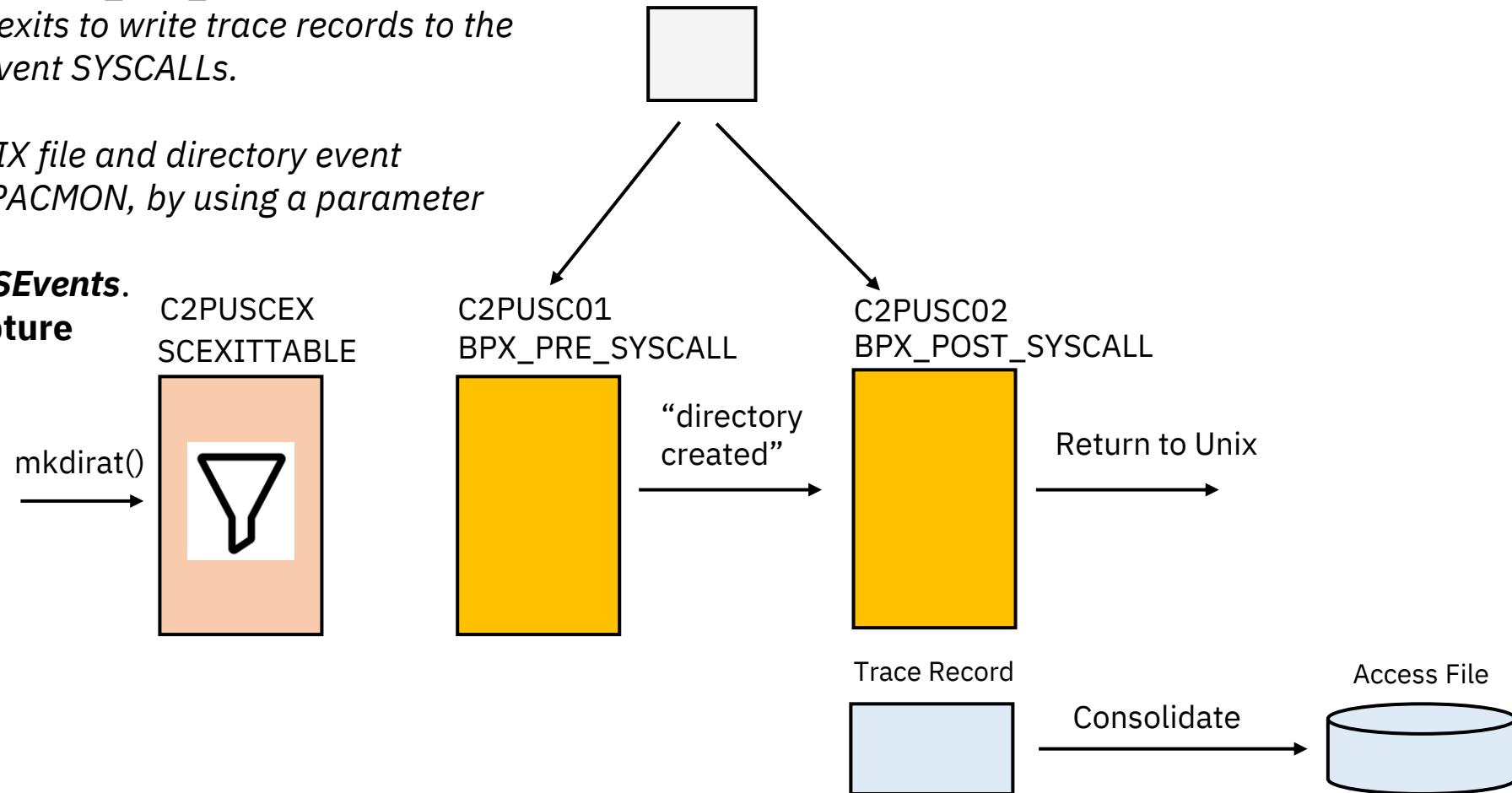
Access Monitor – UNIX

Access Monitor – capturing UNIX events

Access Monitor uses the BPX_PRE_SYSCALL and BPX_POST_SYSCALL exits to write trace records to the AM buffers, not to prevent SYSCALLs.

To start collecting UNIX file and directory event information, start C2PACMON, by using a parameter file with

**OPTION CaptureUSSEvents.
DIAGNOSE USSCapture**



Access Monitor – new UNIX syscalls

Example SCEXITTABLE

A substantial set of syscalls has been added of the form *at(), for example, openat(), mkdirat() etc.

These take a file descriptor and a relative pathname.

```
VIEW          CRMA.D.ZSSDEV.$BASE.SCKRSAMP(C2PUSCEX) - 01.17
Command ==>
000018 /* 250618 3.2.0 PH L0001649: Add new unix syscalls
000019 ****
000020 BPX1ACC /* access */
000021 BPX1ATM /* attach_execmvs */
000022 BPX1ATX /* attach_exec */
000023 BPX1CHA /* chaudit */
000024 BPX1CHD /* chdir */
000025 BPX1CHM /* chmod */
000026 BPX1CHO /* chown */
000027 BPX1CHR /* chattr */
000028 BPX1CMA /* fchmodat */
000029 BPX1COA /* fchownat */
000030 BPX1CRT /* chroot */
000031 BPX1EXC /* exec */
000032 BPX1EXM /* execmvs */
000033 BPX1EXT /* extlink_np */
000034 BPX1FAA /* faccessat */
000035 BPX1FCD /* fchdir */
000036 BPX1FSA /* fstatat */
```

The BPX1 prefix is for 31-bit calls; 64-bit calls use BPX4.
You need to specify only one form--both calls are captured.

TYPE=ACCESS field UNIX_EVENT

Validation

Installation & Configuration

- The zSecure 3.2 base level will be provided
 - This includes a file in the SCKRPAX data set that contains the z/OSMF plug-in that is the zSecure Admin Web UI
- Be aware that the 31-bit version CKR4Z196 of the engine is no longer there. Instead, there is now a CKR8Z15 that should work better for z15 and up.
- For zSCC 1.3, container images need to be obtained separately, per the memo distributed via ShopZ

Summary

- zSecure 3.2 is required for full support of z/OS 3.2. Incremental updates will be made in a number of code drops.
- zSecure Visual is reaching end of marketing. The future of RACF administration is a Web UI that is being developed as part of zSecure Admin. Design iterations are in full swing, this is a good time to chime in.
- RACF and z/OS currency support are core business for zSecure.
- For zSCC and zSecure Audit compliance standards are quite important.