

What is new in IBM z Security MFA 2.0 and zSecure 2.4 update

David Z. Rossi
IBM Cyber Security Archtiect

November 2019
Session FH

Place your
custom session
QR code here.
Please remove
the border and
text beforehand.



What's new in IBM Z Security

Presentation

This session will provide an overview of the new features provided in IBM Z Multi-Factor Authentication V2R0 and IBM Security zSecure Suite V2R4.

Speakers

(FH)

Stream: Enterprise Security

Room: Melbourne

Time: 11:45 - 12:45

Agenda

- MFA 2.0
- zSecure 2.4

How are users authenticating without MFA?

Users authenticate with:

Passwords

Password phrases

Problems with passwords:

Common passwords

Employees are selling their passwords

Password reuse

People write down passwords

Malware

Key log

Password cracking



What is multi-factor authentication?

SOMETHING THAT YOU KNOW

- Usernames and passwords
- PIN Code

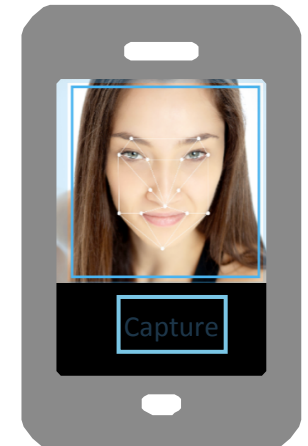


SOMETHING THAT YOU HAVE

- ID Badge
- One time passwords
- Time-based



SOMETHING THAT YOU ARE - Biometrics



IBM Z Multi-Factor Authentication

Raise the assurance level of critical applications, data, identities and hosting environments



- **Achieve regulatory compliance** and meet best practices (PCI-DSS, DISA-STIG...)
- **Gain flexibility** with support and integration for the broadest array of factors and vendors
- **Extend IBM RACF** with no changes to authenticate users with multiple factors
- **Fast, flexible,** deeply integrated, easy to deploy, manage and use

What works with IBM Z MFA?

Proprietary Protocol:

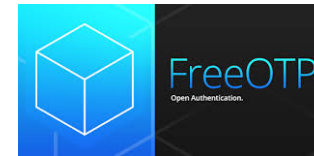


In-Band

RADIUS Based Factors:



TOTP Support:



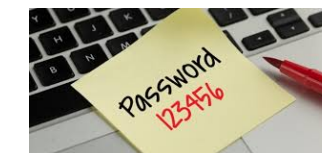
Out-of-Band

Certificate Authentication:



Password/Passphrase:

RACF Password/Passphrase can be used in conjunction with all in-band authentication methods.



Target Personas for MFA

Question: Who should be covered with MFA?

Answer: Everyone



Employees that work with personally identifiable info.

- Human Resources
- Healthcare workers
- Law Clerks
- DMV Clerks



Employees that have authority over managing money

- Brokers, Traders, Analysts
- Tellers
- Payroll
- Credit Card Processing



Users that have knowledge of Corporate Intellectual Property

- Executives
- Engineers



Business Partners – that access YOUR data

- Agents – Travel, Insurance
- Contract organization – Outsourcers



Users managing key IT assets

- Systems Programmers
- Security Administrators
- Database Admins, Developers

Target personas for IBM MFA include anyone with access to data a client would *not want released to the public*

RACF Support

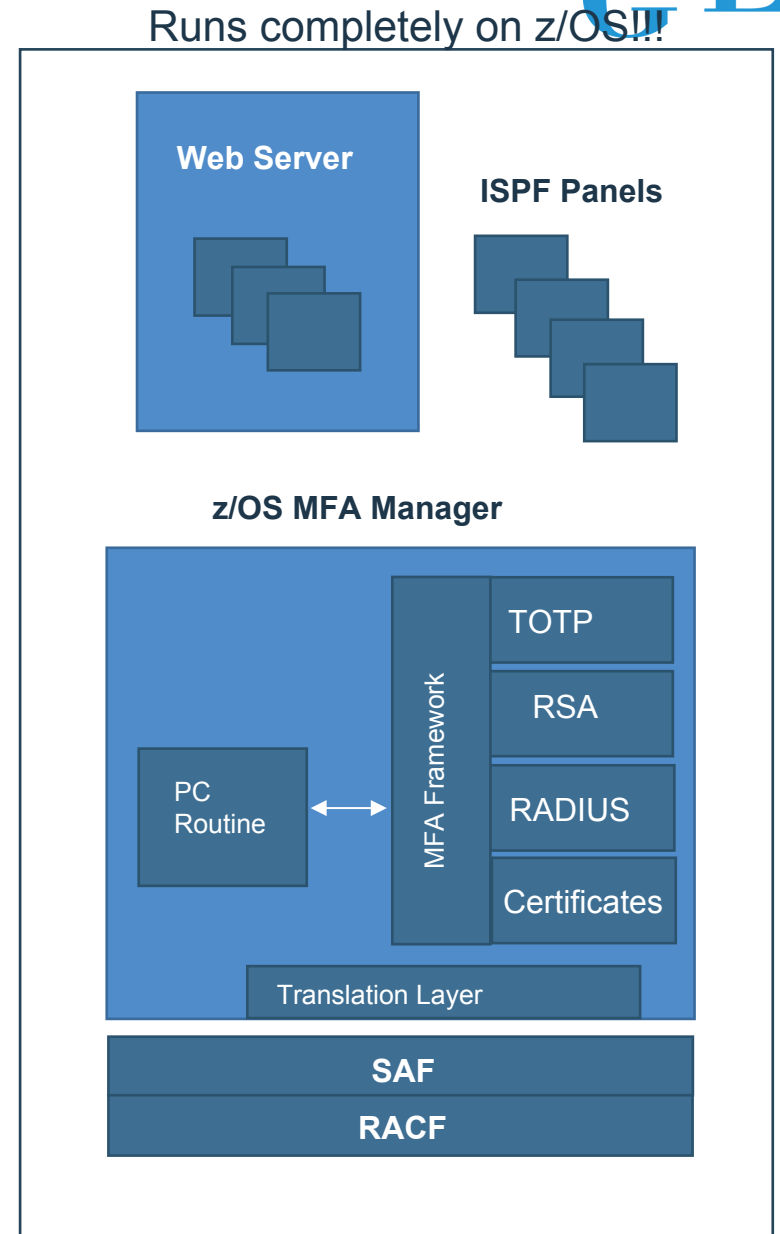
RACF

- User related commands
 - Allow the provisioning and definition of the acceptable MFA tokens for a user
- Extensions to authentication processing
 - Allows supported tokens to be used by any z/OS application
- Extensions to SAF programming interfaces
 - Provides a new SAF service for IBM MFA allowing access to MFA data stored in the RACF database
- Auditing extensions
 - Tracks that MFA was used during the authentication process for a given user
- Utilities
 - RACF Database unload non-sensitive fields added to the RACF database used by MFA processing
 - SMF Unload – unloads additional relocate sections added to SMF records



IBM Z Multi-Factor Authentication

- MFA ISPF panels for configuration and management of authentication tokens
- MFA Web Interface
 - User Interface supports factors such as Smart Cards and serves as web interface for registration – depending on factor type
- MFA Manager Services
 - Provides MFA main logic
 - Register MFA Factor Data for a z/OS user
 - Validates a user provided factor against RACF MFA Data
 - Accesses MFA Data via SAF/RACF via callable services



What's new in 2.0? (GA: May 17, 2019)

- New Name
- ISAM Integration (ISAM pick up OTP, CIV Integration via RADIUS)
- Native Yubikey
- LDAP Simple Bind
- Policy First Update
- JWT Support
- Out of Band - National Language Support & Customization
- Self-Service Password Change

IBM Z MFA Support in zSecure

zSecure Admin and Audit

- Selection and display of MFA fields in RACF profiles. Extra fields and formatting added for easier display.
- Selection and display of new relocate section and MFA information in SMF records.
- New field available in SYSTEM report about presence of RACF MFA support.

zSecure Access Monitor

- Detection and reporting of use of MFA for every RACINIT, including TSO logon.

zSecure Command Verifier

- Support for parsing new command syntax.
- New Policy Profiles to control management of MFA information, and updates to command recording in Command Audit Trail.

zSecure Adapters for SIEM

- Include MFA information to QRadar for analytics

zSecure Visual

- User context menu extensions for MFA factors and policies; MFPOLICY edit

What's new in zSecure 2.4.0?

- Command Ticket Logging
- File Integrity Monitoring
- z/OS 2.4 support
 - Custom data for general and dataset resource profiles
 - SMF Enhancements
 - Privilege escalation detection (new alert added)
- Compliance
 - Show differences (progress or regression?)
 - Compliance ACF2 252/357 circa 70%, new report type ACF2_SENSRESOURCE_ACCESS
 - STIG Currency
 - More IMS security settings made available, including OTMA
- QRadar events ICSF statistics, MFA audit trail (83-7)

Command and Ticket Logging

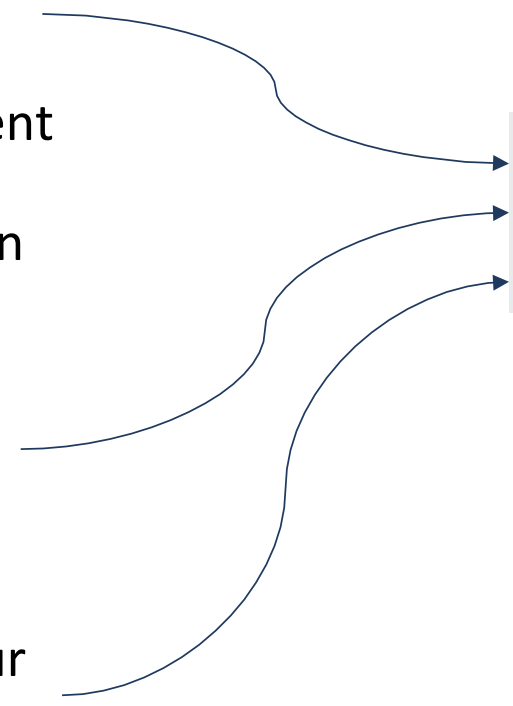
Command and Ticket Logging

- What is it?
 - New feature in zSecure Admin.
 - Provides a mechanism for administrators to record the approval record associated with a given change.
- Client Value
 - Auditors will ask “What was the change request number?”. Prior to this support it was a manual process to get the answer, if they could at all.
 - With this support, very easy to provide the answer.
- Also available in 2.3.1 – PTFs UA99126,UA99127,UA99128

- The Command and Ticket Logging feature zSecure Admin

CKXLOG started task

- Writes to system or sysplex wide CKXLOG log stream.
- Command logging requests are sent to CKXLOG by zSecure Admin and zSecure Command Verifier with an optional ticket id.
- Characteristics are defined once during install for a model logstream.
- Remembering a current ticket in the server is limited here to 1 hour after last use (HHMM is 0100).



```
SETUP LSNAME(&SYSPLEX..CKXLOG)  
SETUP LSMODEL(MODEL.CKXLOG)  
SETUP TICKETEXPIRE(0100)
```

- The Command and Ticket Logging feature zSecure Admin

Enter ticket number in Admin

- Extra fields in many ISPF user interface panels.
- There is even space for a full ticket URL in the description field (tag More if longer than field on panel)

```

Menu          Options          Info          Commands          Setup
-----
zSecure Admin - Mass update - Copy group
Command ==> _____

From group . . . . . oldgroup
To id . . . . . newgroup
_____
_____
_____
_____

Ticket identifier
ID . . . . . UZ180B050
Description _____ More _

_ Do not create OMVS segment
_ Copy permits only (target id may be a group or a user)
_ Generate RACF commands even when the target group exists
_ Copy CUSTOMDATA
Specify options for new group
_ Copy catalog aliases (only if CKFREEZE is present)
/ Issue ADDSD/RDEF for user resources
  / Copy RACFVARS profiles/members too (if option above selected)

```

- The Command and Ticket Logging feature zSecure Admin

CKXLOG primary command

- Or in the zSecure UI, type CKXLOG and modify the current change ticket number plus any extra description required by the auditors.

```
zSecure Admin - Change ticket ID/Description  
Command ==> _____  
Ticket ID  
UZ180B050 test2 _____  
Description  
_____  
_____  
_____  
Press ENTER to accept changes.
```

- The Command and Ticket Logging feature zSecure Admin

Command Review option

- A new primary option menu item CR for *Command Review* has been added to zSecure Admin.
- You can easily run members with RACF commands (CR.1).
- You can easily review and run commands in the CKXLOG command log (CR.2).

```

zSecure Suite - Main menu
Option ==>
SE  Setup      Options and input data sets
RA  RACF       RACF Administration
AA  ACF2       ACF2 Administration
AU  Audit      Audit security and system resources
RE  Resource   Resource protection reports
AM  Access     RACF Access Monitor
EV  Events     Event reporting from SMF and other logs
CR  Command review  Review and run commands
  1  Libraries  Review and run commands from library
  2  CKXLOG     Review and re-run commands in commands execution log
CU  CARLa     Work with CARLa queries and libraries
IN  Information  Information and documentation
LO  Local     Locally defined options
X   Exit      Exit this panel
  
```

- The Command and Ticket Logging feature zSecure Admin

CKXLOG input

- The SETUP FILES can select the *active* command log stream (last 24 hours), or a *specific* log stream, or an *offloaded* or *unloaded* data set.
- In CARLa, the files are allocated with ALLOC TYPE=CKXLOG.

```

Menu          Options          Info          Commands          Setup
-----
zSecure Admin - Setup - Input files Row 1 to 13 of 13
Command ==> _____ Scroll ==> CSR

Select the type of data set or file

Type          Description
-----
ACCESS        RACF ACCESS monitor data set
ACT.BACK      The backup RACF database of your active system
ACT.CKXLOG    Live command execution logstream
ACT.PRIM      The primary RACF database of your active system
ACT.SYSTEM    Live settings
CKFREEZE      System resource information data set
CKRCMD        A file for generated RACF commands
CKX.LOGSTR    Command execution logstream
CKXLOG        Command execution log
COPY.RACF     A copy of a single data set RACF database
COPY.SEC      A non-first component of a multiple data set RACF databas
COPY.TEMP     The first component of a multiple data set RACF database
UNLOAD        An unloaded RACF database

***** Bottom of data *****

```


- The Command and Ticket Logging feature zSecure Admin

Select command log records

- In the CR.2 selection panel, select records and specify how you want to *summarize*
- *Concise report* will show just time / user / command overview under the summary, but will show detail when zooming in.

```

zSecure Suite - Command review
Command ==> _____

Show command execution log records that fit all of the following criteria
Userid/logonid/ACID . . . _____ (ESM id or EGN mask)
Job name . . . . . _____ (job name or EGN mask)
System . . . . . _____ (system or EGN mask)
Profile . . . . . _____ (profile or EGN mask)
Class . . . . . _____ (class or EGN mask)
Ticket id . . . . . _____ (search)

Advanced selection criteria
_ Date time          _ Other

Output/run options
Summarize by _  1. Ticket id  3. User      5. Command  7. Class+Profile
                2. System    4. Orig. user 6. Component 8. Complex

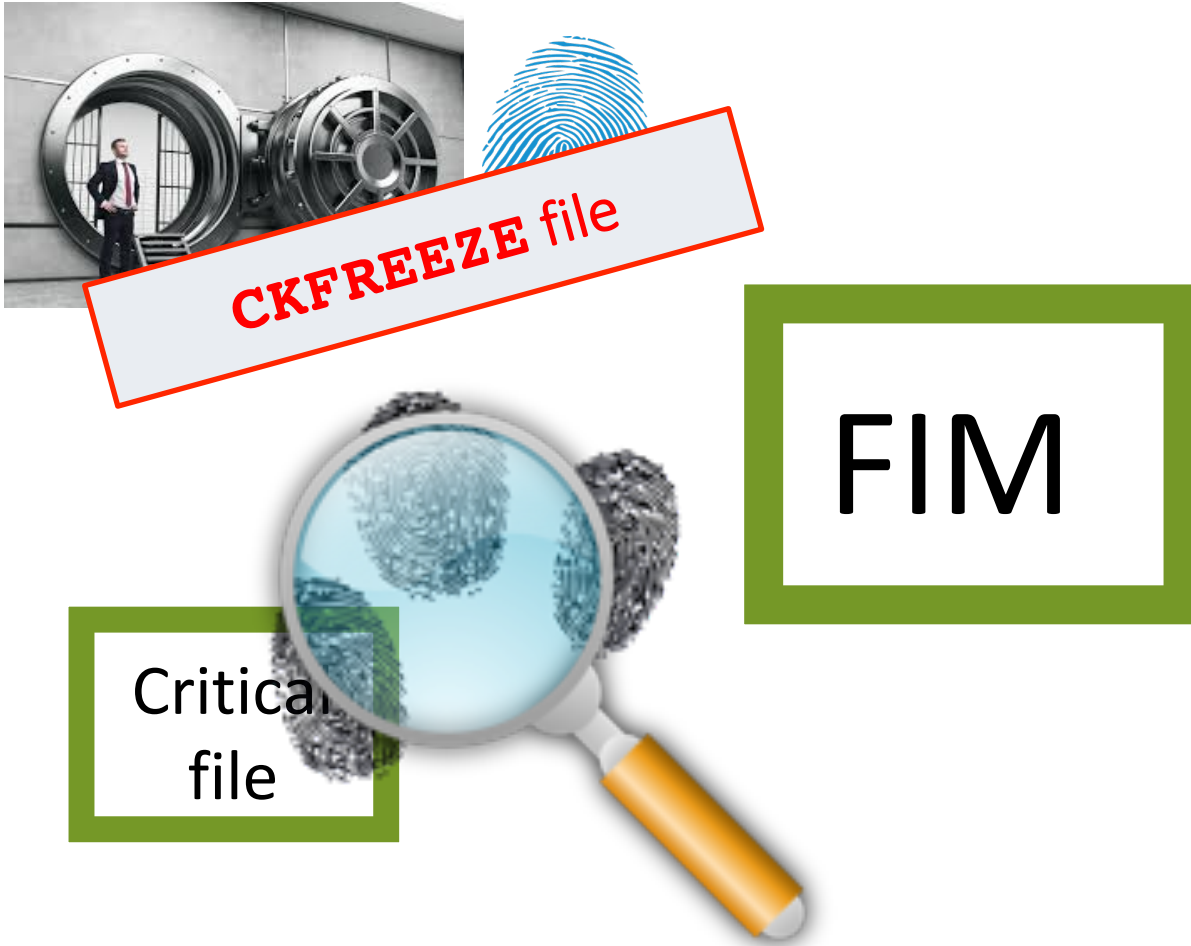
Ticket ID width . . . _____ (1-32)
/_ Concise report  _ Suppress pre-exec ESM cmds
_ Recreate commands Set ticket id
_ Print format    _ Send as e-mail      Background run
  
```

File Integrity Monitoring

File Integrity Monitoring

- What is it?
 - New feature in zSecure.
 - Provides a mechanism to show administrators and auditors if a file has been changed or tampered with.
- Client Value
 - Intrusion detection
 - Integrity validation
 - Several regulations benefit from FIM for compliance!
 - PCI-DSS
 - 10.5.5: data log integrity
 - 11.5: critical file comparison
 - HIPAA
 - GDPR

Take fingerprints with zSecure Collect



zSecure Collect

- CHECK=
 - Select critical data sets
 - Or use CHECK=YES
- CHECK_ALGORITHM=
 - Select algorithm
 - OLD – backward compatible
 - SHA2-512
 - SHA3-512

Two types computed by zSecure Collect

FINGERPRINT

- Based on the contents of a data set or a library
- Same across customers
- Usage: identify duplicates

ANTI_TAMPER_DIGEST

- Based on the contents and metadata, e.g., names, IDR/ZAP
- Site specific
- Usage: anti-malware protection

RE.F: FIM in zSecure Suite – which data sets changed

```

Menu          Options      Info      Commands      Setup
-----
zSecure Admin+Audit for RACF - Main menu

Option ==> _____ More: +

SE  Setup      Options and input data sets
RA  RACF       RACF Administration
AU  Audit      Audit security and system resources
RE  Resource   Resource protection reports
   C  CICS      CICS region and resource reports
   D  DB2      DB2 region and resource reports
   F  FIM      File integrity monitoring
   H  Hardware  Hardware like physical DASD volumes
   I  IP stack  TCP/IP stack reports
   J  JES      Job entry subsystem and started tasks
   K  Keys     Cryptographic key information
   M  IMS     IMS control region and resource reports
   N  VTAM    VTAM reports
   O  z/OS    z/OS options
   P  Programs Executable programs, especially authorized
   Q  MQ      MQ region and resource reports
   T  Trusted  Trusted users and sensitive resources reports
   U  Unix    Unix filesystem reports

F1=Help      F3=Exit      F4=Return    F10=Actions  F12=CRetrie
  
```

RE.F: FIM in zSecure Suite – which data sets changed

zSecure Suite - Resource - FIM

Option ==>

M	Members	Members
D	Data sets	Data sets

RE.F.M: FIM in zSecure Suite – Show program

```
Programs
Command ==>

Member  Alias of Comp Sensitivity APF AC1 Lng Complex      System  Dataset
CKR8Z12      CHG  APF library APF      Lng NMPIPL87      ZS14    CONSUL.CKRNEW.S

Identification
Member name           CKR8Z12
Data set name         CONSUL.CKRNEW.SCKRLOAD
DASD box serial number and id IBM-75-0000000VD781-BA0F
Volume serial        CON016
Volume serial or SMS managed CON016
Member of PDSE       Yes      TTR
System name          ZS14      Complex name      NMPIPL87
Type of sensitive resource APF library

Changes
ANTI_TAMPER_DIGEST(changed)
BYTES(13709312->13725696)
FINGERPRINT(changed)
LAST_CHANGE( 4 Sep 2019 02:38:08.417395-> 5 Sep 2019 02:39:04.150573)
LKEDDATE( 3 Sep 2019-> 4 Sep 2019)
LKEDTIME(09:38:16->04:30:39)
SSI(00A66192->0091E192)
STORSIZE(10211696->10223216)

Detail information
Data set APF this system      Yes
Authorization code AC=1      No
PARM longer than 100 OK     Yes
Application                  IBM Security zSecure
Addressing mode              64
```

In this case, clearly a new program version was linked. We suppress the actual digest values here.

Extended zSecure Admin with a new feature

z/OS 2.4 support

- zSecure z/OS 2.4 support

RACF 2.4 has new general resource segments

- Select on presence, absence, display of 3 new general resource segment types:
- CSDATA
- adds custom data fields
- IDTPARMS
- defines how to authenticate identity tokens
- JES
- defines how to encrypt JES spool – *for future use*

```

zSecure Suite - RACF - Resource Segments
Command ==>
All profiles
Only select general resource profiles with a specific segment:
Select one segment
- CDTINFO CDT Dynamic Class Descriptor Table data
- CERTDATA DIGTCERT Digital certificate data
- CERTDATA DIGTRING Digital certificate ring data
- CFDEF CFIELD Custom Fields
- CSDATA any class Custom defined data
- DLFDATA DLFCLASS Data Lookaside Facility data
- EIM FACILITY/LDAPBIND Enterprise Identity Manager data
- ICSF xCSFKEY Integrated Cryptographic Facility data
- ICTX LDAPBIND ICTX Identity caching data
- IDTPARMS IDTDATA Identity Token data
- JES JESJOBS JES Spool encryption data
- KERB REALM Kerberos Realm data
- MFPOLICY MFADEF Multi Factor Authentication Policy
- PROXY FACILITY/LDAPBIND LDAP proxy server data
- SESSION APPCLU Session data
- SIGVER PROGRAM Program signature data
  
```

SMF Enhancements

- Success logging now includes CRITERIA
 - Field RECORDDESC extended:
RACF ACCESS success for CRMBJU1: (READ,READ) on CSFKEYS ZSECKEY8
 - New TYPE=SMF field CRITERIA shown with default prefix header:
Criteria condition satisfied
- More ICSF record detail
- SMF 83-7 MFA record
 - New TYPE=SMF fields MFA_FACTOR, MFA_POLICY, populate 5 fields

SMF 83-7 MFA record

Event log record detail information

Command ==>

Date/time	Description
10Dec18 12:41:34.04	Failed MFA in-band invalid credential for CRMBVK2; factor AZFT0TP1
10Dec18 12:41:39.14	Failed MFA in-band invalid credential for CRMBVK2; factor AZFT0TP1

Event log record detail information

Command ==>

Record identification

Jobname + id: AZF#IN00
 SMF date/time: Mon 10 Dec 2018 12:42:43.14
 SMF system: ZS14 record type: 83 7 record no: CKR7SM00 5

Event identification

RACF event description	MFA in-band (Failure:MFA invalid credential)
RACF event qualifier	8
RACF descriptor for event	Violation
RACF reason for logging	
SAF authority used	
Unix Audit Function Code	
Access intent	
Access allowed	
Audit/message logstring	AZF2227I User CRMBVK2 denied access in-band by factor AZFT0TP1

Privilege Escalation Detection

- Detects ACEE updates not done by RACF
- New class ACEECHK
- New alert 1123 upon detection
- New audit concern if software installed but class inactive

```

zSecure Suite - Setup - Alert Row 1 to 20 of 20
Command ==> _____ Scroll ==> CSR

User alerts
Select the alert you want to work with.
The following line commands are available: A(Preview), C(opy), D(elete),
E(dit), I(nsert), W(Who/Where), S(elect), U(nselect), B(rowse)
-----
Alert                                     Id      Sel  gECSWUA CA EM
_ Logon by unknown user                   1101   Yes  gE      ___ N
_ Logon with emergency userid             1102   No   gE      Y   N
_ Logon of a userid with UID(0) (Unix superuser) 1103   Yes  gE      ___ N
_ Highly authorized user revoked for pwd violatio 1104   No   gE      ___ N
_ System authority granted                1105   No   gE      ___ N
_ System authority removed                1106   No   gE      ___ N
_ Group authority granted                 1107   No   gE      ___ N
_ Group authority removed                 1108   No   gE      ___ N
_ SPECIAL authority used by non-SPECIAL user   1109   No   gE      ___ N
_ non-OPERATIONS user accessed data set with OPER 1110   No   gE      ___ N
_ Invalid password attempts exceed limit      1111   Yes  gE      ___ N
_ Password history flushed                 1112   No   gE      ___ N
_ Suspect password changes                1113   No   gE      ___ N
_ Connect authority>=CREATE set           1114   No   gE      ___ N
_ Too many violations                     1115   No   gE      Y   N
_ Non-expiring password enabled           1119   No   gE      ___ N
_ Major administrative activity           1120   No   gE      Y   N
_ Protected status removed                1121   No   gE      ___ N
_ Logon with sensitive userid (from C2PACMON) 1122   No   gE      Y   N
_ Privilege escalation detected            1123   No   gE      ___ N
***** Bottom of data *****
  
```

Enhance zSecure Audit productivity

Compliance framework enhancements

AU.R enhancement - comparison

- TYPE=COMPLIANCE
* newlist types have been enhanced to support comparison

```

zSecure Suite - Audit - Evaluate
Command ==> _____

Specify evaluation standards to run:
/ STIG          _ PCI-DSS
_ GSD           / zSecure extra
Specify members for other evaluation standards to run:
_ _____ _ _____ _ _____ _ _____

Evaluate rules applicable to systems that fit the following criteria
Complex . . . . . _____ (complex or filter)
System  . . . . . _____ (system or filter)

Compliance result selection
_ Compliant          _
_ Assertions due in _

Output/run options
_ Show differences
_ Print format
_ Background run

zSecure Suite - Show differences
Command ==> _____

Select the type(s) of difference for display
/ ADD  Entries that were added into selected set
/ DEL  Entries that were deleted from selected set
/ CHG+ Changes that improve security
/ CHG- Changes that reduce security
/ CHGu Changes with effect on overall security unknown
_ SAME Identical entries
_ BASE Baseline records
  
```

AU.R enhancement - comparison

- The first is on the rule set level just comparing percentages – 4 STIG rules have difference
- 3 object types have a difference
- 389 objects have some difference in test result

```

zSecure Suite Display Selection
Command ==> _____
Name      Summary Records Title
_ STDRULES      1         4 Standard rule set compliance summary
_ STDYPES      1         3 Standard object type compliance summary
_ STDTESTS     2        389 Standard compliance test
***** Bottom of Data ****
  
```


IMS Region Open Transaction Manager Access (OTMA) support

- New repeat group in TYPE=IMS_REGION.
- Filled in if OTMA active
- Scroll down in RE.M.R

- Show default RACF setting

- Show client RACF setting

- Resource added: IMSXCF.group.mem

```

                                IMS region display
Command ==> _____
All IMS region records

    OTMA settings
    OTMA active                    Yes
    OTMA RACF security            PROFILE
    SECURE cmd issued             No
    XCF group name                IMSOGRP
    IMS member name               IMSO

    OTMA clients
    Client name Client type      ClientRACF CommandIssued
    IMSOC0N     IMS Connect     PROFILE      No
    IMSOC01     IMS Connect     PROFILE      No
    IMSOC02     IMS Connect     PROFILE      No
  
```

ACF2 resource access compliance

- New NEWLIST TYPE=ACF2_SENSRESOURCE_ACCESS
- Similar to ACF2_SENSDSN_ACCESS
- Purpose is writing compliance rules for general resources in ACF2
- Coverage is now at **70%**

IBM Security Community

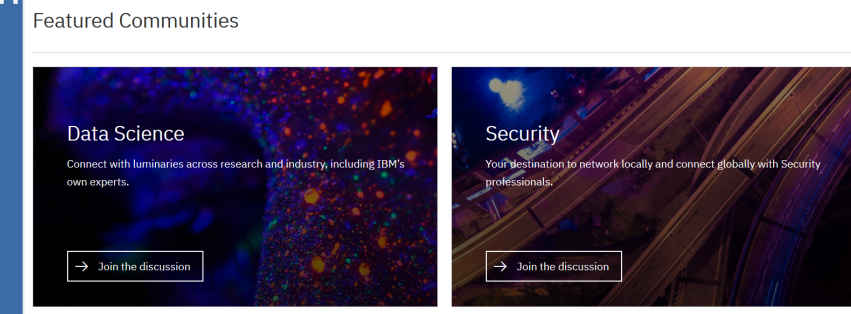
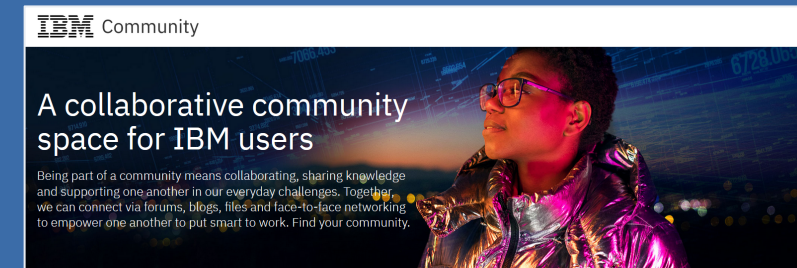
An online digital platform to support all aspects of community



Learn: Come to one place where IBM Security customers, experts, teams and a broader audience converge to share, solve, synergize

Network: Connect with the IBM Security ecosystem through engagement, education & the championing of users and their work

Share: Get equipped to solve business challenges today to deliver tomorrow's business outcomes.



community.ibm.com/security

4,000+ Members Strong!

IBM Security / © 2019
IBM Corporation

Questions?



Please submit your session feedback!

- Do it online at <http://conferences.gse.org.uk/2019/feedback/nn>
- This session is FH



1. What is your conference registration number?

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

2. Was the length of this presentation correct?

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

1 2 3 4 5 6 7 8 9

3. Did this presentation meet your requirements?

💡 1 to 4 = "No" 5 = "OK" 6-9 = "Yes"

1 2 3 4 5 6 7 8 9

4. Was the session content what you expected?

💡 1 to 4 = "No" 5 = "OK" 6-9 = "Yes"

1 2 3 4 5 6 7 8 9