z/OS V2.5 IBM Education Assistant

Solution Name: zSecure Suite 2.5.0

Agenda

- Trademarks
- Objectives
- Overview
- Timeline
- 2020 Q4 SSE content
- 2021 Q2 SSE content
- 2021 Q2 zSecure 2.5 content
- 2021 continuous delivery zSecure 2.5
- 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.
- 3rd party Trademarks:
  - Broadcom
  - CA
  - BMC

Objectives

- Provide evidence for compliance checking (PCI-DSS, DISA STIG, …)
- Provide evidence for SOX Continued Business Need decisions
- Enable all thousands of existing features of zSecure on z/OS 2.5

Overview

- Who (Audience)
  - z/OS security administrators, analysts, auditors, and systems programmers

- What (Solution)
  - zSecure Admin
    - Access Monitor support UNIX files, PROGRAMs, local RACLIST FASTAUTH
  - zSecure Audit
    - New report types and information related to INETD and SSH daemons, CL/Supersession, CA-1,
  - zSecure Adapters for SIEM
    - Feed more z/OS Connect, DB2, CICS, IMS related data to Qradar, Arcsight, or Splunk
- Wow (Benefit / Value, Need Addressed)
  - SOX CBN for UNIX file access lists and user/group/world file access, PROGRAM access, and subsystems using FASTAUTH after a local RACLIST
  - End-to-end event correlation between z/OS Connect, CICS, and DB2 events
  - Support for tape data set sensitivity and trust relations

Timeline

- 2019 Q3 GA zSecure 2.4.0 (worldwide F2F user groups)
- 2019 Q4 SSE (previously held webinar)
- 2020 Q1 SSE (previously held webinar)
- 2020 Q2 SSE (previously held webinar)
- 2020 Q4 SSE
- 2021 Q2 SSE
- …
- 2021 Q3 GA zSecure 2.5.0

2020 Q4 SSE

DISA STIG

2020 Q4 SSE: STIG controls

- Automation of additional 41 RACF STIG controls
  - Also some additional ACF2, TSS automations
- Status of the automation in zSecure, based on STIG v6

				% of Total		
	RACF	**ACF2**	**TSS**	**RACF**	**ACF2**	**TSS**
Total	377	359	400			
Automated/ Procedural	358	228	84	95%	64%	21%
Not fully automated	19	25	17	5%	7%	4%
Missing	0	106	299	0%	30%	75%

2020 Q4 SSE: Customization members (1/2)

- New library: SCKACUST
- There is no more need to run job CKAZCUST to create new CKACUST members
- The new SCKACUST library is added to the concatenation for DDname CKACUST
  - New CKACUST members that are introduced in compliance controls are now automatically provided in SCKACUST

2020 Q4 SSE: Customization members (2/2)

- New library: SCKACUSV
- The existing CKACUST data set has records limited to 80 characters
- The new CKACUSV data set allows for longer values than 80 characters
  - for example the issuer name of digital certificates
- Example:
  - The CNFTRUST customization member is used to list certificate name filters that are approved by the ISSM. It’s used for reporting in the RACF STIG ICERR030 control

2020 Q4 SSE: STIG controls – new report types

- 7 new report types that facilitate automation
  - NEWLIST TYPE=CERTIFICATE
    - describes digital certificates present on a particular system
  - NEWLIST TYPE=IOAENV
    - shows the security settings of active BMC INCONTROL IOA environments
  - NEWLIST TYPE=IP_INETD
    - shows configuration of network services that the inetd daemon manages
  - NEWLIST TYPE=JES_DEVICE
    - shows the available JES2 devices and the information that is used to secure them
  - NEWLIST TYPE=JES_REMOTE
    - shows the available remote JES2 workstations, and the information that is used to secure them
  - NEWLIST TYPE=SSH_DAEMON
    - shows the configuration of the z/OS OpenSSH SSH daemons that run in the UNIX address spaces
  - NEWLIST TYPE=SUPSESS_REGION_CP
    - can be used to report about IBM CL/SuperSession; each record describes a Network Access Manager Control Point

NEWLIST TYPE=CERTIFICATE

- Describes digital certificates as they are present on a particular RACF system
  - Annotated with information such as the use of the certificate by a particular sub-system, e.g., MQ
- Example fields:
  - CERT_PRIVATE_KEY_STORE Certificate private key store
  - CERT_SUBSYS_TYPE Subsystem type using certificate
  - CERTIFICATE_ALT_* Certificate AltName domain, e-mail, IP addr, URI
  - CERTIFICATE_*_DATE Certificate start/end date
  - CERTIFICATE_ISSUER Issuer's distinguished name
  - CERTIFICATE_KEYUSAGE Certificate key usage
  - CERTIFICATE_LABEL Digital certificate label
  - CERTIFICATE_OWNER Certified userid
  - CERTIFICATE_SERIAL Certificate serial number
  - CERTIFICATE_SIGNING_ALG Certificate signing algorithm
  - CERTIFICATE_STORE Certificate store
  - CERTIFICATE_SUBJECT Subject's distinguished name
  - CERTIFICATE_TRUSTED Certificate is trusted
  - LABEL_IN_[PKDS|TKDS] PKDS/TKDS token label
  - MQ_* e.g., Certificate is MQ default
  - NAMED_KEYRING Keyring name (owner.name)
  - NAMED_KEYRING_DEFAULT Default cert for this keyring
  - NAMED_KEYRING_USAGE Cert. usage in this keyring
- Not in UI yet except through AU.R.E / STIG

NEWLIST TYPE=CERTIFICATE in RACF STIG controls

- Compliance checks select trusted certificates and verify that they are not expired; the controls also report on issuers or certificate name filters
  - ICERR010 Trusted CA
  - ICERR020 Expired certificates
  - ICERR030 Certificate name filters

NEWLIST TYPE=IOAENV

- QNAME used in constructing SAF resource names
- Compliance checking for:
  - IOAENV shared defaults
    - Fields IOA_*: ASID DEFMCHKI DFMI06 DFMI07 DFMI09 DFMI12 DFMI16 DFMI32 DFMI40 DFMI42 IOACLASS IOATCBSIOAXCLAS JOBNAME RACSCLAS SAFSCLAS SECTOLI
  - BMC Control/D local overrides
    - Fields CTD_*: ASID DEFMCHKD DFMD01 DFMD04 DFMD08 DFMD19 DFMD23 DFMD24 DFMD26 DFMD27 JOBNAME SECTOLD
  - BMC Control/M local overrides
    - Fields CTM_*: ASID DEFMCHKM DFMM01 DFMM02 DFMM08 DFMM21 JOBNAME MSUBCHK RACJCARD SAFJCARD SECTOLM TSSJCARD
  - BMC Control/O local overrides
    - Fields CTO_*: ASID AUTOMLOG DEFMCHKO DFMO01 DFMO02 DFMO03 DFMO04 DFMO08 DFMO10 DFMO15 JOBNAME RUNTCACH RUNTIME_SECURITY SECTOLO

- Not in UI yet except through AU.R.E / STIG

NEWLIST TYPE=IP_INETD

- Shows which SERVICES to listen for and automatically open when connect attempted.
- Compliance checks verify the absence of certain restricted services.
  - ZUSS0014 UNIX inetd sec params
- Fields:
  - ASID Address space number
  - COMPLEX Complex name
  - IP_CHAR IP address
  - PID Unix process id
  - PROGRAM Program path
  - PROGRAM_ARGS Program arguments
  - PROTOCOL Protocol
  - SERVICE Service name
  - SOCKET Socket
  - SYSTEM System name
  - USERID User ID
  - VER Version from ALLOC
  - WAIT Wait flag
- Not in UI yet except through AU.R.E / STIG (but added to RE.I in 2.5.0)

NEWLIST TYPE=JES_DEVICE

- Shows JES device security settings
- Fields:
  - ACF2_ACL ACF2 access list
  - ACF2_RULE_ENTRY ACF2 rule entry
  - C SAF resource class
  - CLASS SAF resource class
  - COLLECT_DATETIME CKFREEZE creation timestamp
  - COMPLEX Security complex name
  - NAME JES device name
  - PARENT JES device parent
  - RACF_ACL RACF access list
  - RACF_AUDITF Failure audit access level
  - RACF_AUDITS Success audit access level
  - RACF_CLASS RACF Resource class
  - RACF_GLOBAL_ACCESS RACF global access
  - RACF_IDSTAR_ACCESS RACF ID * access
  - RACF_PROFILE RACF Profile name
  - RACF_PROFTYPE RACF Profile type
  - RACF_UACC RACF universal access
  - RACF_WARN_ONLY Warn only (do not protect)
  - RESOURCE SAF resource name
  - SUBSYS JES subsystem name
  - SYSTEM System name
  - TYPE JES device type
  - UNIT JES device unit
  - VER Version from ALLOC
- Not in UI yet except through AU.R.E / STIG (but added to RE.J.D in 2.5.0)

NEWLIST TYPE=JES_DEVICE in RACF STIG controls

- Compliance checks verify auditing and UACC /ID(*)/warning mode of JESINPUT and WRITER JES devices; the controls also verify if access to them is restricted to appropriate personnel
  - ZJES0022 JES2 JESINPUT
  - ZJES0032 JES2 WRITER

NEWLIST TYPE=JES_REMOTE

- Shows JES remote terminal definitions and security settings
- For compliance checks of proper SAF protection of work / command through remote terminals
  - ZJES0011 JES2 RJE user IDs
  - ZJES0014 RJE/NJE controlled
- Fields:

ACF2_ACL	ACF2 access list
ACF2_RULE_ENTRY	ACF2 rule entry
CLASS	SAF resource class
NAME	JES remote terminal name
RACF_ACL	RACF access list
RACF_AUDITF	Failure audit access level
RACF_AUDITS	Success audit access level
RACF_CLASS	RACF Resource class
RACF_GLOBAL_ACCESS	RACF global access
RACF_IDSTAR_ACCESS	RACF ID * access
RACF_PROFILE	RACF Profile name
RACF_PROFTYPE	RACF Profile type
RACF_UACC	RACF universal access
RACF_WARN_ONLY	Warn only (do not protect)
RESOURCE	SAF resource name
SAF_USER_EXISTS	SAF user exists
SUBSYS	JES subsystem name

- Not in UI yet except through AU.R.E / STIG (but added to RE.J.R in 2.5.0)

NEWLIST TYPE=SSH_DAEMON

- Shows SSHD configuration settings
- Fields:
  - ASID — Address space number
  - BANNER — Connect banner path/dsn
  - BANNER_MATCH — Banner matches
  - CIPHER — Encryption cipher
  - CIPHERS_SOURCE — Ciphers implementation source
  - COMPLEX — Complex name
  - FIPSMODE — OpenSSH running in FIPS mode
  - HOST_KEY_FILE — Private host key file
  - HOST_KEY_RING_LABEL — Private host key ring label
  - JOBNAME — Job name
  - LISTEN_ADDRESS — Listening address
  - MAC — Message Authentication Code
  - MACS_SOURCE — MACs implementation source
  - MATCH — Match criteria
  - PID — UNIX process id
  - PORT — Listening port
  - PROTOCOL_VERSION — SSH protocol version
  - SERVER_SMF — Collect server SMF records
  - SYSTEM — System name
  - VER — Version from ALLOC
- Not in UI yet except through AU.R.E / STIG (but added to RE.I in 2.5.0)

NEWLIST TYPE=SSH_DAEMON in STIG controls

- Compliance checks verify if sshd is properly configured, e.g.,
  - if it uses the SSHv2 protocol and a FIPS 140-2 compliant cryptographic algorithm,
  - If it uses SAF keyrings for key storage, or
  - if it writes SMF records or displays a banner
  - ZSSH0010 sshd SSHv2 protocol
  - ZSSH0020 sshd FIPS 140-2
  - ZSSH0030 ssh logon warning banner
  - ZSSH0040 sshd SMF config
  - ZSSH0050 sshd SAF keyrings

NEWLIST TYPE=SUPSESS_REGION_CP

- Can be used to report about IBM CL/SuperSession. Each record in the TYPE=SUPSESS_REGION_CP report describes a Network Access Manager Control Point
- Fields
  - APPL — Override of ACB name VFY APPL
  - CLASSES — Protected class list CLASSES
  - CONTROL_POINT — Control point name
  - DB/RACF/SAF — Resource validation by NAM DB/uses RACF/calls SAF
  - EXIT — Access control override EXIT
  - NAF — Exception message log via NAF
  - NAF_DSNAME — Record messages in NAF DSNAME
  - NAM_DxNAME — Security database NAM DDNAME/DSNAME
  - NOTIFY — Exception msg via CT/E NOTIFY
  - REQSTOR — SAF requestor VERIFY REQSTOR
  - SMF — Record type to log NAF in SMF
  - SMF_TYPE_ACTIVE — Record type on in SMF subsys
  - STAT — Statistics if set in ESM STAT
  - SUBSYS — SAF subsys VERIFY SUBSYS
  - VGWAPLST_APPL — Override of ACB name AUT APPL
  - VGWAPLST_EXTERNAL — Class dyn appl list EXTERNAL
  - VGWAPLST_REQSTOR — SAF dyn appl list AUT REQSTOR
  - VGWAPLST_SUBSYS — SAF dyn appl list AUT SUBSYS
- Not in UI yet except through AU.R.E / STIG

NEWLIST TYPE=SUPSESS_REGION_CP in STIG controls

- Compliance checks verify if CL/SuperSession is properly configured to generate SMF records or if security options of the network control points are correctly specified
  - ZCLS0041 CL/SuperSession SMF records written
  - ZCLS0042 SS KLVINNAM config
  - ZCLS0043 SS APPCLASS config

2021Q2 SSE

DISA STIG

2021 Q2 SSE: STIG controls

- RFE CR145939: implement a Site Security Plan that allows for non-unique user IDs assigned to started tasks
  - it includes changes to RACF0650 and all ~30 and ~32 controls about started tasks in RACF product STIGs, e.g., ZCA1R030 and ZCA1R032

- Further automations
  - All ESMs: IFTP0040, IUTN0020
  - ACF2: ACP00130, ACP00135, ZUSS0046
- Improvements
  - ACF2: ACF0390, ACF0570
  - Add N/A tests in numerous controls to make sure that they always show a result, e.g., IUTN0010, RACF0740, RACF ZJES0011
  - Stylistic changes to lots of controls, to improve readability of the reports, mostly add CAPTIONs and DOMAIN descriptions
  - Add sensitive tape data sets

Classified Tape Data Sets

TYPE=DSN and TYPE=SENSDSN tape data sets (1/2)

- New records with tape data sets added, originating from:
  - IBM RMM Control Data Set
  - Broadcom CA-1 Tape Management Catalog,
  - Broadcom CA-TLMS Volume Master File,
  - ICF catalog entries with device class TAPE,
  - Current address space allocations with device class TAPE.
- Previously only available in TYPE=REPORT_PROFILE and other REPORT_ types
- SIMULATE CLASS=... RISK=… and SIMULATE SENSITIVE now also applied to tape data sets
- Toggle inclusion of data sets on scratch tapes: REPORT SCRATCH
  - Because read-sensitive data still readable from scratch tapes
- Performance for ACF2 systems reported in TYPE=DSN subsets greatly improved

TYPE=DSN and TYPE=SENSDSN tape data sets (2/2)

- New fields:
  - DEVICE_CLASS DASD or TAPE
  - FIRST_VOLSER First volume serial in a potentially multi-volume, multi-file tape complex.
  - FSEQN File sequence number in complex
  - IS_SCRATCH Tape in scratch status but not erased yet
- PRIV_SENSTYPE and SENSTYPE can now be filled for tape data sets.
- Refer to RE.O.T to see global security settings for device class TAPE data sets and volumes.
- UI in RE.F.D and AU.S / MVS EXTENDED / SENSITIVE

RE.F.D tape data sets - selection

- New summary
- Device class selection

```
                         zSecure Suite - FIM - Data sets
Command ===> ____________________________________________________________________

Show data sets that fit all of the following criteria
Data set name  . . . ____________________________________________
Volume serial  . . . ______  (volser or EGN mask)
System . . . . . . . ____    (system or EGN mask)
Encryption key label ____________________________________________________________
Sensitivity  . . . . ___________

Additional selection criteria
_  Other attributes

Output/run options
Summarize by _  1. Complex  3. Volser   5. Key label  7. Sensitivity
                2. System   4. DSN      6. HLQ        8. Tape complexes
_  Show differences   _  Only duplicates    _  Include scratch
_  Print format          Send as e-mail
      Background run     Full detail form      Narrow print
```

RE.F.D tape data sets – summary output

- Summary by VER and FIRST_VOLSER
- For tapes, secondary volumes / DSNs are shown

z/OS data sets

Command ===> _____

	Ver	DvCl	Vol1	#Seq nums	#Data sets
__		TAPE	JKE01	1	1
__		TAPE	JKE02	2	2
__		TAPE	JKE1	1	1
__		TAPE	JKE2	2	2
__		TAPE	L00000	1	1
__		TAPE	MR1000	1	1
__		TAPE	TAPE01	3	6
__		TAPE	TAPE03	1	1
__		TAPE	7226	1	1
__		TAPE	7227	1	1
__		TAPE	7228	1	1
__		TAPE	7229	1	1

RE.F.D tape data sets – further selection

- ‘Other attributes’ leads to

```
                          zSecure Suite - FIM - Data sets
Command ===> ____________________________________________________________

Show data sets that fit all of the following criteria
Device class . . . . _  1. DASD   2. Tape

Specify data set flag attributes (Y/N/blank)
AND  _  Anti-tamper digest     _  Encrypted

Specify TAPE data set flag attributes (Y/N/blank)
AND  _  Primary file           _  Primary volume        _  Scratch
```

RE.F.D tape data sets – overview display

- Default sort order is by DSN

```
                 z/OS data sets                                                                                  Line 664 of 721
Command ===> _____________________________________________________________________________________________ Scroll===> CSR
                                                                                          25 Mar 2021 14:09
   Data set name                                VolSMS Complex       Syst Sysname  DvCl DsnTyp Vol1   Fseqn Scr VolSer VolSer Mnt
__ BACKUP.U4CK02.#170521                               EEND          EEND EEND     TAPE ummtap 900047   128      900047 900047
__ BACKUP.U4PG01.#170521                               EEND          EEND EEND     TAPE ummtap 900013   129      900013 900013
__ BACKUP.U4PG01.#170521                               EEND          EEND EEND     TAPE ummtap 900047   129      900047 900047
__ BACKUP.U4PG02.#170521                               EEND          EEND EEND     TAPE ummtap 900013   130      900013 900013
__ BACKUP.U4PG02.#170521                               EEND          EEND EEND     TAPE ummtap 900047   130      900047 900047
__ BACKUP.U4PG03.#170521                               EEND          EEND EEND     TAPE ummtap 900013   131      900013 900013
__ BACKUP.U4PG03.#170521                               EEND          EEND EEND     TAPE ummtap 900047   131      900047 900047
__ BACKUP.U4SP01.#170521                               EEND          EEND EEND     TAPE ummtap 900013   132      900013 900013
__ BACKUP.U4SP01.#170521                               EEND          EEND EEND     TAPE ummtap 900047   132      900047 900047
__ BACKUP.U4SY01.#170521                               EEND          EEND EEND     TAPE ummtap 900013   133      900013 900013
__ BACKUP.U4SY01.#170521                               EEND          EEND EEND     TAPE ummtap 900047   133      900047 900047
__ BCSCGB1.BCSCGB1.DUMP.DELETE                         ADCDPL        AHJB S0W1     TAPE cnntap XYZTAP     1      XYZTAP XYZTAP
__ CRMAROB.TAPEDS                                      EEND          EEND EEND     TAPE cnntap ROB123     1      ROB123 ROB123
__ CRMBERT.DUMPISPP                                    EEND          EEND EEND     TAPE cnntap TEST03     1      TEST03 TEST03
__ CRMBERT.P390.DUMP.SOFTWR.DD970328                   EEND          EEND EEND     TAPE cnntap TEST03     1      8BCL23 8BCL23
__ CRMBERT.P390.MVS522.HFSDUMP.TAPE                    EEND          EEND EEND     TAPE cnntap HFSDMP     1      HFSDMP HFSDMP
__ CRMBERT.VSCPMV5.FULLDUMP                            EEND          EEND EEND     TAPE cnntap TEST04     1      TEST04 TEST04
__ CRMBERT.ZOS19DMP.DMTP01.DD080610                    EEND          EEND EEND     TAPE cnntap 459718     1      459718 459718
__ CRMBHJ1.TAPE.FSEQ.#10000.V000000.A                  EEND          EEND EEND     TAPE cnntap 000000 10000      000000 000000
__ CRMBHJ1.TAPE.FSEQ.#10000.V331000.A                  EEND          EEND EEND     TAPE cnntap 331000 10000      331000 331000
__ CRMBTKR.SMFTIPT2.MES9911.COPY                       EEND          EEND EEND     TAPE cnntap 331315     1      331315 331315
__ CRMBTKR.SMFTIPT2.MES9911.COPY                       EEND          EEND EEND     TAPE cnntap 331315     1      331320 331320
__ DFHSM.ABARS.C.C01V0014                              ADCDPL        AHJB S0W1     TAPE cnntap HA0001     4      HA0001 HA0001
__ DFHSM.ABARS.C.C01V0015                              ADCDPL        AHJB S0W1     TAPE cnntap HA0002     4      HA0002 HA0002
__ DFHSM.ABARS.D.C01V0014                              ADCDPL        AHJB S0W1     TAPE cnntap HA0001     1      HA0001 HA0001
__ DFHSM.ABARS.D.C01V0015                              ADCDPL        AHJB S0W1     TAPE cnntap HA0002     1      HA0002 HA0002
__ DFHSM.ABARS.I.C01V0014                              ADCDPL        AHJB S0W1     TAPE cnntap HA0001     3      HA0001 HA0001
__ DFHSM.ABARS.I.C01V0015                              ADCDPL        AHJB S0W1     TAPE cnntap HA0002     3      HA0002 HA0002
```

RE.F.D tape data sets – detail display

- Extra information shown
- Type ummtap means: uncataloged data set name of managed file on managed tape volume

```
                    z/OS data sets
Command ===>

  Identification
_ Security complex name          EEND
_ System name                    EEND EEND
_ Data set name                  BACKUP.U4CK02.#170521
  Data set type                  ummtap
  Device class                   TAPE        Unit type
  Volume serial or SMS managed               Volume is scratch              No
  Start of multi-file complex    900047      File sequence number           128
  Volume serial                  900047      Data set is migrated           No
  Real volume serial             900047      Volume is mounted              No
_ Real data set name             UP.U4CK02.#170521
  DASD box serial number and id
  Catalog name
  Catalog volume

  Detail information
  Type of sensitive data set
  Catalog alias
  Related name
  Related name (resolved)
  In Volume Table Of Contents    No          In master catalog              No
  In VSAM Volume Data Set        No          Non-standard catalog           No
  System can decrypt data set                In connected catalog           No
  Data key label

  SAF and ESM information
  SAF resource class             DATASET
  SAF resource name              BACKUP.U4CK02.#170521
  Volume serial passed to SAF    900047
```

RE.F.D tape data sets –ACF2 tape pseudo DSN

- ACF2 allows volume level protection by pseudo Data Set Names depending on GSO options

```
                    z/OS data sets
Command ===> ____________________________________________________________________

_ Data set name                    TAPE01.DATASET
  Data set type                    cnntap
  Device class                     TAPE      Unit type
  Volume serial or SMS managed               Volume is scratch              No
  Start of multi-file complex      000001    File sequence number           1
  Volume serial                    000001    Data set is migrated           No
  Real volume serial               000001    Volume is mounted              No
_ Real data set name               TAPE01.DATASET
  DASD box serial number and id
  Catalog name                     CATALOG.T60991
  Catalog volume                   T60991

  Detail information
  Type of sensitive data set       Site-blup4
  Catalog alias
  Related name
  Related name (resolved)
  In Volume Table Of Contents      No        In master catalog              No
  In VSAM Volume Data Set          No        Non-standard catalog           No
  System can decrypt data set                In connected catalog           No
  Data key label

  SAF and ESM information
  SAF resource class               DATASET
  SAF resource name                @000001.VOLUME
  Volume serial passed to SAF      000001
  Owning qualifier                 @000001
  Owning HLQ is a userid           No        Owning HLQ is a group          No
```

TSO session IP

TSO via TN3270 IP address

- Enrich SMF processing with IP address telnet client based on terminal LU
  - Field SRCIP now available where TERMINAL is available and matches a LU from 119-20 or 118-20.
- Enrich SMF with changed terminal LU name on TSO reconnect
  - In SMF 20/30/32 feed replace TERMINAL from SMF with TERMINAL from job tag cache
  - Works only if at least one SMF 80 record is written after reconnect.
- TERMINAL and SRCIP available on all specific data set activity records that identify job name and reader date/time.

End-to-end audit

TYPE=SMF new fields

- Enable correlating SMF records for
  - CICS TOR, CICS AOR, and DB2 via new field UOWID
  - z/OS Connect and CICS via new field TRACKING_TOKEN
  - Passed to SIEM

- Summary UOWID

```
USIBMWZ.TEC2TOR1.C312AAA88FE8
        2
                    2Nov2020 10:51:34.42   110     1 127.0.0.1       KENISHI CICS transaction TEC2TOR1 CSMI
                    2Nov2020 10:51:34.49   110     1 192.168.48.122  KENISHI CICS transaction TEC2AOR1 CSMI
```

- Summary TRACKING_TOKEN:

```
BAQ.1.TECPLEX.TEC2.2020-11-02T14:51:33.903633
        3
                   2Nov2020 10:51:33.90   110     1 192.168.48.122  KENISHI CICS transaction TEC2AOR1 CSMI
                   2Nov2020 10:51:34.42   110     1 127.0.0.1       KENISHI CICS transaction TEC2TOR1 CSMI
                   2Nov2020 10:51:35.27   123     1 192.168.48.95   z/OS Connect ZCEESRVR API GET healthcareinfo showVitals, user
                                                                    KENISHI, HTTPresp 200, 0.001s 0/102 bytes in/out, URI
                                                                    /healthcareinfo/vitals/1445, CICS-1.0 cicsConn USIBMWZ .TEC2TOR1
                                                                     CSMI,HCT1BI01
```

Access Monitor

Access Monitor enhancements

Three new data sources for event collection

- Local RACLISTed resource classes.
  - Required for applications that still don’t use GLOBAL=YES on the RACROUTE REQUEST=LIST macro.
- Program access events
  - Uses a special form of RACROUTE REQUEST=FASTAUTH.
    Can not be captured through regular RACF exits.
- UNIX file/directory access events
  - Needs special UNIX related exits to capture events.

Access Monitor enhancements

Local RACLISTed resource classes - The problem

- Applications that don’t use GLOBAL=YES on the RACROUTE REQUEST=LIST.
  - Profiles are kept in LSQA, instead of in a dataspace.
  - Refresh needs to be done in the application, and not through SETROPTS.
  - Access checking does not invoke RACF exit ICHRFX04, but only ICHRFX02.
    Runs in unpredictable user environment (e.g. user key, problem state)
    Not enough working storage to build an Access record.
  - It was assumed that existing applications would be updated to exploit benefits of RACF 2.1 GLOBAL RACLIST support (1994).

Access Monitor enhancements

Local RACLISTed resource classes - The solution

- Access Monitor now installs RACF ICHRFX02 exit.
  - Exit exploits a new Program Call (PC) to verify and collect data, and build an Access record that is passed to the Access Monitor started task.
  - Access record has identical layout and contents as existing one created by ICHRFX04. No indication if data is captured by ICHRFX02 or ICHRFX04.
  - Special processing to avoid capturing the same event twice (in some environments, RACF calls both ICHRFX04 and ICHRFX02).
- User interface was not changed.

Access Monitor enhancements

Local RACLISTed resource classes - The solution

- New keyword on OPTION statement in Access Monitor configuration member:

```
┌─NoCaptureLocalRaclist─┐
──────────────────────────┼──
└─CaptureLocalRaclist───┘
```

- Default is not to collect events for local RACLISTed resource profiles.
- ICHRFX02 exit is only supported with RACFExitMode(Faststore).
- Started task needs access to resource C2X.ICHRFX02 in the XFACILIT class.
- For migration, use documented process:
  F C2PACMON,SIPL or a SYSTEM IPL, followed by a START.

Access Monitor enhancements

Program access events - The problem

- Contents Supervisor uses RACROUTE REQUEST=FASTAUTH to check if the user has access to a program.
  - RACF router uses Requestor and Subsys to direct requests to a special FASTAUTH routine.
  - Regular FASTAUTH exits are not invoked. Only the SAF router exit is called.
  - SAF router exit is a pre-exit ==> no information about RACF results.
  - No source for complete information.
  - Protection of program is divided over PROFILE and Library/Volser.

Access Monitor enhancements

Program access events - The partial solution

- Access Monitor exploits SAF router exit ICHRTX00 to collect information about the RACROUTE REQUEST.
  - No information about the request results.
    - No profile information.
    - No success/violation information.
    - Access INTENT is READ
    - No access ALLOWED information
  - Information about program name, library name, volser, and definition status of the program (next page).

Access Monitor enhancements

Program access events - The partial solution

- Definition status of the program.
  - Not protected at all,
  - Matched by profile (independent of library/volser),
  - Loaded from controlled library
  - Controlled program (profile match and library match)
  - Specific program (same as Controlled program, but exclude * and **)
- Library names can be “JPA-LPA”
  - Program is already loaded in storage, cannot be a controlled program.
  - Intercepted to be able to count usage of program.

Access Monitor enhancements

Program access events - The partial solution

- New keyword on OPTION statement in Access Monitor configuration member:
- Parameter matches the type as described on previous page.
- Without subparameter, all program events are captured.
  Main reason for subparameter is to reduce number of Access records.

```
┌─NoCapturePrograms──────────────────────────┐
├────────────────────────────────────────────┤
└─CapturePrograms(──┬─────────────────────┬─)─┘
                    ├─DefProgram──────────┤
                    ├─CtlProgram──────────┤
                    ├─SpecProgram─────────┤
                    └─CtlLibrary──────────┘
```

- Default is not to collect events for Programs
- ICHRTX00 exit is only supported with RACFExitMode(Faststore).
- Started task needs access to resource C2X.ICHRTX00 in the XFACILIT class.
- For migration, use documented process.

Access Monitor enhancements

Program access events - Reporting

- Same reporting functions as other resource classes.

```
                    IBM Security zSecure ACCESS summary
Command ===>
Access monitor records for Classes like PROGRAM
   Occurrence Class    First occurrenc Last occurrence
          166 PROGRAM  11Mar2021 03:33 11Mar2021 03:36
   Occurrence Profile key used
          166
   Occurrence Intent   Type   RetAll AccRC
          166 READ     Fast
   Occurrence POEClass:POE port
          166
   Occurrence Resource
__          2 C2PENVTM/JPA-LPA/*NONE*
__          1 C64/CEE.SCEERUN2/A4RES2
__          2 ERBSMFI/SYS1.SERBLINK/A4RES1
__          4 EXEC/JPA-LPA/*NONE*
__         16 EZASUH03/TCPIP.SEZALOAD/A4RES1
__         21 FREE/SYS1.CMDLIB/A4RES1
__         10 USSN/ADCD.Z24A.UTAMLIB/A4SYS1
__          1 USSN/SYS21032.T084545.RA000.CKFCOLL1.R0100034/A4SYS1
__          1 USSN/SYS21032.T084847.RA000.CKFCOLL1.R0100184/A4SYS1
```

Resource name: program/dsname/volser

Program is already present in storage.

Some APF programs load programs using generated data set names.

Access Monitor enhancements

Program access events - Reporting

```
                IBM Security zSecure ACCESS summary
Command ===> _
Access monitor records for Classes like PROGRAM
   Occurrence Userid   Name                    Jobname  First occurrenc Last occurrence
__        656 +BPXAS                           BPXAS     9Feb2021 03:20 24Feb2021 08:50
__         35 +BPXOINI                         BPXOINIT  8Feb2021 02:35 22Feb2021 04:11
__        771 +CONSOLE                         CONSOLE  11Feb2021 03:35 23Feb2021 10:34
__         35 +IZUANG1                         IZUANG1   8Feb2021 02:35 22Feb2021 04:11
__         42 +IZUSVR1                         IZUSVR1   8Feb2021 02:35 22Feb2021 04:11
__       2650 +MASTER+                         *MASTER*  4Feb2021 05:08 24Feb2021 23:30
__         42 +RESOLVE                         RESOLVER  8Feb2021 02:35 22Feb2021 04:11
__         49 +TNF                             TNF       8Feb2021 02:35 22Feb2021 04:11
__         49 +VMCF                            VMCF      8Feb2021 02:35 22Feb2021 04:11
```

During address space creation, a temporary userid is assigned.
After full initialization, proper userid is assigned and used.

Access Monitor enhancements

Program access events - Reporting - Summary

```
Occurrence Resource
         1 C64/CEE.SCEERUN2/A4RES2
Occurrence Userid   Name                    Jobname
         1 IZUSVR   ZOSMF STARTED TASK 0 IZUSVR1
Occurrence Complex  Syst RGPJCAVP GUGSOPGX SOA PCSL First occurrenc Last c
         1 IDFX     AHJB                     PC L 11Mar2021 03:33 11Mar2
Occurrence LocalTimestamp
         1 11Mar2021 03:33
********************************************************************** Bottom of Data **
```

Program match
Controlled program
Specific profile
Controlled Library

Program access events - Reporting - Detail

```
Access-time user attributes              Program status
User systemwide SPECIAL        No        Defined program (any lib)     Yes
User systemwide OPERATIONS     No        Controlled program            Yes
User systemwide (RO)AUDITOR    No        Specific controlled program   No
                                         Controlled library (any pgm)  Yes
```

Access Monitor enhancements

Program access events – Selection criteria

- No simulation support.
  - Can’t select on simulated fields.
  - Summary by simulated fields shows blanks or “nothing selected”
  - Can’t compare against current RACF database (AM.2)
- Extra further selection for programs only:

```
Resource action   Intended access    Result            Program status
_  Define         __  _  1. Read     _  Success        _  Defined program
_  Delete                2. Update   _  No profile     _  Controlled program
_  Addvol                3. Control  _  Not authorized _  Specific program
_  Chgvol                4. Alter    _  Other          _  Controlled library
```

Access Monitor enhancements

UNIX file/directory access events – The problem

- RACF verification of UNIX access is done through RACF Callable Services. Standard exits are not involved. A dedicated RACF CS exit is available.
  - All Access Controls are maintained in the File System itself.
  - RACF CS Exit does not get a full path name, but only Audit File ID. There is no simple fast interface to translate FID to pathname.
  - RACF CS Exit is called for every directory in the path. A single file access involves tens of RACF calls. Not feasible to record each of them.
- FSACCESS events only occur during a File System switch
- Need other, non-RACF intercept of file/directory access.

Access Monitor enhancements

UNIX file/directory access events – The solution

- Implement UNIX Syscall exits.
  - Called for all UNIX callable services. Separate pre- and post-exits.
    Need to be activated per callable service.
  - Callable services are used by the application.
    Events occur on a “human scale”.
  - Path name is either a full path, or a relative path (current working directory)
- New Access record type, and new fields.

Access Monitor enhancements

Program access events - The partial solution

- New keyword on OPTION statement in Access Monitor configuration member:

```
  ┌─NoCaptureUSSEvents─┐
──┤                    ├──
  └─CaptureUSSEvents───┘
```

- Default is not to collect events for UNIX events
- Exits are only supported with RACFExitMode(Faststore).
- For migration, use documented process.

- Exits need to be enabled using SC_EXITTABLE in BPXPRMxx.

Access Monitor enhancements

UNIX file/directory access events – The solution

- New Access record type, and new fields.
- Needs updated CARLa in all Consolidation/Conversion CARLa members.
- New reports, new User Interface option AM.U
- No simulation support
- New fields for identification, event, and new value:
  UNIX_EVENT UNIX_INTENT, UNIX_FILE_ATTR_RAW, UNIX_GID, UNIX_NEW_AAUDIT, UNIX_NEW_APF, UNIX_NEW_GID, UNIX_NEW_LINK, UNIX_NEW_MODE, UNIX_NEW_PATHNAME, UNIX_NEW_PROG, UNIX_NEW_UAUDIT, UNIX_NEW_UID, UNIX_PATHNAME, UNIX_REQ_OPTIONS, UNIX_REQ_SET_AAUDIT, UNIX_REQ_SET_ACL, UNIX_REQ_SET_APF, UNIX_REQ_SET_MODE, UNIX_REQ_SET_OWNER, UNIX_REQ_SET_PROG, UNIX_REQ_SET_TIME, UNIX_REQ_SET_UAUDIT, UNIX_RESULT UNIX_UID

Access Monitor enhancements

UNIX file/directory access events – Sample output

- Summary by event

Occurrence	Int	Event	Return code	First occurrence	Last occurrence
30113	-r--	access	EOK	[illegible]	2Mar2021 11:51
1096	---x	access	EOK	[illegible]	2Mar2021 08:42
284	--w-	access	EOK	22Feb2021 08:11	2Mar2021 08:42
253	----	access	ENOENT	22Feb2021 08:06	1Mar2021 17:08
252	--wx	access	EOK	22Feb2021 10:11	1Mar2021 17:08
63	----	access	EOK	22Feb2021 10:11	2Mar2021 08:46
10	--w-	access	EROFS	22Feb2021 15:20	22Feb2021 16:00
3	-r--	access	EACCES	22Feb2021 10:11	1Mar2021 08:10
253940	----	chdir	EOK	18Feb2021 0[illegible]	[illegible]
2782	----	chmod	EOK	22Feb2021 0[illegible]	[illegible]
23	----	chown	EOK	22Feb2021 1[illegible]	[illegible]
2096252	----	lstat	EOK	18Feb2021 0[illegible]	[illegible]
85268	----	lstat	ENOENT	18Feb2021 1[illegible]	[illegible]
1803	----	mkdir	EOK	18Feb2021 15:52	1Mar2021 17:15
421	----	mkdir	ENOENT	22Feb2021 08:10	1Mar2021 17:15
384	----	mkdir	EEXIST	22Feb2021 08:11	1Mar2021 08:21
155034	----	opendir	EOK	18Feb2021 08:00	2Mar2021 09:38
4	----	opendir	ENOENT	22Feb2021 10:28	1Mar2021 08:32

Event type

UNIX return code mnemonic.

Access Monitor enhancements

UNIX file/directory access events – Sample output

- Next summary level

```
Occurrence Int  Event            Return code      First occurrenc Last occurrence
     30113 -r-- access           EOK              18F
Occurrence UNIX pathname                                          urrenc Last occurrence
        18 /S0W1/dev/random                                       10:13  1Mar2021 17:08
        54 /S0W1/dev/urandom                                      22Feb2021 10:13  1Mar2021 17:08
         8 /S0W1/etc/profile                                      22Feb2021 15:08  2Mar2021 08:42
         3 /S0W1/etc/rc                                           22Feb2021 10:11  1Mar2021 08:09
         1 /S0W1/var/zosconnect/v3r0/extensions/imsmobile.properties  22Feb2021 15:49 22Feb2021 15:49
         2 /S0W1/var/zosconnect/v3r0/extensions/zosconnect.properties  22Feb2021 15:48 22Feb2021 15:48
         1 /S0W1/var/zosconnect/v3r0/servers/defaultServer/logs/messages.lo 22Feb2021 15:49 22Feb2021 15:49
         1 /S0W1/var/zosconnect/v3r0/servers/defaultServer/logs/messages_21 22Feb2021 15:49 22Feb2021 15:49
```

Resolved pathname

- Identification part of detail display:

```
Access summary
Security complex name        IDFX
RACF userid                  BCSCGB1  GUUS BONNES
Job name for some userids    BCSCGB1
Pathname                     /S0W1/var/zosconnect/v3r0/extensions/imsmobile.properties
UNIX uid                     0
UNIX gid                     0
UNIX event                   access
Access intent                -r--
UNIX return code             EOK
```

Effective UID and GID at time of event

Access: check if user has access
-r-- request READ access
EOK Yes

Access Monitor enhancements

UNIX file/directory access events – Sample output

- Detail request information:

```
Unix request flags
UNIX set owner

UNIX set mode                    Yes
UNIX set auditor audit
UNIX set user audit
UNIX extattr (NO)APF
UNIX extattr (NO)prog.ctl
UNIX set ACL
UNIX set time field

Secondary pathname
UNIX new pathname
UNIX new link pathname

Other flags
UNIX OPEN and ACCESS options

Access-time user attributes
Privileged/trusted user          No
User systemwide SPECIAL          Yes
User systemwide OPERATIONS       No
User systemwide (RO)AUDITOR      Yes
```

```
New values
UNIX new uid
UNIX new gid
UNIX new mode                    rwxr-xr-t
UNIX new auditor-spec. audit
UNIX new user-spec. audit
UNIX extattr APF on
UNIX extattr prog.ctl on
```

What the user specified, e.g. new access mode

What the user requested, e.g. chmod

Access Monitor enhancements

Extra changes in support of UNIX

- All events now show if user has the AUDITOR or ROAUDIT attribute.
  Auditor has READ access to all directories.
- New DIAGNOSE option for operator:
  - Show status of UNIX Syscall Exits
  - Show hex dump of contents of UNIX Exit Table
    Has readable name of active SC_EXITTABLE in BPXPRMxx
    Bitarray of specified exits (for IBM diagnostic purposes only)

Access Monitor enhancements

Other Access Monitor Improvements

- IDIDMAP profile names (UTF8) now properly displayed.
- AM.8 (remove) and AM.9 (cleanup) can now also be run in background (batch job).
- Jobname collection can now be activated specifying a prefix. For example in C2PAMJOB:

```
----+----1----+----2
IBM     YES
```

- PortOfEntry collection also activated when class is missing.

Access Monitor enhancements

Other Access Monitor Changes

- Line length of ACCESS files increased to 2123 to accommodate UNIX path information.
- Use of “command=no” no longer excludes FASTAUTH events.
- More DEFINE events are now recognized as command related.

zSecure Audit

zSecure 2.5.0 RE.J update

- New options for JES device and remote terminals

```
                                zSecure Suite - Resource - JES
 Option ===>

 D     Devices          Devices
 J     Jobclass         Job class definition
 N     NJE nodes        Network job entry node protection
 R     Remotes          Remote terminals
 S     STC              Started task protection
```

zSecure 2.5.0 RE.J.D JES devices

- New option RE.J.D to select and display or print JES devices

```
                          zSecure Suite - JES - Devices
Command ===> ____________________________________________________________________

Show devices that fit all of the following criteria
Name . . . . _________
Subsystem    ____                 System . . . ________
Complex  . . _______              Class  . . . ________  (WRITER/JESINPUT)
Parent . . . _______              Type . . . . ____
SAF resource ________________

Advanced selection criteria
_  RACF settings

Output/run options
Summarize by _  1. Parent    2. Type      3. Subsystem    4. System

_  Show differences
_  Print format          Send as e-mail
      Background run     Full detail form      Narrow print
```

zSecure 2.5.0 RE.J.D JES devices

- Shows SAF protection and auditing

```
                 JES Devices overview for RACF                                                                  Line 1 of 84
Command ===> _____________________________________________________________________________________________ Scroll===> CSR
                                                                                                  24 Mar 2021 23:45
   Complex  System   Ver  Devices
   NMPIPL87 ZS14              84
   Name       Subs System   Complex  Type Unit Parent   UACC    IDSAcc  Success Failure Wrn Class    Profile
__ L1.JR1     HASP ZS14     NMPIPL87 NJR       HSSVMA   READ                    READ    No  JESINPUT **
__ L1.JR1     JES2 ZS14     NMPIPL87 NJR       HSSVMA   READ                    READ    No  JESINPUT **
__ L1.JR2     HASP ZS14     NMPIPL87 NJR       HSSVMA   READ                    READ    No  JESINPUT **
__ L1.JR2     JES2 ZS14     NMPIPL87 NJR       HSSVMA   READ                    READ    No  JESINPUT **
__ L1.JT1     HASP ZS14     NMPIPL87 NJT       HSSVMA   NONE                            WRITER
__ L1.JT1     JES2 ZS14     NMPIPL87 NJT       HSSVMA   ALTER                   READ    No  WRITER   JES2.**
__ L1.JT2     HASP ZS14     NMPIPL87 NJT       HSSVMA   NONE                            WRITER
__ L1.JT2     JES2 ZS14     NMPIPL87 NJT       HSSVMA   ALTER                   READ    No  WRITER   JES2.**
__ L1.SR1     HASP ZS14     NMPIPL87 NSR       HSSVMA   READ                    READ    No  JESINPUT **
__ L1.SR1     JES2 ZS14     NMPIPL87 NSR       HSSVMA   READ                    READ    No  JESINPUT **
__ L1.SR2     HASP ZS14     NMPIPL87 NSR       HSSVMA   READ                    READ    No  JESINPUT **
__ L1.SR2     JES2 ZS14     NMPIPL87 NSR       HSSVMA   READ                    READ    No  JESINPUT **
__ L1.ST1     HASP ZS14     NMPIPL87 NST       HSSVMA   NONE                            WRITER
__ L1.ST1     JES2 ZS14     NMPIPL87 NST       HSSVMA   ALTER                   READ    No  WRITER   JES2.**
__ L1.ST2     HASP ZS14     NMPIPL87 NST       HSSVMA   NONE                            WRITER
__ L1.ST2     JES2 ZS14     NMPIPL87 NST       HSSVMA   ALTER                   READ    No  WRITER   JES2.**
__ OFF1.JR    HASP ZS14     NMPIPL87 OJR       OFFLOAD1 READ                    READ    No  JESINPUT OFF1.JR
__ OFF1.JR    JES2 ZS14     NMPIPL87 OJR       OFFLOAD1 READ                    READ    No  JESINPUT OFF1.JR
__ OFF1.JT    HASP ZS14     NMPIPL87 OJT       OFFLOAD1 NONE                            WRITER
__ OFF1.JT    JES2 ZS14     NMPIPL87 OJT       OFFLOAD1 ALTER                   READ    No  WRITER   JES2.**
__ OFF1.SR    HASP ZS14     NMPIPL87 OSR       OFFLOAD1 READ                    READ    No  JESINPUT **
__ OFF1.SR    JES2 ZS14     NMPIPL87 OSR       OFFLOAD1 READ                    READ    No  JESINPUT **
__ OFF1.ST    HASP ZS14     NMPIPL87 OST       OFFLOAD1 NONE                            WRITER
__ OFF1.ST    JES2 ZS14     NMPIPL87 OST       OFFLOAD1 ALTER                   READ    No  WRITER   JES2.**
__ OFF3.JR    HASA ZS14     NMPIPL87 OJR       OFFLOAD3 READ                    READ    No  JESINPUT **
__ OFF3.JR    JESA ZS14     NMPIPL87 OJR       OFFLOAD3 READ                    READ    No  JESINPUT **
__ OFF3.JT    HASA ZS14     NMPIPL87 OJT       OFFLOAD3 NONE                            WRITER
```

zSecure 2.5.0 RE.J.R JES remote terminals

- New option RE.J.R to select and display or print JES remote terminal security

```
                        zSecure Suite - JES - Remotes          0.0 s CPU, RC=4
Command ===> ____________________________________________________________________

Show remote terminals that fit all of the following criteria
Name . . . . . . . . . . ________
Subsystem  . . . . . . . ____
System . . . . . . . . . ________
Complex . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
SAF ID exists  . . . . . _  (Y/N)
FACILITY RJE.name exists _  (Y/N)

Output/run options
Summarize by _  1. Subsystem    2. System

_  Show differences
_  Print format          Send as e-mail
      Background run     Full detail form      Narrow print
```

zSecure 2.5.0 RE.J.R JES remote terminals

- Shows SAF protection and auditing

JES Remotes overview for RACF

Command ===>

Password verification via RACF

Complex	System	Ver	Remotes
NMPIPL87	ZS14		12

	Name	Subs	System	Complex	Usr	Class	Profile	ProfType	Prof
__	RMT1	HASP	ZS14	NMPIPL87	Yes	FACILITY	RJE.RMT1*	GENERIC	Yes
__	RMT1	JES2	ZS14	NMPIPL87	Yes	FACILITY	RJE.RMT1*	GENERIC	Yes
__	RMT11	HASA	ZS14	NMPIPL87	No	FACILITY	RJE.RMT1*	GENERIC	Yes
__	RMT11	JESA	ZS14	NMPIPL87	No	FACILITY	RJE.RMT1*	GENERIC	Yes
__	RMT12	HASA	ZS14	NMPIPL87	No	FACILITY	RJE.RMT1*	GENERIC	Yes
__	RMT12	JESA	ZS14	NMPIPL87	No	FACILITY	RJE.RMT1*	GENERIC	Yes
__	RMT13	HASA	ZS14	NMPIPL87	No	FACILITY	RJE.RMT1*	GENERIC	Yes
__	RMT13	JESA	ZS14	NMPIPL87	No	FACILITY	RJE.RMT1*	GENERIC	Yes
__	RMT2	HASP	ZS14	NMPIPL87	Yes	FACILITY		missing	No
__	RMT2	JES2	ZS14	NMPIPL87	Yes	FACILITY		missing	No
__	RMT3	HASP	ZS14	NMPIPL87	No	FACILITY		missing	No
__	RMT3	JES2	ZS14	NMPIPL87	No	FACILITY		missing	No

********** Bottom of Data *****

zSecure 2.5.0 RE.I update

- New options for INETD and SSH

```
                         zSecure Suite - Resource - IP stack Selection
Command ===> ____________________________________________________   _ start panel

Show TCP/IP stack configuration data that fit all of the following criteria:
Stack name . . . . . . ________ (name or filter)
System . . . . . . . . ________ (system or filter)
Sysplex  . . . . . . . ________ (sysplex or filter)


Output/run options
_  Ports                  _  Rules                  _  VIPA
_  Interfaces             _  Routes                 _  Netaccess
_  AUTOLOG                _  Resolver               _  FTP daemon
/  Telnet server/ports    _  SSH daemon             _  Inetd daemon
_  Show differences
_  Print format              Customize title           Send as e-mail
      Background run
```

zSecure 2.5.0 RE.I SSH daemon

- Shows SSH configuration masks, FIPS compliance, key rings, SMF recording

```
                 Unix SSH daemon display                                                                    Line 1 of 6
Command ===> ____________________________________________________________________________________ Scroll===> CSR
All SSH daemon configuration records                                                  24 Mar 2021 23:45
   Jobname  Asid Complex  System   140 Match criteria                              PID          CollSrvrSMF
__ SSHD     0077 NMPIPL87 ZS14                                                      33554505 TYPE119_U84
__ SSHD3    0039 TVT6003  ZS34     Yes                                              16777242
__ SSHD3    0039 TVT6003  ZS34     Yes user crmbju1                                 16777242 none
__ SSHD3    0039 TVT6003  ZS34     Yes user crmbju2                                 16777242 TYPE119_U83
__ SSHD3    0039 TVT6003  ZS34     Yes User CRMBLU2                                 16777242
__ SSHD4    0049 TVT5007  ZS17                                                      16777241
*************************************************** Bottom of Data ***************************************************
```

zSecure 2.5.0 RE.I SSH daemon

- Configuration per matching criterion
- Banner file and banner compliance verification
- SMF recording
- Ciphers allowed

```
                    Unix SSH daemon display
Command ===>
All SSH daemon configuration records



  System identification
_ Complex name                    TVT6003
  System name                     ZS34

  SSH daemon match block identification
  Job name                        SSHD3
  Match criteria                  user crmbju2
  Address space number            0039
  UNIX process id                     16777242

  General settings
  Connect banner path/dsn         /home/crmbju1/ssh/sshd_with_o_Banner.sh
  Banner matches
_ Ciphers implementation source ICSF
  OpenSSH running in FIPS mode    Yes
  MACs implementation source      ICSF §
  Match criteria                  user crmbju2
  Collect server SMF records      TYPE119_U83

  Ciphers
  aes256-cbc
  aes256-ctr
  chacha20-poly1305@openssh.com
  aes256-cbc
```

zSecure 2.5.0 RE.I SSH daemon

- Show SAF keyring owner
- Shows listening ports
- Shows MAC algorithms allowed
- Shows SSH protocol version

```
                    Unix SSH daemon display
Command ===>
All SSH daemon configuration records


  Private host key ring labels
  SSHDAEM/* host-ssh-rsa

  Listening addresses
  127.0.0.1:30002
  127.0.0.1:30004
  nmpipl84.svl.ibm.com:22

  Ports
  30000
  30001
  30003

  Message authentication codes
  hmac-sha1
  umac-64@openssh.com

  Protocol versions
  1
*****************************************************
```

zSecure Alert

Alert enhancements

Improved job tag cache for SMF record completion.

- Some information is not present in all SMF records.
  - For example USERID is not present in SMF 14, 15, 17, 18, etc.
  - Obtained from other SMF records, and used to annotate SMF records.
  - If no other SMF records encountered, the information is missing.
- zSecure Alert issue:
  - Every environment refresh, the cached information is discarded.
    By default every hour.
    → Information in alert messages is not consistent.

Alert enhancements

Improved job tag cache for SMF record completion.

- New option in Alert configuration:

```
                 ┌External┐
─RefreshMode(────┼────────┼──)─
                 └Internal┘
```

- In User Interface:

```
Interval  . . . . . . . . 60                    (in seconds)
Environment refresh . . . 10                    (in minutes)
Use internal refresh     Y                      (Y/N/blank)
Average . . . . . . . . . 300                   (in seconds)
Buffer size . . . . . . . 1      MB             (in KB/MB)
Number of buffers . . . . 10
TCP keepalive interval   ___                    (in seconds)
```

- CKRCARLA reporting engine refreshes all information without dropping data used for inter-record annotation.

Alert enhancements

Improved job tag cache for SMF record completion.

- Uses additional above the bar private storage to retain information:
  Approximately 1 gigabyte / 8 million jobs.
  → Check/Update REGION in Started Task procedure.

- Effect of operator modify commands:

  - REFRESH — All in-storage buffers are kept, and
    Cached information (job tag data) is retained.
  - RESTART — All in-storage buffers are freed and reallocated.
    Cached information (job tag data) is discarded.

- Related messages in DISPLAY response:

```
C2P0725I Refresh of alert reporting task uses internal restart mode
C2P0726I CKRCARLA program has been restarted 217 times
C2P0727I Job tag information retained for 178 jobs
```

Alert enhancements

Keepalive option to prevent dropping TCPIP connection.

- Does not prevent close by partner.

```
Interval  . . . . . . . . 60__                    (in seconds)
Environment refresh . . 10__                      (in minutes)
Use internal refresh    Y                         (Y/N/blank)
Average . . . . . . . . . 300                     (in seconds)
Buffer size . . . . . . . 1___   MB               (in KB/MB)
Number of buffers . . . . 10
TCP keepalive interval  ____                      (in seconds)
```

Alert enhancements

Batch interface to manage Alert configuration

- Export, import, and compare Alert configurations.
- Select and unselect alerts and alert ranges.
- Build configuration, and
- Test alert configuration from SMF dump data set
- Refresh/Activate configuration.
- Upgrade configuration after zSecure maintenance.

Alert enhancements

Enhancements to the Alert configuration ISPF user interface

- Copy of configuration also copies alert destinations and parameters.
- Alert destinations can be consistently managed per Configuration/Category/Alert.
  - If lower level is cleared, next higher level is used.
  - Current destination level shown in alert overview
- Cursor remains at the entry that was last modified

Alert enhancements

New and Updated alerts

- 1217/1218: Added/removed APF dataset (based on SMF90-37
- EM alerts: Use CKRCARLA run-time to show when Extended Monitoring detected the change in status.

Maximum length of alert message string increased, from 450 to approx. 15,000 chars.

Improved messages for unrecognized PARMLIB statements.

Planned

Continuous Delivery

New function 2.5.0

- Support for RACF database in VSAM linear data sets
- Easy lookup of RACF Custom Data (CSDATA segment fields)
- Support for ICSF updates

zSecure 2.5.0: plans for STIG controls

- We're working on migration of the RACF STIG from v6 to v8
  - z/OS RACF STIG v8 comprises approx 220 controls

Interactions & Dependencies

- Hardware Dependencies
  - 64 bit storage model operation requires z12
  - 31 bit storage model operation requires z196

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Sysplex must be at the new z/OS level: No
- List any toleration/coexistence APARs/PTFs: None

Installation & Configuration

- SMP/E install, see installation and customization manual
- PTFs with more support expected to be delivered

Summary

- What works from start is
  - RACF STIG automation
  - New report types INETD, SSHD, SuperSession, IOA gateway, and JES for compliance testing
  - Sensitive Tape data set support (RACF and ACF2)
  - Access Monitor for UNIX
  - Access Monitor for PROGRAM
  - Access Monitor for local RACLIST
  - IP origin for TSO telnet sessions available in SRCIP
- More to come

Appendix

- PDFs with preliminary documentation will be posted
- General information:
  - https://www.ibm.com/security/mainframe-security/zsecure