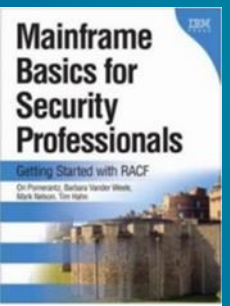
VANGUARD SECURITY & COMPLIANCE 2024

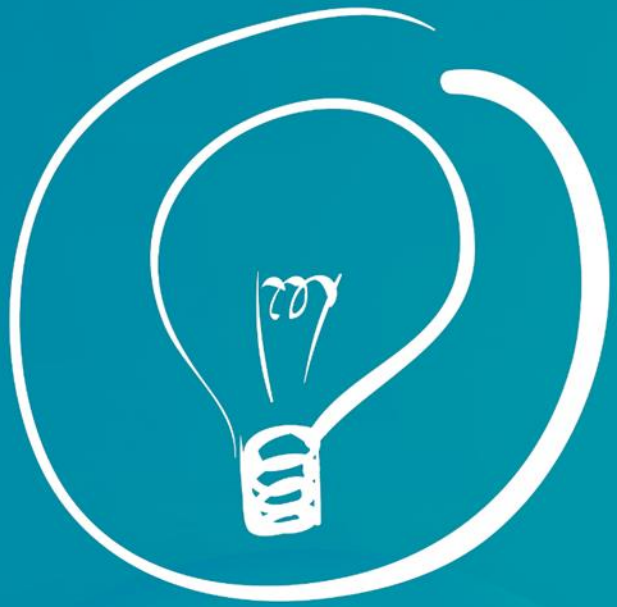
RACF Update

Mark Nelson, CISSP ® ,CSSLP ®,

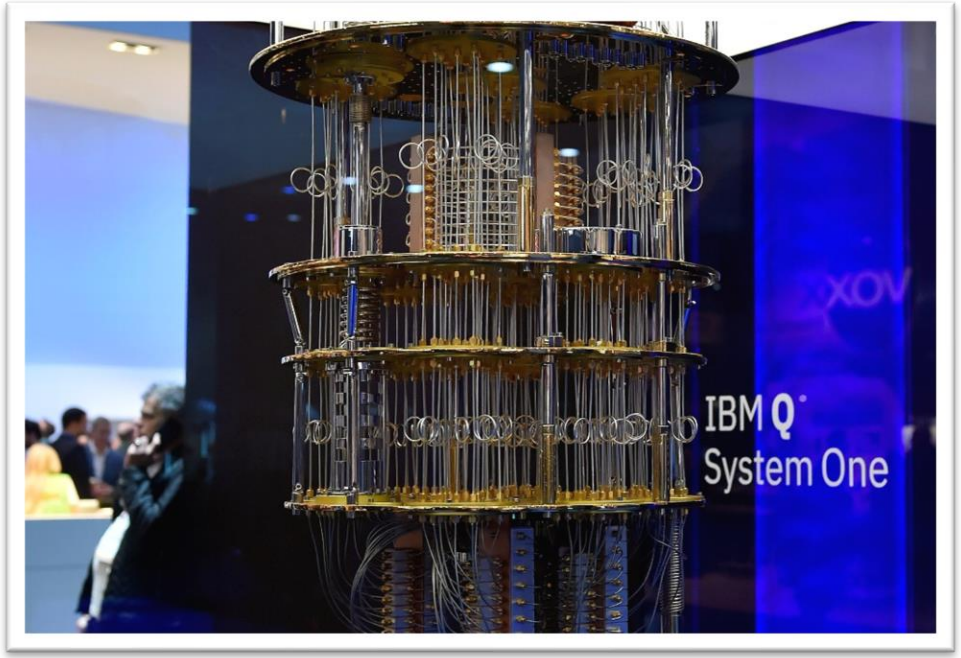
Senior Technical Staff Member

IBM





KNOWLEDGE
is your best defense



IBM Poughkeepsie Lab

RACF Update: What's New Since V2.5?

z/OS® 3.1 Only

- APPLAUDIT Enhancements
- Custom Field Information in ACEE

z/OS 2.5 – Continuous Delivery

- Identity Token Enhancements
- Passphrase Interval
- Support for the IBM Z Security and Compliance Center
- Center for Internet Security (CIS) IBM z/OS V2R5 with RACF Benchmark
- Encrypted RACF VSAM data set as RACF database
- Ability to Disable Additional logon attempts for a RACF-SPECIAL user after exceeding the SETROPTS PASSWORD(REVOKE(nnn)) value
- Sharing RACF data base with RACF on z/VM
- UNMAP and erase on scratch
- KDFAES protection for RVARY Passwords
- Stronger Encryption for Enveloped Passwords/Password Phrases

z/OS Statements Direction

- Validated Boot
- Tape Encryption
- Anomaly Detection, Notification, Quarantine
- Data Set Encryption Simplification

z/OS 3.1 Enhancements

APPLAUDIT

- **RACF now supports the auditing of application logons for all applications instead of just APPC applications**
  - Enabled by SETROPTS APPLAUDIT and successful access logging requested (AUDIT/GAUDIT) on the APPL specified on the REQUEST=VERIFY

- **Logons to z/OS UNIX applications (SESSION=OMVSSRV) can request logging using the new OPTAUDIT class**
  - The existence of “switch” profile APPLAUDIT.FOR.UNIX enables the recording of logons for these applications

- **The RACF Subsystem is required for APPLAUDIT for z/OS UNIX applications**
  - Listens for ENF 62 signals indicating that the OPTAUDIT class has been refreshed

- **SMF 80 “Logoff” records (created by a RACROUTE REQUEST=DELETE) now contain the APPL= name used to create the ACEE even if it was not on the RACROUTE REQUEST=DELETE call.**

ACEE Custom Fields

- **Custom fields are fields within the RACF database that an installation can customize to store security information in RACF profiles for Users, Groups, Data Sets and General Resources (starting in V2.4)**

- **Custom Fields in the ACEE:** Starting with z/OS 3.1 you can direct RACF to place custom field information from a user profile into the ACEE for retrieval by the R_GetInfo (IRRSGI00) callable service.

- **New ACEE(YES|NO) on CFIELD definition:**

```
–RDEFINE CFIELD USER.CSDATA.EMPSER   UACC(NONE) CFDEF(TYPE(NUM)
FIRST(NUMERIC) OTHER(NUMERIC)MAXLENGTH(8) MINVALUE(100000)
MAXVALUE(99999999) ACEE(YES)
HELP('SERIAL NUMBER, 6 - 8 DIGITS')LISTHEAD('EMPLOYEE SERIAL=‘))
```

ACEE Custom Fields – R_GetInfo

- **R_GetInfo -** New Function Code 3 **-** Get CSDATA from ACEE
- **Authorization:**
  - FLAC – Field Level Access Checking – Granted via profiles in FIELD class
    - Determines which fields (including custom fields) the caller can view or modify
  - Authorized callers can optionally skip FLAC
  - Authorized callers can provide an ACEE_ptr to extract CSDATA from.
- **Invocation:**

  CALL IRRSGI00 (

  ...

  Num_parms, - New Value: 16 for function code X'0003'

  ...

  Function_code, - New value: X'0003'- Get CSDATA from ACEE

  Option, - Single / All fields? NOFLAC*? (supervisor state only)

  ...

  Result_entries, - For FC 3 - CSDATA fields return area

  CSDATA_keyword_name, - **New:** Field to retrieve or null for all

  ACEE_ptr) - **New:** ACEE address

Continuous Delivery Enhancements

Identity Token Support (IDT)

Identity Token:

- An Identity Token is used to assert user claims which can be trusted by the consumer of the token.
- RACF use adheres to the JSON Web Token (JWT) IETF specifications: RFC 7519
- Generated/validated with RACROUTE REQUEST=VERIFY based on IDTDATA profiles
- Used to provide a
  - "Stateful" REQUEST=VERIFY service
  - Allow the replaying of proof of authentication

z/OS 3.1 base and 2.4/2.5 with APARs OA63462 (RACF) and OA63463 (SAF)

- Generate/authenticate an IDT from ACEE
- Generate/authenticate an IDT for a protected user

  New IDTPARMs KEYWORD PROTALLOWED (YES | NO): Specifies whether an Ide
  (IDT) validated with this profile can be used to authenticate a protected user.
- Generate an IDT from an ACEE using INITacee

PassPhrase Change Interval

- **z/OS 3.1 and 2.5 APAR OA61951 (RACF, PTF UJ90043)**
  OA61952 (SAF, PTF UJ90042)

- **Password Phrase Interval:**
  - RACF provides a new separate password phrase specific change interval(PHRASEINT) which can be different than the existing password interval and supports values from 0 (not specified) to 65,534 days (179 years)

- **The password phrase interval can be set at:**
  - The system level with the SETROPTS command
  - The user level with the PASSWORD/PHRASE command.
    - Unlike a password interval, users cannot set their own password phrase interval

PassPhrase Change Interval…

- **The RACF_PASSWORD_CONTROL health check is updated to raise an exception if the installation is using phrase intervals and the maximum days a password phrase is valid is greater than 365. (z/OS 3.1 only)**

- **SMF Record / RACF SMF Unload (IRRADU00) Record Updates**
  - SMF type 80 record for SETROPTS and PASSWORD/PHRASE commands contain the PHRASEINT information
  - SMF type 81 initialization record contains the password phrase interval

- **RRSF Considerations**
  - PASSWORD PHRASEINT(nnn)/ NOPHRASEINT and SETROPTS PHRASEINT(nnn) will not work on a remote node without this support
  - Uplevel systems will see a message if a downlevel system does not have this support
    - `IRRI007I ATTENTION: LOCAL NODE localnode HAS A DIFFERENT SETROPTS PASSWORD(option) THAN PARTNER NODE partnernode.`

RACF SMF 1154/83 Records

- **RACF creates SMF1154 subtype 83 records in support of the IBM Z Security and Compliance Center (zSCC)**

- **Applications can request that participating z/OS applications cut security related SMF records:**
  - Request comes from a zOSMF REST API (such the IBM Z Security and Compliance Center)
  - RACF will create an SMF 1154 Subtype 83 record which contains compliance information.

- **The RACF 1154 Subtype 83 SMF record is documented in RACF Macros and Interfaces**

RACF SMF 1154/83 Record Contents

SMF Record Section	Contents
RACFSMRY: RACF Summary information (SETROPTS, etc.)	RACF ACTIVE/INACTIVE, definition of IBMUSER, SAUDIT,CMDVIOL, OPERAUDIT, MIXEDCASE, password rules, password exit status, password interval, password history, maximum failed password attempts, user inactivity, default RVARY passwords, password encryption algorithm, CATDSNS, ERASE, ACEECHK, BATCHALLRACF…
RACFCRIT: Critical RACF general resources	UACC, ID(*), WARNING AUDIT, GAUDIT information for critical RACF general resources (e.g. BPX.SUPERUSER)
RACFAPFL: Critical data set	UACC, ID(*), WARNING information for APF, RACF, LINKLIST, RRSF and PARMLIB data sets.
RACFACTL: Programs defined in the RACF Authorized Callers Table (Non-recommended options)	Module name and module location (LPA, not in LPA).

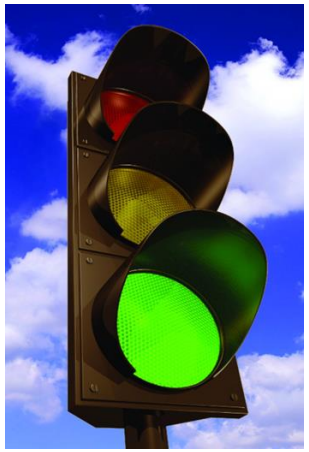
Encrypted VSAM Data Set Support in RACF

Encrypted RACF DB

- 3.1 base and V2.5 APAR OA62267 allows an encrypted DB and removes several restrictions

Base z/OS V2.5 restrictions, removed with APAR OA62267

- ~~Non-shared (may be on a device marked as shared)~~
- ~~Non-split RACF data set~~
- ~~Non-SMS managed (which means not encrypted)~~
- ~~Not in RACF sysplex communications mode or RACF data sharing mode~~
- All systems sharing the RACF DB must be at z/OS V2.5
- Not defined in MSTRJCL
- Running in application identity mapping (AIM stage 3)
- That is free from internal errors (IRRUT200 and IRRDBU00 run without error)



RACF APAR OA62267:

- PTF UJ08531, available 8 June 2022

Changes with a RACF VSAM Data Set

- **No change to the RACF programming interfaces:**
  - RACROUTE, ICHEINTY, RACF Callable Services, IRRXUTIL, RACF commands

- **No changes to the RACF serialization structure:**
  - Major names of SYSZRACF, SYSZRACn
  - But there is a new SYSVSAM ENQ.

- **Applications which read the RACF data base directly *may* have actions to take to support VSAM**
  - Disclosed at the vendor disclosure meeting in April 2020 and September 2020 and through ICN 1775 (18 August, 2020)

SPECIAL User Password Revocation Prompt

- **SETROPTS PASSWORD(REVOKE(nnn))**
  - Establishes the maximum number of incorrect authentication attempts before a user is revoked.

- **When an incorrect logon attempt exceeds the REVOKE limit:**
  - Non-SPECIAL users are revoked immediately
  - Users with the SPECIAL attribute get a message sent to the console to ask the operator if the user should be revoked or allowed an additional attempt

- **ICH301I MAXIMUM PASSWORD ATTEMPTS BY SPECIAL USER *userid* [AT TERMINAL *terminalid*.]**
  - **ICH302D REPLY Y TO ALLOW ANOTHER ATTEMPT OR N TO REVOKE USERID *userid*.**
    - Y – Allows the attempt to logon and does not revoke the user
    - N – Revokes the user

Disabling the Excessive Password Prompt

- **With OA63091 (V2.3, V2.4, V2.5) you can disable additional logon attempts for a RACF SPECIAL user once the SETROPTS PASSWORD(REVOKE(nnn)) value has been exceeded**
  - The disablement can be enabled on an application-by-application basis

- **Enabled with the definition of an XFACILIT class discrete profile of the name:**
  - **`IRR.DENY.SPECIAL.USER.ADDITIONAL.PASSWORD.ATTEMPTS.APPL.appl-name`**
  - The appl-name must match the APPL= value on the RACROUTE REQUEST=VERIFY.
  - If no appl-name was specified on the REQUEST=VERIFY, then it defaults to the same derivation method as used in PassTicket application name derivation.
  - This is a profile existence check only. No profile attributes (UACC, access list, etc.) are considered.

What's New with Erase-on-Scratch

- **DFSMSdfp APAR OA61492 introduces UNMAP support for DS8900 solid state drives (SSDs) which have DS8900 firmware release 9.3.2 installed**
  - UNMAP provides *very substantial performance benefits* over traditional EoS.
  - Applies to data sets which have the ERASE indicator specified in the RACF profile or temporary data sets
  - *Does not apply to any data set in any form of Copy Services relationship*

- **UNMAP is enabled by the presence of a FACILITY class profile named STGADMIN.SMS.DADSM.UNMAP.PREFER**
  - If the profile above is present, and the data set is marked for erasure by either the data set profile and/or the SETROPTS ERASE setting and the data set resides on a SSD enabled for EoS, the storage will be UNMAPed instead of ERASEd.
  - Otherwise, traditional erasure (X'00' overwrite) will be performed.
  - For temporary data sets, if the profile above is present and ERASE(ALL) is not in effect, when the data set is deleted its space will be UNMAPed. If the UNMAP is not successful, the data set will not be overwritten with X'00's

What's New with Erase-on-Scratch…

- **APAR Documentation:** https://www.ibm.com/support/pages/apar/OA61492 and subsequent APAR https://www.ibm.com/support/pages/apar/OA63169 .
- **SHARE presentation "Watson and Walker's 2023 zRoadshow", SHARE Atlanta 2023 Proceedings**
- **"Latest on Erase-on-Scratch and SSDs and the UNMAP Function", upcoming article Cheryl Watson's Tuning Letter, 2023, No.1**
- **DFSMS Storage Administration:** https://www-40.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R5sc236860/$file/idas200_v2r5.pdf
- **DFSMS Using Data Sets:** https://www-40.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R5sc236855/$file/idad400_v2r5.pdf
- **Requirement to extend support to data sets engaged in Copy Services relationship**: https://ibm-sys-storage.ideas.ibm.com/ideas/DS80-I-198

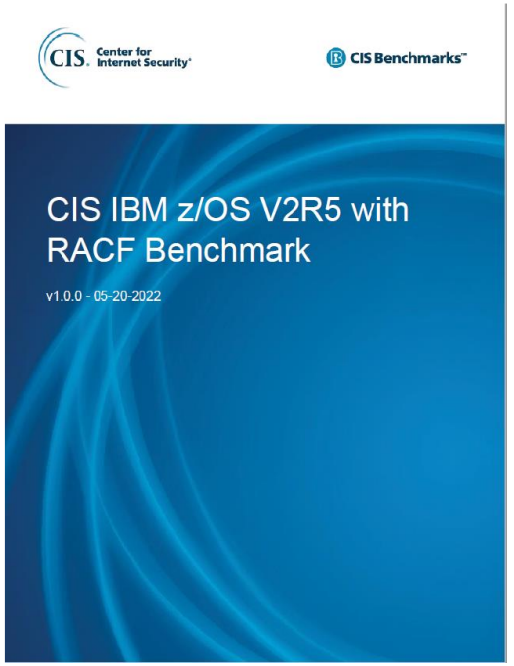
Sharing a z/OS RACF DB with z/VM

- **Starting with z/VM 7.3, RACF z/OS and z/VM will not be able to share the RACF database.**
  - Attempts to IPL z/OS with a z/VM 7.3 RACF database will fail and the operator will be prompted for a different RACF database.
  - This change comes with APAR OA62875.
  - For details, see: https://www.vm.ibm.com/zvm730/announce.html

CIS Benchmark for z/OS 2.5 with RACF

- **The Center for Internet Security, Inc. (CIS®):**
  - Community-driven not-for-profit organization responsible for the CIS Controls® and CIS Benchmarks™, best practices for securing IT systems and data.

- **The z/OS V2R5 with RACF Benchmark:**
  - Contains 219 recommendations across 9 domains
    1. Identification and Authentication
    2. Authorization and Access Control Management
    3. Logging and Auditing
    4. System Resilience
    5. Storage Management
    6. Networking
    7. Cryptography and Encryption
    8. Job Management
    9. UNIX System Services



- https://www.cisecurity.org/benchmark/ibm_z
  - Provide contact information, link e-mailed

AES Support for PKCS#12 Packages

- Previously, an attempt to ADD (import) digital certificates from a PKCS#12 package protected with PBES2 (Password-Based Encryption Scheme 2) failed with

```
IRRD104I The input data set does not contain a valid certificate.
```

  - Now, ADD just works. There are no new externals.
- RACDCERT EXPORT has a new keyword: PBE(AES)
- Introduced with APAR OA65002 (RACF), OA65003 (PKI Services)
- PKI Services provides an option to build the PKCS#12 package with Password Based Encryption Scheme Version 2 (PBES2)
- New keyword PKCS12EncryptAlg in the pkiserv.conf configuration file is

KDFAES protection for RVARY passwords

- OA65905 provides stronger protection of RVARY passwords
- It requires an action to change the passwords using a new KDFAES keyword of the SETROPTS RVARYPW command
- The action should not be performed until all system sharing the RACF database are IPLed with the PTF for OA65905
  - In a sharing environment, the action need only be performed once, from any one of the sharing systems
  - The action can be performed immediately on a non-sharing system
- *The service will be required co-existence for z/OS Next*

KDFAES protection for RVARY passwords…

- Today's SETROPTS LIST output:

```
PASSWORD PROCESSING OPTIONS:
  THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS KDFAES
  PASSWORD CHANGE INTERVAL IS  30 DAYS.
  PASSWORD CHANGE INTERVAL IS IN EFFECT FOR PASSWORD PHRASES.
  PASSWORD MINIMUM CHANGE INTERVAL IS   0 DAYS.
  MIXED CASE PASSWORD SUPPORT IS NOT IN EFFECT
  SPECIAL CHARACTERS ARE ALLOWED.
  NO PASSWORD HISTORY BEING MAINTAINED.
  USERIDS NOT BEING AUTOMATICALLY REVOKED.
  NO PASSWORD EXPIRATION WARNING MESSAGES WILL BE ISSUED.
  NO INSTALLATION PASSWORD SYNTAX RULES ARE PRESENT.
INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.
INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.
```

KDFAES protection for RVARY passwords…

- After IPLing with the service:

```
INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.
  KDFAES PASSWORD CONVERSION IS PENDING. (SEE APAR OA65905)
INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.
  KDFAES PASSWORD CONVERSION IS PENDING. (SEE APAR OA65905)
```

- This is how you can confirm that the service is installed on a given system

KDFAES protection for RVARY passwords…

- When all sharing systems have the service, change your passwords to pick up the new KDFAES protection:

```
SETROPTS RVARYPW(SWITCH(xxxxxxxx) STATUS(yyyyyyyy) KDFAES)
```

- SETROPTS LIST now shows:

```
INSTALLATION DEFINED RVARY SWITCH KDFAES PASSWORD IS IN EFFECT.
INSTALLATION DEFINED RVARY STATUS KDFAES PASSWORD IS IN EFFECT.
```

- This is how you know that you've completed the action

KDFAES protection for RVARY passwords…

- You have entered ‘KDFAES mode’ and you never need to specify the KDFAES keyword again when changing RVARY passwords
- This works even if changing the password to the default (future changes to an installation-defined value will use KDFAES)
  - We recommend you don’t run with the default
- You can ‘change’ the passwords to their existing values
  - We recommend you take the opportunity to establish a new value

Stronger Encryption for Enveloped Passwords/Password Phrases

- OA66067 (z/OS 3.1) provides stronger, quantum-safe protection of RACF passwords and password phrases

- The RACF password enveloping symmetric encryption and signing algorithms are configured with the APPLDATA() keyword in profiles in the RACFEVNT class:
  - Password Envelope Policy for passwords:

    ```
    RDEFINE RACFEVNT PASSWORD.ENVELOPE APPLDATA('MD5/STRONG')
    ```

  - Password Envelope Policy for password phrase:

    ```
    RDEFINE RACFEVNT PASSPHRASE.ENVELOPE APPLDATA('MD5/STRONG')
    ```

SDSF for z/OS 3.1

- **SDSF for z/OS 3.1 contains five new RACF display functions:**

```
 Display  Filter  View  Print  Options  Search  Help
------------------------------------------------------------------------------
SDSF MENU 3.1    LOCAL     RACFR31                      LINE 64-78 (99)
COMMAND INPUT ===>                                        SCROLL ===> HALF
PREFIX=*  DEST=(ALL)  OWNER=*  SORT=NAME/A  SYSNAME=
NP    NAME     Description               Group     Status
      PUN      Punches                   JES
      RAC      RACF classes              Security
      RACG     RACF groups               Security
      RACO     RACF options              Security
      RACP     RACF profiles             Security
      RACU     RACF users                Security
      RDR      Readers                   JES
      REPC     WLM report classes        WLM
      RES      WLM resources             WLM
      RGRP     WLM resource groups       WLM
      RM       Resource monitor          JES
      RMA      Resource monitor alerts   JES
      SE       Scheduling environments   WLM
      SMFD     SMF data sets             System
      SMFO     SMF options               System
PF 1=HELP      2=SPLIT     3=END       4=RETURN    5=RFIND     6=BOOK
PF 7=UP        8=DOWN      9=SWAP     10=LEFT     11=RIGHT    12=RETRIEVE
```

Statements of Direction

Recent Statements of Direction - 1

- **Validated Boot for z/OS - *Delivered August, 2023***

  IBM plans to deliver a solution providing Validated Boot, also known as **Secure Boot or Boot Integrity Validation**, capability for z/OS IPLs and is designed to meet the requirements for achieving the National Information Assurance Partnership (**NIAP**) OS Protection Profile 4.3 Certification.

Recent Statements of Direction - 2

- **The fine print**
  - *Statements by IBM regarding its plans, directions, and intent are subject to change or withdrawal without notice at the sole discretion of IBM. Information regarding potential future products is intended to outline general product direction and should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for IBM products remain at the sole discretion of IBM.*

Recent Statements of Direction - 2

- **Encryption of tape data sets**

  IBM intends to **enhance pervasive encryption** to perform **encryption within the access methods for tape data sets**. It is expected to be **transparent to the application** program **unless it uses EXCP**. This new data set encryption support is intended to be independent of any encryption that occurs in the tape subsystem.

  (*) See the disclaimer.

Recent Statements of Direction - 3

- **Anomaly Detection, Notification, Quarantine**

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

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

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

(*) See the disclaimer.

Recent Statements of Direction - 4

- **Data Set Encryption Simplification**

IBM also plans to provide a software solution that **simplifies z/OS data set encryption, encrypting and re-encrypting data** at scale **for both key rotation and initial encryption,** and leveraging analytics to minimize application downtime. This is designed to simplify adherence to expanded compliance regulations such as PCI DSS v4.0.

https://www.ibm.com/docs/en/announcements/statement-direction-security-zos

(*) See the disclaimer.

Shameless Plugs

Shameless Plug #1: Podcasts

- **IBM Developer Works: Mainframe, Performance, Topics**
  - Hosts: Marna Walle, Martin Packer
  - https://anchor.fm/marna-walle
  - …as well as several Android podcast platforms

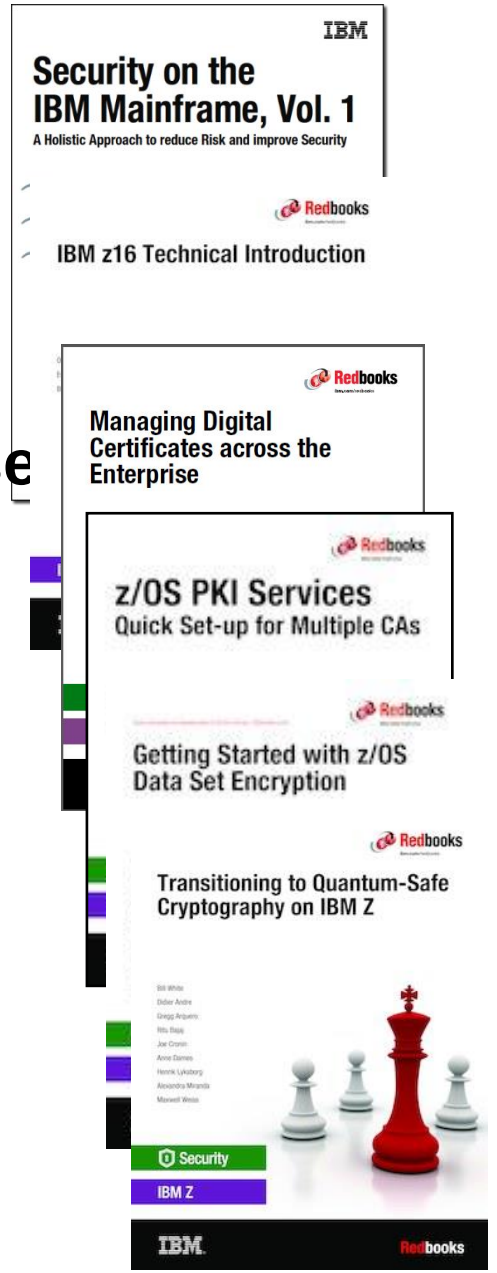
- **Terminal Talk**
  - Hosts: Frank DeGillio, Jeff Bisti
  - Available on many podcast platforms

Shameless Plug #2: zPet Test Community

- **IBM Z Platform Evaluation Test Community and Blog**
  - Real-world experiences configuring and operating the latest IBM Z technologies
  - http://ibm.biz/zPETBlog

Shameless Plug #3: Redbooks

- **Security on the IBM Mainframe**
- **IBM z16 Technical Introduction**
- **Managing Digital Certificates across the Enterprise**
- **z/OS PKI Services: Quick Set-up for Multiple CAs**
- **Getting Started with z/OS Data Set Encryption**
- **Transitioning to Quantum-Safe Cryptography on IBM Z**



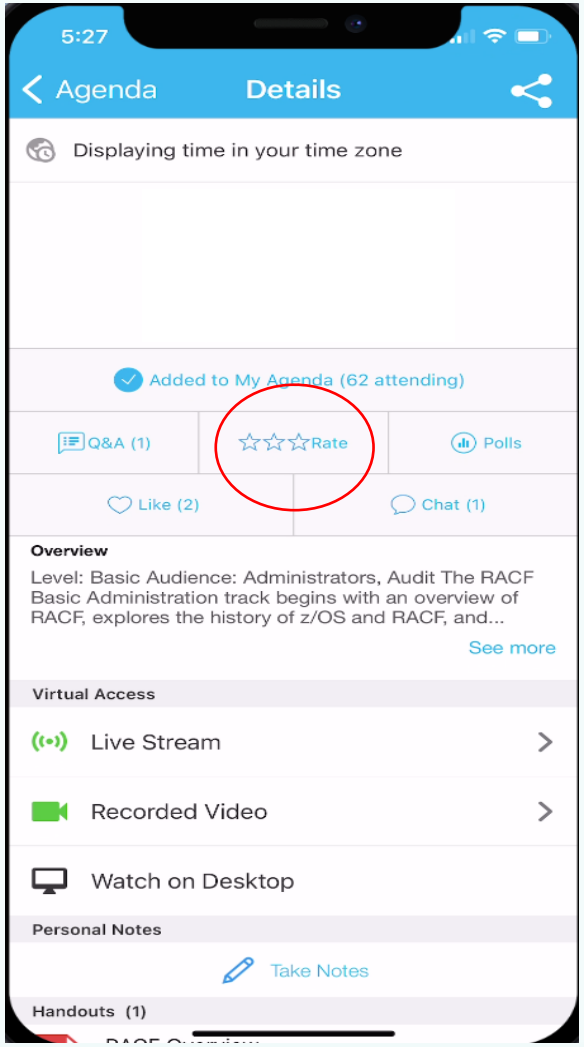
https://www.redbooks.ibm.com/

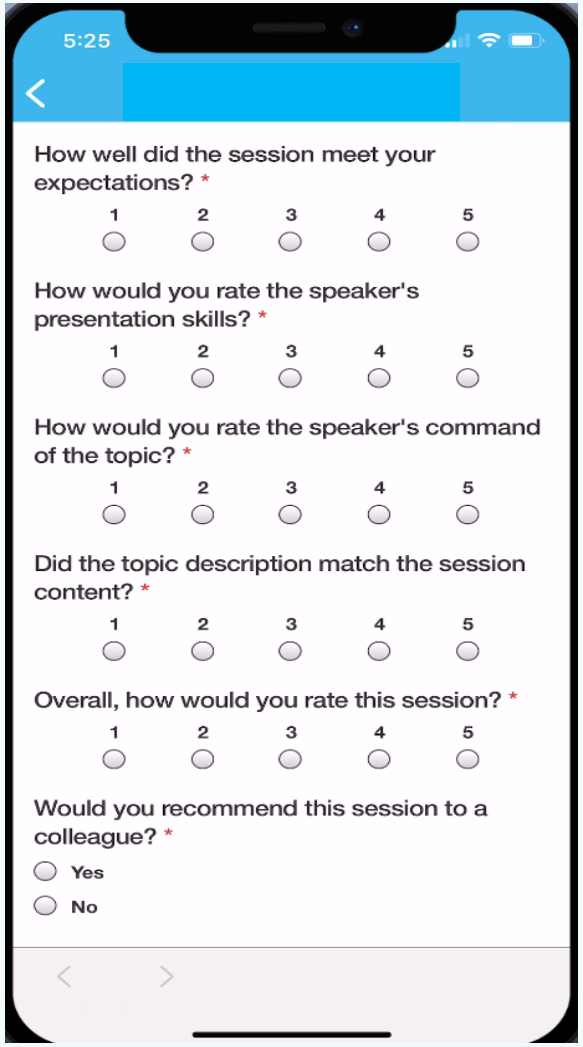
Session Evaluation

VANGUARD SECURITY & COMPLIANCE

Be sure to rate your experience using the VSC2024 app.

Your opinion helps us bring you the best experience.
Please let us know your thoughts.





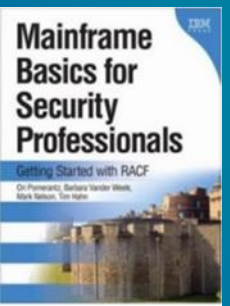
VANGUARD SECURITY & COMPLIANCE 2024

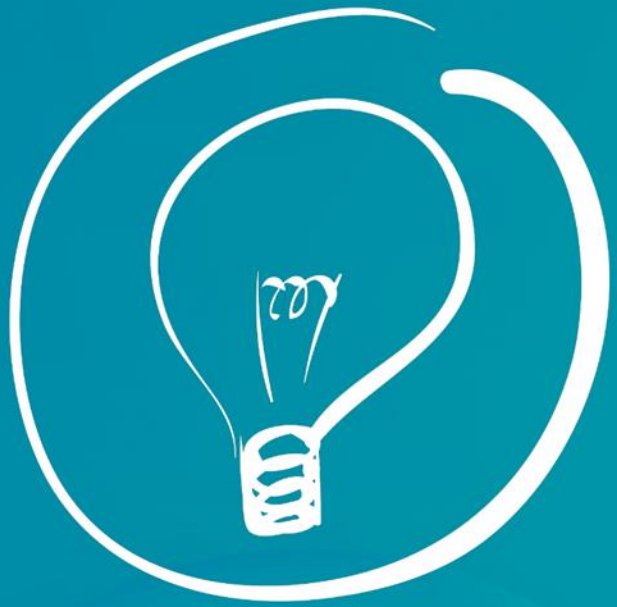
RACF Update

Mark Nelson, CISSP ® ,CSSLP ®,

Senior Technical Staff Member

IBM





KNOWLEDGE
is your best defense