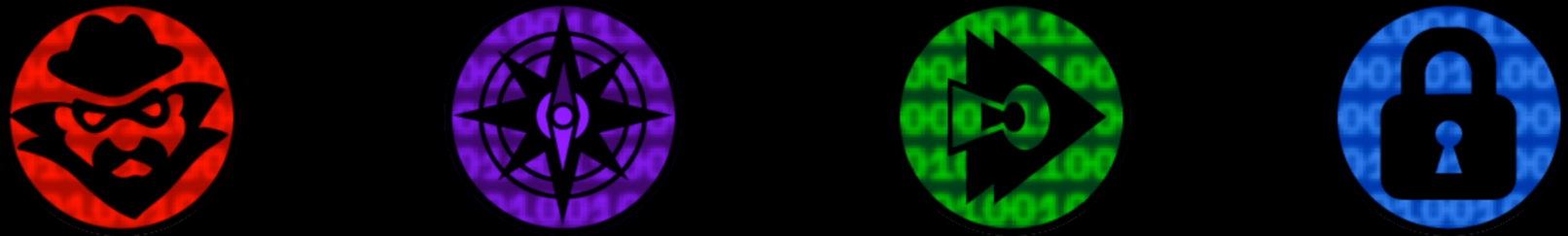
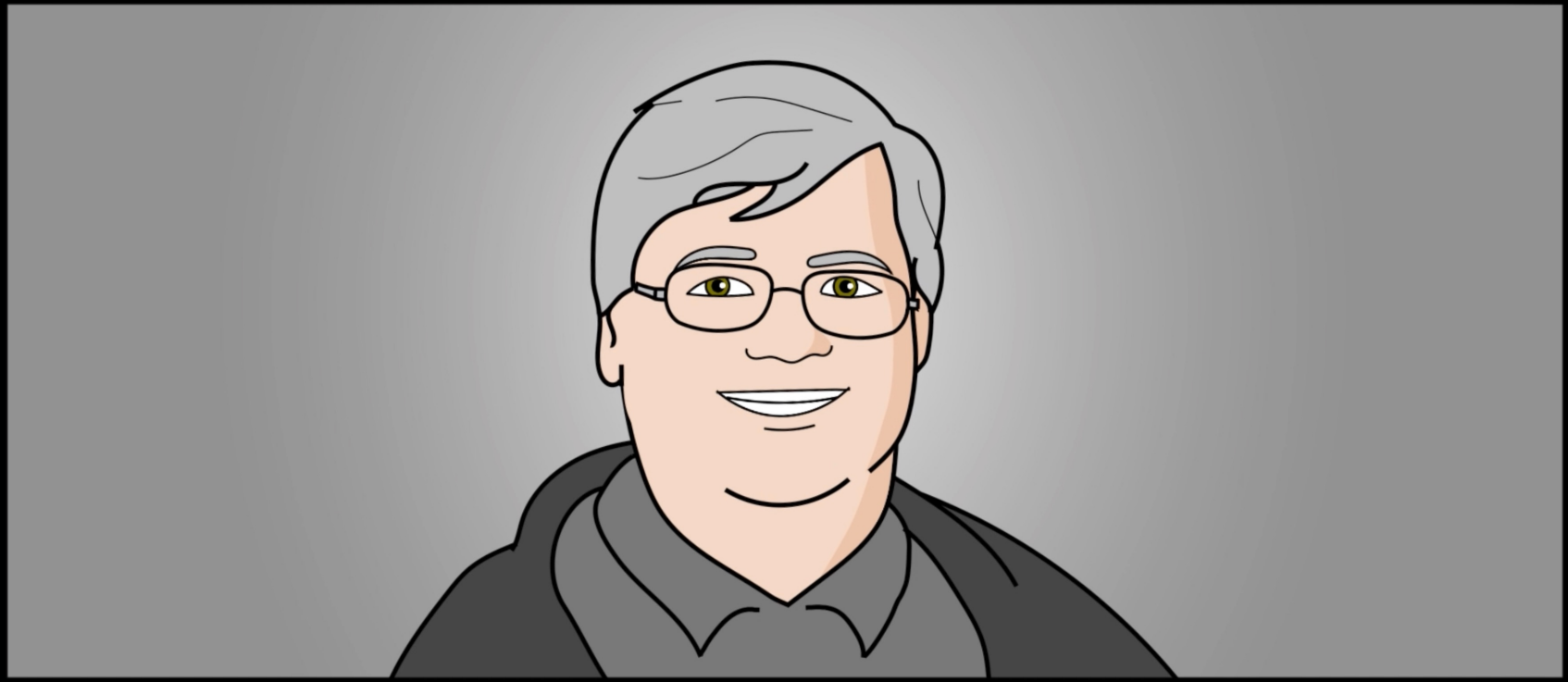
Enterprise Knights Insights



“Zero Trust in RACF”

Mark Nelson, RACF SME

Enterprise Knights Insights

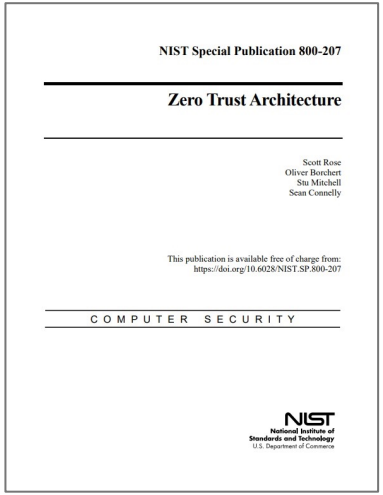


Mark Nelson, RACF SME

Zero Trust: Let's Go to the Source

NIST Special Publication 800-207 is considered by many to the foundation for Zero Trust discussions

- It defines the **Zero Trust (ZT) model** and its principles and **the Zero Trust Architecture (ZTA)** that is built on the Zero Trust model. "**ZT is not a single architecture but a set of guiding principles** for workflow, system design and operations that can be used to improve the security posture of any classification or sensitivity level" (p.1)
- "**Transitioning to ZTA is a journey** concerning how an organization evaluates risk in its mission and cannot simply be accomplished with a wholesale replacement of technology (p.1)
- "Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, **least privilege** per-request access decisions in information systems and services in the face of a network viewed as compromise" (p.4).
- "**The enterprise monitors and measures the integrity and security posture** of all owned and associated assets." (p. 6)


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Zero Trust and the “Fundamental Principles “ of Security

Zero Trust leverages all our Generally Accepted Principles of Security

- **Least Privilege** ✓✓✓
  - Each system component or process should have the least authority necessary to perform its duties
- **Separation of Duties** ✓
  - At least two individuals are responsible for the completion of a task
- **Defense in Depth** ✓✓✓
  - The practice of arranging defensive lines or fortifications so that they can defend each other, especially in case of an enemy incursion
- **Fail Securely** ✓✓
  - A failure will cause no harm or at least a minimum of harm to other devices or danger to personnel, and doesn't cause the system to be insecure
- **Establish Secure Defaults** ✓✓✓
  - The default configuration settings are the most secure settings possible, which are not necessarily the most user-friendly settings
- **Minimize the Attack Surface** ✓✓
  - “A chain is only as strong as its weakest link”
  - Keep security simple

Monitoring with RACF Health Checks

“The enterprise monitors and measures the integrity and security posture of all owned and associated assets.” (p. 6)

RACF provides 27 health checks in the IBM Health Checker for z/OS that examine:

- **The protection of key system data sets:**
  - RACF_SENSITIVE_RESOURCES
  - RACF_RRSF_RESOURCES
- **The active status of these classes:**
  - TEMPDSN, TAPEVOL, TSOAUTH, JESSPOOL, OPERCMDS, CSFSERV, CSFKEYS, JESJOBS, FACILITY
- **RACF system configuration options:**
  - PROTECTALL, BATCHALLRACF, erase-on-scratch, password encryption algorithm, application identity mapping (AIM) stage, audit controls
- **RACF operational configuration**
  - RACF address space activation, use of ICSF for PassTicket keys
- **RACF installation-defined health checks that monitor resources that *you* define**

RACF_SENSITIVE_RESOURCES Health Check

- **The RACF_SENSITIVE_RESOURCES health check examines the profile protecting key system data sets to validate that excessive access is not granted to all users**

- **The check examines the universal access (UACC), ID(*) access list entry and the WARNING profile attributes of these data sets:**
  - Authorized program facility (APF)
  - RACF data base
  - PARMLIB
  - Link List
  - System REXX
  - ICSF

How do I get to the RACF Health Checks?

- **The easiest way to get to your RACF Health checks is through SDSF***

```
 Display  Filter  View  Print  Options  Search  Help
-------------------------------------------------------------------------------
SDSF MENU V2R5M0    LOCAL     RACFR25                  LINE 1-15 (74)
COMMAND INPUT ===>                                      SCROLL ===> DATA
PREFIX=*  DEST=(ALL)  OWNER=*  SORT=NAME/A  SYSNAME=
NP   NAME     Description              Group    Status
     AD       Address space diagnostic Jobs
     APF      APF data sets            System
     AS       Address space memory     Jobs
     BPXO     OMVS options             OMVS
     CFC      CF connections           Sysplex
     CFD      Couple data sets         Sysplex
     CFS      CF structures            Sysplex
s    CK       Health checker           System
     CS       Common storage subpools  Memory
     CSR      Common storage remaining Memory
     DA       Active users             Jobs
     DEV      Device activity          Devices
     DYNX     Dynamic exits            System
     EMCS     Extended consoles        Sysplex
     ENC      Enclaves                 WLM
```

*** or equivalent product**

How do I get to the RACF Health Checks...

- **... then go to the RACF checks**

```
  Display  Filter  View  Print  Options  Search  Help
-------------------------------------------------------------------------------
SDSF HEALTH CHECKS  RACFR25                          LINE 1-15 (169)
COMMAND INPUT ===> find racf                            SCROLL ===> DATA
PREFIX=*  DEST=(ALL)  OWNER=*  SORT=Locale/A  SYSNAME=  FILTERS=1
NP   NAME                              CheckOwner       State              Statu
     ALLOC_ALLC_OFFLN_POLICY           IBMALLOC         ACTIVE(ENABLED)    SUCCE
     ALLOC_SMSHONOR_STATE              IBMALLOC         ACTIVE(ENABLED)    SUCCE
     ALLOC_SPEC_WAIT_POLICY            IBMALLOC         ACTIVE(ENABLED)    SUCCE
     ALLOC_TAPELIB_PREF                IBMALLOC         ACTIVE(DISABLED)   ENV N
     ALLOC_TIOT_SIZE                   IBMALLOC         ACTIVE(ENABLED)    SUCCE
     ASM_LOCAL_SLOT_USAGE              IBMASM           ACTIVE(ENABLED)    EXCEP
     ASM_NUMBER_LOCAL_DATASETS         IBMASM           ACTIVE(ENABLED)    SUCCE
     ASM_PAGE_ADD                      IBMASM           ACTIVE(ENABLED)    SUCCE
     ASM_PLPA_COMMON_SIZE              IBMASM           ACTIVE(ENABLED)    EXCEP
     ASM_PLPA_COMMON_USAGE             IBMASM           ACTIVE(ENABLED)    EXCEP
     CATALOG_ATTRIBUTE_CHECK           IBMCATALOG       ACTIVE(ENABLED)    EXCEP
     CATALOG_IMBED_REPLICATE           IBMCATALOG       ACTIVE(ENABLED)    EXCEP
     CATALOG_RNLS                      IBMCATALOG       ACTIVE(ENABLED)    SUCCE
     CNZ_AMRF_EVENTUAL_ACTION_MSGS     IBMCNZ           ACTIVE(ENABLED)    SUCCE
     CNZ_CONSOLE_MASTERAUTH_CMDSYS     IBMCNZ           ACTIVE(ENABLED)    SUCCE
```

How do I get to the RACF Health Checks...

- **... then go to the RACF checks**

```
Display  Filter  View  Print  Options  Search  Help
-------------------------------------------------------------------------------
SDSF HEALTH CHECKS  RACFR25                              CHARS 'RACF' FOUND
COMMAND INPUT ===>                                         SCROLL ===> DATA
PREFIX=*  DEST=(ALL)  OWNER=*  SORT=Locale/A  SYSNAME=  FILTERS=1
NP   NAME                              CheckOwner       State               Statu
     RACF_AIM_STAGE                    IBMRACF          ACTIVE(ENABLED)     SUCCE
     RACF_AUDIT_CONTROLS               IBMRACF          ACTIVE(ENABLED)     EXCEP
     RACF_BATCHALLRACF                 IBMRACF          ACTIVE(ENABLED)     SUCCE
     RACF_CERTIFICATE_EXPIRATION       IBMRACF          ACTIVE(ENABLED)     EXCEP
     RACF_CSFKEYS_ACTIVE               IBMRACF          ACTIVE(ENABLED)     SUCCE
     RACF_CSFSERV_ACTIVE               IBMRACF          ACTIVE(ENABLED)     SUCCE
     RACF_ENCRYPTION_ALGORITHM         IBMRACF          ACTIVE(ENABLED)     SUCCE
     RACF_ERASE_ON_SCRATCH             IBMRACF          ACTIVE(ENABLED)     SUCCE
     RACF_FACILITY_ACTIVE              IBMRACF          ACTIVE(ENABLED)     SUCCE
     RACF_GRS_RNL                      IBMRACF          ACTIVE(DISABLED)    ENV N
     RACF_IBMUSER_REVOKED              IBMRACF          ACTIVE(ENABLED)     EXCEP
     RACF_ICHAUTAB_NONLPA              IBMRACF          ACTIVE(ENABLED)     SUCCE
     RACF_JESJOBS_ACTIVE               IBMRACF          ACTIVE(ENABLED)     SUCCE
     RACF_JESSPOOL_ACTIVE              IBMRACF          ACTIVE(ENABLED)     SUCCE
     RACF_OPERCMDS_ACTIVE              IBMRACF          ACTIVE(ENABLED)     SUCCE
```

How do I get to the RACF Health Checks...

- **... and scroll down and select the RACF_SENSITIVE_RESOURCES check**

```
 Display  Filter  View  Print  Options  Search  Help
-------------------------------------------------------------------------------
SDSF HEALTH CHECKS  RACFR25                              LINE 73-87 (169)
COMMAND INPUT ===>                                          SCROLL ===> DATA
PREFIX=*  DEST=(ALL)  OWNER=*  SORT=Locale/A  SYSNAME=  FILTERS=1
NP   NAME                            CheckOwner       State              Statu
     RACF_OPERCMDS_ACTIVE            IBMRACF          ACTIVE(ENABLED)    SUCCE
     RACF_PASSWORD_CONTROLS          IBMRACF          ACTIVE(ENABLED)    EXCEP
     RACF_PROTECTALL_FAIL            IBMRACF          ACTIVE(ENABLED)    EXCEP
     RACF_RRSF_RESOURCES             IBMRACF          ACTIVE(ENABLED)    SUCCE
s    RACF_SENSITIVE_RESOURCES        IBMRACF          ACTIVE(ENABLED)    EXCEP
     RACF_SYSPLEX_COMMUNICATION      IBMRACF          ACTIVE(ENABLED)    EXCEP
     RACF_TAPEVOL_ACTIVE             IBMRACF          ACTIVE(ENABLED)    EXCEP
     RACF_TEMPDSN_ACTIVE             IBMRACF          ACTIVE(ENABLED)    EXCEP
     RACF_TSOAUTH_ACTIVE             IBMRACF          ACTIVE(ENABLED)    SUCCE
     RACF_UNIX_ID                    IBMRACF          ACTIVE(ENABLED)    SUCCE
     RACF_UNIXPRIV_ACTIVE            IBMRACF          ACTIVE(ENABLED)    EXCEP
     RCF_PCCA_ABOVE_16M              IBMRCF           ACTIVE(ENABLED)    SUCCE
     RSM_AFQ                         IBMRSM           ACTIVE(ENABLED)    SUCCE
     RSM_HVCOMMON                    IBMRSM           ACTIVE(ENABLED)    SUCCE
     RSM_HVSHARE                     IBMRSM           ACTIVE(ENABLED)    SUCCE
```

Check Output

- **Check output: Basic Check Information**

```
Display  Filter  View  Print  Options  Search  Help
 ------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY RACF_SENSITIVE_RESOURCES      LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                            SCROLL ===> DATA
******************************** TOP OF DATA *********************************
CHECK(IBMRACF,RACF_SENSITIVE_RESOURCES)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 01/21/2022 13:33:52.327015
CHECK DATE: 20120106  CHECK SEVERITY: HIGH

                           APF Dataset Report

S Data Set Name                            Vol    UACC Warn ID*  User
- ----------------------------------------- ------ ---- ---- ---- ----
E ASM.SASMMOD1                             ZDR25B Altr No   ****
V ATC.V2R1M4.AUTHLIB                       DRVPSL
V CBC.SCBCCMP                              ZDR25B
  CBC.SCCNCMP                              ZDR25B Read No   ****
  CBC.SCLBDLL                              ZDR25B Read No   ****
  CBC.SCLBDLL2                             ZDR25B Read No   ****
  CEE.SCEERUN                              ZDR25B Read No   ****
```

Basic Check information includes:

- Check owner
- Check name
- Scope of the check
- System name
- Start time
- Definition date of the check
- Check severity

Check Output...

- **Check output: Section Header**

```
Display  Filter  View  Print  Options  Search  Help
 ------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY RACF_SENSITIVE_RESOURCES      LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                            SCROLL ===> DATA
******************************** TOP OF DATA ********************************
CHECK(IBMRACF,RACF_SENSITIVE_RESOURCES)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 01/21/2022 13:33:52.327015
CHECK DATE: 20120106  CHECK SEVERITY: HIGH

                          APF Dataset Report

S Data Set Name                           Vol    UACC Warn ID*  User
- ---------------------------------------- ------ ---- ---- ---- ----
E ASM.SASMMOD1                            ZDR25B Altr No   ****
V ATC.V2R1M4.AUTHLIB                      DRVPSL
V CBC.SCBCCMP                             ZDR25B
  CBC.SCCNCMP                             ZDR25B Read No   ****
  CBC.SCLBDLL                             ZDR25B Read No   ****
  CBC.SCLBDLL2                            ZDR25B Read No   ****
  CEE.SCEERUN                             ZDR25B Read No   ****
```

The section headers are:

- APF Dataset Report
- RACF Dataset Report
- PARMLIB Dataset Report
- Current Link List Dataset Report
- System Rexx Dataset Report
- ICSF Dataset Report
- Sensitive General Resources Report
- ICHAUTAB Report

Check Output...

- **Check output: S (“status”) Column**

```
Display  Filter  View  Print  Options  Search  Help
 ------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY RACF_SENSITIVE_RESOURCES      LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                           SCROLL ===> DATA
******************************** TOP OF DATA ********************************
CHECK(IBMRACF,RACF_SENSITIVE_RESOURCES)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 01/21/2022 13:33:52.327015
CHECK DATE: 20120106  CHECK SEVERITY: HIGH

                          APF Dataset Report

S Data Set Name                           Vol    UACC Warn ID*  User
- ---------------------------------------- ------ ---- ---- ---- ----
E ASM.SASMMOD1                            ZDR25B Altr No   ****
V ATC.V2R1M4.AUTHLIB                      DRVPSL
V CBC.SCBCCMP                             ZDR25B
  CBC.SCCNCMP                             ZDR25B Read No   ****
  CBC.SCLBDLL                             ZDR25B Read No   ****
  CBC.SCLBDLL2                            ZDR25B Read No   ****
  CEE.SCEERUN                             ZDR25B Read No   ****
```

The status values are:

- <blank>: No exception
- ‘E’: Exception
- ‘V’: Not on volume
- ‘M’: Migrated

Check Output...

- **Check output: Data Set Name Column**

```
Display  Filter  View  Print  Options  Search  Help
 ------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY RACF_SENSITIVE_RESOURCES      LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                           SCROLL ===> DATA
******************************** TOP OF DATA ********************************
CHECK(IBMRACF,RACF_SENSITIVE_RESOURCES)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 01/21/2022 13:33:52.327015
CHECK DATE: 20120106  CHECK SEVERITY: HIGH

                          APF Dataset Report

S Data Set Name                          Vol    UACC Warn ID*  User
- ---------------------------------------- ------ ---- ---- ---- ----
E ASM.SASMMOD1                           ZDR25B Altr No   ****
V ATC.V2R1M4.AUTHLIB                     DRVPSL
V CBC.SCBCCMP                            ZDR25B
  CBC.SCCNCMP                            ZDR25B Read No   ****
  CBC.SCLBDLL                            ZDR25B Read No   ****
  CBC.SCLBDLL2                           ZDR25B Read No   ****
  CEE.SCEERUN                            ZDR25B Read No   ****
```

The data set name, as returned from a system service like CSVAPF

Check Output...

- **Check output: Vol (“Volume Name”) Column**

```
Display  Filter  View  Print  Options  Search  Help
 ------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY RACF_SENSITIVE_RESOURCES      LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                            SCROLL ===> DATA
******************************** TOP OF DATA *********************************
CHECK(IBMRACF,RACF_SENSITIVE_RESOURCES)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 01/21/2022 13:33:52.327015
CHECK DATE: 20120106  CHECK SEVERITY: HIGH

                          APF Dataset Report

S Data Set Name                           Vol    UACC Warn ID*  User
- ---------------------------------------- ------ ---- ---- ---- ----
E ASM.SASMMOD1                            ZDR25B Altr No   ****
V ATC.V2R1M4.AUTHLIB                      DRVPSL
V CBC.SCBCCMP                             ZDR25B
  CBC.SCCNCMP                             ZDR25B Read No   ****
  CBC.SCLBDLL                             ZDR25B Read No   ****
  CBC.SCLBDLL2                            ZDR25B Read No   ****
  CEE.SCEERUN                             ZDR25B Read No   ****
```

The volume name, usually returned from the service returning the dataset name. If no volume is returned, the check calls catalog services to get the volume name

Check Output...

- **Check output: UACC (“Universal Access”) Column**

```
Display  Filter  View  Print  Options  Search  Help
 ------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY RACF_SENSITIVE_RESOURCES      LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                            SCROLL ===> DATA
******************************** TOP OF DATA ********************************
CHECK(IBMRACF,RACF_SENSITIVE_RESOURCES)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 01/21/2022 13:33:52.327015
CHECK DATE: 20120106  CHECK SEVERITY: HIGH

                          APF Dataset Report

S Data Set Name                            Vol    UACC Warn ID*  User
- ----------------------------------------- ------ ---- ---- ---- ----
E ASM.SASMMOD1                             ZDR25B Altr No   ****
V ATC.V2R1M4.AUTHLIB                       DRVPSL
V CBC.SCBCCMP                              ZDR25B
  CBC.SCCNCMP                              ZDR25B Read No   ****
  CBC.SCLBDLL                              ZDR25B Read No   ****
  CBC.SCLBDLL2                             ZDR25B Read No   ****
  CEE.SCEERUN                              ZDR25B Read No   ****
```

The UACC column shows the universal access from the profile covering the named data set. If no UACC is shown, it means that there was no profile covering the named data set. In this case, the SETROPTS PROTECTALL setting determines if there is an exception. PROTECTALL(FAIL) is needed to prevent the exception.

Check Output...

- **Check output: Warn (“Warning”) Column**

```
Display  Filter  View  Print  Options  Search  Help
 ------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY RACF_SENSITIVE_RESOURCES      LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                           SCROLL ===> DATA
******************************** TOP OF DATA ********************************
CHECK(IBMRACF,RACF_SENSITIVE_RESOURCES)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 01/21/2022 13:33:52.327015
CHECK DATE: 20120106  CHECK SEVERITY: HIGH

                          APF Dataset Report

S Data Set Name                            Vol    UACC Warn ID*  User
- ----------------------------------------- ------ ---- ---- ---- ----
E ASM.SASMMOD1                             ZDR25B Altr No   ****
V ATC.V2R1M4.AUTHLIB                       DRVPSL
V CBC.SCBCCMP                              ZDR25B
  CBC.SCCNCMP                              ZDR25B Read No   ****
  CBC.SCLBDLL                              ZDR25B Read No   ****
  CBC.SCLBDLL2                             ZDR25B Read No   ****
  CEE.SCEERUN                              ZDR25B Read No   ****
```

The Warn column shows the WARNING attribute of the profile covering the data set.

- Valid values are Yes an No
- If there is no value specified, then there was no profile covering the data set and the system SETROPTS PROTECTALL value the WARNING attribute
- WARNING allows all levels of access to the data set

Check Output...

- **Check output: ID* Column**

```
Display  Filter  View  Print  Options  Search  Help
 ------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY RACF_SENSITIVE_RESOURCES      LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                           SCROLL ===> DATA
******************************** TOP OF DATA ********************************
CHECK(IBMRACF,RACF_SENSITIVE_RESOURCES)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 01/21/2022 13:33:52.327015
CHECK DATE: 20120106  CHECK SEVERITY: HIGH

                          APF Dataset Report

S Data Set Name                            Vol    UACC Warn ID*  User
- ----------------------------------------- ------ ---- ---- ---- ----
E ASM.SASMMOD1                             ZDR25B Altr No   ****
V ATC.V2R1M4.AUTHLIB                       DRVPSL
V CBC.SCBCCMP                              ZDR25B
  CBC.SCCNCMP                              ZDR25B Read No   ****
  CBC.SCLBDLL                              ZDR25B Read No   ****
  CBC.SCLBDLL2                             ZDR25B Read No   ****
  CEE.SCEERUN                              ZDR25B Read No   ****
```

The ID* column shows the access level assigned to the “*” access list entry, which is any RACF-defined user

- Valid values are Read, Updt, Ctrl, Alter and ****.
- **** indicates that there is no “*” access list entry
- If there is no value specified, then there was no profile covering the data

Check Output...

- **Check output: The Sensitive General Resource Report**

```
 Display  Filter  View  Print  Options  Search  Help
 ------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY RACF_SENSITIVE_RESOURCES      LINE 191     COLUMNS 02- 81
 COMMAND INPUT ===>                                            SCROLL ===> DATA

                  Sensitive General Resources Report

S Resource Name                            Class    UACC Warn ID*  User
- ----------------------------------------- -------- ---- ---- ---- ----
  BPX.DAEMON                               FACILITY None No   ****
  BPX.DEBUG                                FACILITY None No   ****
  BPX.FILEATTR.APF                         FACILITY None No   ****
  BPX.FILEATTR.PROGCTL                     FACILITY None No   ****
  BPX.FILEATTR.SHARELIB                    FACILITY None No   ****
  BPX.JOBNAME                              FACILITY None No   ****
  BPX.POE                                  FACILITY None No   ****
  BPX.SERVER                               FACILITY None No   ****
  BPX.SMF                                  FACILITY None No   ****
  BPX.STOR.SWAP                            FACILITY None No   ****
  BPX.SUPERUSER                            FACILITY None No   ****
  BPX.UNLIMITED.OUTPUT                     FACILITY None No   ****
```

The RACF_SENSITIVE_RESOURCES also examines specific general resources in the FACILITY, OPERCMDS, TSOAUTH, and UNIXPRIV classes.

Just like the data set reports, there are status, resource name, class, UACC, warning, ID(*) and user columns. There is no volume column as general resources do not have volumes. The class name is shown instead.

If there is no value specified in the UACC, warning, or ID(*) column, then there was no profile then there was no profile covering the resource. The access allowed will be determined by the default return code for the class.

Check Output...

- **Check output: User Column**

```
Display  Filter  View  Print  Options  Search  Help
 ------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY RACF_SENSITIVE_RESOURCES      LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                            SCROLL ===> DATA
******************************** TOP OF DATA ********************************
CHECK(IBMRACF,RACF_SENSITIVE_RESOURCES)
SYSPLEX:    LOCAL     SYSTEM: RACFR25
START TIME: 01/21/2022 17:04:22.521656
CHECK DATE: 20120106  CHECK SEVERITY: HIGH
CHECK PARM: NOTAUTH


                          APF Dataset Report

S Data Set Name                           Vol    UACC Warn ID*  User
- ---------------------------------------- ------ ---- ---- ---- ----
E ASM.SASMMOD1                            ZDR25B Altr No   **** >Read
V ATC.V2R1M4.AUTHLIB                      DRVPSL
V CBC.SCBCCMP                             ZDR25B
  CBC.SCCNCMP                             ZDR25B Read No   ****
  CBC.SCLBDLL                             ZDR25B Read No   ****
```

You can configure the health check to perform authorization checks as a specific user

The user ID should represent a "non authorized" , "general" user who should not have system-level access privileges

The user can be specified:

- In the Health Checker PARMLIB member (HZSPRMxx)
- Through SDSF
- Using the z/OS console with the MODIFY command issued against the IBM Health Checker for z/OS address space

Is that all There is? No!

The RACF health checks are only a starting point for examining your environment for excessive access

These other RACF commands/utilities are excellent ways to find excessive access:

- Define your own health checks that examine the data sets which are sensitive to your organization
- Use the RACF Database Unload Utility (IRRDBU00) to unload the RACF data base and search for UACCs other than none (ICETOOL sample in 'SYS1.SAMPLIB(IRRICE)')
- Use the RACF SEARCH command to find data sets and general resources to which an ordinary user has at least READ authority

In addition, IBM's zSecure product provides comprehensive analysis and monitoring

Parting Thoughts on Zero Trust and RACF

- **The Zero Trust guiding principles are an application of the generally accepted security principles**
- **Getting started on your Zero Trust journey requires implementing effective controls and monitoring on your z/OS environment**
- **The IBM Health Checker for z/OS and the RACF Health Checks are an important part of your RACF access control and monitoring environment**

See URL:
https://www.ibm.com/legal/copytrade
for a list of trademarks

The Mike Kelly character, the Mock-Up Service Enterprises business, and associated events mentioned in this video are fictitious. Any resemblance to actual persons, living or dead, or actual events is purely coincidental. When a subject matter expert is introduced, the illustration does depict an actual person, and any message from that illustration is an audio recording of that person's voice. The information in this video is provided as is and without warranty of any kind. Following the instructions does not guarantee your system will be secure.
You remain responsible for the security of your system.

The Enterprise Knights of IBM Z

A user group within the IBM Z and LinuxONE Community
providing insights to cyber security & resiliency

www.ibm.biz/ek-ibm-z