

CIS IBM z/OS with RACF Benchmark

v1.0.0 - 10-08-2025

Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is **NEVER** acceptable to host a CIS Benchmark in **ANY** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Terms of Use	1
Table of Contents	2
Overview	10
Important Usage Information	10
Key Stakeholders	10
Apply the Correct Version of a Benchmark	11
Exceptions	11
Remediation	12
Summary	12
Target Technology Details	13
Intended Audience.....	15
Consensus Guidance	16
Typographical Conventions.....	17
Recommendation Definitions.....	18
Title.....	18
Assessment Status.....	18
Automated	18
Manual.....	18
Profile	18
Description.....	18
Rationale Statement	18
Impact Statement.....	19
Audit Procedure.....	19
Remediation Procedure.....	19
Default Value.....	19
References	19
CIS Critical Security Controls® (CIS Controls®).....	19
Additional Information.....	19
Profile Definitions	20
Acknowledgements	21
Recommendations	22
1 Identification and Authentication	22
1.1 Password Control	23
1.1.1 Ensure that the SETROPTS PASSWORD(INTERVAL and PHRASEINT) values are set to a maximum of 365 (Automated)	24

1.1.2 Ensure that the SETROPTS PASSWORD(HISTORY) value is set to a minimum of 5 (Automated)	27
1.1.3 Ensure that at least one SETROPTS PASSWORD(RULE) is defined with (LENGTH(8) MIXEDALL(1:8)) (Automated)	29
1.1.4 Ensure that the SETROPTS PASSWORD(MINCHANGE) value is set to a minimum of 1 (Automated)	32
1.1.5 Ensure that the SETROPTS PASSWORD(REVOKE) value is set to a maximum of 6 (Automated)	34
1.1.6 Ensure that the SETROPTS PASSWORD(ALGORITHM) value is set to KDFAES (Automated)	36
1.1.7 Ensure that the SETROPTS PASSWORD(WARNING) value is set to a minimum of 5 (Automated)	39
1.1.8 Ensure that the SETROPTS RVARYPW values are secured with KDFAES (Automated)	41
1.1.9 Ensure SETROPTS PASSWORD(MIXEDCASE) is in effect (Automated)	43
1.1.10 Ensure SETROPTS PASSWORD(SPECIALCHARS) is in effect (Automated)	45
1.2 System Settings	47
1.2.1 Ensure that the SETROPTS INACTIVE value is set to a maximum of 45 (Automated) ..	48
1.2.2 Ensure that the STARTED resource class is used to assign user IDs to started tasks (Automated)	51
1.2.3 Ensure user propagation is controlled (Automated)	56
1.2.4 Ensure that started tasks defined with the TRUSTED attribute are justified (Manual) ..	59
1.2.5 Ensure that the OPERCMDS resource class is enabled (Automated)	61
1.2.6 Ensure that the CONSOLE resource class is enabled (Automated)	63
1.2.7 Ensure that the FACILITY resource class is enabled (Automated)	65
1.2.8 Ensure that inapplicable PPT entries have been invalidated (Manual)	67
1.2.9 Ensure that LNKAUTH=APFTAB is specified in the IEASYSxx members currently active parmlib data sets (Automated)	70
1.2.10 Ensure that the CONSOLxx members are configured (Manual)	72
1.2.11 Ensure that no expired digital certificates are used (Automated)	74
1.2.12 Ensure that the SETROPTS RVARYPW are set to non-default values (Automated) ..	77
1.2.13 Ensure that RACF default user ID IBMUSER is disabled (Automated)	79
1.3 User Attributes	81
1.3.1 Ensure that the use of RACF SPECIAL attribute is justified (Manual)	82
1.3.2 Ensure that SYS1.UADS contains only recovery user IDs (Manual)	84
1.3.3 Ensure that MCS console user IDs are protected (Manual)	87
1.3.4 Ensure that STARTED resource class profiles assign PROTECTED user IDs (Automated)	91
1.3.5 Ensure that the assignment of RACF CLAUTH authority is justified (Automated)	93
2 Authorization and Access Control Management	94
2.1 Data Protection	95
2.1.1 Ensure that access to DASDVOL and STGADMIN resources are controlled (Automated)	96
2.1.2 Ensure that access to active SMF collection files is controlled (Automated)	103
2.1.3 Ensure that the SETROPTS WHEN(PROGRAM) value is active (Automated)	106
2.1.4 Ensure that access to the ICHDSM00 (DSMON) program is controlled (Automated) ..	108
2.1.5 Ensure that access to the IRRDPI00 program is controlled (Automated)	111
2.1.6 Ensure that the SETROPTS ERASE value is set to ALL (Automated)	116
2.1.7 Ensure that the TEMPDSN class is active (Automated)	118
2.1.8 Ensure that access to RACF database data sets is controlled (Automated)	120
2.1.9 Ensure that access to the RACF remote sharing facility data sets is controlled (Automated)	124
2.1.10 Ensure that access to the RACF parameter library is controlled (Automated)	128
2.1.11 Ensure that RACF remote sharing connections use the TCP/IP protocol (Automated)	131

2.1.12 Ensure that access to memory and privileged program dumps is controlled (Automated)	133
2.1.13 Ensure that access to system TRACE data sets is controlled (Automated)	137
2.1.14 Ensure that access to system backup data sets is controlled (Automated)	140
2.1.15 Ensure that access to system DUMP data sets is controlled (Automated)	143
2.1.16 Ensure that access to SMF collection offload data sets is controlled (Automated)	146
2.2 Resource Protection	149
2.2.1 Ensure that the access to update system dynamic lists is controlled (Automated)	150
2.2.2 Ensure that access to IEASYMUP resources is controlled (Manual)	154
2.2.3 Ensure that PASSWORD protection for data sets is not used (Manual)	158
2.2.4 Ensure that access to data sets in the PARMLIB concatenation is controlled (Automated)	160
2.2.5 Ensure that access to all LPA libraries is controlled (Manual)	163
2.2.6 Ensure that access to system MASTER catalogs is controlled (Manual)	166
2.2.7 Ensure that access to all APF-authorized objects is controlled (Manual)	169
2.2.8 Ensure that access to the SYS1.SVCLIB data set is controlled (Automated)	175
2.2.9 Ensure that access to the SYS1.IMAGELIB data set is controlled (Manual)	178
2.2.10 Ensure that access to libraries that contain PPT modules is controlled (Automated)	181
2.2.11 Ensure that access to the SYS1.NUCLEUS data set is controlled (Automated)	184
2.2.12 Ensure that access to all system PROCLIB data sets is controlled (Automated)	187
2.2.13 Ensure that access to System REXX IRRPWREX exit is controlled (Automated)	191
2.2.14 Ensure that access to the SYS1.LINKLIB data set is controlled (Automated)	195
2.2.15 Ensure that access to all system-level product installation libraries is controlled (Automated)	198
2.2.16 Ensure that access to RACF resources in the FACILITY class is controlled (Automated)	201
2.2.17 Ensure that access to VTAMAPPL resources is controlled (Manual)	205
2.2.18 Ensure that access to IBM Health Checker resources is controlled (Automated)	209
2.3 System Settings	213
2.3.1 Ensure that the SETROPTS TERMINAL value is set to NONE (Automated)	214
2.3.2 Ensure that the SETROPTS GENERIC is enabled for ACTIVE classes (Automated)	216
2.3.3 Ensure that the SETROPTS PROTECTALL value is set to FAIL (Automated)	219
2.3.4 Ensure that ALTER access authority in DISCRETE profiles is limited (Automated)	221
2.3.5 Ensure that the ACEECHK resource class is enabled (Automated)	225
2.3.6 Ensure that SETROPTS ENHANCEDGENERICOWNER is in effect (Automated)	227
2.3.7 Ensure that SETROPTS NOADDCREATOR is in effect (Automated)	229
2.4 User Privilege	231
2.4.1 Ensure that the assignment of the RACF OPERATIONS attribute is justified (Automated)	232
2.4.2 Ensure that access to TSOAUTH resources is controlled (Automated)	234
2.4.3 Ensure that access to SURROGAT resources is controlled (Automated)	239
2.4.4 Ensure that the assignment of the UNIX uid(0) is justified (Automated)	243
2.4.5 Ensure that started tasks defined with the PRIVILEGED attribute is justified (Automated)	245
2.4.6 Ensure that access to libraries containing EXIT modules is controlled (Automated)	247
2.4.7 Ensure that access to LINKLIST libraries is controlled (Automated)	250
2.4.8 Ensure that access to the SYS1.UADS data set is controlled (Automated)	253
2.4.9 Ensure that access to system page data sets is controlled (Automated)	256
2.4.10 Ensure that MCS console access is controlled through profiles in the CONSOLE resource class (Manual)	259
2.4.11 Ensure that access to system USER catalogs is controlled (Automated)	263
2.4.12 Ensure that access to Libraries containing EXIT modules is controlled (Automated)	267
3 Logging and Auditing	270
3.1 Ensure that SETROPTS CMDVIOL is in effect (Automated)	271
3.2 Ensure that SETROPTS SAUDIT is in effect (Automated)	273

3.3 Ensure that SETROPTS AUDIT is enabled for ACTIVE classes (Automated)	275
Remediation Procedure	276
3.4 Ensure that SETROPTS OPERAUDIT is in effect (Automated).....	277
3.5 Ensure that SETROPTS INITSTATS is in effect (Automated)	279
3.6 Ensure that the assignment of the RACF AUDITOR or ROAUDIT attribute is justified (Automated)	282
3.7 Ensure that effective SMF records collection options are set (Automated).....	284
3.8 Ensure that an automated process is in place to collect and retain SMF data (Manual) .	286
3.9 Ensure that required SMF data record types are collected (Automated)	288
3.10 Ensure that RACF audit logs is reviewed on a regular basis (Manual)	294
3.11 Ensure regular audits of AC=1 modules in APF authorized libraries are conducted (Manual).....	296
3.12 Ensure that only supported software is installed and active on the system (Manual)	297
3.13 Ensure all OS software on your system is supported (Manual)	298
3.14 Implement sensitive z/OS data set monitoring (Manual).....	299
3.15 Ensure that SETROPTS REALDSN is in effect (Automated).....	300
4 System Resilience	302
4.1 Ensure that RACF database is backed up on a scheduled basis (Manual)	303
4.2 Ensure that the RACF PRIM and BACK databases are isolated (Manual).....	304
Remediation Procedure	304
4.3 Ensure sensitive data sets are encrypted with z/OS data set encryption (Manual)	306
4.4 Ensure that RACF application identity mapping (AIM) is at stage 3 (Manual)	309
4.5 Ensure that RACF ENQ names are not in the Global Resource Serialization (GRS) Resource Name List (Manual)	311
4.6 Ensure that SETROPTS GRPLIST is in effect (Automated)	313
4.7 Ensure that SETROPTS NOSTATISTICS(*) is in effect (Automated).....	315
4.8 Ensure that RACF is enabled for Sysplex communication (Automated)	317
4.9 Ensure that Validated Boot for z/OS is in effect (Manual)	319
4.10 Ensure that the site is registered to the IBM Z and IBM LinuxONE Security Portal (Manual).....	320
5 Storage Management.....	322
5.1 Ensure that DFSMS is configured (Manual)	323
5.2 Ensure that access to the Tape Bypass Label Processing (BLP) resource is controlled (Automated)	325
5.3 Ensure that SETROPTS ADSP is disabled (Automated)	329
5.4 Ensure that access to DFSMS control data sets is controlled (Automated).....	331
6 Networking	335
6.1 CSSMTP Recommendations.....	336
6.1.1 Ensure CSSMTP started task user ID is PROTECTED (Automated)	337
6.1.2 Ensure that the STARTED resource class is used to assign user IDs to CSSMTP started tasks (Automated).....	339
6.1.3 Ensure AT-TLS protection is enabled for CSSMTP (Manual)	342
6.1.4 Ensure that access to CSSMTP started task data sets is controlled (Automated)	344
6.2 FTP Recommendations	348
6.2.1 Ensure that the STARTED resource class is used to assign user IDs with proper parameters to FTP server started tasks (Automated)	349
6.2.2 Ensure startup parameters for the FTP daemon do not allow ANONYMOUS or INACTIVE keywords (Manual).....	353
6.2.3 Ensure FTP.DATA configuration statements enforce secure configuration (Manual)...	355
6.2.4 Ensure FTP.DATA configuration statements enforce AT-TLS protection (Manual).....	357
6.2.5 Ensure user exits for the FTP server are not used without approval (Manual)	359
6.2.6 Ensure that access to the warning banner for the FTP server is controlled (Automated)	361
6.2.7 Ensure SMF recording options for the FTP Server are configured (Manual)	365

6.2.8 Ensure UNIX permission and user audit bits for FTP server are configured (Manual)	367
6.2.9 Ensure access to FTP server FTP.DATA data sets is controlled (Manual)	369
6.2.10 Ensure access to FTP control card data sets is controlled (Manual)	372
6.3 OpenSSH	375
6.3.1 Ensure SSH daemon is configured to only use the SSHv2 protocol (Manual)	376
6.3.2 Ensure SSH daemon is configured to use FIPS 140-2 compliant cryptographic provider (Manual)	378
6.3.3 Ensure SSH daemon is configured with a logon banner (Manual)	380
6.3.4 Ensure SSH daemon is configured for SMF logging (Manual)	382
6.3.5 Ensure SSH daemon is configured to use SAF keyrings for key storage (Manual)	384
6.4 Syslogd Recommendations	386
6.4.1 Ensure syslog daemon is started at z/OS initialization (Manual)	387
6.4.2 Ensure that the STARTED resource class is used to assign user IDs with proper parameters to syslog daemon started tasks (Manual)	389
6.4.3 Ensure permission and user audit bits for syslog daemon component are configured (Manual)	393
6.4.4 Ensure that access to syslog daemon archive data sets is controlled (Manual)	395
6.5 TCP/IP Recommendations	398
6.5.1 Ensure configuration files for the TCP/IP stack are explicitly specified (Manual)	399
6.5.2 Ensure TCP/IP stack configuration defined in TCPIP.DATA meets minimum requirements (Manual)	401
6.5.3 Ensure hosts identified by the NSINTERADDR statement are protected (Manual)	403
6.5.4 Ensure TCP/IP stack configuration defined in PROFILE.TCPIP meets minimum requirements (Manual)	405
Audit Procedure	405
6.5.5 Ensure permission and user audit bits for z/OS UNIX file system objects that are part of the base TCP/IP component are configured (Manual)	408
6.5.6 Ensure access to TCP/IP SAF resources is controlled (Manual)	410
6.5.7 Ensure that the SERVAUTH resource class is enabled (Manual)	416
6.5.8 Ensure that the STARTED resource class is used to assign user IDs with proper parameters to base TCP/IP component started tasks (Manual)	418
6.5.9 Ensure access to data sets for the base TCP/IP component is controlled (Manual)	422
6.6 TN3270 Recommendations	425
6.6.1 Ensure configuration statements for the TN3270E telnet server are configured (Manual)	426
6.6.2 Ensure VTAM session setup controls for the TN3270E telnet server are configured (Manual)	428
6.6.3 Ensure a warning banner for the TN3270 telnet server is configured (Manual)	431
6.6.4 Ensure AT-TLS protection is enabled for the TN3270 telnet server (Manual)	433
6.6.5 Ensure SMF recording options for the TN3270 telnet server are configured (Manual)	435
6.6.6 Ensure that access to the otelnetd and EZATNTLE programs is controlled (Manual)	437
6.7 VTAM Recommendations	441
6.7.1 Ensure VTAM USSTAB definitions are being used for secured terminals (Manual)	442
6.7.2 Ensure that access to the system data sets used to support the VTAM network is controlled (Manual)	444
7 Cryptography and Encryption	447
7.1 ICSF Installation and Configuration	448
7.1.1 Ensure that access to ICSF installation data sets is controlled (Manual)	449
7.1.2 Ensure that the STARTED resource class is used to assign user IDs with proper parameters to ICSF started tasks (Automated)	453
7.1.3 Ensure CSFINPV2 requires signature verification (Manual)	457
7.1.4 Ensure ICSF is configured to start during IPL (Manual)	459
7.1.5 Ensure that ICSF Master Keys are managed by a Trusted Key Entry (TKE) workstation (Manual)	461
7.2 ICSF Component Configuration	462

7.2.1 Ensure crypto usage statistics are enabled (Manual).....	463
7.2.2 Ensure crypto key lifecycle auditing is enabled (Manual).....	465
7.2.3 Ensure crypto key usage auditing is enabled (Manual).....	467
7.2.4 Ensure ICSF key data sets have a system backup (Manual).....	469
7.2.5 Ensure ICSF master keys have a backup procedure (Manual).....	470
7.2.6 Ensure all ICSF key data sets are in common record format (Manual).....	471
7.2.7 Ensure all ICSF key data sets are enabled for sysplex sharing (Manual).....	472
7.2.8 Ensure ICSF is running with FIPSMODE enabled (Manual).....	474
7.2.9 Ensure CCA operational keys are created with WRAPENH3 key wrapping (Manual).....	476
7.3 ICSF Security Configuration.....	478
7.3.1 Ensure that the CSFSERV class is active (Manual).....	479
7.3.2 Ensure that the CSFKEYS class is active (Manual).....	481
7.3.3 Ensure that the CRYPTOZ class is active (Manual).....	483
7.3.4 Ensure that the XCSFKEY class is active (Manual).....	485
7.3.5 Ensure ICSF key store policy controls are enabled (Manual).....	487
7.3.6 Ensure access to ICSF key data sets is controlled (Manual).....	489
7.3.7 Ensure access to ICSF administrative services is controlled (Manual).....	492
7.3.8 Ensure access to ICSF operator commands is controlled (Manual).....	496
8 Job Management JES2.....	500
8.1 JES2 Commands.....	501
8.1.1 Ensure that access to JES2 system commands is controlled (Manual).....	502
8.2 JES2 SPOOL.....	507
8.2.1 Ensure that the JESSPOOL resource class is enabled (Manual).....	508
8.2.2 Ensure that access to JES2 spool resources is controlled (Manual).....	510
8.2.3 Ensure that access to JES2 trace resources is controlled (Manual).....	514
8.2.4 Ensure that access to JESNEWS resources is controlled (Manual).....	518
8.3 Job Level Protection.....	522
8.3.1 Ensure that the JESJOBS resource class is configured (Manual).....	523
8.3.2 Ensure that access to JESJOBS CANCEL resources is controlled (Manual).....	527
8.3.3 Ensure that access to JESJOBS GROUPREG resources is controlled (Manual).....	531
8.3.4 Ensure that access to JESJOBS HOLD resources is controlled (Manual).....	535
8.3.5 Ensure that access to JESJOBS JOBCLASS resources is controlled (Manual).....	539
8.3.6 Ensure that access to JESJOBS JOBNFY resources is controlled (Manual).....	543
8.3.7 Ensure that access to JESJOBS MODIFY resources is controlled (Manual).....	547
8.3.8 Ensure that access to JESJOBS PURGE resources is controlled (Manual).....	551
8.3.9 Ensure that access to JESJOBS RELEASE resources is controlled (Manual).....	555
8.3.10 Ensure that access to JESJOBS REROUTE resources is controlled (Manual).....	559
8.3.11 Ensure that access to JESJOBS SPIN resources is controlled (Manual).....	563
8.3.12 Ensure that access to JESJOBS SPOOLIO resources is controlled (Manual).....	567
8.3.13 Ensure that access to JESJOBS START resources is controlled (Manual).....	571
8.3.14 Ensure that access to JESJOBS SUBMIT resources is controlled (Manual).....	575
8.3.15 Ensure that access to JESJOBS RESTART resources is controlled (Manual).....	579
8.4 Enable Encryption of Data Set on SPOOL.....	583
8.4.1 Ensure that data sets on SPOOL are encrypted (Manual).....	584
8.5 Control Access to Data Sets Used by JES2.....	588
8.5.1 Ensure that access to the data sets used by JES2 is controlled (Automated).....	589
8.5.2 Ensure that RACF is called for data sets opened by JES2 (Manual).....	592
8.6 Device Management.....	594
8.6.1 Ensure that access to JES2 output devices is controlled (Manual).....	595
8.6.2 Ensure that bypass label processing is not set on any JOBCLASS (Manual).....	599
8.6.3 Ensure that access to JES2 input sources is controlled (Manual).....	601
8.7 JES2 Networking.....	605
8.7.1 Ensure that RJE workstations and NJE nodes enforce password protection (Manual).....	606
8.7.2 Ensure that RJE workstations have paired user IDs (Manual).....	608
8.8 Require User Identification.....	611

8.8.1 Ensure that the SETROPTS JES(BATCHALLRACF) is enabled (Automated)	612
8.8.2 Ensure that the SETROPTS JES(XBMALLRACF) is enabled (Automated)	614
9 UNIX System Services	616
9.1 Ensure that access to z/OS UNIX SURROGAT resources is controlled (Automated)	617
9.2 Ensure that access to superuser resources in the UNIXPRIV class is controlled (Automated)	621
9.3 Ensure that general users are not allowed to change their file ownership (Automated) ..	625
9.4 Ensure that RESTRICTED users cannot access UNIX files to which they are not explicitly permitted (Automated)	627
9.5 Ensure that newly assigned UID and GID are unique values (Automated)	631
9.6 Ensure that z/OS UNIX user accounts are defined with compliant values (Automated) ..	633
9.7 Ensure that RACF Classes required to secure the z/OS UNIX environment are active (Automated)	635
9.8 Ensure that RACF Classes required to secure the z/OS UNIX environment are RACLISTed (Automated)	637
9.9 Ensure that the user account for the z/OS UNIX kernel is defined with compliant attributes (Automated)	639
9.10 Ensure that z/OS UNIX automount configuration files are configured with compliant values (Automated)	642
9.11 Ensure that entries in /etc/inetd.conf are active and secure (Automated)	644
9.12 Ensure that z/OS UNIX OMVS parameters in IEASYSxx are configured (Automated) ..	647
9.13 Ensure that z/OS UNIX BPXPRMxx parameters in PARMLIB are configured for security (Automated)	649
9.14 Ensure that z/OS UNIX permission bits and audit bits are configured to audit sensitive file access (Automated)	651
9.15 Ensure that access to BPX resources in the FACILITY class is controlled (Automated)	653
9.16 Ensure that security parameters in /etc/profile are configured (Automated)	657
9.17 Ensure that security commands in /etc/rc are safe (Automated)	659
9.18 Ensure that the BPXROOT user account is configured with compliant values (Manual)	662
9.19 Ensure that each RACF group for UNIX is defined with a unique GID (Automated)	665
9.20 Ensure that access to data sets used as step libraries in /etc/steplib is controlled (Automated)	667
9.21 Ensure that ability to switch into superuser mode is controlled (Automated)	670
9.22 Ensure access to zFS data sets is controlled (Automated)	674
9.23 Ensure USS Telnet server is not active (Automated)	677
9.24 Ensure rlogin is not active (Manual)	678
9.25 Ensure that the FSSEC resource class is enabled (Manual)	679
9.26 Ensure that programs cannot execute from the /tmp directory (Automated)	681
9.27 Ensure that data sets containing user file systems do not have the user ID as the high-level qualifier (Manual)	685
9.28 Ensure that daemons are running with z/OS UNIX level security (Automated)	686
9.29 Ensure that servers are running with z/OS UNIX level security (Automated)	690
9.30 Ensure that access to file systems containing critical data is controlled (Manual)	694
9.31 Ensure that file systems are mounted Read Only wherever possible (Manual)	698
Audit Procedure	698
9.32 Ensure that file systems are mounted with set-id files disabled wherever possible (Manual)	700
9.33 Ensure that no file systems are mounted with security disabled (Automated)	702
Appendix: Summary Table	704
Appendix: CIS Controls v8 IG 1 Mapped Recommendations	723
Appendix: CIS Controls v8 IG 2 Mapped Recommendations	734

<i>Appendix: CIS Controls v8 IG 3 Mapped Recommendations</i>	<i>746</i>
<i>Appendix: CIS Controls v8 Unmapped Recommendations.....</i>	<i>758</i>
<i>Appendix: Change History</i>	<i>759</i>

Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

Important Usage Information

All Benchmarks are available free for non-commercial use from the [CIS Website](#). They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- [CIS Configuration Assessment Tool \(CIS-CAT® Pro Assessor\)](#)
- [CIS Benchmarks™ Certified 3rd Party Tooling](#)

These tools make the hardening process much more scalable for large numbers of systems and applications.

NOTE: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that **ALL** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.
- **Use the most recent version of a Benchmark:** This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Remediation

CIS has developed [Build Kits](#) for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
 - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
 - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
 - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
 - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
 - When the initial deployment above is completed successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the [CIS Website](#). All other formats of the CIS Benchmarks™ (MS Word, Excel, and [Build Kits](#)) are available for CIS [SecureSuite](#)® members.

CIS-CAT® Pro is also available to CIS [SecureSuite](#)® members.

Target Technology Details

This benchmark provides recommendations for establishing a baseline, secure configuration posture for IBM z/OS mainframe systems which are using IBM RACF as the External Security Manager (ESM).

This benchmark was written such that conformity with its recommendations can be assessed using only commands or utilities natively provided by IBM z/OS and IBM RACF. A frequent source of data is reports generated from RACF Database Unload (IRRDUB00) utility output, which creates a sequential file from a RACF database. Because this file can be processed in a variety of ways - viewed directly, used as input by installation-written programs, manipulated with sort/merge utilities, loaded into a database manager, etc. - we have not provided a preferred report format or method. Instead, we have provided guidance on what data needs to be included in reports generated by the site for assessing conformity with the recommendation.

Note: A site may choose to use industry standard security software solutions for assessing conformity with these recommendations in place of native tools and commands.

Refer to <https://www.ibm.com/legal/copytrade> for listing of United States trademarks owned by IBM and related information. UNIX is a registered trademark of The Open Group in the United States and other countries.

To obtain the latest version of this guide, please visit <http://workbench.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Access Control List (ACL) Recommendations

This benchmark makes frequent reference to the following table when providing Access Control List (ACL) recommendations:

Type of Privileged Users	Short Name	Description
Auditors	AUDITOR	A security auditor assesses and evaluates z/OS operating system and its related hardware and software to identify vulnerabilities, weaknesses, and compliance gaps.
Production Control Specialists	PRODCNTL	A production control specialist manages and monitors batch processing and production schedules on z/OS mainframe systems.
Security Administrators	SECADMIN	A security administrator is responsible for managing and maintaining the security configurations and definitions of z/OS mainframe systems.

Type of Privileged Users	Short Name	Description
Storage Administrators	STGADMIN	A storage administrator is responsible for provisioning, managing, and maintaining the data storage systems and subsystems of z/OS mainframe systems.
Systems Operators	OPERATOR	A systems operator monitors and controls the operation of z/OS mainframe hardware and software.
Systems Programmers	SYSPROG	A systems programmer is responsible for managing, maintaining, and enhancing the z/OS operating system and related hardware and software.
z/OS Started Task (STC)	STCUSER	User IDs assigned to address spaces that run unattended as the result of a START command.

Notes:

- We have provided a "Short Name" (limited to 8 characters in length) to be used as a base set of reserved identifiers that can be leveraged by tooling or reports, as well as benchmark remediation command examples.
- When you encounter privileged user types on ACL recommendations, it generally means that "this type of privileged user" is expected to have "this level of access" to "this type of resource".

It does not describe specific *roles* (<https://csrc.nist.gov/glossary/term/role>), but instead community accepted terms for a minimal set of common *types of privileged users* that manage z/OS mainframe systems and their associated software and hardware.

It is understood that a site will have an existing Role Based Access Control (RBAC) structure with site-specific (or even system-specific) naming conventions and categorizations. This RBAC structure may or may not encompass all *types of privileged users* table entries, which also may or may not have more or less granularity, for common privileged users (i.e. "*Junior Systems Programmers*" and "*Senior Systems Programmers*"). IBM RACF allows a site to define arbitrarily named groups with no prescribed nesting order (aside from the reserved root-level **SYS1** group) and allows for access to be permitted to individual user IDs, groups. or generically - or a combination of these options.

To account for this flexibility, this benchmark frequently concludes ACL recommendations with the line "**IDs authorized to access these resources at this level**". It is a shortened form of the full sentence:

***IDs (either user or group) authorized** by the site with appropriate approval and risk acceptance **to access these resources at this level** because they have a documented justification for this access with (where appropriate) an expiration date for access that is not required for business as usual.*

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate IBM z/OS.

Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
<code><Monospace font in brackets></code>	Text set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like Notes , Warnings , or Cautions (usually just the word itself and the rest of the text normal).

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Items in this profile intend to:

- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

This profile extends the "Level 1 - Server" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author

Daniel Burk

Contributor

Mark Nelson
Shaun Kelley
Barb Leinberger
Bruce Wells
Didier Andre
Christopher Meyer
Joe Welsh
Bob Petti
Thomas Wasik
Genaro Lopez Baez
Matthew Brown
Steve Hosie
Marina Zografova
Graham Eames

Editor

Anuja Deedwaniya
Eric Pinnell

Recommendations

1 Identification and Authentication

This section provides guidance on how to uniquely identify a user of a system and to prove that a user is genuinely who that person claims to be. It also provides guidance on setting up secure defaults for system and user accounts and their environments.

1.1 Password Control

This section describes the Password Control recommendations.

1.1.1 Ensure that the SETROPTS PASSWORD(INTERVAL and PHRASEINT) values are set to a maximum of 365 (Automated)

Profile Applicability:

- Level 1

Description:

The **SETROPTS INTERVAL** parameter specifies the system default for the maximum number of days that each user's password and password phrase remain valid. The **PHRASEINT** parameter specifies the system default for the number of days that each user's password phrase remains valid and overrides the **INTERVAL** setting for password phrases.

Rationale:

Excessive password expiration requirements do more harm than good, because these requirements make users select predictable passwords, composed of sequential words and numbers that are closely related to each other. In these cases, the next password can be predicted based on the previous one (incrementing a number used in the password for example). Also, password expiration requirements offer no containment benefits because attackers will often use credentials as soon as they compromise them. Instead of recommending a mandatory password change interval, immediate password changes should be based on key events including, but not limited to:

- Indication of compromise
- Change of user roles
- When a user leaves the organization.

Impact:

We recommend a yearly password change primarily because for all their good intentions users will share credentials across accounts. Therefore, even if a breach is publicly identified, the user may not see this notification, or forget they have an account on that site. This could leave a shared credential vulnerable indefinitely. Having an organizational policy of a 1-year (annual) password expiration is a reasonable compromise to mitigate this with minimal user burden.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **PASSWORD PROCESSING OPTIONS:** section.

Look for the following message:

```
PASSWORD CHANGE INTERVAL IS <nnn> DAYS.
```

Verify the value is equal to or less than 254 days.

Note: 254 is the maximum value allowed for **INTERVAL**.

Look for the following message:

```
PASSWORD PHRASE CHANGE INTERVAL IS <nnn> DAYS.
```

Verify the value is equal to or less than 365 days.

Note: The message **PASSWORD CHANGE INTERVAL IS IN EFFECT FOR PASSWORD PHRASES.** may appear instead, indicating that the **INTERVAL** keyword value is also used to control the password phrase interval. Use that value for verification.

Remediation:

To modify the **INTERVAL** and **PHRASEINT** parameters use the RACF **SETROPTS** command:

```
SETROPTS PASSWORD (INTERVAL (254) PHRASEINT (365) )
```

Default Value:

INTERVAL(30) and **PHRASEINT(0)** is in effect when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000800

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Setting the maximum and minimum change interval \(PASSWORD option\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			

1.1.2 Ensure that the SETROPTS PASSWORD(HISTORY) value is set to a minimum of 5 (Automated)

Profile Applicability:

- Level 1

Description:

HISTORY specifies the number of previous passwords that RACF saves for each user ID and compares with an intended new password. If there is a match with one of the previous passwords, or with the current password, RACF rejects the intended new password.

PASSWORD(HISTORY(nn)) command enables you to specify the number of previous passwords and password phrases (1 - 32) that RACF saves for each user and compares it with an intended new value. For passwords, RACF stores only previous passwords in each user's history. For password phrases, RACF saves the user's current password phrase in addition to the user's previous password phrases. Therefore, for password phrases, RACF saves one fewer previous value than the number you specify for history.

Example: If you specify 12 for your **HISTORY** number using the command **SETROPTS PASSWORD(HISTORY(12))** RACF saves up to 12 previous passwords and up to 11 previous password phrases for each user. Effective immediately, the values when executing that command are the default values for new users whom you define to RACF through the **ADDUSER** command.

Rationale:

A password history policy prevents users from immediately reusing an old password by enforcing a minimum number of new, unique passwords that must be used before a previous one can be reused. This is a crucial security measure against password recycling and brute force attacks. We recommend a **HISTORY** value of 5 to avoid user frustration while balancing security and usability.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **PASSWORD PROCESSING OPTIONS:** section.

Look for the following message:

```
<nn> GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
```

Verify the value is equal to or greater than 5 generations.

Remediation:

To modify the **HISTORY** parameter use the RACF **SETROPTS** command:

```
SETROPTS PASSWORD(HISTORY(5))
```

Default Value:

NOHISTORY is in effect when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000810

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Extending password and user ID processing \(PASSWORD option\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			

1.1.3 Ensure that at least one SETROPTS PASSWORD(RULE) is defined with (LENGTH(8) MIXEDALL(1:8)) (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS PASSWORD(RULE<n>) specifies up to eight password syntax rules to verify that new passwords meet the installation standards. These rules allow you to control:

- The minimum and maximum length of passwords
- The character content of installation-selected positions in the passwords

Rationale:

Password composition or complexity requirements are used to increase the strength of a user-created password of a given length. For example, a complex password would need some amount of characters from all three of the following categories:

- Uppercase characters
- Lowercase characters
- Non-alphabetic characters such as numbers or special characters

By implementing this recommendation a user will be required to create a complex password of the maximum allowable length (8).

Impact:

MIXEDALL includes all allowable password characters separated into the following categories. There are either three or four "active" categories, depending on whether **SETROPTS PASSWORD(MIXEDCASE)** is in effect:

1. The national characters.
 - And special characters if **SETROPTS PASSWORD(SPECIALCHARS)** is in effect.
2. Numeric characters.
3. Uppercase alphabetic characters (not including the national characters).
4. Lowercase alphabetic characters, if **SETROPTS PASSWORD(MIXEDCASE)** is in effect.

Note: When four or more **MIXEDALL** positions are specified *and* **SETROPTS PASSWORD(MIXEDCASE)** is enabled, then at least *one* of every category must be specified anywhere across the designated positions.

If **SETROPTS PASSWORD(MIXEDCASE)** is not enabled, then there is no change in behavior from having three **MIXEDALL** positions, other than in the number of positions over which the three active categories may be spread.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **PASSWORD PROCESSING OPTIONS:** section.

Verify that at least 1 rule in the **INSTALLATION PASSWORD SYNTAX RULES:** section matches the following value:

```
RULE <n>  LENGTH(8)  xxxxxxxx
```

Remediation:

To modify or add a password **RULE<n>** parameter use the RACF **SETROPTS** command:

```
SETROPTS PASSWORD(RULE1(LENGTH(8) MIXEDALL(1:8)))
```

Default Value:

SETROPTS PASSWORD(NORULES) is in effect when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000770

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Establishing password syntax rules \(PASSWORD option\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			

1.1.4 Ensure that the SETROPTS PASSWORD(MINCHANGE) value is set to a minimum of 1 (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS PASSWORD(MINCHANGE(<nnn>)) specifies the number of days that must pass between a user's password and password phrase changes. Users can not change their own passwords and password phrases within the minimum change interval. Permitting users to change their password more than once in a day allows users to quickly cycle through their password history and maintain the same password indefinitely. The **SETROPTS PASSWORD(MINCHANGE(<nnn>))** value, either specified or defaulted, is in effect for all users. A security administrator may set a password within the **MINCHANGE** window.

Rationale:

How frequently a password can be changed should be limited to prevent a user from immediately changing the password multiple times to get back to the original one.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **PASSWORD PROCESSING OPTIONS:** section.

Look for the following message:

```
PASSWORD MINIMUM CHANGE INTERVAL IS <nnn> DAYS.
```

Verify the value is equal to or greater than 1 days.

Remediation:

To modify the **MINCHANGE** parameter use the RACF **SETROPTS** command:

```
SETROPTS PASSWORD(MINCHANGE(1))
```

Default Value:

MINCHANGE(0) is in effect when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000790

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Setting the maximum and minimum change interval \(PASSWORD option\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			

1.1.5 Ensure that the SETROPTS PASSWORD(REVOKE) value is set to a maximum of 6 (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS PASSWORD(REVOKE(<nnn>)) enables you to specify how many consecutive incorrect password and password phrase attempts RACF permits before it revokes the user ID on the next attempt.

Note: If you specify **REVOKE**, **INITSTATS** must be in effect.

Rationale:

The overall goal is it to make it difficult for an attacker to guess a password by trying it against an account, while allowing a user the ability to correct a mistakenly entered password in a reasonable way.

Impact:

Limiting failed login attempts does not prevent testing a password guess via *password spraying techniques* (i.e. using the same password against many different user accounts). Instead, it tends to encourage attackers into using this technique to avoid lockouts, which results as an obvious anomaly and likely detectable via SMF monitoring.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ATTRIBUTES =** section.

Verify that **INITSTATS** appears.

Review the command output in the **PASSWORD PROCESSING OPTIONS:** section.

Look for the following message:

```
AFTER <nnn> CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,  
A USERID WILL BE REVOKED.
```

Verify the value is equal to or less than 6 attempts.

Remediation:

To modify the **REVOKE** parameter use the RACF **SETROPTS** command:

```
SETROPTS PASSWORD(REVOKE(6))
```

If you specify **REVOKE**, **INITSTATS** must be in effect. To enable **INITSTATS** use the RACF **SETROPTS** command:

```
SETROPTS INITSTATS
```

Default Value:

The following values are in effect when RACF is using a newly initialized database:

- **INITSTATS**
- **NOREVOKE**

References:

1. IBM z/OS RACF STIG: RACF-ES-000480
2. IBM z/OS RACF STIG: RACF-ES-000490

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Extending password and user ID processing \(PASSWORD option\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			

1.1.6 Ensure that the SETROPTS PASSWORD(ALGORITHM) value is set to KDFAES (Automated)

Profile Applicability:

- Level 2

Description:

The **SETROPTS PASSWORD(ALGORITHM)** algorithm is used to encrypt passwords and password phrases, but not **OIDCARD** data. The RACF KDFAES algorithm is designed to be resistant to offline attacks by incorporating the following properties:

- Each instance of a RACF password injects randomly generated text into the encryption process. This prevents the use of pre-computed password hashes. That is, an offline attack must perform the full encryption process for every password guess, as opposed to simply comparing the password hash against a list of pre-computed values. This slows down the attack, making it take much longer to guess passwords.
- Thousands of hash operations are performed against the password and random text in order to generate a key which is then used to encrypt the user ID. This also serves to slow down an offline attack, which must perform the same number of operations for each password guess. However, the authorized user logging on to the system using his clear text password will not notice the increased overhead.

Rationale:

By default passwords stored in RACF are protected using a weak DES based algorithm. Using off the shelf applications and hardware, it is a relatively simple operation to reverse engineer the encryption key – RACF user ID's password – or perform a brute-force offline attack. Any user with access to RACF database may obtain the passwords for all user IDs in the system.

Impact:

KDFAES passwords require more space in the RACF database than the legacy methods require. This changed format requires updates from some other software applications for them to keep functioning under the new algorithm. Be sure that you have all the available updates before you enable KDFAES.

Refer to [z/OS Security Server RACF System Programmer's Guide: Planning Considerations for enabling KDFAES](#) for more information.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **PASSWORD PROCESSING OPTIONS:** section.

Verify the following message is present:

```
THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS KDFAES
```

Remediation:

To modify the **ALGORITHM** parameter use the RACF **SETROPTS** command:

```
SETROPTS PASSWORD (ALGORITHM(KDFAES) )
```

Note: After **ALGORITHM(KDFAES)** enablement, the existing algorithm continues to be used to evaluate a user's password or password phrase until the user's password or password phrase is changed. The first time a user's password or password phrase is changed, the new algorithm is used from that point forward.

After KDFAES is enabled, you might want to strengthen passwords immediately, rather than wait for users to change them on their normal schedule. The **PWCONVERT** operand of the **ALTUSER** command can be used. **PWCONVERT** converts a DES password and DES password history entries to KDFAES format without requiring the password to be changed.

```
ALTUSER <user-id> PWCONVERT
```

Notes:

1. Conversion assumes that the existing password and password history are in DES format. **Do not** perform the conversion if you have passwords that are masked or installation-encoded.
2. Conversion does not affect password phrases or phrase history.
3. If an older copy of your RACF database containing DES passwords is compromised and an attacker is able to decrypt a password value, a conversion to KDFAES will not protect against the attacker using that password to gain access to your system.

Default Value:

NOALGORITHM is in effect when RACF is using a newly initialized database.

Note: In this case, the algorithm in effect is determined by the **ICHDEX01** exit, with DES being the default if there is no exit installed.

References:

1. IBM z/OS RACF STIG: RACF-ES-000820

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: Specifying the encryption method for user passwords](#)
- [z/OS Security Server RACF System Programmer's Guide: Planning Considerations for enabling KDFAES](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			

1.1.7 Ensure that the SETROPTS PASSWORD(WARNING) value is set to a minimum of 5 (Automated)

Profile Applicability:

- Level 1

Description:

WARNING specifies the number of days before a password expires when RACF is to issue a warning message to the user.

Note: If you specify **WARNING**, **INITSTATS** must be in effect.

Rationale:

System users should be warned about impending password expiration to allow secure passwords to be chosen and to allow the changing of a password at a convenient time to help minimize password change impact.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ATTRIBUTES =** section.

Verify that **INITSTATS** appears.

Review the command output in the **PASSWORD PROCESSING OPTIONS:** section.

Look for the following message:

```
PASSWORD EXPIRATION WARNING LEVEL IS <nnn> DAYS.
```

Verify the value is equal to or greater than 5 days.

Remediation:

To modify the **WARNING** parameter use the RACF **SETROPTS** command:

```
SETROPTS PASSWORD (WARNING (5) )
```

Note: If you specify a **WARNING** value that exceeds the **INTERVAL** value, a warning message is issued at each logon. If you do not want the warning with each logon, specify a value for **WARNING** that is **less** than the value you specify for **INTERVAL**.

If you specify **WARNING**, **INITSTATS** must be in effect. To enable **INITSTATS** use the RACF **SETROPTS** command:

```
SETROPTS INITSTATS
```

Default Value:

The following values are in effect when RACF is using a newly initialized database:

- **INITSTATS**
- **NOWARNING**

References:

1. IBM z/OS RACF STIG: RACF-ES-000810

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Extending password and user ID processing \(PASSWORD option\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

1.1.8 Ensure that the SETROPTS RVARYPW values are secured with KDFAES (Automated)

Profile Applicability:

- Level 1

Description:

RVARY passwords are used to respond to requests to approve **RVARY** command processing, where **SWITCH** is the response to a request to switch RACF databases or change the operating mode of RACF, and **STATUS** is the response to a request to change RACF or database status from **ACTIVE** to **INACTIVE** or from **INACTIVE** to **ACTIVE**.

Rationale:

Strengthens security of **RVARY** passwords by protecting them with the KDFAES password hashing algorithm.

Impact:

The action should not be performed until all system sharing the RACF database are IPLed with the PTF for OA65905.

Notes:

- 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

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Verify the following messages are present:

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

Remediation:

To modify the **RVARYPW** parameter use the RACF **SETROPTS** command:

```
SETROPTS RVARYPW(SWITCH(XXXXX) STATUS/YYYYY) KDFAES)
```

Note: You may use your existing passwords. **SETROPTS** does not keep a history for **RVARY** passwords.

Additional Information:

[OA65905: KDFAES PROTECTION FOR RACF RVARV PASSWORDS](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			

1.1.9 Ensure SETROPTS PASSWORD(MIXEDCASE) is in effect (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS PASSWORD(MIXEDCASE) indicates that all applications on this system and those that share the RACF database support mixed-case and lowercase passwords.

Rationale:

Password composition or complexity requirements are used to increase the strength of a user-created password of a given length. For example, a complex password would need some amount of characters from all three of the following categories:

- Uppercase characters
- Lowercase characters
- Non-alphabetic characters such as numbers or special characters

By implementing this recommendation a user will be enabled to create a password with mixed-case and lowercase characters.

Impact:

SETROPTS PASSWORD(MIXEDCASE) is intended to be activated after evaluating and updating applications and implementing appropriate password syntax rules, and never deactivated.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the PASSWORD PROCESSING OPTIONS: section.

Verify the following messages are present:

```
MIXED CASE PASSWORD SUPPORT IS IN EFFECT
```

Remediation:

To enable mixed-case and lowercase passwords use the **MIXEDCASE** parameter of the RACF **SETOPTS** command:

```
SETOPTS PASSWORD(MIXEDCASE)
```

Default Value:

SETOPTS PASSWORD(NOMIXEDCASE) is in effect when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000770

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Allowing mixed-case passwords \(PASSWORD option\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			

1.1.10 Ensure SETROPTS PASSWORD(SPECIALCHARS) is in effect (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS PASSWORD(SPECIALCHARS) indicates that all applications on this system and those that share the RACF database support additional special characters in passwords.

Rationale:

Password composition or complexity requirements are used to increase the strength of a user-created password of a given length. For example, a complex password would need some amount of characters from all three of the following categories:

- Uppercase characters
- Lowercase characters
- Non-alphabetic characters such as numbers or special characters

By implementing this recommendation a user will be enabled to create a password with additional special characters.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **PASSWORD PROCESSING OPTIONS:** section.

Verify the following messages are present:

```
SPECIAL CHARACTERS ARE ALLOWED.
```

Remediation:

To enable additional special characters in passwords use the **SPECIALCHARS** parameter of the RACF **SETROPTS** command:

```
SETROPTS PASSWORD(SPECIALCHARS)
```

Default Value:

SETROPTS PASSWORD(NOSPECIALCHARS) is in effect when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000770

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Allowing special characters in passwords \(PASSWORD option\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			

1.2 System Settings

This section describes the System Settings recommendations.

1.2.1 Ensure that the SETROPTS INACTIVE value is set to a maximum of 45 (Automated)

Profile Applicability:

- Level 1

Description:

PASSWORD(INACTIVE(<nnn>)) command specifies the number of days (1 - 255) that a user ID can remain unused and still be considered valid. RACF user verification checks the number of days since the last successful time the user accessed the system against the **INACTIVE** value and, if the former is larger, revokes the user's right to use the system.

INACTIVE does not apply to Protected user IDs. Protected user IDs are protected from being revoked through inactivity. If you specify **INACTIVE**, **INITSTATS** must be in effect. If the backup database is needed but does not contain current information, some user IDs can be revoked because they appear to have been unused beyond the number of days specified on the **INACTIVE** operand.

NOINACTIVE specifies that RACF user verification is not to check user IDs against an unused-userid-interval.

Inactive user IDs are to be revoked after a period of inactivity not to exceed 45 days.

Rationale:

Inactive user IDs are vulnerable to attack because no one is watching these IDs. Revoking inactive user IDs reduces a potential compromise vector. We have chosen 45 days as our recommend threshold to align with CIS Critical Security Controls Version 8.

Impact:

This setting could potentially disable accounts for personnel that are on leave. This should be taken into account and potentially a longer period configured if this impacts local site personnel.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ATTRIBUTES =** section.

Verify that **INITSTATS** appears.

Look for the following message:

```
INACTIVE USERIDS ARE BEING AUTOMATICALLY REVOKED AFTER <nnn> DAYS.
```

Verify the value is equal to or less than 45 days.

Remediation:

To modify the **INACTIVE** parameter use the RACF **SETROPTS** command:

```
SETROPTS INACTIVE(45)
```

Notes:

1. **INACTIVE** does not apply to Protected user IDs. Protected user IDs are protected from being revoked through inactivity.
2. If the backup database is needed but does not contain current information, some user IDs can be revoked because they appear to have been unused beyond the number of days specified on the **INACTIVE** operand. For more information, see [z/OS Security Server RACF System Programmer's Guide](#).

If you specify **INACTIVE**, **INITSTATS** must be in effect. To enable **INITSTATS** use the RACF **SETROPTS** command:

```
SETROPTS INITSTATS
```

Default Value:

NOINACTIVE is in effect when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000760

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Setting the maximum and minimum change interval \(PASSWORD option\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.3 <u>Disable Dormant Accounts</u> Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.			

1.2.2 Ensure that the *STARTED* resource class is used to assign user IDs to started tasks (Automated)

Profile Applicability:

- Level 1

Description:

Started procedures have system generated job statements that do not contain the user, group, or password statements. To enable the started procedure to access the same protected resources that users and groups access, started procedures must have an associated user ID. If a user ID is not associated with the started procedure, the started procedure will not have access to the resources.

User ID can be assigned through the RACF **STARTED** class or through the **ICHRIN03** table. As it is easily auditable, does not require assembler knowledge or a system IPL for changes, we require the usage of the RACF **STARTED** class.

Rationale:

If a user ID is not associated with the started procedure, the started procedure will not have access to the resources. By default started procedures should be assigned a user ID with limited privileges to prevent otherwise undefined tasks from getting unintentional access to resources secured by RACF.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES** = section.

Verify that **STARTED** appears.

Review the command output in the **GENERIC PROFILE CLASSES** = section.

Verify that **STARTED** appears.

Review the command output in the **SETR RACLIST CLASSES** = section.

Verify that **STARTED** appears.

Request the following **DSMON** report:

```
FUNCTION SYSTEM RACSPT
```

Review the **FROM PROFILES IN THE STARTED CLASS:** section.

Verify that no entries contain:

Request IRRUT100 cross reference output and reports generated using IRRDBU00 output that will allow you to:

Verify the following catch-all profile is defined:

- A single **GENERIC** profile in the **STARTED** class named: **** or *. ***

Verify that this catch-all profile in the **STARTED** class has a **STDATA** segment with:

- A **GROUP** value that is a valid RACF group ID
- A **USER** value that is a valid RACF user ID

Verify that the RACF group specified in the **STDATA** segment **GROUP** value of the catch-all profile in the **STARTED** class:

- Does not appear on any RACF data set or general resource access list
- Does not have any segments beyond base (ex. no **OMVS** segment)

Verify that the RACF user ID specified in the **STDATA** segment **USER** value of the catch-all profile in the **STARTED** class:

- Has the **PROTECTED** attribute
- Has the **RESTRICTED** attribute
- Has the **UAUDIT** attribute
- Does not appear on any RACF data set or general resource access list
- Does not have any segments beyond base (ex. no **OMVS** segment)
- Does not have any extra system or group privileges (ex. **ROAUDIT**, **CLAUTH**, **group-JOIN**, etc.)

Remediation:

Notes:

1. RACF cannot be initialized if **ICHRIN03** is not present so even when a catch-all ****** profile in the **STARTED** class is used to assign user IDs, a dummy **ICHRIN03** is shipped with and installed by RACF.
2. For installations that have an existing **ICHRIN03** in place and want to migrate to using the **STARTED** class, a sample REXX exec is provided in member **ICHSPTCV** in **SYS1.SAMPLIB** to process the output of the RACF **DSMON** program and build RACF **RDEFINE** commands to replicate current **ICHRIN03** entries.
3. It is recommended that a minimal set of STC definitions be maintained in the **ICHRIN03**, such that an IPL can be completed and the system can be brought up in cases of RACF failure.

To activate the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(STARTED)
```

To enable generic profile checking for the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(STARTED)
```

To RACLIST the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(STARTED)
```

To create dedicated IDs for the **STDATA** segment use the RACF **ADDGROUP**, **ADDUSER**, and **CONNECT** commands:

```
ADDGROUP STGRP +
  OWNER(<group>) +
  SUPGROUP(<group>) +
  DATA('CATCH-ALL STC PROFILE GROUP')

ADDUSER STCUSER +
  OWNER(STGRP) +
  DFLTGRP(STGRP) +
  NOPASSWORD +
  RESTRICTED +
  UAUDIT +
  DATA('CATCH-ALL STC PROFILE USER')

CONNECT STCUSER +
  GROUP(STGRP) +
  OWNER(STGRP)
```

To create a catch-all **STARTED** profile use the RACF **RDEFINE** and **SETROPTS** commands:

```
RDEFINE STARTED ** +  
    UACC(NONE) +  
    DATA('CATCH-ALL TO PREVENT ICHRIN03 FALLBACK') +  
    STDATA( +  
        USER(STCUSER) +  
        GROUP(STCGRP) +  
    )  
  
SETROPTS REFRESH RACLIST(STARTED)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(<class>) +  
    DELETE ID(<non-compliant>)
```

Default Value:

- The **STARTED** class is **INACTIVE** when RACF is using a newly initialized database.
- The **ICHRIN03** started procedures table is used to associate the names of started procedures with user IDs.

References:

1. IBM z/OS RACF STIG: RACF-ES-000720

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: Setting up the STARTED class](#)
- [z/OS Security Server RACF Security Administrator's Guide: Started procedure considerations](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 <u>Allowlist Authorized Software</u> Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.			
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	5.5 <u>Establish and Maintain an Inventory of Service Accounts</u> Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			

1.2.3 Ensure user propagation is controlled (Automated)

Profile Applicability:

- Level 1

Description:

Batch jobs that are user-submitted to the operating system should inherit the user ID of the submitter. This will identify the batch job with the user for the purpose of accessing resources. In some environments, such as CICS jobs submitted without the **USER** operand specified on the **JOB** statement, that job runs under a user ID other than the user submitting the job, in this case, the CICS user ID. This situation presents a security violation in that the issuer of the job will inherit the authority of the CICS user ID. The **PROPCNTL** Class was designed to prevent this from occurring. Utilize propagation control (**PROPCNTL**) for system-level address spaces that submit jobs on behalf of users.

Rationale:

Jobs submitted without the **USER** operand specified on the **JOB** statement which run under a user ID other than the user submitting the job present a security violation in that the issuer of the job will inherit the authority of the user ID and may allow access to resources they would not ordinarily have access to.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **PROPCNTL** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **PROPCNTL** appears.

Request reports generated using IRRDBU00 output that will allow you to:

Verify that all user IDs that require propagation control have a dedicated profile in the **PROPCNTL** class.

Remediation:

To activate the **PROPCNTL** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT (PROPCNTL)
```

To RACLIST the **PROPCNTL** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST (PROPCNTL)
```

To create a **PROPCNTL** profile use the RACF **RDEFINE** and **SETROPTS** commands:

```
RDEFINE PROPCNTL <user-id>  
  
SETROPTS REFRESH RACLIST (PROPCNTL)
```

Note:

1. For a profile in the **PROPCNTL** class, RACF checks only for the presence or absence of a profile in this class. If a profile exists for a particular user ID, user ID propagation does not occur for that user ID.
2. RACF performs no logging and issues no messages for profiles in the **PROPCNTL** class.
3. **PROPCNTL** profiles only control propagation for local jobs. If the installation uses **&RACLNDE** for its remote nodes, only the **PROPCNTL** profiles are necessary. For more information on the use of **&RACLNDE**, see [Defining nodes as local input sources](#). If the installation uses **NODES** profiles, it must also use them to control propagation (see [Controlling user ID propagation in an NJE environment](#)).
4. If you have controlled a user ID using the **PROPCNTL** class, and that user wants to submit a batch job to run from that user ID, the **JOB** statement must contain both the user ID and proper password. For example, if user **A** submits a job with **USER=A**, **PASSWORD=password** must also be specified. However, if a different user wants to submit a job using the controlled user ID, that user can either specify the user ID and password as above, or use the facilities provided by the **SURROGAT** class and just specify the user ID. For example, if you controlled user **A** using the **PROPCNTL** class, user **B** could submit a job, specifying only **USER=A** with the appropriate **SURROGAT** authorization.

Default Value:

The **PROPCNTL** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000250

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling user ID propagation in a local environment](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	6.7 <u>Centralize Access Control</u> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.			

1.2.4 Ensure that started tasks defined with the *TRUSTED* attribute are justified (Manual)

Profile Applicability:

- Level 1

Description:

The **TRUSTED** attribute allows a started task to bypass RACF checking. It is vital that this attribute is **not** granted to unauthorized started tasks which could then obtain unauthorized access to the system.

Rationale:

Unauthorized started tasks obtaining unauthorized access to the system could result in the compromise of the confidentiality, integrity, and availability of the operating system, RACF, or customer data.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACSPT

Review the report and for any profiles that have **YES** in the **TRUSTED** column:

Verify that the **TRUSTED** attribute assignment is justified.

Note: Examples of **TRUSTED** assignment justification includes, but is not limited to:

- The started task or address space creates or accesses a wide variety of unpredictably named data sets.
- Insufficient authority to an accessed resource might risk an unsuccessful IPL or other critical system functionality error.
- It is listed as a requirement by the product documentation or vendor.

Remediation:

To remove the **TRUSTED** from a **STARTED** profile use the RACF **RALTER** and **SETROPTS** commands:

```
RALTER STARTED <profile> +  
    STDATA (NOTRUSTED)  
  
SETROPTS REFRESH RACLIST (STARTED)
```

IBM provides guidance on z/OS started tasks and address spaces that require **TRUSTED** in the MVS Initialization and Tuning Reference, linked in the additional information section.

Default Value:

NOTRUSTED is the default for **STARTED** profiles.

References:

1. IBM z/OS RACF STIG: RACF-ES-000130

Additional Information:

[MVS Initialization and Tuning Reference: Assigning the RACF TRUSTED attribute](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			

1.2.5 Ensure that the OPERCMDS resource class is enabled (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS CLASSACT(OPERCMDS) specifies that the class **OPERCMDS** will have RACF protection is to be in effect for it.

These values become effective immediately after the command **SETROPTS CLASSACT(OPERCMDS)** is issued.

Rationale:

If no setting is found, the system-wide defaults will be used. The improper setting of any subsystem fields, individually or in combination with another, can compromise the security of the processing environment. Failure to define access to z/OS system commands could result in unauthorized personnel issuing sensitive system commands. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **OPERCMDS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **OPERCMDS** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **OPERCMDS** appears.

Remediation:

To activate the **OPERCMDS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT (OPERCMDS)
```

To enable generic profile checking for the **OPERCMDS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC (OPERCMDS)
```

To RACLIST the **OPERCMDS** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST (OPERCMDS)
```

Default Value:

The **OPERCMDS** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000100

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

1.2.6 Ensure that the CONSOLE resource class is enabled (Automated)

Profile Applicability:

- Level 1

Description:

MCS consoles can be used to issue operator commands. Failure to control access to MCS consoles could result in unauthorized personnel issuing sensitive operator commands.

Rationale:

Failure to control access to MCS consoles could result in unauthorized personnel issuing sensitive operator commands. This may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **CONSOLE** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **CONSOLE** appears.

Remediation:

To activate the **CONSOLE** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT (CONSOLE)
```

To RACLIST the **CONSOLE** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST (CONSOLE)
```

Default Value:

The **CONSOLE** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000110

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

1.2.7 Ensure that the FACILITY resource class is enabled (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS CLASSACT(FACILITY) specifies that the class **FACILITY** class is active and that RACF protection is to be in effect for it.

These values become effective immediately after the command **SETROPTS CLASSACT(FACILITY)** and **SETROPTS RACLIST(FACILITY)** are issued.

Rationale:

If no setting is found, the system-wide defaults will be used. The improper setting of any subsystem fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the RACF options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **FACILITY** appears.

Remediation:

Note: The **FACILITY** class can be used for a wide variety of purposes depending on the products installed on your system. Care must be taken when enabling the class for the first time.

To activate the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FACILITY)
```

To enable generic profile checking for the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FACILITY)
```

To RACLIST the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FACILITY)
```

Default Value:

The **FACILITY** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000090

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Planning for profiles in the FACILITY class](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

1.2.8 Ensure that inapplicable PPT entries have been invalidated (Manual)

Profile Applicability:

- Level 1

Description:

The program properties table (PPT) contains entries for special attributes of programs. One of these entries indicates whether or not the program is allowed to bypass datasets password protection (PPTNOPAS), or access key protected storage.

Rationale:

If invalid or inapplicable PPT entries exist, a venue is provided for the introduction of Trojan Horse modules with security bypass capabilities.

Audit:

Request the following DSMON report:

```
FUNCTION SYSTEM SYSPPT
```

Verify that each privileged PROGRAM NAME entry is valid.

Note: To determine if a program entry is valid issue the following TSO command:

```
ISRDDN LOAD <privileged-module>
```

If the return message is Load Failed the entry can be considered invalid.

Remediation:

Although you cannot remove entries from the PPT, you can create the *effect* of removing an entry from the PPT by defining the program name in the PARMLIB member SCHEDxx without special attributes. This statement overrides the existing entry in the PPT, and causes any APF-authorized program with a matching name to run with the same attributes as a problem program.

Update the SCHEDxx member:

```
PPT PGMNAME(<privileged-module>)
```

Notes:

- If you specify more than one PPT statement with the same program name, the systems accept only the first occurrence of the name and issues error message IEF732I for all subsequent occurrences of that name.
- When referring to a DD statement, the system does not honor requests for special properties as defined in the PPT.

Default Value:

No IBM-supplied default for SCHEDxx.

References:

1. IBM z/OS RACF STIG: RACF-OS-000290

Additional Information:

- [MVS Initialization and Tuning Reference: IBM-supplied program properties table \(PPT\) values](#)
- [MVS Initialization and Tuning Reference: Statements and parameters for SCHEDxx](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>2.6 Allowlist Authorized Libraries</u> Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.			
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

1.2.9 Ensure that LNKAUTH=APFTAB is specified in the IEASYSxx members currently active parmlib data sets (Automated)

Profile Applicability:

- Level 1

Description:

Specifying **LNKAUTH=APFTAB** in the **IEASYSxx** member(s) currently active **PARMLIB** data set(s) allows libraries other than those designated as **APF** to contain authorized modules by adding to this list all libraries in the **LNKLST** concatenation when accessed as part of the linklist concatenation.

Rationale:

Failure to specify **LNKAUTH=APFTAB** allows libraries other than those designated as **APF** to contain authorized modules which could bypass security and violate the integrity of the operating system environment. This expanded authorization list inhibits the ability to control exclusion of unauthorized modules.

Audit:

Issue the following z/OS console command:

```
D IPLINFO
```

Use the following message to determine the **xx** suffix values for active **PARMLIB IEASYSxx** members:

```
IEASYS LIST=(xx, ..)
```

Check the current **PARMLIB IEASYSxx** parameters and look for the **LNKAUTH** parameter.

Verify that **LNKAUTH=APFTAB**.

Remediation:

Update non-compliant entries in **PARMLIB IEASYSxx** members and re-IPL the system.

Default Value:

LNKAUTH=LNKLST

References:

1. IBM z/OS RACF STIG: RACF-OS-000300

Additional Information:

[MVS Initialization and Tuning Reference: Overview of IEASYSxx parameters](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.6 <u>Allowlist Authorized Libraries</u> Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.			
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

1.2.10 Ensure that the CONSOLxx members are configured (Manual)

Profile Applicability:

- Level 1

Description:

MCS consoles can be used to issue operator commands. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Rationale:

Failure to control access to MCS consoles could result in unauthorized personnel issuing sensitive operator commands.

Audit:

Review the current **PARMLIB CONSOLxx** members.

Verify that the **DEFAULT** statement for each **CONSOLxx** member specifies **LOGON(REQUIRED)**.

Note: At the discretion of the site ISSO **LOGON(AUTO)** may be used. If **LOGON(AUTO)** is used **verify** that the console user IDs are defined with minimal access.

Verify that the **CONSOLE** statement for each console:

- Assigns a unique name using the **NAME** parameter.
- Specifies a default authority of **INFO** using the **AUTH** parameter. Exceptions:
 - The **AUTH** parameter is not valid for consoles defined with **UNIT(PRT)**.
 - The system console is allowed to use **AUTH** value of **MASTER**.

Note: The site should be able to determine the system consoles.

Remediation:

Update non-compliant entries in **PARMLIB CONSOLxx** members and re-IPL the system.

Default Value:

No IBM-supplied default for **CONSOLxx**. If no **CONSOLxx** member is supplied, the system messages go to the system console and the system uses the defaults for the other values in **CONSOLxx**:

- **AUTH(INFO)** is the default for all consoles except the system console, which is forced to be **AUTH(MASTER)**.
- If your operator specifies **CON=NONE**, or if you do not **NAME** the system console in **CONSOLxx**, MVS tries to use the name of the system to which the console is attached as the name of the system console, as long as that name is unique and cannot be confused with a device number that the system can use. If you do not name the system console in **CONSOLxx**, use a system name that cannot be confused with a device number that the system can use.
- **LOGON(OPTIONAL)**

References:

1. IBM z/OS RACF STIG: RACF-ES-000680

Additional Information:

[MVS Initialization and Tuning Reference: CONSOLxx \(console configuration definition\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			

1.2.11 Ensure that no expired digital certificates are used (Automated)

Profile Applicability:

- Level 1

Description:

When an X.509 certificate stored in RACF has the **TRUST** or **HIGHTRUST** status, it can be used by RACF for its intended purpose (map to a user ID, or treat as a trusted certificate authority or trusted site).

Rationale:

X.509 certificates expire to prevent prolonged use of potentially compromised private keys and outdated cryptographic algorithms, ensuring that security infrastructure remains up-to-date against evolving threats and that the information within the certificate remains trustworthy over time.

Impact:

The overall impact depends on the X.509 certificate type:

- For a personal certificate, a trusted certificate can be used to authenticate a user ID.
- For a certificate-authority certificate, a trusted certificate is one that can be used to authenticate a user's certificate by indicating that the entity identified in the certificate (for example, the certificate authority) can issue certificates that this system honors. This implies that a user can gain access to the system based on the information contained in the certificate if the user's certificate was signed by a trusted certificate authority.
- For site certificates, a trusted certificate is one indicating that the entity identified in the certificate (for example, the site) can gain access to the system based on information contained within the certificate. Because the authority that issued the certificate might not be defined to the system as a certificate authority, this certificate information might not be able to be authenticated.

Audit:

Note: Certificates used for password enveloping can continue to be used after expiring and should **not** be removed if password enveloping is still active.

Request reports generated using **IRRDBU00** output that will allow you to:

- **Verify** that each certificate with a **TRUST** or **HIGHTRUST** status is not expired.

Alternatively, if IBM Health Checker for z/OS is installed and active, you can request the **HZSPRINT** output for:

```
CHECK (IBMRACF,RACF_CERTIFICATE_EXPIRATION)
```

Verify that the health check returns this message:

```
IRRH277I No exceptions are detected. Expired certificates that are not  
trusted or are associated with only a virtual key ring are not exceptions
```

Remediation:

Note: Certificates used for password enveloping can continue to be used after expiring and should **not** be removed if password enveloping is still active.

Follow site procedures for certificate life cycle management.

Default Value:

If no trust value is specified on the **RACDCERT ADD** command, the following processing will take place to determine the trust status:

- If the certificate's signature can be verified, the certificate has not expired, and the certificate's validity date range is within the validity date range of the certifying authority's certificate, the trust status is set to the trust status of the certifying authority's certificate. For self-signed certificates the certificate being added is set to **TRUST** by default. If the self-signed certificate has already been added, its trust status is not changed.
- If the certificate has expired, has an incorrect validity date range, or cannot be verified because it either has an unknown encryption algorithm or RACF cannot locate its certifying authority's certificate, the status is set to **NOTRUST** by default.
- If the trust status is to be set from the status of the certifying certificate and the certifying certificate is **HIGHTRUST**, the status will be **TRUST**.

References:

1. IBM z/OS RACF STIG: RACF-CE-000020

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: RACF and digital certificates](#)
- [IBM Health Checker for z/OS: RACF_CERTIFICATE_EXPIRATION](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

1.2.12 Ensure that the SETROPTS RVARYPW are set to non-default values (Automated)

Profile Applicability:

- Level 1

Description:

The **SETROPTS RVARYPW([SWITCH(*switch-pw*)][STATUS(*status-pw*)])** command specifies the passwords that the operator is to use to respond to requests to approve **RVARY** command processing, where **switch-pw** is the response to a request to switch RACF databases or change the operating mode of RACF, and **status-pw** is the response to a request to change RACF or database status from **ACTIVE** to **INACTIVE** or from **INACTIVE** to **ACTIVE**. Different passwords can be specified for each response.

Note: **NO** is not a valid password for either **SWITCH** or **STATUS**.

Rationale:

Failure to change the documented default values will allow any general user to change the status of the RACF database.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Verify the following messages are present:

```
INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.  
INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.
```

Remediation:

To modify the **RVARYPW** values use the RACF **SETROPTS** command:

```
SETROPTS RVARYPW(SWITCH(<password>))  
SETROPTS RVARYPW(STATUS(<password>))
```

Default Value:

When RACF is first initialized, the **RVARYPW SWITCH** and **STATUS** passwords are both set to **YES**.

References:

1. IBM z/OS RACF STIG: RACF-ES-000550

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Setting the RVARYPW option](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

1.2.13 Ensure that RACF default user ID IBMUSER is disabled (Automated)

Profile Applicability:

- Level 1

Description:

The default **IBMUSER** user ID is intended for use only during the initial RACF installation process.

Rationale:

After installation, the **IBMUSER** user ID should be revoked so that it cannot be used by unauthorized users.

Audit:

Request reports generated using **IRRDBU00 output that will allow you to:**

Verify That the **IBMUSER** user ID:

- Has the **REVOKE** status
- Has the **PROTECTED** attribute
- Has the **RESTRICTED** attribute
- Has the **UAUDIT** attribute
- Does not appear on any RACF data set or general resource access list
- Does not have any segments beyond base (ex. no **OMVS** segment)
- Does not have any extra system or group privileges (ex. **SPECIAL**, **OPERATIONS**, **group-JOIN**, etc.)

Remediation:

To adjust **IBMUSER** properties use the **ALTUSER** and **CONNECT** commands:

```
ALTUSER IBMUSER +
      NOPASSWORD +
      RESTRICTED +
      UAUDIT +
      REVOKE +
      NOSPECIAL +
      NOAUDIT +
      NOOPERATIONS +
      NOROAUDIT +
      NOTSO +
      NOOMVS +
      NOCICS

CONNECT IBMUSER +
      GROUP(group) +
      AUTHORITY(USE) +
      NOAUDITOR +
      NOOPERATIONS +
      NOSPECIAL
```

To remove **IBMUSER** from an access list entry use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(<class>) +
      DELETE ID(IBMUSER)
```

Default Value:

NOREVOKE is in effect for **IBMUSER** when RACF is using a newly initialized database.

Additional Information:

[IBM Health Checker for z/OS: RACF IBMUSER REVOKED](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

1.3 User Attributes

This section describes the User Attributes recommendations.

1.3.1 Ensure that the use of RACF SPECIAL attribute is justified (Manual)

Profile Applicability:

- Level 1

Description:

The **SPECIAL** user attribute allows full authorization to modify all profiles in RACF database and allows the user to perform all RACF functions, except those requiring **AUDITOR** or **ROAUDIT** attributes. The **group-SPECIAL** attribute allows decentralized RACF control of datasets and resources. In cases where the scope of authority granted to a **group-SPECIAL** Administrator has an impact on system security, the installation needs to be fully aware and approve its use. This privilege should be limited to the security group and administrators because of the extreme control that these users have.

Rationale:

Users with **SPECIAL** privilege can alter any profile and give themselves permissions to alter data, including logging and audit data.

Audit:

Request the following **DSMON** report:

```
FUNCTION  SYSTEM  RACUSR
```

Review the **SPECIAL** column under the **ATTRIBUTE TYPE** grouping.

Verify when **SYSTEM** or **GROUP** appears if the assignment is justified for the user.

Remediation:

To remove the **SPECIAL** attribute use the RACF **ALTUSER** command:

```
ALTUSER <user-id> NOSPECIAL
```

To remove **group-SPECIAL** authority use the RACF **CONNECT** command:

```
CONNECT <user-id> +  
        GROUP(<group>) +  
        NOSPECIAL
```

Default Value:

The default user ID **IBMUSER** is assigned system **SPECIAL** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000720

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: The SPECIAL attribute](#)
- [z/OS Security Server RACF Security Administrator's Guide: Suggestions for assigning user attributes](#)
- [z/OS Security Server RACF Security Administrator's Guide: Suggestions for assigning group authorities](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			

1.3.2 Ensure that SYS1.UADS contains only recovery user IDs (Manual)

Profile Applicability:

- Level 1

Description:

SYS1.UADS is a dataset where user IDs are be maintained with applicable password information for whenever RACF is not functional.

Rationale:

If an unauthorized user has access to **SYS1.UADS** they could enter their user ID and password into the **SYS1.UADS** dataset and could give themselves access to the system.

Audit:

Issue the following TSO command:

```
ACCOUNT
```

Issue the following **ACCOUNT** sub-command to list all entries in **SYS1.UADS**:

```
LIST (*)
```

Verify that only recovery IDs are defined in **SYS1.UADS**.

If there are recovery IDs defined in **SYS1.UADS, request **IRRUT100** cross reference output and reports generated using **IRRDBU00** output that will allow you to:**

Verify that the recovery user IDs defined in **SYS1.UADS** have a paired RACF user ID with limited privileges:

- User ID has the **PROTECTED** attribute
- User ID has the **RESTRICTED** attribute
- User ID has the **UAUDIT** attribute
- User ID has been revoked
- User ID does not appear on any RACF data set or general resource access list
- User ID does not have any segments beyond base (ex. no **OMVS** segment)
- User ID does not have any extra system or group privileges (ex. **ROAUDIT**, **CLAUTH**, **group-JOIN**, etc.)

Remediation:

To remove a user ID from **SYS1.UADS** use the TSO **ACCOUNT-DELETE** subcommand:

```
ACCOUNT  
DELETE (<user-id>)  
END
```

Use the **RACONVRT** command if needed as an aid in converting users from **SYS1.UADS** to the RACF database:

```
RACONVRT INCLUDE USERID(userid)
```

Notes:

- If RACF is installed and active, you require RACF **SPECIAL** authority to issue the command.
- **RACONVRT** generates the RACF commands needed to update or create RACF user profiles, and places these commands into members of a partitioned data set. This data set, **<prefix>.IKJ.RACONVRT.CLIST**, contains the commands necessary to convert to the RACF data base. **RACONVRT** creates, but does not execute the RACF commands; therefore, you can edit and change the data set's members to customize the conversion process before issuing the RACF commands.

To modify RACF entries for recovery user IDs use the RACF **ALTUSER** or **CONNECT** commands:

```
ALTUSER <user-id> +  
    NOPASSWORD +  
    RESTRICTED +  
    UAUDIT +  
    REVOKE +  
    NOSPECIAL +  
    NOAUDIT +  
    NOOPERATIONS +  
    NOROAUDIT +  
    NOTSO +  
    NOOMVS +  
    NOCICS  
  
CONNECT <user-id> +  
    GROUP(<group>) +  
    AUTHORITY(USE) +  
    NOAUDITOR +  
    NOOPERATIONS +  
    NOSPECIAL
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(<class>) +  
    DELETE ID(<non-compliant>)
```

Default Value:

SYS1.UADS has no user IDs defined.

References:

1. IBM z/OS RACF STIG: RACF-ES-000040

Additional Information:

- [z/OS TSO/E Customization: Converting to the RACF data base](#)
- [z/OS TSO/E Customization: Maintaining UADS for recovery mode](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			

1.3.3 Ensure that MCS console user IDs are protected (Manual)

Profile Applicability:

- Level 1

Description:

MCS consoles can be used to issue operator commands. When using the **LOGON(AUTO)** control, a user with the name of the MCS console will be used for access checking.

Rationale:

Failure to control access to MCS consoles could result in unauthorized personnel issuing sensitive operator commands.

Audit:

Review the current **PARMLIB CONSOLxx** members.

For each console name found request **IRRUT100** cross reference output and reports generated using **IRRDBU00** output that will allow you to:

Verify that the **<console-name>** has been defined in RACF as a user ID with limited privileges:

- Have the **PROTECTED** attribute
- Have the **RESTRICTED** attribute
- Does not have any segments beyond base (ex. no **OMVS** segment)
- Does not have any extra system or group privileges (ex. **ROAUDIT**, **CLAUTH**, **group-JOIN**, etc.)
- Does not appear on any RACF data set or general resource access lists.
Exceptions are:
 - A paired **MVS.MCSOPER.<console-name>** profile in the **OPERCMDs** class
 - A paired **<console-name>** profile in the **CONSOLE** class

Note: If **LOGON(AUTO)** is specified in the currently active **CONSOLxx** parmlib member additional access may be required. Permissions for the console userids or console group may be given to the following resources at the discretion of the site:

Class	Resource	Access
OPERCMDs	MVS.CONTROL	READ
OPERCMDs	MVS.DISPLAY	READ
OPERCMDs	MVS.MONITOR	READ
OPERCMDs	MVS.STOPMN	READ

Remediation:

To create dedicated IDs for consoles named in **CONSOLxx** use the RACF **ADDGROUP**, **ADDUSER**, and **CONNECT** commands:

```
ADDGROUP CONGRP +
    OWNER(<group>) +
    SUPGROUP(<group>) +
    DATA('DEFAULT CONSOLE OWNING GROUP')

ADDUSER <console-name> +
    OWNER(CONGRP) +
    DFLTGRP(CONGRP) +
    NOPASSWORD +
    RESTRICTED +
    DATA('MCS CONSOLE ID')

CONNECT <console-name> +
    GROUP(CONGRP) +
    OWNER(CONGRP)
```

To create a paired profiles in the **OPERCMDS** and **CONSOLE** classes use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE OPERCMDS MVS.MCSOPER.<console-name> +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('EXTENDED MCS CONSOLE ACCESS') +
    NOWARNING

PERMIT OPERCMDS MVS.MCSOPER.<console-name> +
    ACCESS(READ) ID(<console-name>)

RDEFINE CONSOLE <console-name> +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    NOWARNING

PERMIT CONSOLE <console-name> +
    ACCESS(READ) ID(<console-name>)
```

Notes:

1. Depending on the RACF class settings you may be required to issue a RACF **SETROPTS REFRESH** command for updates to be effective.
2. You cannot specify the **WHEN** operand on the **RDEFINE** and **RALTER** commands for profiles in the **CONSOLE** class.
3. After you define a console in the **CONSOLE** class and protect it with a **UACC of NONE**, no one can log on to the console until you grant users access authority to the console profile.

Default Value:

No IBM-supplied default for **CONSOLxx**. If no **CONSOLxx** member is supplied, the system messages go to the system console and the system uses the defaults for the other values in **CONSOLxx**:

- **LOGON(OPTIONAL)**

References:

1. IBM z/OS RACF STIG: RACF-ES-000690

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: Protecting consoles](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

1.3.4 Ensure that STARTED resource class profiles assign PROTECTED user IDs (Automated)

Profile Applicability:

- Level 1

Description:

PROTECTED user IDs are protected from being used to logon to the system and from being revoked through inactivity or unsuccessful attempts to access the system using incorrect passwords and password phrases. However, they can be revoked using the **ALTUSER REVOKE** command.

Rationale:

We recommend assigning **PROTECTED** user IDs to z/OS UNIX, and to the UNIX daemons, started procedures, applications, servers or subsystems associated with z/OS UNIX, to minimize their exposure to inadvertent or malicious misuse or revocation.

Impact:

A **PROTECTED** user ID cannot be used to enter the system by any method that uses, a supplied password, such as TSO logon, CICS signon, PassTicket authentication, z/OS UNIX rlogin, batch job submission when a password is specified using the **PASSWORD** parameter of the **JOB** statement, or by supplying a password phrase.

Before assigning the **PROTECTED** attribute to a user ID, you should ensure that the user ID will not be used in any situation where specification of a password, PassTicket, or password phrase is required.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACSPT

Use the **ASSOCIATED USER** column to generate the list of user IDs to review.

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that the started task RACF user ID:

- Has the **PROTECTED** attribute

Remediation:

To make a user ID **PROTECTED** use the RACF **ALTUSER** command:

```
ALTUSER <user-id> +  
      NOPASSWORD +  
      NOPHRASE +  
      NOOIDCARD
```

Default Value:

When the **ADDUSER** command is issued to create a user ID and you specify **NOOIDCARD** (or you allow this option to default), do not specify **PHRASE**, and if you specify **NOPASSWORD** or you omit the **PASSWORD** keyword, by default the ID will be created with the **PROTECTED** attribute.

References:

1. IBM z/OS RACF STIG: RACF-ES-000720

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Defining protected user IDs](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			

1.3.5 Ensure that the assignment of RACF CLAUTH authority is justified (Automated)

Profile Applicability:

- Level 1

Description:

Users receive the **CLAUTH** attribute on a *class-by-class* basis. If a user has the **CLAUTH** attribute in a class, or in a class that shares the same POSIT value in the class descriptor table (CDT), RACF allows the user to utilize a subset of commands for delegated administration of profiles in that class.

Rationale:

Users with **CLAUTH** privilege have a delegated control over profiles in the specified class.

Audit:

Request reports generated using **IRRDBU00** output that will allow you to identify user IDs with **CLAUTH** authority.

Verify if the assignment is justified for the user.

Remediation:

To remove **CLAUTH** authority the RACF **ALTUSER** command:

```
ALTUSER <user-id> NOCLAUTH(<class-name>)
```

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: The CLAUTH \(class authority\) attribute](#)
- [z/OS Security Server RACF Security Administrator's Guide: The CLAUTH attribute \(Summary of authorities and commands\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			

2 Authorization and Access Control Management

This section provides guidance on how to ensure that users only have access to the system resources necessary for their role.

Authorization is dependent on identification and authentication.

2.1 Data Protection

2.1.1 Ensure that access to DASDVOL and STGADMIN resources are controlled (Automated)

Profile Applicability:

- Level 1

Description:

Users responsible for direct access storage device (DASD) administration must be given access to perform necessary functions through profiles in the **DASDVOL** class (for **non-SMS** volumes) as well as **STGADMIN** prefixed profiles in the **FACILITY** and **XFACILIT** classes for **SMS** managed volumes.

Rationale:

Failure to properly control and log access to DASD administration resources reduces the integrity and availability of the operating system environment, as well as increases the risk for compromise of confidential data.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES** = section.

Verify that **DASDVOL** and **FACILITY** and **XFACILIT** appears.

Review the command output in the **GENERIC PROFILE CLASSES** = section.

Verify that **DASDVOL** and **FACILITY** and **XFACILIT** appears.

Review the command output in the **SETR RACLIST CLASSES** = section.

Verify that **DASDVOL** and **FACILITY** and **XFACILIT** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that:

- The **DASDVOL** entry has:
 - **-- GLOBAL INACTIVE -- or -- NO ENTRIES --**
- The **FACILITY** entry has:
 - **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering **IGG**, **IHJ**, and **STGADMIN** prefixed resources
- The **XFACILIT** entry has:
 - **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering **STGADMIN** prefixed resources

Request reports generated using IRRDBU00 output that will allow you to:

Verify the following catch-all profiles are defined:

- A **GENERIC** profile in the **DASDVOL** class named: ******
- A **GENERIC** profile in the **FACILITY** class named: **STGADMIN.** or STGADMIN.* or STGADMIN.*.****
- A **GENERIC** profile in the **FACILITY** class named: **STGADMIN.ADR.STGADMIN.** or STGADMIN.ADR.STGADMIN.* or STGADMIN.ADR.STGADMIN.*.****
- A **GENERIC** profile in the **FACILITY** class named: **STGADMIN.ARC.ENDUSER.** or STGADMIN.ARC.ENDUSER.* or STGADMIN.ARC.ENDUSER.*.****
- A **GENERIC** profile in the **XFACILIT** class named: **STGADMIN.** or STGADMIN.* or STGADMIN.*.****
- A **GENERIC** profile in the **XFACILIT** class named: **STGADMIN.IGG.DELAUDIT.** or STGADMIN.IGG.DELAUDIT.* or STGADMIN.IGG.DELAUDIT.*.****

Verify that a fully qualified **IGG.CATLOCK** profile is defined in the **FACILITY** class that:

- Has **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Storage Administrators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Verify that any **IHJ.CHKPT** prefixed profiles defined in the **FACILITY** class:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Storage Administrators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Note: **IHJ.CHKPT** prefixed profiles are *optional* profiles a site may define for control of checkpoint data sets on shared DASD volumes. This recommendation *does not* require these profiles be defined, but does provide recommendations *if* they are defined.

Verify that the `STGADMIN.ADR.STGADMIN` catch-all profile in the `FACILITY` class:

- Has `UACC` of `NONE`
- Is not in `WARNING` mode
- `AUDIT` a minimum of `SUCCESS(READ)` and `FAILURES(READ)`
- `ID(*)` is not used to grant access
- `READ` and higher permits are restricted to:
 - Storage Administrators
 - IDs authorized to access these resources at this level

Verify that all `STGADMIN.ARC.ENDUSER` prefixed profiles in the `FACILITY` class:

- Have `UACC` of `NONE`
- Are not in `WARNING` mode
- `AUDIT` a minimum of `FAILURES(READ)`
- `ID(*)` is not used to grant access greater than `READ`
- `UPDATE` and higher permits are restricted to:
 - Storage Administrators
 - IDs authorized to access these resources at this level

Verify that the `STGADMIN.IGG.DELAUDIT.**` profile in the `XFACILIT` class:

- Have `UACC` of `NONE`
- Are not in `WARNING` mode
- `AUDIT` a minimum of `SUCCESS(READ)` and `FAILURES(READ)`
- `ID(*)` is not used to grant access
- `READ` and higher permits are restricted to:
 - Storage Administrators
 - IDs authorized to access these resources at this level

Verify that any fully qualified `STGADMIN.IGG.DEFDEL.UALIAS` profile in the `FACILITY` class:

- Has `UACC` of `NONE`
- Is not in `WARNING` mode
- `AUDIT` a minimum of `SUCCESS(READ)` and `FAILURES(READ)`
- `ID(*)` is not used to grant access
- `READ` and higher permits are restricted to:
 - Security Administrators
 - Storage Administrators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Note: `STGADMIN.IGG.DEFDEL.UALIAS` is an *optional* profiles a site may define to grant delegated access to define or delete an alias related to a usercatalog, for example to allow security personnel to add a catalog alias when provisioning a new ID. This recommendation *does not* require this profile to be defined, but does provide recommendations *if* it is defined.

Verify that all profiles in the `DASDVOL` class, as well as all remaining `STGADMIN` prefixed profiles in the `FACILITY` and `XFACILIT` classes:

- Have `UACC` of `NONE`
- Are not in `WARNING` mode
- `AUDIT` a minimum of `FAILURES(READ)`
- `ID(*)` is not used to grant access
- `READ` and higher permits are restricted to:
 - Storage Administrators
 - IDs authorized to access these resources at this level

Note: If the site is using DFSMSrmm for tape management, they may choose to permit access to DFSMSrmm resources aligned with [DFSMSrmm Implementation and Customization Guide](#) guidance. In that case refer to the correct version of the Guide for the system's level of support when evaluating permits to `STGADMIN.EDG` prefixed profiles in the `FACILITY` class.

Remediation:

To activate RACF classes use the RACF `SETROPTS` command:

```
SETROPTS CLASSACT(DASDVOL)
SETROPTS CLASSACT(FACILITY)
SETROPTS CLASSACT(XFACILIT)
```

To enable generic profile checking for a RACF class use the RACF `SETROPTS` command:

```
SETROPTS GENERIC(DASDVOL)
SETROPTS GENERIC(FACILITY)
SETROPTS GENERIC(XFACILIT)
```

To RACLIST a RACF class use the RACF `SETROPTS` command:

```
SETROPTS RACLIST(DASDVOL)
SETROPTS RACLIST(FACILITY)
SETROPTS RACLIST(XFACILIT)
```

To create catch-all profiles use the RACF `RDEFINE` command:

```

RDEFINE DASDVOL ** +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('CATCH-ALL PROFILE')

PERMIT ** CLASS(DASDVOL) +
    ACCESS(ALTER) ID(STGADMIN)

SETROPTS REFRESH RACLIST(DASDVOL)

RDEFINE FACILITY IGG.CATLOCK +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('CONTROLS WHO CAN LOCK/UNLOCK CATALOGS AND WHO CAN ACCESS LOCKED
CATALOGS')

PERMIT IGG.CATLOCK CLASS(FACILITY) +
    ACCESS(ALTER) ID(STGADMIN SYSPROG)

RDEFINE FACILITY STGADMIN.** +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('STORAGE ADMINISTRATION CATCH-ALL PROFILE')

PERMIT STGADMIN.** CLASS(FACILITY) +
    ACCESS(ALTER) ID(STGADMIN)

RDEFINE FACILITY STGADMIN.ADR.STGADMIN.** +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    DATA('DFSMSDSS ADMINISTRATOR KEYWORD CATCH-ALL PROFILE')

PERMIT STGADMIN.ADR.STGADMIN.** CLASS(FACILITY) +
    ACCESS(ALTER) ID(STGADMIN)

RDEFINE FACILITY STGADMIN.ARC.ENDUSER.** +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('DFSMSHSM USER COMMANDS')

PERMIT STGADMIN.ARC.ENDUSER.** CLASS(FACILITY) +
    ACCESS(READ) ID(*)

RDEFINE FACILITY STGADMIN.IGG.DEFDEL.UALIAS +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    DATA('DEFINE OR DELETE AN ALIAS RELATED TO A USERCATALOG WITHOUT
FURTHER AUTHORIZATION CHECKING')

PERMIT STGADMIN.IGG.DEFDEL.UALIAS CLASS(FACILITY) +
    ACCESS(ALTER) ID(SECADMIN STGADMIN SYSPROG)

SETROPTS REFRESH RACLIST(FACILITY)

RDEFINE XFACILIT STGADMIN.** +

```

```

        UACC(NONE) +
        AUDIT(FAILURES(READ)) +
        DATA('STORAGE ADMINISTRATION CATCH-ALL PROFILE')

PERMIT STGADMIN.** CLASS(XFACILIT) +
        ACCESS(ALTER) ID(STGADMIN)

RDEFINE XFACILIT STGADMIN.IGG.DELAUDIT.** +
        UACC(NONE) +
        AUDIT(ALL(READ)) +
        DATA('ACCESS TO DELETE DATA SET CATALOGED IN SPECIFIED CATALOG
WITHOUT ALTER ACCESS TO DATA SET')

PERMIT STGADMIN.IGG.DELAUDIT.** CLASS(XFACILIT) +
        ACCESS(ALTER) ID(STGADMIN)

SETROPTS REFRESH RACLIST(XFACILIT)

```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** command:

```

RALTER <class> <profile> +
        UACC(NONE) +
        AUDIT(FAILURES(READ)) +
        NOWARNING

```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```

PERMIT <profile> CLASS(<class>) +
        DELETE ID(<non-compliant>)

```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```

RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)

```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```

RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)

```

Default Value:

The **DASDVOL**, **FACILITY**, and **XFACILIT** classes are **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000150
2. IBM z/OS RACF STIG: RACF-SM-000040

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: DASD volume authority](#)
- [Storage Administration \(STGADMIN\) Profiles in the FACILITY Class or XFACILIT Class](#)
- [FACILITY class profiles for the ADMINISTRATOR keyword](#)
- [Protecting DFSMSHsm user commands with RACF FACILITY class profiles](#)
- [DFSMSrmm Implementation and Customization Guide: Authorizing resources](#)
- [Controlling Who Can Lock a Catalog \(IGG.CATLOCK Profile\)](#)
- [Control of checkpoint data sets on shared DASD volumes](#)
- [IBM z/OS DFSMSdss Storage Administration: FACILITY class profiles for the ADMINISTRATOR keyword](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.1.2 Ensure that access to active SMF collection files is controlled (Automated)

Profile Applicability:

- Level 1

Description:

SMF data collection is the system activity journaling facility of the z/OS system. With the proper parameter designations, it serves as the basis to ensure individual user accountability. **SYS1.MANxx** datasets should be created once and reused when cleared.

Update and allocate access to SMF collection files (i.e., **SYS1.MANx**, **logger**) are limited to system programmers and/or batch jobs that perform SMF dump processing. Control access based on type - separate collection as much as possible.

Rationale:

Users may have **UPDATE** access to the datasets, but **ALTER** allows for dataset deletion and should be avoided. **ALTER** access reduces the integrity and availability of the operating system environment and reduces compromises of confidential customer data.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entry covering **SYS1.MANxx** datasets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that **SYS1.MANxx** data sets are secured by RACF profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD 'SYS1.MAN*' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      DATA('SMF COLLECTION FILES')  
  
PERMIT 'SYS1.MAN*' GENERIC +  
      ACCESS(ALTER) ID(SYSprog)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD 'SYS1.MAN*' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT 'SYS1.MAN*' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000540

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Security for system data sets](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.1.3 Ensure that the SETROPTS WHEN(PROGRAM) value is active (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS WHEN(PROGRAM) activates RACF program control, which includes both access control to load modules and program access to data sets.

To set up access control to load modules, you must identify your controlled programs by creating a profile for each in the **PROGRAM** class. To set up program access to data sets, you must add a conditional access list to the profile of each program-accessed data set. Then, when program control is active, RACF ensures that each controlled load module is executed only by callers with the defined authority. RACF also ensures that each program-accessed data set is opened only by users who are listed in the conditional access list with the proper authority and who are executing the program specified in the conditional access list entry.

Ensure that RACF will perform program control.

Rationale:

Not protecting critical programs and not ensuring a clean address space can compromise the security of the processing environment. In addition, failure to establish standardized settings for RACF control options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ATTRIBUTES =** section.

Look for the following message:

```
WHEN (PROGRAM -- BASIC)
```

Verify that the message appears.

Note: The message may specify **BASIC**, **ENHANCED-WARNING**, or **ENHANCED**. This is determined by the **IRR.PGMSECURITY** profile in the **FACILITY** resource class, and the specific value in the message is not relevant for this control.

Remediation:

To modify the **WHEN(PROGRAM)** parameter use the RACF **SETROPTS** command:

```
SETROPTS WHEN (PROGRAM)
```

Default Value:

NOWHEN(PROGRAM) is in effect when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000610

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Activating program control \(WHEN\(PROGRAM\) option\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●

2.1.4 Ensure that access to the ICHDSM00 (DSMON) program is controlled (Automated)

Profile Applicability:

- Level 1

Description:

ICHDSM00 is the data security monitor utility (DSMON). READ authority to this program in the PROGRAM class is one way a user can have authority to run the utility. RACF ships the utility in SYS1.LINKLIB. Further, SYS1.LINKLIB is generally one of the code libraries identified in the PROGRAM * or ** profile and is always treated as UACC(READ), even if the profile itself has a more restrictive UACC.

Therefore, a more specific PROGRAM profile should be defined to protect ICHDSM00.

Rationale:

ICHDSM00 provides information on the security posture of the system. Such information should not be available to general users.

Audit:

Request the following DSMON report:

FUNCTION SYSTEM RACGAC

Verify that the PROGRAM entry has:

- -- GLOBAL INACTIVE -- or -- NO ENTRIES -- or contains no entry covering the ICHDSM00 resource

Request reports generated using IRRDBU00 output that will allow you to:

Verify that a ICHDSM00 profile in the PROGRAM class is defined and:

- Has a UACC of NONE
- Is not in WARNING mode
- AUDIT a minimum of SUCCESS(READ) and FAILURES(READ)
- ID(*) is not used to grant access
- READ and higher permits are restricted to:
 - Auditors
 - Security Administrators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To create a **PROGRAM** profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE PROGRAM ICHDSM00 +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    ADDMEM('SYS1.LINKLIB'//NOPADCHK) +  
    DATA('DATA SECURITY MONITOR UTILITY (DSMON)')  
  
PERMIT ICHDSM00 CLASS(PROGRAM) +  
    ACCESS(READ) ID(AUDITOR SECADMIN SYSPROG)  
  
SETROPTS REFRESH WHEN(PROGRAM)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER PROGRAM ICHDSM00 +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    NOWARNING  
  
SETROPTS REFRESH WHEN(PROGRAM)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT ICHDSM00 CLASS(PROGRAM) +  
    DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH WHEN(PROGRAM)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **PROGRAM** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Maintaining a clean environment in BASIC or ENHANCED modes](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.1.5 Ensure that access to the IRRDPI00 program is controlled (Automated)

Profile Applicability:

- Level 1

Description:

ICHDP100 is the program that is used to update the dynamic parse function in RACF, and to refresh in-storage custom field data after making updates in the **CFIELD** class. **READ** authority to this program in the **PROGRAM** class is one way a user can have authority to run the program. RACF ships the program in **SYS1.LINKLIB**. Further, **SYS1.LINKLIB** is generally one of the code libraries identified in the **PROGRAM *** or ****** profile, and is always treated as **UACC(READ)**, even if the profile itself has a more restrictive **UACC**.

Therefore, a more specific **PROGRAM** profile should be defined to protect **IRRDPI00**.

Rationale:

IRRDPI00 updates the RACF configuration, and thus access should not be allowed for general users.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify FACILITY appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify FACILITY appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify FACILITY appears.

Request the following **DSMON** report:

```
FUNCTION SYSTEM RACGAC
```


Verify that:

- The **FACILITY** entry has:
 - **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entry covering the **IRRDPI00** resource
- The **PROGRAM** entry has:
 - **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entry covering the **IRRDPI00** resource

Request reports generated using IRRDBU00 output that will allow you to:

Verify that a IRRDPI00 profile in the FACILITY class is defined and:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Security Administrators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Verify that a IRRDPI00 profile in the PROGRAM class is defined and:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Security Administrators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Note: Granting **IRRDPI00** access via the **FACILITY** class profile is preferred. It is not required, but recommended, to remove permits from the **PROGRAM** profile where possible.

Remediation:

To activate RACF classes use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FACILITY)
```

To enable generic profile checking for a RACF class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FACILITY)
```

To RACLIST a RACF class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FACILITY)
```

To create a **PROGRAM** profile use the RACF **RDEFINE**, **PERMIT**, and **SETROPTS** commands:

```
RDEFINE PROGRAM IRRDPI00 +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    ADDMEM('SYS1.LINKLIB'//NOPADCHK) +
    DATA('UPDATE RACF DYNAMIC PARSE FUNCTION')

PERMIT IRRDPI00 CLASS(PROGRAM) +
    ACCESS(READ) ID(SECADMIN SYSPROG)

SETROPTS REFRESH WHEN(PROGRAM)
```

To create a **FACILITY** profile use the RACF **RDEFINE**, **PERMIT**, and **SETROPTS** commands:

```
RDEFINE FACILITY IRRDPI00 +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    DATA('UPDATE RACF DYNAMIC PARSE FUNCTION')

PERMIT IRRDPI00 CLASS(FACILITY) +
    ACCESS(READ) ID(SECADMIN SYSPROG)

SETROPTS REFRESH RACLIST(FACILITY)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** and **SETROPTS** commands:

```

RALTER PROGRAM IRRDPI00 +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    NOWARNING

SETROPTS REFRESH WHEN(PROGRAM)

RALTER FACILITY IRRDPI00 +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    NOWARNING

SETROPTS REFRESH RACLIST(FACILITY)

```

To remove a non-compliant access list entries use the RACF **PERMIT** and **SETROPTS** commands:

```

PERMIT ICHDSM00 CLASS(PROGRAM) +
    DELETE ID(<non-compliant>)

SETROPTS REFRESH WHEN(PROGRAM)

PERMIT IRRDPI00 CLASS(FACILITY) +
    DELETE ID(<non-compliant>)

SETROPTS REFRESH RACLIST(FACILITY)

```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```

RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)

```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```

RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)

```

Default Value:

The **PROGRAM** and **FACILITY** classes are **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: Maintaining a clean environment in BASIC or ENHANCED modes](#)
- [z/OS Security Server RACF System Programmer's Guide: RACF authorization of the IRRDPI00 command](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.1.6 Ensure that the SETROPTS ERASE value is set to ALL (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS ERASE(ALL) specifies that data management is to erase all scratched data sets including temporary data sets. **NOERASE** specifies that no DASD data sets are erased when deleted.

The system-wide options control the default settings for determining how RACF will function when handling requests for access to the operating system environment, RACF, and customer data. RACF provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used.

Rationale:

Not maintaining these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for RACF control options introduces the possibility of exposure during migration process or contingency plan activation.

Impact:

The impact of **SETROPTS ERASE(ALL)** is directly proportional to the amount of DASD space which is being deleted. While recent releases of z/OS have substantially improved the performance of data set erasure, there may be system impacts if a large amount of DASD space is being erase.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output and look for the following message:

```
ERASE-ON-SCRATCH IS ACTIVE, CURRENT OPTIONS:  
ERASE-ON-SCRATCH FOR ALL DATA SETS IS IN EFFECT
```

Verify that the message appears.

Alternatively, if IBM Health Checker for z/OS is installed and active, you can request the **HZSPRINT** output for:

```
CHECK(IBMRA CF, RACF_ERASE_ON_SCRATCH)
```

Verify that the health check returns this message for each system:

```
IRRH338I SETROPTS ERASE(ALL) is in effect.
```

Remediation:

To modify the **ERASE** parameter use the RACF **SETROPTS** command:

```
SETROPTS ERASE(ALL)
```

Default Value:

NOERASE is in effect when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000840

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: Erasing scratched or released data \(ERASE option\)](#)
- [IBM Health Checker for z/OS: RACF_ERASE_ON_SCRATCH](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.5 Securely Dispose of Data Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.			

2.1.7 Ensure that the TEMPDSN class is active (Automated)

Profile Applicability:

- Level 1

Description:

The **TEMPDSN** class provides protection for temporary data sets if these data sets are not deleted by the job or session which created them. These values become effective immediately after the command **SETROPTS CLASSACT(TEMPDSN)** is issued.

Rationale:

You can protect temporary data sets. Normally, these data sets are considered protected from any accesses except by the job or session that created them, and therefore do not need to be protected by RACF. However, the following situations could leave a temporary data set unprotected:

- A system failure
- An initiator failure or initiator termination by the FORCE command
- An automatic restart - between the failure and the restart

In these cases, if the **TEMPDSN** class is active, only users with the **OPERATIONS** attribute or users authorized to specific DFSMSdss functions can scratch any residual temporary data sets remaining on a volume.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **TEMPDSN** appears.

Alternatively, if IBM Health Checker for z/OS is installed and active, you can request the **HZSPRINT** output for:

```
CHECK(IBMRA CF, RACF _TEMPDSN _ACTIVE)
```

Verify that the health check returns this message:

```
IRR H228I The class TEMPDSN is active.
```

Remediation:

To activate the **TEMPDSN** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT (TEMPDSN)
```

Default Value:

The **TEMPDSN** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000120

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: Protecting DFP-managed temporary data setst](#)
- [IBM Health Checker for z/OS: RACF classname ACTIVE](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.1.8 Ensure that access to RACF database data sets is controlled (Automated)

Profile Applicability:

- Level 1

Description:

RACF database files contain all access control information for the operating system environment and system resources as well as user registry, user permissions and user authentication data (including encrypted passwords and passphrases), private X.509 certificate keys, and more.

It is important that the data sets containing the primary and backup databases are properly protected. You should also ensure that data sets containing RACF database information, such as backup copies and unloaded versions of the RACF database, are also protected. In protecting these data sets, you should ensure that only those users who have a definite job-related need to read or update the data have access. Any other users should not have access to the data sets containing your RACF databases.

Note: The RACF **IRRUT200** and **IRRUT400** utilities create exact copies of the RACF database, and are often used to create point-in-time copies as part of a backup strategy. It is critical to ensure these copies are secured and logged in the same manner as the active RACF databases.

Rationale:

An unsecured RACF database poses significant risks, including unauthorized access to sensitive data, system compromise, and potential operational disruption, due to the comprehensive access control information it stores. Consequences of unauthorized access can include but are not limited to data theft, manipulation, system outages, and reputational damage.

Impact:

It is **critical** to ensure that direct access to RACF database files is restricted to the minimum number of users and all access is logged. Failure to do so can undermine the IBM z/OS System Integrity Statement for all systems secured by the affected RACF database.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE --** or **-- NO ENTRIES --** or contains no entries covering RACF primary and backup databases as well as any copies

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that the RACF primary and backup databases as well as any copies are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** permits are restricted to:
 - Auditors
 - Security Administrators
 - Systems Programmers
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD 'SYS1.RACF.*' GENERIC +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('RACF DTABASE')  
  
PERMIT 'SYS1.RACF.*' GENERIC +  
      ACCESS(ALTER) ID(SYSprog)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD 'SYS1.RACF.*' GENERIC +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT 'SYS1.RACF.*' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000370

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Security for system data sets](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	3.14 <u>Log Sensitive Data Access</u> Log sensitive data access, including modification and disposal.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.1.9 Ensure that access to the RACF remote sharing facility data sets is controlled (Automated)

Profile Applicability:

- Level 1

Description:

When using the RACF remote sharing facility (**RRSF**) to propagate RACF requests across the network, each node in the configured network has a pair of VSAM files (**INMSG** and **OUTMSG**) to save queued work until it is sent, and its receipt is confirmed by the remote node. These files must be protected.

Rationale:

Disclosure of this information can compromise user credentials and give clues to the protection mechanisms in effect.

Audit:

Note: The subsystem-prefix must be supplied by the site. For example if a site has chosen "@" then the command would be @TARGET.

Issue the following TSO command:

```
<subsystem-prefix>TARGET LIST NODE (*)
```

Review the command output in the **FILE USAGE** section to determine the **RRSF** workspace data sets to be evaluated.

Alternatively, if IBM Health Checker for z/OS is installed and active, you can request the **HZSPRINT** output for:

```
CHECK (IBMRACF, RACF_RRSF_RESOURCES)
```

To obtain a list of **RRSF** workspace data sets.

Issue the following TSO command for each RRSF workspace data set:

```
LISTCAT ENTRY('<dataset>') ALL
```

Review the command output in the **ENCRYPTIONDATA** section.

Verify the following message is present:

```
DATA SET ENCRYPTION----- (YES)
```

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **DATASET** entry has:

- -- GLOBAL INACTIVE -- or -- NO ENTRIES -- or contains no entries covering the **RRSF** workspace data sets

Request reports generated using IRRDBU00 output that will allow you to:

Verify That the **RRSF** workspace data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD 'SYS1.RACF.NODE1.**' GENERIC +  
      UACC(NONE) +  
      AUDIT(FAILURES(READ)) +  
      DATA('RACF REMOTE SHARING FACILITY (RRSF) FILES')  
  
PERMIT 'SYS1.RACF.NODE1.**' GENERIC +  
      ACCESS(ALTER) ID(SYSPROG)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD 'SYS1.RACF.NODE1.**' GENERIC +  
      UACC(NONE) +  
      AUDIT(FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT 'SYS1.RACF.NODE1.**' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Encrypting the files requires the standard data set encryption setup (see Additional Information below). Because the RACF subsystem always holds serialization on these files, there is an additional step to perform after the data set encryption setup is complete. The **NEWWORKSPACE** keyword of the **TARGET** command can be used to change the files being used to new ones that are set up for encryption. The same command can be used to restore use of the original files after their encryption setup has been performed.

Default Value:

- **SETROPTS NOPROTECTALL** is in effect for data sets when RACF is using a newly initialized database.
- Data sets are not encrypted.

Additional Information:

- [z/OS Security Server RACF System Programmer's Guide: Modifying the attributes of workspace data sets](#)
- [z/OS DFSMS Using Data Sets: Data set encryption](#)
- [IBM Health Checker for z/OS: RACF RRSF RESOURCES](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.1.10 Ensure that access to the RACF parameter library is controlled (Automated)

Profile Applicability:

- Level 1

Description:

The started procedure in **SYS1.PROCLIB** that starts the RACF subsystem address space contains an optional **RACFPARM DD** statement that identifies a file containing commands to run during subsystem initialization. This file must be protected with a **DATASET** profile.

Rationale:

When these commands execute, they do so under the identity associated with the RACF subsystem, and **OPERCMDS** checking is not performed. Anyone with **UPDATE** access can insert commands.

Audit:

Request a list of any and all RACF parameter library data sets referenced by the **RACFPARM DD**.

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering the RACF parameter library data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That the RACF parameter library data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD 'SYS1.RACF.PARM' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      DATA('RACF PARAMETER LIBRARY')  
  
PERMIT 'SYS1.RACF.PARM' GENERIC +  
      ACCESS(ALTER) ID(SYSprog)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD 'SYS1.RACF.PARM' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT 'SYS1.RACF.PARM' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Security considerations for the RACF parameter library](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.1.11 Ensure that RACF remote sharing connections use the TCP/IP protocol (Automated)

Profile Applicability:

- Level 1

Description:

Each individual RACF remote sharing (RRSF) connection to a remote node can use either the original APPC protocol or the newer TCP/IP protocol. TCP/IP allows for much stronger protection of the communications using AT-TLS (Application Transparent TLS) technology, complimented by technology such as z/OS Encryption Readiness Technology (zERT) that can monitor the sets of cryptographic algorithms used to protect communications.

Rationale:

APPC can only use DES-based encryption, which is far weaker than the encryption offered by TCP/IP.

Audit:

Note: The subsystem-prefix must be supplied by the site. For example if a site has chosen "@" then the command would be @TARGET.

Issue the following TSO command:

```
<subsystem-prefix>TARGET LISTPROTOCOL
```

Verify that the string APPC does not appear in the resulting IRRM009I messages.

Remediation:

Consult the [z/OS Security Server RACF System Programmer's Guide](#) for guidance on modifying and securing RRSF connections.

Default Value:

APPC is the default communication protocol.

Additional Information:

- [z/OS Security Server RACF System Programmer's Guide: Changing the protocol for a connection](#)
- [z/OS Security Server RACF System Programmer's Guide: Setting up your RRSF system to use TCP/IP](#)
- [z/OS Security Server RACF System Programmer's Guide: Setting up AT-TLS](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

2.1.12 Ensure that access to memory and privileged program dumps is controlled (Automated)

Profile Applicability:

- Level 1

Description:

Access to memory and privileged program dumps running Trusted Control Block (TCB) key 0-7 may hold passwords, encryption keys, or other sensitive data that must not be made available.

Rationale:

Failure to control access to these facilities could result in unauthorized personnel modifying sensitive z/OS lists. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **FACILITY** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **FACILITY** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering the following resources
 - **IEAABD.DMPAKEY**
 - **IEAABD.DMPAUTH**

Request reports generated using IRRDBU00 output that will allow you to:

Verify that the **IEAABD.DMPAKEY** and **IEAABD.DMPAUTH** resources are secured by profiles in the **FACILITY** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits for **IEAABD.DMPAKEY** are restricted to:
 - Systems Programmers
- **READ** permits for **IEAABD.DMPAUTH** are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level
- **UPDATE** and higher permits for **IEAABD.DMPAUTH** are restricted to:
 - Systems Programmers

Remediation:

To activate RACF classes use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FACILITY)
```

To enable generic profile checking for a RACF class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FACILITY)
```

To RACLIST a RACF class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FACILITY)
```

To create a **FACILITY** profile use the RACF **RDEFINE**, **PERMIT**, and **SETROPTS** commands:

```
RDEFINE FACILITY IEAABD.DMPAKEY +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    DATA('DUMP PROGRAMS WITH SYSTEM KEY < 8')

PERMIT IEAABD.DMPAKEY CLASS(FACILITY) +
    ACCESS(READ) ID(SYSPROG)

RDEFINE FACILITY IEAABD.DMPAUTH +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    DTA('GENERATE PROGRAM DUMPS')

PERMIT IEAABD.DMPAUTH CLASS(FACILITY) +
    ACCESS(UPDATE) ID(SYSPROG)

SETROPTS REFRESH RACLIST(FACILITY)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** and **SETROPTS** commands:

```
RALTER FACILITY <profile> +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    NOWARNING

SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant access list entry use the RACF **PERMIT** and **SETROPTS** commands:

```
PERMIT <profile> CLASS(FACILITY) +
    DELETE ID(<non-compliant>)

SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:


```
RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **FACILITY** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000060

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Protecting program dumps using the FACILITY class](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.1.13 Ensure that access to system TRACE data sets is controlled (Automated)

Profile Applicability:

- Level 1

Description:

SYS1.TRACE is used to trace and debug system problems. It can contain sensitive information. In fact, this same consideration applies to any sort of trace log, many of which are application specific.

Rationale:

Unauthorized access to **TRACE** data sets can divulge sensitive system information.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE --** or **-- NO ENTRIES --** or contains no entries covering system **TRACE** data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That the system **TRACE** data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD 'SYS1.TRACE*' GENERIC +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('SYSTEM TRACE FILES')  
  
PERMIT 'SYS1.TRACE*' GENERIC +  
      ACCESS(ALTER) ID(SYSprog)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD 'SYS1.TRACE*' GENERIC +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT 'SYS1.TRACE*' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000230

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Security for system data sets](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.1.14 Ensure that access to system backup data sets is controlled (Automated)

Profile Applicability:

- Level 1

Description:

System backup data sets are necessary for recovery of DASD resident data sets.

Update access to System backup files is limited to system programmers and/or batch jobs that perform DASD backups.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- -- **GLOBAL INACTIVE** -- or -- **NO ENTRIES** -- or contains no entries covering system backup data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That the system backup data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('SYSTEM BACKUP FILES')  
  
PERMIT '<profile>' GENERIC +  
      ACCESS(ALTER) ID(SYSprog)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<profile>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000220

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.1.15 Ensure that access to system DUMP data sets is controlled (Automated)

Profile Applicability:

- Level 1

Description:

System DUMP data sets are used to record system data areas and virtual storage associated with system task failures.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the DATASET entry has:

- -- GLOBAL INACTIVE -- or -- NO ENTRIES -- or contains no entries covering system DUMP data sets

Request reports generated using IRRDBU00 output that will allow you to:

Verify That the system DUMP data sets are secured by profiles in the DATASET class that:

- Have UACC of NONE
- Are not in WARNING mode
- AUDIT a minimum of SUCCESS(READ) and FAILURES(READ)
- ID(*) is not used to grant access
- READ permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level
- UPDATE and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +
      UACC(NONE) +
      AUDIT(ALL(READ)) +
      DATA('SYSTEM DUMP FILES')

PERMIT '<profile>' GENERIC +
      ACCESS(ALTER) ID(SYSprog)

SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<profile>' GENERIC +
      UACC(NONE) +
      AUDIT(ALL(READ)) +
      NOWARNING

SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<profile>' GENERIC +
      DELETE ID(<non-compliant>)

SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000330

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Security for system data sets](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.1.16 Ensure that access to SMF collection offload data sets is controlled (Automated)

Profile Applicability:

- Level 1

Description:

SMF backup data sets are those data sets to which SMF data has been offloaded to ensure a historical tracking of individual user accountability. This includes the output of the SMF Unload utility (IRRADU00).

Rationale:

Minimizing access to a need-to-know basis maintains the integrity and availability of the operating system environment and avoids compromise of the confidentiality of customer data.

Audit:

Request the following DSMON report:

FUNCTION SYSTEM RACGAC

Verify that the DATASET entry has:

- -- GLOBAL INACTIVE -- or -- NO ENTRIES -- or contains no entries covering SMF backup data sets

Request reports generated using IRRDBU00 output that will allow you to:

Verify That the SMF backup data sets are secured by profiles in the DATASET class that:

- Have UACC of NONE
- Are not in WARNING mode
- AUDIT a minimum of SUCCESS(READ) and FAILURES(READ)
- ID(*) is not used to grant access
- READ permits are restricted to:
 - Auditors
 - Security Administrators
 - Systems Programmers
 - IDs authorized to access these resources at this level
- UPDATE and higher permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +
      UACC(NONE) +
      AUDIT(ALL(READ)) +
      DATA('SMF LOG BACKUPS')

PERMIT '<profile>' GENERIC +
      ACCESS(ALTER) ID(SYSprog)

SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<profile>' GENERIC +
      UACC(NONE) +
      AUDIT(ALL(READ)) +
      NOWARNING

SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<profile>' GENERIC +
      DELETE ID(<non-compliant>)

SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(entry)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000330

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Security for system data sets](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2 Resource Protection

2.2.1 Ensure that the access to update system dynamic lists is controlled (Automated)

Profile Applicability:

- Level 1

Description:

Dynamic lists provide a method of making z/OS system changes without interrupting the availability of the operating system.

Rationale:

Failure to control access to these facilities could result in unauthorized personnel modifying sensitive z/OS lists. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **FACILITY** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **FACILITY** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES -- or** contains no entries covering resources prefixed with:
 - **CSVAPF**
 - **CSVDYLPA**
 - **CSVDYNEX**
 - **CSVDYNL**
 - **CSVLLA**

Request reports generated using IRRDBU00 output that will allow you to:

Verify That the **CSVAPF**, **CSVDYLPA**, **CSVDYNEX**, **CSVDYNL**, and **CSVLLA** prefixed resources are secured by profiles in the **FACILITY** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers

Verify That the **CSVDYNEX.LIST** resources is secured by a profile in the **FACILITY** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** permits are restricted to:
 - Auditors
 - Systems Programmers
 - IDs authorized to access these resources at this level
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To activate RACF classes use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FACILITY)
```

To enable generic profile checking for a RACF class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FACILITY)
```

To create a **FACILITY** profile use the RACF **RDEFINE**, **PERMIT**, and **SETROPTS** commands:


```

RDEFINE FACILITY CSV*.** +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    DATA('ACCESS TO MAKE DYNAMIC CHANGES TO -
    LLA, APF, LPA, EXITS, AND LINKLIST')

PERMIT CSV*.** CLASS(FACILITY) +
    ACCESS(READ) ID(SYSPROG)

RDEFINE FACILITY CSVVDYNEX.LIST +
    UACC(NONE) +
    AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +
    DATA('LIST INFORMATION ABOUT DYNAMIC EXITS')

PERMIT CSVVDYNEX.LIST CLASS(FACILITY) +
    ACCESS(UPDATE) ID(SYSPROG)

PERMIT CSVVDYNEX.LIST CLASS(FACILITY) +
    ACCESS(READ) ID(AUDITOR)

SETROPTS REFRESH RACLIST(FACILITY)

```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** and **SETROPTS** commands:

```

RALTER FACILITY CSV*.** +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    NOWARNING

RALTER FACILITY CSVVDYNEX.LIST +
    UACC(NONE) +
    AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +
    NOWARNING

SETROPTS REFRESH RACLIST(FACILITY)

```

To remove a non-compliant access list entry use the RACF **PERMIT** and **SETROPTS** commands:

```

PERMIT CSV*.** CLASS(FACILITY) +
    DELETE ID(<non-compliant>)

PERMIT CSVVDYNEX.LIST CLASS(FACILITY) +
    DELETE ID(<non-compliant>)

SETROPTS REFRESH RACLIST(FACILITY)

```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```

RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)

```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **FACILITY** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000200

Additional Information:

- [MVS Planning - Operations: Using RACF to control APF lists](#)
- [MVS Planning - Operations: Using RACF to control dynamic exits](#)
- [MVS Planning - Operations: Using RACF to control LNKST concatenations](#)
- [MVS Planning - Operations: Using RACF to control dynamic LPA](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2.2 Ensure that access to IEASYMUP resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that the System level symbolic (**IEASYMUP**) resources are defined to the **FACILITY** resource class and protected.

Rationale:

Failure to control access to **IEASYMUP** resources in use could result in unauthorized personnel modifying sensitive z/OS symbolics. This exposure may threaten the integrity and availability of the operating system environment.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **FACILITY** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **FACILITY** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering resources prefixed with **IEASYMUP**

Request reports generated using IRRDBU00 output that will allow you to:

Verify That the **IEASYMUP** prefixed resources are secured by profiles in the **FACILITY** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **UPDATE** and higher permits are restricted to:
 - Storage Administrators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To activate RACF classes use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FACILITY)
```

To enable generic profile checking for a RACF class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FACILITY)
```

To RACLIST a RACF class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FACILITY)
```

To create a **FACILITY** profile use the RACF **RDEFINE**, **PERMIT**, and **SETROPTS** commands:

```
RDEFINE FACILITY IEASYMUP.** +
    UACC(NONE) +
    AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +
    DATA('SYSTEM LEVEL SYMBOLICS')

PERMIT IEASYMUP.** CLASS(FACILITY) +
    ACCESS(UPDATE) ID(STGADMIN SYSPROG)

SETROPTS REFRESH RACLIST(FACILITY)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** and **SETROPTS** commands:

```
RALTER FACILITY IEASYMUP.** +
    UACC(NONE) +
    AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +
    NOWARNING

SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant access list entry use the RACF **PERMIT** and **SETROPTS** commands:

```
PERMIT IEASYMUP.** CLASS(FACILITY) +
    DELETE ID(<non-compliant>)

SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **FACILITY** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000430

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2.3 Ensure that PASSWORD protection for data sets is not used (Manual)

Profile Applicability:

- Level 1

Description:

All protection of system resources must come from RACF.

Rationale:

If multiple protection mechanisms are in place, the accessibility of data, specifically under contingency plan execution, is subject to compromise.

Failure to ensure dataset passwords are not used reduces the integrity and availability of the operating system environment and reduces compromises of confidential customer data.

Audit:

Interview question to check if system **PASSWORD** data set and OS passwords are being used.

Remediation:

Migrate from **PASSWORD** protection for data sets to RACF profiles in the **DATASET** class.

Default Value:

PASSWORD protection for data sets is not used by default, but is provided for compatibility with other IBM operating systems.

References:

1. IBM z/OS RACF STIG: RACF-OS-000220

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: Protecting data sets](#)
- [z/OS DFSMSdfp Advanced Services: Using Password Protected Data Sets](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.4 Ensure that access to data sets in the PARMLIB concatenation is controlled (Automated)

Profile Applicability:

- Level 1

Description:

The z/OS **PARMLIB** concatenation contains the parameters which control system Initial Program Load (IPL), configuration characteristics, security facilities, and performance.

Rationale:

Unauthorized **UPDATE** authority could result in the compromise of the operating system environment, RACF, and customer data. Unauthorized **READ** authority provides a means for the surveillance and mapping of the system configuration.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering **PARMLIB** data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That **PARMLIB** data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** permits are restricted to:
 - Security Administrators
 - Systems Operators
 - Systems Programmers
 - z/OS Started Task (STC)
 - IDs authorized to access these resources at this level
- **UPDATE** permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level
- **CONTROL** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('PARMLIB')  
  
PERMIT '<profile>' GENERIC +  
      ACCESS(ALTER) ID(SYSprog)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<profile>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000500

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2.5 Ensure that access to all LPA libraries is controlled (Manual)

Profile Applicability:

- Level 1

Description:

LPA modules, once loaded into the Link Pack Area, are capable of performing APF-authorized functions.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE --** or **-- NO ENTRIES --** or contains no entries covering LPA library data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That LPA library data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access greater than **READ**
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      DATA('LPA LIBRARY')  
  
PERMIT '<profile>' GENERIC +  
      ACCESS(READ) ID(*)  
  
PERMIT '<profile>' GENERIC +  
      ACCESS(ALTER) ID(SYSPROG)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<profile>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000300

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2.6 Ensure that access to system MASTER catalogs is controlled (Manual)

Profile Applicability:

- Level 1

Description:

System MASTER catalogs are the basis for locating all files on the system.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Request the following DSMON report:

FUNCTION SYSTEM RACGAC

Verify that the DATASET entry has:

- -- GLOBAL INACTIVE -- or -- NO ENTRIES -- or contains no entries covering system MASTER catalogs

Request reports generated using IRRDBU00 output that will allow you to:

Verify That system MASTER catalog data sets are secured by profiles in the DATASET class that:

- Have UACC of NONE
- Are not in WARNING mode
- AUDIT a minimum of SUCCESS(UPDATE) and FAILURES(READ)
- ID(*) is not used to grant access greater than READ
- UPDATE and higher permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<master-catalog>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      DATA('MASTER CATALOG')  
  
PERMIT '<master-catalog>' GENERIC +  
      ACCESS(READ) ID(*)  
  
PERMIT '<master-catalog>' GENERIC +  
      ACCESS(ALTER) ID(SYSPROG)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<master-catalog>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<master-catalog>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000300

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2.7 Ensure that access to all APF-authorized objects is controlled (Manual)

Profile Applicability:

- Level 1

Description:

The Authorized Program List (APF) designates those libraries that can contain program modules which possess a significant level of security bypass capability.

The **extattr** command can grant the same capability in the UNIX file system, and is secured by the **BPX.FILEATTR.APF** resource in the **FACILITY** class.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES** = section.

Verify that **FACILITY** and **OPERCMDS** appears.

Review the command output in the **GENERIC PROFILE CLASSES** = section.

Verify that **FACILITY** and **OPERCMDS** appears.

Review the command output in the **SETR RACLIST CLASSES** = section.

Verify that **FACILITY** and **OPERCMDS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering APF data sets

Verify that the **FACILITY** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering the **BPX.FILEATTR.APF** resource

Verify that the **OPERCMDS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering the following resources:
 - **MVS.SETPROG**
 - **MVS.SET.PROG**

Request reports generated using IRRDBU00 output that will allow you to:

Verify That APF data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access greater than **READ**
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Verify That the **BPX.FILEATTR.APF** resource is secured by a profile in the **FACILITY** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers

Verify That the **MVS.SETPROG** and **MVS.SET.PROG** resources are secured by profiles in the **OPERCMDS** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To activate RACF classes use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FACILITY)
SETROPTS CLASSACT(OPERCMDS)
```

To enable generic profile checking for a RACF class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FACILITY)
SETROPTS GENERIC(OPERCMDS)
```

To RACLIST a RACF class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FACILITY)
SETROPTS RACLIST(OPERCMDS)
```

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +
      UACC(NONE) +
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +
      DATA('APF LIBRARY')

PERMIT '<profile>' GENERIC +
      ACCESS(READ) ID(*)

PERMIT '<profile>' GENERIC +
      ACCESS(ALTER) ID(SYSPROG)

SETROPTS REFRESH GENERIC(DATASET)
```

To create a **FACILITY** or **OPERCMDS** profile use the RACF **RDEFINE**, **PERMIT**, and **SETROPTS** commands:

```

RDEFINE FACILITY BPX.FILEATTR.APF +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    DATA('ACCESS TO SET APF AUTHORIZATION ON UNIX FILE')

PERMIT BPX.FILEATTR.APF CLASS(FACILITY) +
    ACCESS(READ) ID(SYSPROG)

SETROPTS REFRESH RACLIST(FACILITY)

RDEFINE OPERCMDS MVS.SETPROG +
    UACC(NONE) +
    AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +
    DATA('SETPROG COMMAND')

PERMIT MVS.SETPROG CLASS(OPERCMDS) +
    ACCESS(UPDATE) ID(SYSPROG)

RDEFINE OPERCMDS MVS.SET.PROG +
    UACC(NONE) +
    AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +
    DATA('SET PROG=(XX) COMMAND')

PERMIT MVS.SET.PROG CLASS(OPERCMDS) +
    ACCESS(UPDATE) ID(SYSPROG)

SETROPTS REFRESH RACLIST(OPERCMDS)

```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```

ALTDSD '<profile>' GENERIC +
    UACC(NONE) +
    AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +
    NOWARNING

SETROPTS REFRESH GENERIC(DATASET)

```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** and **SETROPTS** commands:

```

RALTER FACILITY BPX.FILEATTR.APF +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    NOWARNING

SETROPTS REFRESH RACLIST(FACILITY)

RALTER OPERCMDS MVS.SETPROG +
    UACC(NONE) +
    AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +
    NOWARNING

RALTER OPERCMDS MVS.SET.PROG +
    UACC(NONE) +
    AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +
    NOWARNING

SETROPTS REFRESH RACLIST(OPERCMDS)

```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```

PERMIT '<profile>' GENERIC +
    DELETE ID(<non-compliant>)

SETROPTS REFRESH GENERIC(DATASET)

PERMIT BPX.FILEATTR.APF CLASS(FACILITY) +
    DELETE ID(<non-compliant>)

SETROPTS REFRESH RACLIST(FACILITY)

PERMIT MVS.SETPROG CLASS(OPERCMDS) +
    DELETE ID(<non-compliant>)

PERMIT MVS.SET.PROG CLASS(OPERCMDS) +
    DELETE ID(<non-compliant>)

SETROPTS REFRESH RACLIST(OPERCMDS)

```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```

RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)

```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

- **SETROPTS NOPROTECTALL** is in effect for data sets when RACF is using a newly initialized database.
- The **FACILITY** and **OPERCMDS** classes are **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000340

Additional Information:

- [z/OS UNIX System Services Planning: Setting up the UNIX-related FACILITY and SURROGAT class profiles](#)
- [z/OS MVS System Commands: MVS commands, RACF access authorities, and resource names](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2.8 Ensure that access to the SYS1.SVCLIB data set is controlled (Automated)

Profile Applicability:

- Level 1

Description:

The **SYS1.SVCLIB** data set is automatically APF-authorized, contains system SVCs, and may also contain I/O appendages.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering **SYS1.SVCLIB**

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That the **SYS1.SVCLIB** data set is secured by a profile in the **DATASET** class that:

- Has **UACC** of **NONE**
- IS not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access greater than **READ**
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD 'SYS1.SVCLIB' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      DATA('SYSTEM SUPERVISOR CALLS (SVCS)')  
  
PERMIT 'SYS1.SVCLIB' GENERIC +  
      ACCESS(READ) ID(*)  
  
PERMIT 'SYS1.SVCLIB' GENERIC +  
      ACCESS(ALTER) ID(SYSPROG)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD 'SYS1.SVCLIB' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT 'SYS1.SVCLIB' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000270

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2.9 Ensure that access to the SYS1.IMAGELIB data set is controlled (Manual)

Profile Applicability:

- Level 1

Description:

SYS1.IMAGELIB is a partitioned data set containing Universal Character Set (UCS), Forms Control Buffer (FCB), and printer control information. Most IBM standard UCS images are included in **SYS1.IMAGELIB** during system installation. This data set should be protected as a z/OS system data set.

SYS1.IMAGELIB is automatically APF-authorized. This data set contains modules, images, tables, and character sets which are essential to system print services.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- -- GLOBAL INACTIVE -- or -- NO ENTRIES -- or contains no entries covering **SYS1.IMAGELIB**

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That the **SYS1.IMAGELIB** data set is secured by a profile in the **DATASET** class that:

- Has **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access greater than **READ**
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD 'SYS1.IMAGELIB' GENERIC +
      UACC(NONE) +
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +
      DATA('SYSTEM UNIVERSAL CHARACTER SET (UCS), FORMS CONTROL -
      BUFFER (FCB), AND PRINTER CONTROL INFORMATION')

PERMIT 'SYS1.IMAGELIB' GENERIC +
      ACCESS(READ) ID(*)

PERMIT 'SYS1.IMAGELIB' GENERIC +
      ACCESS(ALTER) ID(SYSPROG)

SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD 'SYS1.IMAGELIB' GENERIC +
      UACC(NONE) +
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +
      NOWARNING

SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT 'SYS1.IMAGELIB' GENERIC +
      DELETE ID(<non-compliant>)

SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000270

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2.10 Ensure that access to libraries that contain PPT modules is controlled (Automated)

Profile Applicability:

- Level 1

Description:

Specific PPT (Program Properties Table) designated program modules possess significant security bypass capabilities.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Request the following DSMON report:

FUNCTION SYSTEM RACGAC

Verify that the DATASET entry has:

- -- GLOBAL INACTIVE -- or -- NO ENTRIES -- or contains no entries covering libraries that contain PPT modules

Request reports generated using IRRDBU00 output that will allow you to:

Verify That libraries that contain PPT modules are secured by profiles in the DATASET class that:

- Have UACC of NONE
- Are not in WARNING mode
- AUDIT a minimum of SUCCESS(UPDATE) and FAILURES(READ)
- ID(*) is not used to grant access greater than READ
- UPDATE and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      DATA('PPT MODULE LIBRARY')  
  
PERMIT '<profile>' GENERIC +  
      ACCESS(READ) ID(*)  
  
PERMIT '<profile>' GENERIC +  
      ACCESS(ALTER) ID(SYSPROG)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<profile>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000020

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2.11 Ensure that access to the SYS1.NUCLEUS data set is controlled (Automated)

Profile Applicability:

- Level 1

Description:

The **SYS1.NUCLEUS** data set contains a large portion of the system Initial Program Load (IPL) programs and pointers to the master and alternate master catalog.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- -- GLOBAL INACTIVE -- or -- NO ENTRIES -- or contains no entries covering **SYS1.NUCLEUS**

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That the **SYS1.NUCLEUS** data set is secured by a profile in the **DATASET** class that:

- Has **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access greater than **READ**
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD 'SYS1.NUCLEUS' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      DATA('SYSTEM SUPERVISOR (KERNEL) MODULES')  
  
PERMIT 'SYS1.NUCLEUS' GENERIC +  
      ACCESS(READ) ID(*)  
  
PERMIT 'SYS1.NUCLEUS' GENERIC +  
      ACCESS(ALTER) ID(SYSPROG)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD 'SYS1.NUCLEUS' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT 'SYS1.NUCLEUS' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000010

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2.12 Ensure that access to all system PROCLIB data sets is controlled (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that all UPDATE and higher access to all system **PROCLIB** data sets referenced in the Master JCL and JES2 or JES3 procedure for started tasks (STCs) and TSO logons are restricted to systems programming personnel only.

Rationale:

Unauthorized access to **PROCLIB** data sets referenced in the JES2 procedure can allow unauthorized modifications to STCs and other system level procedures. This could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Refer to the following for the **PROCLIB** data sets that contain the STCs and TSO logons from the following sources:

- **MSTJCLxx** member used during an IPL. The **PROCLIB** data sets are obtained from the **IEFPDSI** and **IEFJOBS DD** statements.
- **PROCxx DD** statements and JES2 Dynamic **PROCLIBs**. Where **xx** is the **PROCLIB** entries for the **STC** and **TSU JOBCCLASS** configuration definitions.

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering system **PROCLIB** data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That the **PROCLIB** data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<data set>' GENERIC +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('SYSTEM PROCLIB')  
  
PERMIT '<data set>' GENERIC +  
      ACCESS(ALTER) ID(SYSprog)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD 'SYS1.TRACE*' GENERIC +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<data set>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

In the absence of a covering profile, the **SETROPTS PROTECTALL** setting determines the access allowed.

References:

1. IBM z/OS RACF STIG: RACF-ES-000390

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2.13 Ensure that access to System REXX IRRPWREX exit is controlled (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that read access is restricted to security administrators, systems programmers, and auditors.

Rationale:

Unauthorized access could result in the compromise of passwords, the operating system environment, RACF, and customer data.

Audit:

Note: Refer to the zOS system **REXXLIB** concatenation found in **SYS1.PARMLIB(AXR)** for the data set that contains the Rexx for the password exit named **IRRPWREX** and the defined **AXRUSER**.

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering the dataset containing **IRRPWREX**

Request reports generated using **IRRDBUG** output that will allow you to:

Verify That the dataset containing **IRRPWREX** is secured by a profile in the **DATASET** class that:

- Has **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** permits are restricted to:
 - Auditors
 - Security Administrators
 - Systems Programmers
 - IDs authorized to access these resources at this level
- **UPDATE** and **CONTROL** permits are restricted to:
 - Security Administrators
 - Systems Programmers
- **ALTER** permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +
      UACC(NONE) +
      AUDIT(ALL(READ)) +
      DATA('SYSTEM REXX LIBRARY')

PERMIT '<profile>' GENERIC +
      ACCESS(ALTER) ID(SYSprog)

SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<profile>' GENERIC +
      UACC(NONE) +
      AUDIT(ALL(READ)) +
      NOWARNING

SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<profile>' GENERIC +
      DELETE ID(<non-compliant>)

SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000360

Additional Information:

[GitHub: IBM RACF Rexx Password Exit](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2.14 Ensure that access to the SYS1.LINKLIB data set is controlled (Automated)

Profile Applicability:

- Level 1

Description:

The **SYS1.LINKLIB** data set is automatically APF-authorized, contains system SVCs and the base PPT.

Minimizing access to a need-to-know basis maintains the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- -- GLOBAL INACTIVE -- or -- NO ENTRIES -- or contains no entries covering **SYS1.LINKLIB**

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That the **SYS1.LINKLIB** data set is secured by a profile in the **DATASET** class that:

- Has **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD 'SYS1.LINKLIB' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      DATA('SYSTEM SVCS AND THE BASE PPT LIBRARY')  
  
PERMIT 'SYS1.LINKLIB' GENERIC +  
      ACCESS(ALTER) ID(SYSprog)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD 'SYS1.LINKLIB' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT 'SYS1.LINKLIB' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000350

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2.15 Ensure that access to all system-level product installation libraries is controlled (Automated)

Profile Applicability:

- Level 1

Description:

System-level product installation libraries constitute the majority of the systems software libraries. The ability to change the contents of these libraries must be restricted to system system programmers.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering system-level product installation libraries

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That system-level product installation libraries data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<system-installation-library>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE),FAILURES(READ)) +  
      DATA('SYSTEM LEVEL PRODUCT INSTALLATION LIBRARY')  
  
PERMIT '<system-installation-library>' GENERIC +  
      ACCESS(ALTER) ID(SYSPROG)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<system-installation-library>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE),FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<system-installation-library>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000320

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2.16 Ensure that access to RACF resources in the FACILITY class is controlled (Automated)

Profile Applicability:

- Level 1

Description:

RACF-defined resources, prefixed with **IRR** in the **FACILITY** class, consist of sensitive capabilities including RACF commands and certain SAF callable services.

Rationale:

Missing or inaccurate protection of these resources could allow a user to access sensitive data, modify or delete data and operating system controls, or issue commands that could negatively impact system availability.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **FACILITY** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **FACILITY** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering **IRR** prefixed resources

Request reports generated using IRRDBU00 output that will allow you to:

Verify that **IRR** prefixed profiles in the **FACILITY** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Security Administrators
 - IDs authorized to access these resources at this level

Remediation:

To activate the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FACILITY)
```

To enable generic profile checking for the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FACILITY)
```

To RACLIST the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FACILITY)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** command:

```
RALTER FACILITY IRR.<qualifiers> +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    NOWARNING  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT IRR.<qualifiers> CLASS(FACILITY) +  
    DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **FACILITY** class is **INACTIVE** when RACF is using a newly initialized database.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2.17 Ensure that access to VTAMAPPL resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

You can use resources in the **VTAMAPPL** class to control which users can open the application control block (ACB) indicated by a VTAM application program when the user is not running an APF-authorized program or command processor.

Note: APF-authorized applications, such as APPC and TSO/E, do not need authorization in the **VTAMAPPL** class to open an ACB.

Rationale:

Profiles defined in the **VTAMAPPL** resource class prevent non-APF-authorized programs from opening an ACB for a specific LU, or from registering as a member of a VTAM generic resource group, and thus potentially intercepting requests addressed to that LU name.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **VTAMAPPL** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **VTAMAPPL** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **VTAMAPPL** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that:

- The **VTAMAPPL** entry has:
 - **-- GLOBAL INACTIVE -- or -- NO ENTRIES --**

Request reports generated using IRRDBU00 output that will allow you to:

Verify that all profiles in the **VTAMAPPL** class:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate the **VTAMAPPL** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT (VTAMAPPL)
```

To enable generic profile checking for the **VTAMAPPL** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC (VTAMAPPL)
```

To RACLIST the **VTAMAPPL** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST (VTAMAPPL)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** command:

```
RALTER <class> <profile> +  
      UACC (NONE) +  
      AUDIT (FAILURES (READ)) +  
      NOWARNING
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(<class>) +  
      DELETE ID(<non-compliant>)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **VTAMAPPL** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling the opening of VTAM ACBs](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.2.18 Ensure that access to IBM Health Checker resources is controlled (Automated)

Profile Applicability:

- Level 1

Description:

IBM Health Checker for z/OS is a z/OS component that installations can use to gather information about their system environment and system parameters to help identify potential configuration problems before they impact availability or cause outages.

Rationale:

Failure to control access to Health Checker for z/OS resources in the **XFACILIT** class can result in inadvertent disclosure of system configuration data.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **XFACILIT** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **XFACILIT** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **XFACILIT** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that:

- The **XFACILIT** entry has:
 - **-- GLOBAL INACTIVE --** or **-- NO ENTRIES --** or contains no **HZS** prefixed entries

Request reports generated using IRRDBU00 output that will allow you to:

Verify the following catch-all profile is defined:

- A **GENERIC** profile in the **XFACILIT** class named: **HZS.**** or **HZS.*** or **HZS.*.****

Verify that all **HZS** prefixed profiles in the **XFACILIT** class:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To activate RACF classes use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(XFACILIT)
```

To enable generic profile checking for a RACF class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(XFACILIT)
```

To RACLIST a RACF class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(XFACILIT)
```

To create catch-all profiles use the RACF **RDEFINE** command:

```
RDEFINE XFACILIT HZS.** +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('IBM HEALTH CHECKER CATCH-ALL PROFILE')

PERMIT HZS.** CLASS(XFACILIT) +
    ACCESS(ALTER) ID(SYSPROG)

SETROPTS REFRESH RACLIST(XFACILIT)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** command:

```
RALTER <class> <profile> +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    NOWARNING
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(<class>) +
    DELETE ID(<non-compliant>)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETOPTS REFRESH GLOBAL(<class>)
SETOPTS NOGLOBAL(<class>)
```

Default Value:

The **XFACILIT** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[IBM z/OS SDSF Operations and Customization: Protecting checks](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.3 System Settings

2.3.1 Ensure that the SETROPTS TERMINAL value is set to NONE (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS TERMINAL is used to set the universal access authority (**UACC**) associated with undefined terminals.

Rationale:

The improper setting of this field can compromise the security of the z/OS environment. In addition, failure to establish standardized settings for RACF **SETROPTS** options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ATTRIBUTES =** section.

Verify that **TERMINAL(NONE)** appears.

Remediation:

To modify the **TERMINAL** parameter use the RACF **SETROPTS** command:

```
SETROPTS TERMINAL(NONE)
```

Default Value:

TERMINAL(READ) is in effect when RACF is using a newly initialized database.

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: Protecting undefined terminals \(TERMINAL option\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.3.2 Ensure that the SETROPTS GENERIC is enabled for ACTIVE classes (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS GENERIC controls what classes may have generic profiles. Generic profiles are profiles which cover zero or more resources. They substantially simplify security administration.

Note: It is possible to have characters that would be considered "wildcards" such as *, %, \$, and & in non-generic profiles. If the class is not in the **GENERIC** list, then profiles created with wildcards are not generic profiles.

Rationale:

If no setting is found, the system-wide defaults will be used. The improper setting of any subsystem fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the RACF options introduces the possibility of exposure during migration process or contingency plan activation.

Impact:

Not enabling RACF generic profile processing for a class increases the number of profiles in the RACF data set and makes it less likely that the profile covering a data set is in a RACF cache so I/O to the RACF data base can be avoided.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that active classes appear, with the following exceptions:

- Any class which is defined with any of the following attributes as documented in the [Security Server RACF Macros and Interfaces](#) reference:
 - **GENERIC=DISALLOWED**
 - **GROUP**
 - **PROFDEF=NO**
- Any class defined as "generics not recommended" in the [Security Server RACF Command Language Reference](#), including but not limited to:
 - **CDT**
 - **CFIELD**
 - **DIGTCERT**
 - **DIGTRING**
 - **IDIDMAP**
 - **KERBLINK**
 - **REALM**
 - **SECLABEL**
 - **SECLMBR**
- Any installation-defined classes in the dynamic **CDT** with the **GENERIC(DISALLOWED)** attribute

Remediation:

To enable **GENERIC** for a class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(<class>)
```

Guidelines:

- If you have **GENERIC** turned on for the **DIGTCERT** class when the certificate is created or added and its Issuer's Distinguished Name contains any generic characters (*, & and %), a generic certificate profile will be created. This generic feature will cause unexpected behavior when the certificate is being used by other programs. You need to remove it add it back after turning off **GENERIC** in the **DIGTCERT** class.
- If a general resource class already has discrete profiles with names that contain generic characters (*, &, and %), enabling generic profile checking for the class prevents RACF from using those discrete profiles for authorization checking.
- In general, once you activate generic profile checking for a class and define generic profiles, avoid deactivating it with the **NOGENERIC** operand. RACF will not use your previously defined generic profiles for authorization checking while **NOGENERIC** is in effect.

Default Value:

NOGENERIC is in effect for a class when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Macros and Interfaces: Supplied class descriptor table entries](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.3.3 Ensure that the SETROPTS PROTECTALL value is set to FAIL (Automated)

Profile Applicability:

- Level 1

Description:

When **PROTECTALL** processing is active and set to **FAIL**, the system automatically rejects any request to create or access a data set that is not RACF-protected. This includes DASD data sets, tape data sets, catalogs, and GDG base names. Temporary data sets that comply with standard MVS temporary data set naming conventions are excluded from **PROTECTALL** processing.

Rationale:

The improper setting of this field can compromise the security of the z/OS environment. In addition, failure to establish standardized settings for RACF **SETROPTS** options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Verify the following messages are present:

```
PROTECT-ALL IS ACTIVE, CURRENT OPTIONS:  
PROTECT-ALL FAIL OPTION IS IN EFFECT
```

Alternatively, if IBM Health Checker for z/OS is installed and active, you can request the **HZSPRINT** output for:

```
CHECK(IBMRA CF, RACF_ PROTECTALL_ FAIL)
```

Verify the following message is present:

```
IRRH332I SETROPTS PROTECTALL(FAIL) is in effect.
```

Remediation:

To modify the **PROTECTALL** parameter use the RACF **SETROPTS** command:

```
SETROPTS PROTECTALL (FAILURES)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000570

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: RACF-protecting all data sets \(PROTECTALL option\)\)](#)
- [IBM Health Checker for z/OS: RACF PROTECTALL FAIL](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.3.4 Ensure that ALTER access authority in DISCRETE profiles is limited (Automated)

Profile Applicability:

- Level 2

Description:

When a RACF profile is a **DISCRETE** profile the **ALTER** level of access not only grants access to the resources protected by the profile, but also allows changes to most fields in the base segment of the profile itself, including the default access and the access lists.

Rationale:

Failure to control **ALTER** access authority with **IRR.ALTER** prefixed profiles in the **FACILITY** class can mean that users that require **ALTER** access to a resource are also able to make RACF changes, resulting in separation of duties concerns.

Impact:

This modifies long standing default behavior of RACF, and a site with an existing RACF environment must investigate whether **ALTER** access is being used for profile management before implementing this recommendation.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **FACILITY** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that:

- The **FACILITY** entry has:
 - **-- GLOBAL INACTIVE --** or **-- NO ENTRIES --** or contains no **IRR.ALTER** prefixed entries

Request reports generated using IRRDBU00 output that will allow you to:

Verify that a **GENERIC** profile in the **FACILITY** class named **IRR.ALTER.**** or **IRR.ALTER.*** or **IRR.ALTER.*.**** is defined with:

- Has **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- Has no permits

Verify that there are no other **IRR.ALTER** prefixed profiles in the **FACILITY** class.

Remediation:

To activate RACF classes use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FACILITY)
```

To enable generic profile checking for a RACF class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FACILITY)
```

To **RACLIST** a RACF class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FACILITY)
```

To create a **IRR.ALTER.**** profile use the RACF **RDEFINE** command:

```
RDEFINE FACILITY IRR.ALTER.** +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    DATA('LIMIT RACF ALTER ACCESS AUTHORITY IN DISCRETE PROFILES')  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** command:

```
RALTER FACILITY IRR.ALTER.** +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    NOWARNING  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT IRR.ALTER.** CLASS(FACILITY) +  
    DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To remove non-compliant **IRR.ALTER** prefixed profiles use the RACF **RDELETE** command:

```
RDELETE FACILITY IRR.ALTER.<non-compliant>  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **FACILITY** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Limiting ALTER access authority in discrete profiles](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			

2.3.5 Ensure that the ACEECHK resource class is enabled (Automated)

Profile Applicability:

- Level 2

Description:

The ACEE (Accessor Environment Element) is a control block that contains a description of a user's security environment, including user ID, current connect group, user attributes, and group authorities. An ACEE is constructed during user identification and verification, using information in the user's RACF profile, and is anchored in the user's address space. It is referenced by RACF during command and resource authorization processing to determine if the user is allowed to perform a given action or access a given resource.

An application running in an authorized state can make modifications directly to the ACEE in storage after its creation. Such a modification would be outside the involvement of the security product, and the application must take caution to ensure that such updates do not interfere with normal system processing. This is not necessarily malicious, but the behavior should be visible to make sure that any modification in the user's ACEE complies with the organization's security policy.

Rationale:

When the **ACEECHK** class is active and **RACLIST**ed, RACF command and authorization processing will detect certain changes made to the ACEE that affect authorization. When a modification is detected, RACF issues message **IRR421I** to the security console that contains information to help determine whether the modification is expected.

Impact:

Careful thought and planning should precede any decision to enable the failure option by defining a fully qualified **IRR.ABEND.ON.FAILURE** profile in the **ACEECHK** class. The results of an abend on an application can be unpredictable and largely depend on the recovery mechanisms in place for the programs running in the environment.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES** = section.

Verify that **ACEECHK** appears.

Review the command output in the **SETR RACLIST CLASSES** = section.

Verify that **ACEECHK** appears.

Request reports generated using IRRDBU00 output that will allow you to:

Verify that any **IRR.EXCLUDE** prefixed profile in the **ACEECHK** class has a documented justification.

Note: When RACF detects an ACEE modification it will check the **ACEECHK** class for the existence of a best fit **IRR.EXCLUDE** prefixed profile, which enables **IRR421I** message suppression when the behavior is expected by the site.

Remediation:

To activate the **ACEECHK** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(ACEECHK)
```

To RACLIST the **ACEECHK** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(ACEECHK)
```

Default Value:

The **ACEECHK** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Detecting ACEE modifications](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			

2.3.6 Ensure that *SETOPTS ENHANCEDGENERICOWNER* is in effect (Automated)

Profile Applicability:

- Level 1

Description:

SETOPTS GENERICOWNER restricts the creation of profiles in all general resource classes except the **PROGRAM** class.

To create a profile that is more specific than any existing profile protecting the same resource a user must:

- Have the **SPECIAL** attribute
- Be the **OWNER** of the existing profile
- Have the **group-SPECIAL** attribute if a **GROUP** owns the profile
- Have the group-SPECIAL attribute if the **OWNER** of the profile is in the scope of the **GROUP**.

SETOPTS ENHANCEDGENERICOWNER enables the same functionality as, but also prevents the creation of a more specific profile if the more specific profile is created in the grouping class and is specified on the **ADDMEM** operand.

Note: Both the **GENERICOWNER** and **ENHANCEDGENERICOWNER** options only affect the ability to create new profiles, or add new members to a grouping profile. These options have no effect on permission to resources, or on the ability to alter the definitions of resource profiles.

Rationale:

This offers enhanced restrictions on the creation of profiles for general resources.

Impact:

Issuing **SETOPTS GENERICOWNER** or **ENHANCEDGENERICOWNER** can prevent users with the **CLAUTH** attribute in general resource classes from creating profiles as they are accustomed to. Therefore, make these users **OWNER** of appropriate top generic profiles in the class.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Verify the following message is present:

```
ENHANCED GENERIC OWNER ONLY IS IN EFFECT
```

Remediation:

To enable **ENHANCEDGENERICOWNER** use the RACF **SETROPTS** command:

```
SETROPTS ENHANCEDGENERICOWNER
```

Default Value:

NOGENERICOWNER is in effect when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Restricting the creation of general resource profiles \(GENERICOWNER and ENHANCEDGENERICOWNER options\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			

2.3.7 Ensure that SETROPTS NOADDCREATOR is in effect (Automated)

Profile Applicability:

- Level 1

Description:

The **SETROPTS NOADDCREATOR** parameter specifies that if a user defines any new **DATASET** or general resource profile using **ADDSD**, **RDEFINE** or **RACROUTE REQUEST=DEFINE**, or creates discrete profiles other than **DATASET** and **TAPEVOL** using **RACROUTE REQUEST=DEFINE**, RACF does not place the profile creator's user ID on the profile's access list.

Rationale:

Enabling **NOADDCREATOR** prevents RACF from adding a profile creator to the profile's access list by default.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Verify the following message is present:

```
ADDCREATOR IS NOT IN EFFECT.
```

Remediation:

To modify the parameter use the RACF **SETROPTS** command:

```
SETROPTS NOADDCREATOR
```

Default Value:

The initial setting of the **ADDCREATOR/NOADDCREATOR** keyword depends on whether your database is new or old. When **IRRMIN00** is run with **PARM=NEW**, the initial setting is **NOADDCREATOR**. When **IRRMIN00** is run with anything other than **PARM=NEW**, RACF retains the current value of **ADDCREATOR/NOADDCREATOR**. For compatibility and migration reasons, this value is set to **ADDCREATOR** if no prior specification of **ADDCREATOR** or **NOADDCREATOR** had occurred.

Additional Information:

[z/OS Security Server RACF Auditor's Guide: SETROPTS options for automatic control of access list authority](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.4 User Privilege

2.4.1 Ensure that the assignment of the RACF OPERATIONS attribute is justified (Automated)

Profile Applicability:

- Level 1

Description:

A user possessing the **OPERATIONS** attribute has authorization to do maintenance operations on all RACF-protected data sets, tape volumes, and DASD volumes except those where the access list specifically limits the **OPERATIONS** user to a lower access authority than the operation requires.

Because the **OPERATIONS** and **group-OPERATIONS** privileges allow widespread access they should be limited to users documented with a valid requirement. Delegation of **group-OPERATIONS** processing to other personnel by site-defined Group Administrators is forbidden.

Granting individual authorities using **STGADMIN** prefixed profiles in the **FACILITY** class is the preferred method, where applicable. However, there may be cases where **OPERATIONS** is required.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACUSR

Review the **OPERATIONS** column under the **ATTRIBUTE TYPE** grouping.

Verify when **SYSTEM** or **GROUP** appears if the assignment is justified for the user.

Remediation:

To remove the **OPERATIONS** attribute use the RACF **ALTUSER** command:

```
ALTUSER <user-id> NOOPERATIONS
```

To remove **group-OPERATIONS** authority use the RACF **CONNECT** command:

```
CONNECT <user-id> +  
        GROUP(group) +  
        NOOPERATIONS
```

Default Value:

The default user ID **IBMUSER** is assigned system **OPERATIONS** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000720

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: The OPERATIONS attribute](#)
- [z/OS Security Server RACF Security Administrator's Guide: Suggestions for assigning user attributes](#)
- [z/OS Security Server RACF Security Administrator's Guide: Suggestions for assigning group authorities](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			

2.4.2 Ensure that access to TSOAUTH resources is controlled (Automated)

Profile Applicability:

- Level 1

Description:

The **TSOAUTH** resource class controls sensitive privileges. Several of these privileges offer the ability, or provide a facility, to modify sensitive operating system resources.

Rationale:

Failure to control and restrict access to these privileges may result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **TSOAUTH** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **TSOAUTH** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **TSOAUTH** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **TSOAUTH** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries for the following resources:
 - **ACCT**
 - **CONSOLE**
 - **MOUNT**
 - **OPER**
 - **PARMLIB**
 - **TESTAUTH**

Request reports generated using IRRDBU00 output that will allow you to:

Verify That the **ACCT** resources is secured by a profile in the **TSOAUTH** class that:

- Has **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Security Administrators

Verify That the **CONSOLE** and **OPER** resources are secured by a profile in the **TSOAUTH** class that:

- Has **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Operators
 - Systems Programmers

Verify That the **MOUNT** resources is secured by a profile in the **TSOAUTH** class that:

- Has **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Storage Administrators
 - Systems Programmers

Verify That the **PARMLIB** resources is secured by a profile in the **TSOAUTH** class that:

- Has **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** permits are restricted to:
 - Auditors
 - Systems Programmers
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Verify That the **TESTAUTH** resources is secured by a profile in the **TSOAUTH** class that:

- Has **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To activate RACF classes use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(TSOAUTH)
```

To enable generic profile checking for a RACF class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(TSOAUTH)
```

To RACLIST a RACF class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(TSOAUTH)
```

To create a **TSOAUTH** profile use the RACF **RDEFINE** and **PERMIT** commands:

```

RDEFINE TSOAUTH ACCT +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('ACCOUNT, SYNC, AND RACONVRT COMMANDS')

RDEFINE TSOAUTH CONSOLE +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('CONSOLE AND CONSPROF COMMANDS')

RDEFINE TSOAUTH MOUNT +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('ACCESS TO ISSUE DYNAMIC ALLOCATION REQUESTS THAT RESULT -
IN THE NEED FOR VOLUME MOUNTING')

RDEFINE TSOAUTH OPER +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('OPERATOR COMMAND')

RDEFINE TSOAUTH PARMLIB +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('PARMLIB COMMAND')

RDEFINE TSOAUTH TESTAUTH +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('TESTAUTH COMMAND')

PERMIT <profile> CLASS(TSOAUTH) +
    ACCESS(<level>) ID(compliant-entry)

SETROPTS REFRESH RACLIST(TSOAUTH)

```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```

RALTER TSOAUTH <profile> +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    NOWARNING

SETROPTS REFRESH RACLIST(TSOAUTH)

```

To remove a non-compliant access list entry use the RACF **PERMIT** command:

```

PERMIT <profile> CLASS(TSOAUTH) +
    DELETE ID(<non-compliant>)

SETROPTS REFRESH RACLIST(TSOAUTH)

```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **TSOAUTH** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-TS-000010

Additional Information:

- [z/OS TSO/E Customization: Summary of resources protected using RACF](#)
- [z/OS TSO/E Customization: Limiting the use of the TESTAUTH command](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.4.3 Ensure that access to SURROGAT resources is controlled (Automated)

Profile Applicability:

- Level 1

Description:

Surrogate users have the ability to submit jobs on behalf of another user (the execution user) without specifying the execution user's password.

Jobs submitted by surrogate users run with the identity of the execution user.

Rationale:

Failure to control surrogate users could result in unauthorized personnel accessing sensitive resources. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **SURROGAT** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **SURROGAT** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **SURROGAT** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **SURROGAT** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --**

Request reports generated using IRRDBU00 output that will allow you to:

Verify That any profile in the **SURROGAT** class:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate RACF classes use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(SURROGAT)
```

To enable generic profile checking for a RACF class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(SURROGAT)
```

To RACLIST a RACF class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(SURROGAT)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER SURROGAT <profile> +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    NOWARNING  
  
SETROPTS REFRESH RACLIST(SURROGAT)
```

To remove a non-compliant access list entry use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(SURROGAT) +  
    DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH RACLIST(SURROGAT)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **SURROGAT** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-JS-000110

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Allowing surrogate job submission](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.4.4 Ensure that the assignment of the UNIX uid(0) is justified (Automated)

Profile Applicability:

- Level 1

Description:

RACF user IDs, groups, and started tasks that use z/OS UNIX facilities are defined to RACF with attributes including **UID** and **GID**.

Rationale:

If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Audit:

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That user IDs assigned **UID(0)** in their **OMVS** segment is justified.

Remediation:

To modify the **UID** vlaue use the RACF **ALTUSER** command:

```
ALTUSER <user-id> OMVS (UID (<number>))
```

Default Value:

NOOMVS is the default for **USER** profiles.

References:

1. IBM z/OS RACF STIG: RACF-US-000190

Additional Information:

- [z/OS UNIX System Services Planning: Assigning a UID of 0](#)
- [z/OS Security Server RACF Security Administrator's Guide: Superuser authority](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			

2.4.5 Ensure that started tasks defined with the PRIVILEGED attribute is justified (Automated)

Profile Applicability:

- Level 1

Description:

Some started tasks require access to a broad set of resources, making it impractical to permit the started task to each of these resources individually. In these cases, the security administrator can choose between assigning the **TRUSTED** attribute and the **PRIVILEGED** attribute. While both attributes result in all security checks succeeding, the **TRUSTED** attribute allows for logging those accesses, while **PRIVILEGED** does not. For this reason, **TRUSTED** should be chosen over **PRIVILEGED** except for specialized cases which must be justified.

Rationale:

A lack of logging can result in loss of visibility as to what protected resources a started task is accessing.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES** = section.

Verify that **STARTED** appears.

Review the command output in the **GENERIC PROFILE CLASSES** = section.

Verify that **STARTED** appears.

Review the command output in the **SETR RACLIST CLASSES** = section.

Verify that **STARTED** appears.

Request the following **DSMON** report:

```
FUNCTION SYSTEM RACSPT
```

Review the report and for any profiles that have **YES** in the **PRIVILEGED** column:

Verify that the **PRIVILEGED** attribute assignment is justified.

Note: Examples of **PRIVILEGED** assignment justification includes, but is not limited to:

- It is listed as a requirement by the product documentation.

Remediation:

To activate RACF classes use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(STARTED)
```

To enable generic profile checking for a RACF class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(STARTED)
```

To RACLIST a RACF class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(STARTED)
```

To replace **PRIVILEGED** with **TRUSTED** on a **STARTED** profile use the RACF **RALTER** and **SETROPTS** commands:

```
RALTER STARTED <profile> +  
      STDATA(TRUSTED)  
  
SETROPTS REFRESH RACLIST(STARTED)
```

Default Value:

NOPRIVILEGED is the default for **STARTED** profiles.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			

2.4.6 Ensure that access to libraries containing EXIT modules is controlled (Automated)

Profile Applicability:

- Level 1

Description:

System exits have a wide range of uses and capabilities within any system. Exits may introduce security exposures within the system, modify audit trails, and alter individual user capabilities.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data, and the potential of a hacker adding a routine to a library and possibly creating an exposure.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- -- GLOBAL INACTIVE -- or -- NO ENTRIES -- or contains no entries covering EXIT library data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That EXIT library data sets are secured by profiles in the **DATASET** class that:

- Have UACC of NONE or READ
- Are not in WARNING mode
- AUDIT a minimum of SUCCESS(UPDATE) and FAILURES(READ)
- ID(*) is not used to grant access greater than READ
- UPDATE and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      DATA('EXIT LIBRARY')  
  
PERMIT '<profile>' GENERIC +  
      ACCESS(READ) ID(*)  
  
PERMIT '<profile>' GENERIC +  
      ACCESS(ALTER) ID(SYSPROG)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<profile>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000310

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.4.7 Ensure that access to LINKLIST libraries is controlled (Automated)

Profile Applicability:

- Level 1

Description:

The primary function of the **LINKLIST** is to serve as a single repository for commonly used system modules.

Rationale:

Failure to ensure that the proper set of libraries are designated for **LINKLIST** can impact system integrity, performance, and functionality. For this **reason**, controls must be employed to ensure that the correct set of LINKLIST libraries are used. Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering **LINKLIST** library data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That **LINKLIST** library data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE** or **READ**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access greater than **READ**
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +
      UACC(NONE) +
      AUDIT(SUCCESS(UPDATE),FAILURES(READ)) +
      DATA('LINKLIST LIBRARY')

PERMIT '<profile>' GENERIC +
      ACCESS(READ) ID(*)

PERMIT '<profile>' GENERIC +
      ACCESS(ALTER) ID(SYSPROG)

SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<profile>' GENERIC +
      UACC(NONE) +
      AUDIT(SUCCESS(UPDATE),FAILURES(READ)) +
      NOWARNING

SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<profile>' GENERIC +
      DELETE ID(<non-compliant>)

SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000350

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.4.8 Ensure that access to the SYS1.UADS data set is controlled (Automated)

Profile Applicability:

- Level 1

Description:

SYS1.UADS is the data set in which emergency user IDs are maintained. This ensures that logon processing can occur even if RACF is not functional.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- -- GLOBAL INACTIVE -- or -- NO ENTRIES -- or contains no entries covering **SYS1.UADS**

Request reports generated using **IRRD BU00** output that will allow you to:

Verify That **SYS1.UADS** is secured by a profile in the **DATASET** class that:

- Has **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access greater than **READ**
- **READ** permits are restricted to:
 - Auditors
 - Systems Operators
 - Systems Programmers
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD 'SYS1.UADS' GENERIC +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('SYSTEM USER ATTRIBUTE DATA SET (UADS)')  
  
PERMIT 'SYS1.UADS' GENERIC +  
      ACCESS(ALTER) ID(SYSprog)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD 'SYS1.UADS' GENERIC +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT 'SYS1.UADS' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000190

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Security for system data sets](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.4.9 Ensure that access to system page data sets is controlled (Automated)

Profile Applicability:

- Level 1

Description:

System page data sets hold individual pages of virtual storage when they are paged out of real storage.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data. Page datasets access should be limited to system programmers.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering system page data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That system page data sets are secured by profiles in the **DATASET** class that:

- Has **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(FAILURES(READ)) +  
      DATA('SYSTEM PAGE DATA SET')  
  
PERMIT '<profile>' GENERIC +  
      ACCESS(ALTER) ID(SYSPROG)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<profile>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000190

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.4.10 Ensure that MCS console access is controlled through profiles in the CONSOLE resource class (Manual)

Profile Applicability:

- Level 1

Description:

MCS consoles can be used to issue operator commands. When MCS consoles are configured to force a logon in order to be used, the **CONSOLE** class protects the logon access.

Rationale:

Failure to control access to MCS consoles could result in unauthorized personnel issuing sensitive operator commands. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **CONSOLE** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **CONSOLE** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **CONSOLE** appears.

Review the current PARMLIB CONSOLxx members to obtain the list of MCS <console-name>.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **CONSOLE** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering **<console-name>**

For each <console-name> found request reports generated using IRRDBU00 output that will allow you to:

Verify That the **<console-name>** is secured by a profile in the **CONSOLE** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Operators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To activate RACF classes use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT (CONSOLE)
```

To enable generic profile checking for a RACF class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC (CONSOLE)
```

To RACLIST a RACF class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST (CONSOLE)
```

To create a **CONSOLE** profile use the RACF **RDEFINE**, **PERMIT**, and **SETROPTS** commands:

```
RDEFINE CONSOLE <console-name> +  
    UACC (NONE) +  
    AUDIT (FAILURES (READ)) +  
    DATA ('MCS CONSOLE ACCESS')  
  
PERMIT CONSOLE <console-name> +  
    ACCESS (READ) ID (OPERATOR SYSPROG)  
  
SETROPTS REFRESH RACLIST (CONSOLE)
```

Note: You cannot specify the **WHEN** operand on the **RDEFINE** and **RALTER** commands for profiles in the **CONSOLE** class.

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** and **SETROPTS** commands:

```
RALTER CONSOLE <console-name> +  
    UACC (NONE) +  
    AUDIT (FAILURES (READ)) +  
    NOWARNING  
  
SETROPTS REFRESH RACLIST (CONSOLE)
```

Note: You cannot specify the **WHEN** operand on the **RDEFINE** and **RALTER** commands for profiles in the **CONSOLE** class.

To remove a non-compliant access list entry use the RACF **PERMIT** and **SETROPTS** commands:

```
PERMIT CONSOLE <console-name> +  
    DELETE ID (<non-compliant>)  
  
SETROPTS REFRESH RACLIST (CONSOLE)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **CONSOLE** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000410

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Protecting consoles](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.4.11 Ensure that access to system *USER* catalogs is controlled (Automated)

Profile Applicability:

- Level 1

Description:

System catalogs are the basis for locating all files on the system. A **USER** catalog stores the name and location of a data set. The **MASTER** catalog usually stores only a data set high-level qualifier (HLQ) with the name of the user catalog, which contains the location of all data sets prefixed by this HLQ. The HLQ is called an *alias*.

It is best practices to create separate **USER** catalogs for system data sets to ensure that the ability to modify entries is controlled. The actual catalog structure will be different for each site.

System data sets include, but are not limited to:

- Product libraries
- UNIX file systems
- Datasets with a **SYS<x>** HLQ
- Data sets used by SMP/E

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Request a list of system **USER catalogs from the site.**

Note: General guidance is that any **USER** catalog that general users *should not be able to modify* is in scope of this control.

Request the following **DSMON report:**

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering system **USER** catalogs

Request reports generated using **IRRDBU00 output that will allow you to:**

Verify That system **USER** catalog data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access greater than **READ**
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(FAILURES(READ)) +  
      DATA('SYSTEM USER CATALOG')  
  
PERMIT '<profile>' GENERIC +  
      ACCESS(READ) ID(*)  
  
PERMIT '<profile>' GENERIC +  
      ACCESS(ALTER) ID(SYSPROG)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<profile>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000210

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

2.4.12 Ensure that access to Libraries containing EXIT modules is controlled (Automated)

Profile Applicability:

- Level 2

Description:

System exits have a wide range of uses and capabilities within any system. Exits may introduce security exposures within the system, modify audit trails, and alter individual user capabilities.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data, and the potential of a hacker adding a routine to a library and possibly creating an exposure.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- -- GLOBAL INACTIVE -- or -- NO ENTRIES -- or contains no entries covering **EXIT** library data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That **EXIT** library data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<exit-library>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      DATA('EXIT LIBRARY')  
  
PERMIT '<exit-library>' GENERIC +  
      ACCESS(ALTER) ID(SYSprog)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTSD** command:

```
ALTSD '<exit-library>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<exit-library>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000310

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

3 Logging and Auditing

This section describes • How to configure logging to record events • How to aggregate the log of recorded events • How to review the recorded events (auditing) to ensure that the installation security policy is implemented correctly.

3.1 Ensure that SETROPTS CMDVIOL is in effect (Automated)

Profile Applicability:

- Level 1

Description:

The **SETROPTS CMDVIOL** parameter specifies whether RACF is to log violations detected by RACF commands.

Rationale:

The improper setting of this field can compromise the security of the z/OS environment. In addition, failure to establish standardized settings for RACF **SETROPTS** options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ATTRIBUTES =** section.

Verify that **CMDVIOL** appears.

Alternatively, if IBM Health Checker for z/OS is installed and active, you can request the **HZSPRINT** output for:

```
CHECK (IBMRACF,RACF_AUDIT_CONTROLS)
```

Verify that **SETROPTS CMDVIOL is in effect** has a **Value** of **YES**.

Remediation:

To modify the **CMDVIOL** parameter use the RACF **SETROPTS** command:

```
SETROPTS CMDVIOL
```

Default Value:

CMDVIOL is in effect when RACF is using a newly initialized database.

Additional Information:

- [z/OS Security Server RACF Auditor's Guide: Setting and listing audit controls](#)
- [IBM Health Checker for z/OS: RACF_AUDIT_CONTROLS](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

3.2 Ensure that SETROPTS SAUDIT is in effect (Automated)

Profile Applicability:

- Level 1

Description:

The **SETROPTS SAUDIT** parameter specifies whether RACF is to log RACF commands issued by users with the **SPECIAL** or **group-SPECIAL** attribute.

Rationale:

The improper setting of this field can compromise the security of the z/OS environment. In addition, failure to establish standardized settings for RACF **SETROPTS** options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ATTRIBUTES =** section.

Verify that **SAUDIT** appears.

Alternatively, if IBM Health Checker for z/OS is installed and active, you can request the **HZSPRINT** output for:

```
CHECK (IBMRACF,RACF_AUDIT_CONTROLS)
```

Verify that **SETROPTS SAUDIT is in effect** has a **Value** of **YES**.

Remediation:

To modify the **SAUDIT** parameter use the RACF **SETROPTS** command:

```
SETROPTS SAUDIT
```

Default Value:

SAUDIT is in effect when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000520

Additional Information:

- [z/OS Security Server RACF Auditor's Guide: Setting and listing audit controls](#)
- [IBM Health Checker for z/OS: RACF_AUDIT_CONTROLS](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

3.3 Ensure that SETROPTS AUDIT is enabled for ACTIVE classes (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS AUDIT specifies the names of the classes for which you want RACF to perform auditing. For the classes you specify, RACF logs all uses of the **RACROUTE REQUEST=DEFINE SVC** and all changes made to profiles by RACF commands. When the class specified is **USER**, RACF logs all password and password phrase changes made by **RACROUTE REQUEST=VERIFY**.

Rationale:

The improper setting of this field can compromise the security of the z/OS environment. In addition, failure to establish standardized settings for RACF **SETROPTS** options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **AUDIT CLASSES =** section.

Verify that all **ACTIVE** classes appear.

Remediation:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **AUDIT CLASSES =** section.

Verify that all **ACTIVE** classes appear.

Remediation Procedure

To enable **AUDIT** for all classes use the RACF **SETROPTS** command:

```
SETROPTS AUDIT (*)
```

Notes:

- It is generally recommended to activate auditing for all classes via (*) to ease administrative overhead. INACTIVE classes will not generate audit records so there is no disadvantage to enabling the option.
- If you activate auditing for a class using **SETROPTS AUDIT**, RACF activates auditing for all classes in the class descriptor table that have the same **POSIT** value as the class you specify. For example, the classes **TIMS**, **GIMS**, and **AIMS** all have a **POSIT** value of 4 in their respective class descriptor table entries. If you activate auditing for any one of these classes, you activate auditing for all of them.

Default Value:

NOAUDIT (*) is in effect for a class when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Auditor's Guide: Setting and listing audit controls](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

3.4 Ensure that SETROPTS OPERAUDIT is in effect (Automated)

Profile Applicability:

- Level 1

Description:

The **SETROPTS OPERAUDIT** parameter specifies whether RACF is to log all actions allowed only because a user has the **OPERATIONS** or **group-OPERATIONS** attribute.

Rationale:

The improper setting of this field can compromise the security of the z/OS environment. In addition, failure to establish standardized settings for RACF **SETROPTS** options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ATTRIBUTES =** section.

Verify that **OPERAUDIT** appears.

Alternatively, if IBM Health Checker for z/OS is installed and active, you can request the **HZSPRINT** output for:

```
CHECK (IBMRACF,RACF_AUDIT_CONTROLS)
```

Verify that **SETROPTS OPERAUDIT is in effect** has a **Value** of **YES**.

Remediation:

To modify the **OPERAUDIT** parameter use the RACF **SETROPTS** command:

```
SETROPTS OPERAUDIT
```

Default Value:

NOOPERAUDIT is in effect when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000470

Additional Information:

- [z/OS Security Server RACF Auditor's Guide: Setting and listing audit controls](#)
- [IBM Health Checker for z/OS: RACF_AUDIT_CONTROLS](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

3.5 Ensure that SETROPTS INITSTATS is in effect (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS INITSTATS records statistics on all user profiles in the system.

INITSTATS records the following:

- The date and time RACF processes a **RACROUTE REQUEST=VERIFY** (for example, logon or batch job initiation) for a particular user.
- The number of **RACROUTE REQUEST=VERIFY**s for a user to a particular group.
- The date and time of the last **RACROUTE REQUEST=VERIFY** for a user to a particular group.

These statistics are recorded on both the primary and backup databases the first time each day that the user uses the system, each time the user changes their password or password phrase, and each time the user enters the correct password or password phrase after having previously entered an incorrect one. If **SETROPTS NOINACTIVE** is in effect, the update for the first logon of the day is not recorded in the backup database.

At all other times these statistics are recorded only to the primary database. When resident data blocks are used, some resource statistics might not be updated when there is high volume processing and the same profiles are updated by multiple operations. This is more common when the RACF database is shared.

Rationale:

INITSTATS also allows your installation to take advantage of the **SETROPTS INACTIVE** option and the **REVOKE**, **HISTORY**, and **WARNING** options of **SETROPTS PASSWORD**.

Impact:

When RACF is enabled for sysplex communication, the performance of recording the statistics to the backup database should improve because RACF has in-storage buffers for the backup database.

Installations with many RACF users who log on to various applications many times throughout the day, may choose to limit the impact of **INITSTATS** statistics recording for certain applications. These installations can specify that statistics for certain applications should be recorded for each user only once a day. If daily user statistics are set for a particular application, then, when the application issues a **RACROUTE REQUEST=VERIFY**, statistics are recorded only if no recording has been performed for the particular user that day. This can lessen the impact of serialization on the RACF database. To specify daily user statistics for an application, that application must specify the **APPL** operand on the **RACROUTE REQUEST=VERIFY** macro. When an application specifies the **APPL** operand, the system administrator can use a profile in the **APPL** class to control which users can access the application, and can limit **INITSTATS** processing to collect daily statistics only. **To limit **INITSTATS** processing to collect daily statistics only, the system administrator specifies the string '**RACF-INITSTATS(DAILY)**' in the **APPLDATA** field of the **APPL** class profile.** For more information, refer to [z/OS Security Server RACF Security Administrator's Guide](#).

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ATTRIBUTES =** section.

Verify that **INITSTATS** appears.

Alternatively, if IBM Health Checker for z/OS is installed and active, you can request the **HZSPRINT** output for:

```
CHECK (IBMRACF, RACF_PASSWORD_CONTROLS)
```

Verify that **INITSTATS in effect** has a **Value** of **YES**.

Remediation:

To modify the **INITSTATS** parameter use the RACF **SETROPTS** command:

```
SETROPTS INITSTATS
```

Note: For applications that specify the **APPL** operand on the **RACROUTE REQUEST=VERIFY** macro, you can define a profile in the **APPL** class to specify that the application needs only daily statistics recorded for its users. To do this, specify the **RACF-INITSTATS(DAILY)** string in the **APPLDATA** field.

Default Value:

INITSTATS is in effect when RACF is using a newly initialized database.

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: Using options in RACROUTE REQUEST=VERIFY statistics collection](#)
- [z/OS Security Server RACF Security Administrator's Guide: Reducing application logon statistics](#)
- [IBM Health Checker for z/OS: RACF_PASSWORD_CONTROLS](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.3 <u>Disable Dormant Accounts</u> Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.			

3.6 Ensure that the assignment of the RACF AUDITOR or ROAUDIT attribute is justified (Automated)

Profile Applicability:

- Level 1

Description:

A user having the **AUDITOR** attribute has the authority to specify logging options, gives control of logging SMF data and list auditing information.. The **group-AUDITOR** attribute authority is limited to profiles that are within the scope of that group.

Users with the **ROAUDIT** attribute have similar privileges as the **AUDITOR** attribute, but are unable to specify logging options or to control logging to the SMF data set.

Rationale:

With the **AUDITOR** attribute, a user could alter SMF logging data so no trace of the activity could be found. This could destroy audit trace information for RACF system. This attribute should be limited to a minimum number of people. This also applies to the use of **group-AUDITOR** in cases where users are connected to sensitive system dataset HLQ or general resource owning groups with **group-AUDITOR**.

Alternatively, the **ROAUDIT** attribute can be assigned to users who are responsible for auditing RACF but who are not responsible for setting up or changing the auditing options/controls.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACUSR

Review the **AUDITOR** and **ROAUDIT** columns under the **ATTRIBUTE TYPE** grouping.

Verify when **SYSTEM** or **GROUP** appears if the assignment is justified for the user.

Remediation:

To remove the **AUDITOR** or **ROAUDIT** attributes use the RACF **ALTUSER** command:

```
ALTUSER <user-id> +  
        NOAUDITOR +  
        NOROAUDIT
```

To remove **group-AUDITOR** authority use the RACF **CONNECT** command:

```
CONNECT <user-id> +  
        GROUP(<group>) +  
        NOAUDITOR
```

Default Value:

NOAUDITOR and **NOROAUDIT** are the defaults for the **ADDUSER** RACF command.

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: The AUDITOR attribute](#)
- [z/OS Security Server RACF Security Administrator's Guide: The ROAUDIT attribute](#)
- [z/OS Security Server RACF Security Administrator's Guide: Suggestions for assigning user attributes](#)
- [z/OS Security Server RACF Security Administrator's Guide: Suggestions for assigning group authorities](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			

3.7 Ensure that effective SMF records collection options are set (Automated)

Profile Applicability:

- Level 1

Description:

SMF data collection provides a standardized method for recording all system activity to a recording media (file or logstream). including the audit trails from RACF.

Some recording options are mandatory to ensure an effective recording of the activity and therefore complete audit trails.

Rationale:

If the control options for the recording is not set correctly, system audit could be compromised.

Audit:

Issue the following z/OS console command:

```
D SMF,0
```

Look for the following messages:

```
ACTIVE
JWT (<hhmm>)
MAXDORM (<mmss>)
SYS (<options>)
```

Verify that:

- **ACTIVE** is present
- **JWT** value is equal to or less than 15 minutes
- **MAXDORM** specifies a time value of 5 minutes
- **SYS** specifies **DETAIL**

Remediation:

To make changes persistent update the **SMFPRMxx** parmlib member to use:

```
ACTIVE
JWT(0015)
MAXDORM (0500)
SYS(DETAIL)
```

Note: The two alphanumeric characters, represented by xx, are appended to **SMFPRM** to identify your **SMFPRMxx** member.

The site should follow their standard procedures for cycling the SMF started task to apply the changes.

Default Value:

- **ACTIVTE**, which indicates SMF recording is to be active.
- **JWT(0010)**, which indicates 10 minutes.
- **MAXDORM (3000)**, which indicates 30 minutes.
- **NODETAIL**, which is specified for TSO indicating type 32 SMF records contain only the total count of each TSO/E command used.

References:

1. IBM z/OS RACF STIG: RACF-OS-000130

Additional Information:

[MVS Initialization and Tuning Reference: Statements and parameters for SMFPRMxx](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

3.8 Ensure that an automated process is in place to collect and retain SMF data (Manual)

Profile Applicability:

- Level 1

Description:

SMF data collection provides a standardized method for recording all system activity to a recording media (**DATASET** or **LOGSTREAM**), including the audit trails from RACF.

Rationale:

Failure to collect and manage adequate retention of SMF records can result in the loss of critical system data.

Audit:

Review SMF data collection and retention processes. Ensure that the processes utilized include a process which is automatically started to dump SMF collection files immediately upon their becoming full.

To ensure that all SMF data is collected in a timely manner, and to reduce the risk of data loss.

Remediation:

Ensure that automated mechanisms are in place to collect and retain all SMF data produced on the system. Dump the SMF files (**MANx**) in systems based on the following guidelines:

1. Dump each SMF file as it fills up during the normal course of daily processing.
2. Dump all remaining SMF data at the end of each processing day.

The same procedure applies if you use **LOGSTREAM**.

References:

1. IBM z/OS RACF STIG: RACF-OS-000150

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	8.10 <u>Retain Audit Logs</u> Retain audit logs across enterprise assets for a minimum of 90 days.			

3.9 Ensure that required SMF data record types are collected (Automated)

Profile Applicability:

- Level 1

Description:

SMF data collection provides a standardized method for recording all system activity to a recording media (file or logstream). including the audit trails from RACF.

All SMF records are uniquely identified by a type and an optional subtype value. The type and subtype values reside in the header portion of the SMF record. A record type can reside in the Standard SMF record header or in the Extended SMF record header. Subtype values always reside in the Standard SMF record header.

Rationale:

If the required SMF data record types are not being collected, then accountability cannot be monitored, and its use in the execution of a contingency plan could be compromised.

Audit:

Issue the following z/OS console command:

```
D SMF,O
```

Look for the following messages:

```
TYPE (<{aa,bb|aa,bb:zz|aa,bb:zz,...}>)
```

Verify that at a minimum these types and subtypes are collected:

Type	Subtype	Description
0		IPL
6		External Writer / JES Output Writer / Print Services Facility (PSF)
7		SMF Data Lost
14		INPUT or RDBACK Data Set Activity
15		OUTPUT, UPDAT, INOUT, or OUTIN Data Set Activity
17		Scratch Data Set Status

Type Subtype		Description
18		Rename Non-VSAM Data Set Status
24		JES2 Spool Offload
25		JES3 Device Allocation
26		JES Job Purge
30		Common Address Space Work
30	1	~ Job start or start of other work unit
30	2	~ Activity since previous interval ended
30	3	~ Activity for the last interval before step termination
30	4	~ Step total
30	5	~ Job termination or termination of other work unit
30	6	~ System address space, which did not go through full function start
32		TSO/E User Work Accounting
32	1	~ data on TSO/E activity since the start of the session
32	2	~ data on the cumulative TSO/E activity for the entire session
32	3	~ data on TSO/E activity since the start of the session
32	4	~ data on the cumulative TSO/E activity for the entire session
41		DIV Objects and VLF Statistics
42		DFSMS statistics and configuration
43		JES Start
45		JES Withdrawal / Stop
47		JES SIGNON / Start Line (BSC) / LOGON

Type Subtype	Description
48	JES SIGNOFF / Stop Line (BSC) / LOGOFF
49	JES Integrity
52	JES2 LOGON / Start Line (SNA)
53	JES2 LOGOFF / Stop Line (SNA)
54	JES2 Integrity (SNA)
55	JES2 Network SIGNON
56	JES2 Network Integrity
57	JES2 Network SYSOUT Transmission
58	JES2 Network SIGNOFF
60	VSAM Volume Data Set Updated
61	Integrated Catalog Facility Define Activity
62	VSAM Component or Cluster Opened
64	VSAM Component or Cluster Status
65	Integrated Catalog Facility Delete Activity
66	Integrated Catalog Facility Alter Activity
80	Security product Processing
81	RACF Initialization
82	ICSF record
83	RACF Audit Record For Data Sets
90	System Status
92	File System Activity

Type Subtype		Description
92	1	~ Contains information that was written when a file system is mounted
92	2	~ Contains information that was written after the file system is quiesced (or suspended)
92	4	~ Contains information that was written after the file system is unquiesced (or resumed)
92	5	~ Contains information that was written when the file system is unmounted
92	6	~ Contains information that was written when the file system is remounted
92	7	~ Contains information that was written when the file system is moved
92	12	~ Contains MMAP subtype information
92	13	~ Contains MUNMAP subtype information
92	14	~ Contains information that was written when a file or file directory is deleted or renamed
92	15	~ Contains information that was written when a file's security attributes for APF-authorized, program control, or shared library are changed
92	16	~ Contains information that was written when a socket, character special file, pipe, or FIFO is closed
100		Db2 Statistics
101		Db2 Accounting
102		Db2 Performance
103		IBM HTTP Server
103	1	~ Configuration information
103	2	~ Performance information
110		CICS/ESA Statistics

Type	Subtype	Description
110	0	~ CICS journaling
110	1	~ CICS monitoring
110	2	~ CICS statistics
110	3	~ Shared temporary storage queue server statistics
110	4	~ Coupling facility data table server statistics
110	5	~ Named counter sequence number server statistics
118		TCP/IP Statistics
119		TCP/IP Statistics
123		IBM z/OS Connect EE

Remediation:

To make changes persistent update the **SMFPRMxx** parmlib member to collect the required types. The specific parameter to use will depend on whether a site uses log streams for SMF recording.

Note: The two alphameric characters, represented by xx, are appended to **SMFPRM** to identify your **SMFPRMxx** member.

The site should follow their standard procedures for cycling the SMF started task to apply the changes.

Default Value:

TYPE (0:255), which indicates SMF records type 0 to 255 are to be collected.

References:

1. IBM z/OS RACF STIG: RACF-OS-000110

Additional Information:

[MVS Initialization and Tuning Reference: Statements and parameters for SMFPRMxx](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

3.10 Ensure that RACF audit logs is reviewed on a regular basis (Manual)

Profile Applicability:

- Level 1

Description:

Logging, the recording of data about specific events, is the key to auditing the use of RACF at your installation. But you also need to ensure the logs are reviewed at least daily.

Rationale:

It is very important for any organization to have security logs and actively using them to monitor security-related activities.

Security logs must be monitored and analyzed, even real-time if possible (feeding RACF logs to a SIEM) so attacks can be detected quickly, and appropriate response triggered.

Audit:

Verify that site auditors are reviewing RACF event logs (SMF type 80) at least daily, and analyze any security related events.

Including but not limited to:

- invalid access attempts
- new accounts creation
- elevation of privileges
- change of identity
- access to sensitive resources

Remediation:

Ensure that site auditors are reviewing RACF event logs (SMF type 80) at least daily, and analyze any security related events.

Including but not limited to:

- invalid access attempts
- new accounts creation
- elevation of privileges
- change of identity
- access to sensitive resources

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.1 <u>Establish and Maintain an Audit Log Management Process</u> Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

3.11 Ensure regular audits of AC=1 modules in APF authorized libraries are conducted (Manual)

Profile Applicability:

- Level 1

Description:

The **AC=1** modules that reside in APF authorized libraries should be reviewed annually. It is important maintain documentation identifying the integrity and justification of vendor APF authorized libraries. For non-vendor APF authorized libraries, the source and documentation identifying the integrity and justification that describes the **AC=1** module process should be maintained.

Rationale:

Undocumented and/or unauthorized **AC=1** modules have a possible risk to the confidentiality, integrity, and availability of the system and present a clear risk to the operating system, RACF, and customer data.

Audit:

Verify the **AC=1** documentation and compare it to the actual content of the APF authorized libraries.

Remediation:

Any discrepancy must be fixed: documentation updated and/or libraries/modules removed.

References:

1. z/OS RACF STIG :: Release: 36 Benchmark Date: 27 Apr 2018 Vuln ID: V-86
STIG ID: AAMV0060

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

3.12 Ensure that only supported software is installed and active on the system (Manual)

Profile Applicability:

- Level 1

Description:

When a vendor drops support of software, they no longer maintain security vulnerability patches to the software.

Rationale:

Without vulnerability patches, it is impossible to verify that the system does not contain code which could violate the integrity of the operating system environment.

Audit:

Verify that software products currently installed are still supported by the vendor.

Remediation:

Upgrade the software found at a version less than the current supported version. Replace or remove any software out of support.

References:

1. IBM z/OS RACF STIG: RACF-OS-000250

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 <u>Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			

3.13 Ensure all OS software on your system is supported (Manual)

Profile Applicability:

- Level 1

Description:

Vendors' code may contain vulnerabilities that may be exploited to cause denial of service or to violate the integrity of the system or data on the System. Most vendors do not develop patches to correct these vulnerabilities on unsupported releases of their software.

Rationale:

With unsupported software on the system, it is impossible to verify that the system does not contain code which could violate the integrity of the operating system environment.

Audit:

Verify that site has a formal migration plan for removing or upgrading OS systems software prior to the date the vendor drops security patch support.

Remediation:

Implement a formal migration plan for removing or upgrading OS systems software prior to the date the vendor drops security patch support.

Additional Information:

For IBM products, register for access to the IBM Z and LinuxONE Security Portal System integrity

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 <u>Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			

3.14 Implement sensitive z/OS data set monitoring (Manual)

Profile Applicability:

- Level 1

Description:

It is important to monitor changes, additions or removal from APF and LPA libraries, as well as changes to **SYS1.PARMLIB PDS** members. A monitoring tool should be implemented to monitor the modification to the sensitive z/OS datasets modification.

Rationale:

Failure to monitor and review these reports on a regular basis and validating any changes could threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

Verify the site is monitoring z/OS sensitive datasets modifications.

Remediation:

Implement a z/OS sensitive dataset monitoring tool.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 <u>Deploy and Maintain Anti-Malware Software</u> Deploy and maintain anti-malware software on all enterprise assets.			

3.15 Ensure that SETROPTS REALDSN is in effect (Automated)

Profile Applicability:

- Level 1

Description:

If your installation is using the naming conventions table or installation exits to convert data set names, you can specify that RACF put the actual data set names used by **RACROUTE REQUEST=AUTH** and **REQUEST=DEFINE** into any SMF log record and operator messages by enabling the **SETROPTS REALDSN** option.

Note: This option has no effect on single-qualifier data set names (unless they have been modified by the naming conventions table or an exit routine), whose real data set names continue to be the prefixed ones.

Rationale:

Enabling the **REALDSN** option ensures that log printouts and operator messages identify data sets by their real names rather than by the data set names that are created by installation exit routines to conform to RACF naming conventions.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Verify the following message is present:

```
REAL DATA SET NAMES OPTION IS ACTIVE
```

Remediation:

To enable **REALDSN** use the RACF **SETROPTS** command:

```
SETROPTS REALDSN
```

Default Value:

NOREALDSN is in effect when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Displaying and logging real data set names \(REALDSN option\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			

4 System Resilience

This section describes how to configure your RACF environment to be resilient against hardware and software errors.

4.1 Ensure that RACF database is backed up on a scheduled basis (Manual)

Profile Applicability:

- Level 1

Description:

If backups of the operating environment are not processed, implementation of a contingency plan would not include the data necessary to fully recover from any outage.

RACF database backups reduce system recovery time.

Rationale:

If regularly scheduled backups of this database are not processed, system recovery time could be unacceptably long.

Audit:

Verify that site RACF databases are backed up at least daily.

Remediation:

Implement a daily backup.

References:

1. IBM z/OS RACF STIG: RACF-ES-000640

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.2 Perform Automated Backups Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.			

4.2 Ensure that the RACF PRIM and BACK databases are isolated (Manual)

Profile Applicability:

- Level 1

Description:

RACF backup and recovery data files provide the only means of recovering RACF database in the event of its damage.

Rationale:

In the case where this damage is to the physical volume on which it resides, and any of these recovery data files exist on this volume as well, then complete recovery of the RACF database would be extremely difficult, if even possible.

Audit:

Issue the following TSO command:

```
RVARY LIST
```

Verify that the **VOLUME** values for the **PRIM** and **BACK** are **different** for RACF databases that have **YES** in the **ACTIVE** column.

Remediation:

Issue the following TSO command:

```
RVARY LIST
```

Verify that the **VOLUME** values for the **PRIM** and **BACK** are **different** for RACF databases that have **YES** in the **ACTIVE** column.

Remediation Procedure

Consult the [z/OS Security Server RACF Security System Programmer's Guide](#) for guidance on moving the RACF database data sets.

Note: Depending upon your configuration, modify the **ICHRDSNT** load module table or the **IRRPMMxx PARMLIB** member and plan an IPL of the system (or the entire sysplex if in **DATASHARING** mode).

References:

1. IBM z/OS RACF STIG: RACF-ES-000630

Additional Information:

- [z/OS Security Server RACF Security System Programmer's Guide: RACF database split/merge/extend utility program \(IRRUT400\)](#)
- [z/OS Security Server RACF Security System Programmer's Guide: Specifying RACF database options](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.4 Establish and Maintain an Isolated Instance of Recovery Data Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.			

4.3 Ensure sensitive data sets are encrypted with z/OS data set encryption (Manual)

Profile Applicability:

- Level 1

Description:

With z/OS data set encryption, you are able to protect data residing on disk from being viewed by unauthorized users in the clear. Authorization is based on access to the key label that is associated with the data set and used by the access methods to encrypt and decrypt the data.

Rationale:

Implementing z/OS dataset encryption ensures that even privileged users, like storage administrators, can manage sensitive data sets without being able to view the contents.

Impact:

It is recommended that clients using host-based encryption also use host-based compression before the encryption of the data. If the data is not compressed prior to the encryption there can be consequences other parts of the client infrastructure. For example, replicated data that is being compressed in the SAN infrastructure by DWDM technology will no longer be effective trying to compress encrypted data. Without compressing before to the encryption of the data, additional bandwidth might be required.

Another example might be that tape systems can require additional capacity in terms of disk space, in the case of virtual tape, or tape cartridges. If deduplication of data is supported, host encryption can prevent deduplication from working. Therefore, where possible, use compressed format data sets. With encrypted compressed format data sets, the access methods perform compression before encryption.

See [z/OS DFSMS Using Data Sets: Considerations when planning for data set encryption](#) for more information.

Audit:**Request a list of data sets containing sensitive data.**

Issue the following TSO command for each data set:

```
LISTCAT ALL ENTRIES('<dataset-name>')
```

Review the command output in the **ENCRYPTIONDATA** section.

Verify that the following message appears:

```
DATA SET ENCRYPTION----- (YES)
```

Note: Example acceptable exclusions includes, but is not limited to:

- The data set *is not* managed by the Storage Management Subsystem (SMS).
- The data set type *is not* supported by data set encryption.
- Vendor documentation states the data set must **not** be encrypted (i.e. restrictions documented in [z/OS DFSMS Using Data Sets: Data set encryption](#)).
- There is evidence proving that encryption is managed by the application (i.e. Integrated Cryptographic services Facility (ICSF) xKDS data sets).

Remediation:

Consult the [z/OS DFSMS Using Data Sets: Data set encryption](#) manual section for guidance on establishing z/OS data set encryption.

Default Value:

No encryption is the default for data sets.

References:

1. IBM z/OS RACF STIG: RACF-ES-000630

Additional Information:

[z/OS DFSMS Using Data Sets: Data set encryption](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			

4.4 Ensure that RACF application identity mapping (AIM) is at stage 3 (Manual)

Profile Applicability:

- Level 1

Description:

Application identity mapping in its final stage, stage 3, is an alternative to the use of mapping profiles to associate RACF user and group names with z/OS UNIX, Lotus Notes, and Novell Directory Services identifiers. For these associations, **IRRIRA00** converts the database mapping profile information into an alias index, which uses less space.

Rationale:

RACF database application identity mapping (AIM) stage 3 allows RACF to more efficiently handle authentication and authorization requests from applications such as z/OS UNIX and is required to use some RACF function.

Impact:

If RACF is enabled for sysplex communication, whenever you need to run **IRRIRA00** against a database that is active on a system that is a member of the RACF data sharing group, always run the utility from a system in the group. If you do not, you might damage your RACF database, or receive unpredictable results from the utility.

Audit:

Request the **SYSPRINT** from **IRRIRA00** run without parameters, similar to this example job:

```
//DBSTAGE JOB
//STEP EXEC PGM=IRRIRA00
//SYSPRINT DD SYSOUT=A
```

Verify that the message returned is: **IRR66017I The system is currently operating in stage 3.**

Alternatively, if IBM Health Checker for z/OS is installed and active, you can request the **HZSPRINT** output for:

```
CHECK(IBMRACF,RACF_AIM_STAGE)
```

Verify that the message returned is:

```
IRRH500I The RACF database is at the suggested stage of application
identity mapping (AIM). The database is at AIM stage 03.
```

Remediation:

Refer to the [Security Server RACF System Programmer's Guide](#) for considerations and instructions on using the **IRRIRA00** utility to advance the application identity mapping stage for RACF databases.

Default Value:

RACF databases created with **IRRMIN00 PARM=NEW** for OS/390 Release 10 or later are already initialized for AIM stage 3.

Additional Information:

- [IBM Health Checker for z/OS: RACF_AIM_STAGE](#)
- [Security Server RACF System Programmer's Guide: RACF internal reorganization of aliases utility program \(IRRIRA00\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

4.5 Ensure that RACF ENQ names are not in the Global Resource Serialization (GRS) Resource Name List (Manual)

Profile Applicability:

- Level 1

Description:

During its normal course of processing, RACF performs numerous serialization requests using the Global Resource Serialization (GRS) **RESERVE**, **ENQ**, and **DEQ** services. These serialization requests allow RACF to ensure that changes to the RACF database and RACF control blocks are done in a consistent manner, maintaining the integrity of RACF data.

Depending on the type of the serialization that RACF requires, RACF serializes at either the address space (**SCOPE=STEP**), single MVS image (**SCOPE=SYSTEM**) or multiple MVS image/Sysplex level (**SCOPE=SYSTEMS**). GRS identifies a serialization request by an eight character **QNAME** (or major name) and **RNAME** (or minor name) of up to 255 characters.

GRS allows installations to tailor the processing of **RESERVE**, **ENQ**, and **DEQ** requests through the use of Resource Name Lists (RNLs).

Rationale:

Installations that use GRS to convert RACF **SYSTEMS ENQ** to **SYSTEM ENQ** can corrupt the RACF data base and experience outages.

Audit:

Request the **HZSPRINT** output for:

```
CHECK (IBMRACF, RACF_GRS_RNL)
```

Verify that the message returned is:

```
IRRH203I    No RACF ENQ names were found in the GRS Resource Name List.
```

OR

```
THE CHECK IS NOT APPLICABLE IN THE CURRENT SYSTEM ENVIRONMENT.
```

Remediation:

RACF resource names are removed from the specified resource name list (RNL) returned by the **RACF_GRS_RNL** health check.

Additional Information:

[IBM Health Checker for z/OS: RACF_GRS_RNL](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

4.6 Ensure that SETROPTS GRPLIST is in effect (Automated)

Profile Applicability:

- Level 1

Description:

List-of-groups (**GRPLIST**) authority checking supplements the normal RACF access authority checking by allowing all groups of which a user ID is a member to enter into the access list checking process. This process replaces the checking that compares the current connect group with the resource's access list, and can expand a user's ability to access resources. If **GRPLIST** is active, then regardless of which group the user is logged on to, RACF recognizes the user's group-related authorities in other connect groups. If a user is in more than one group and tries to access a resource, RACF uses the highest authority allowed by the user's list of groups and the resource's access list.

Rationale:

Enabling **GRPLIST** is recommended because it eases administration and minimizes the number of times a user might have to log off and log back on to access resources.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Verify the following message is present:

```
LIST OF GROUPS ACCESS CHECKING IS ACTIVE.
```

Remediation:

To activate list-of-groups authority checking use the RACF **SETROPTS** command:

```
SETROPTS GRPLIST
```

Default Value:

NOGRPLIST is in effect when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Activating list-of-groups checking \(GRPLIST option\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

4.7 Ensure that SETROPTS NOSTATISTICS(*) is in effect (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS NOSTATISTICS(*) bypasses the recording of statistical information in profiles.

We are recommending to bypass resource statistics collection because:

- Access counts kept only on DISCRETE profiles
- Counts are not incremented for GAT permitted access or RACLISTed profiles
- Counts are not accurate in a shared database environment

Rationale:

The statistical information collected is inaccurate and/or misleading, making it an unreliable at best metric that is stored as part of a RACF profile.

Impact:

Failure to bypass resource statistics collection can needlessly increase CPU processing to calculate and I/O to update a profile.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Verify the STATISTICS = section is empty.

Remediation:

To bypass resource statistics collection use the RACF SETROPTS command:

```
SETROPTS NOSTATISTICS (*)
```

Default Value:

STATISTICS is in effect for the DATASET, DASDVOL, TAPEVOL, and TERMINAL classes when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Bypassing resource statistics collection](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

4.8 Ensure that RACF is enabled for Sysplex communication (Automated)

Profile Applicability:

- Level 1

Description:

This recommendation is not applicable for systems that are not part of a Sysplex.

When RACF is enabled for sysplex communication, it uses Cross-system Coupling Facility (XCF) to join the RACF data sharing group, **IRRXCF00**. The data sharing group facilitates communication between systems in the sysplex enabled for sysplex communication.

Rationale:

Because work can be distributed around the sysplex, all systems in the sysplex must have the same security information. Therefore, all systems in a sysplex should use the same RACF database. Additionally, when used definitions for security categories (members of the **CATEGORY** profile in the **SECDATA** general resource class) are likely to cause problems if all systems do not use the same RACF database.

Impact:

When RACF is enabled for sysplex communication, it allocates in-storage buffers for the backup database (20% of the number allocated for the primary database), to reduce I/O to the backup device. Additionally, a minimum of 50 buffers are used for the primary database. As a consequence, you might notice an increased ECSA usage for the in-storage buffers.

Audit:

Request the **HZSPRINT** output from each system in a sysplex for:

```
CHECK (IBMRACF, RACF_SYSPLEX_COMMUNICATION)
```

Verify that the message returned is:

```
IRRH343I Sysplex Communication is enabled.
```

Remediation:

Refer to the [Security Server RACF System Programmer's Guide](#) for considerations and instructions on enabling sysplex communication.

Additional Information:

[IBM Health Checker for z/OS: RACF_SYSPLEX_COMMUNICATION](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 <u>Centralize Account Management</u> Centralize account management through a directory or identity service.		●	●
v8	6.7 <u>Centralize Access Control</u> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●

4.9 Ensure that Validated Boot for z/OS is in effect (Manual)

Profile Applicability:

- Level 2

Description:

Validated Boot for z/OS is a solution that uses digital signatures to provide an initial program load (IPL)-time check that validates that IPL data is intact, not tampered with, and originated from a trusted source. It also enables detection of unauthorized changes to software executables.

Rationale:

By using Validated Boot for z/OS, you have the ability to meet regulatory compliance standards, including National Information Assurance Partnership (NIAP) certification, that are required for certain secure software deployment scenarios. Additionally, you can detect both accidental and malicious IPL data changes earlier, thus reducing the impact of outages and stopping certain kinds of attacks.

Audit:

Issue the following console command on each production z/OS system:

```
D IPLINFO
```

Verify the following message is **not** present:

```
VALIDATED BOOT: NO
```

Remediation:

Consult the dedicated [Validated Boot for z/OS](#) support page.

Additional Information:

[Validated Boot for z/OS](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			

4.10 Ensure that the site is registered to the IBM Z and IBM LinuxONE Security Portal (Manual)

Profile Applicability:

- Level 1

Description:

The IBM Z and IBM LinuxONE Security Portal currently has Security/Integrity (**Sec/Int**) APAR information for the z/OS and z/VM operating systems and associated IBM products that ship fixes via PTF, along with critical Security Notices that address hardware, firmware, and software issues.

IBM does not make **Sec/Int data publicly available for IBM Z.** The Security Portal provides a controlled notification and distribution mechanism to help ensure this critical information is available to IBM Z clients that have completed the required vetting process, including agreement to the terms and conditions.

Rationale:

For z/OS the Security Portal provides enhanced **HOLDDATA** for **Sec/Int** APARs, as well as a CVSS data file. Together, these files can be used by the site's IBM Z patch management team to help identify what APARs are applicable, as well as determine their urgency and the CVSS Vector.

Audit:

Verify that *if* the site is an IBM Z client with a need-to-know, at least **one** person is registered *and* subscribed to the Security Portal.

Remediation:

The instructions for requesting access to the Security Portal can be found at: [IBM Z and IBM LinuxONE Security Portal Registration](#)

Additional Information:

- [IBM Z and IBM LinuxONE Security Portal Registration](#)
- [IBM Z and IBM LinuxONE Security Portal Frequently Asked Questions](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.1 Establish and Maintain a Vulnerability Management Process</u> Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

5 Storage Management

This section describes the Storage Management recommendations.

5.1 Ensure that DFSMS is configured (Manual)

Profile Applicability:

- Level 1

Description:

Configuration properties of DFSMS are specified in various members of the system parmlib concatenation (e.g., **SYS1.PARMLIB**). Statements within these **PDS** members provide the execution, operational, and configuration characteristics of the system-managed storage environment.

In the **IGDSMSxx** member, SMS parameter settings are specified.

Rationale:

Missing or inappropriate configuration values may result in undesirable operations and degraded security. This exposure could potentially compromise the availability and integrity of some system services and customer data.

Audit:

Verify the active **IGDSMSxx** member(s) specifies a minimum of:

- **SMS**
- **ACDS(<dataset-name>)**
- **COMMDS(<dataset-name>)**

Remediation:

To make changes persistent update the **IGDSMSxx** member to use:

```
SMS
ACDS (<dataset-name>)
COMMDS (<dataset-name>)
```

The site should follow their standard procedures for cycling the SMF started task to apply the changes.

Default Value:

If you do not define an **IGDSMSxx** member, the system will attempt to use member **IGDSMS00** by default. IBM does not supply this member; your installation must create it.

References:

1. IBM z/OS RACF STIG: RACF-SM-000050

Additional Information:

[MVS Initialization and Tuning Reference: IGDSMSxx \(storage management subsystem definition\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

5.2 Ensure that access to the Tape Bypass Label Processing (BLP) resource is controlled (Automated)

Profile Applicability:

- Level 1

Description:

Tape Bypass Label Processing (BLP) is extremely sensitive, as it allows the circumvention of security access checking for the data. When BLP is used in z/OS, the only verification that is done is for the data set name in the JCL. Any data set name can be used. A user could specify a data set name that he has access to, the job would pass the validation check, and the job would be processed, giving access to the data. BLP is typically used for tapes that are external to the tape management system used on the processor. BLP should be granted to only a limited number of people, preferably the tape librarian and a few key people from the operations staff. If an unauthorized user possesses BLP authority, they could potentially read any restricted tape and modify any information once it has been copied.

Rationale:

If an unauthorized user possesses BLP authority, they could potentially read any restricted tape and modify any information once it has been copied.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the ACTIVE CLASSES = section.

Verify that FACILITY appears.

Review the command output in the GENERIC PROFILE CLASSES = section.

Verify that FACILITY appears.

Review the command output in the SETR RACLIST CLASSES = section.

Verify that FACILITY appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the FACILITY entry has:

- -- GLOBAL INACTIVE -- or -- NO ENTRIES -- or contains no entries covering the ICHBLP resource

Request reports generated using IRRDBU00 output that will allow you to:

Verify That the ICHBLP resource is secured by a profile in the FACILITY class that:

- Has UACC of NONE
- Is not in WARNING mode
- AUDIT a minimum of FAILURES(READ)
- ID(*) is not used to grant access
- READ and higher permits are restricted to:
 - Storage Administrators
 - Systems Operators
 - Systems Programmers

If the site *does not* use a tape management system, then the following requirements apply:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the ACTIVE CLASSES = section.

- **Verify** that TAPEVOL appears.

Review the command output in the GENERIC PROFILE CLASSES = section.

- **Verify** that TAPEVOL appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that:

- The TAPEVOL entry has:
 - -- GLOBAL INACTIVE -- or -- NO ENTRIES --

Request reports generated using IRRDBU00 output that will allow you to:

Verify that all profiles in the TAPEVOL class:

- Have UACC of NONE
- Are not in WARNING mode
- AUDIT a minimum of FAILURES(READ)
- ID(*) is not used to grant access
- READ and higher permits are restricted to:
 - Storage Administrators
 - IDs authorized to access these resources at this level

Remediation:

To activate RACF classes use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FACILITY)
```

To enable generic profile checking for a RACF class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FACILITY)
```

To RACLIST a RACF class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FACILITY)
```

To create a **FACILITY** profile use the RACF **RDEFINE**, **PERMIT**, and **SETROPTS** commands:

```
RDEFINE FACILITY ICHBLP +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    DATA('TAPE BYPASS LABEL PROCESSING (BLP)')  
  
PERMIT ICHBLP CLASS(FACILITY) +  
    ACCESS(UPDATE) ID(STGADMIN OPERATOR SYSPROG)  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** and **SETROPTS** commands:

```
RALTER FACILITY ICHBLP +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    NOWARNING  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant access list entry use the RACF **PERMIT** and **SETROPTS** commands:

```
PERMIT ICHBLP CLASS(FACILITY) +  
    DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:


```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **FACILITY** and **TAPEVOL** classes are **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000140

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: RACF authorization of bypass label processing \(BLP\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

5.3 Ensure that SETROPTS ADSP is disabled (Automated)

Profile Applicability:

- Level 1

Description:

With the **SETROPTS NOADSP** operand in effect, RACF does not automatically create **DISCRETE DATASET** profiles when users who have the **ADSP** attribute create new data sets.

Rationale:

IBM recommends the **NOADSP** option because it reduces the number of data set profiles in the RACF database. Using **GENERIC** data set profiles is generally more efficient and auditable.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Verify the following message appears:

```
AUTOMATIC DATASET PROTECTION IS NOT IN EFFECT
```

Remediation:

To modify the **ADSP** parameter use the RACF **SETROPTS** command:

```
SETROPTS NOADSP
```

Default Value:

ADSP is in effect when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000740

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Bypassing automatic data set protection \(NOADSP option\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

5.4 Ensure that access to DFSMS control data sets is controlled (Automated)

Profile Applicability:

- Level 1

Description:

DFSMS control data sets provide the configuration and operational characteristics of the system-managed storage environment.

Rationale:

Failure to protect these data sets may result in unauthorized access. This exposure could compromise the availability and integrity of some system services and customer data.

Audit:

request the following values from the active **IGDSMSxx** member(s):

- Source Control Data Set (**SCDS**)
- Active Control Data Set (**ACDS**)
- Communications Data Set (**COMMDS**)
- Automatic Class Selection Routine Source Data Sets (**ACS**)
- Active Data set (**ACDS**) Backup
- Communication Data Set (**COMMDS**) Backup

These are the DFSMS control data sets.

Request the following **DSMON report:**

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering DFSMS control data sets

Request reports generated using **IRRDBU00 output that will allow you to:**

Verify That the DFSMS control data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access higher than **READ**
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +
      UACC(NONE) +
      AUDIT(FAILURES(READ)) +
      DATA('DFSMS CONTROL LIBRARY')

PERMIT '<profile>' GENERIC +
      ACCESS(READ) ID(*)

PERMIT '<profile>' GENERIC +
      ACCESS(ALTER) ID(SYSPROG)

SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<profile>' GENERIC +
      UACC(NONE) +
      AUDIT(FAILURES(READ)) +
      NOWARNING

SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<profile>' GENERIC +
      DELETE ID(<non-compliant>)

SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-SM-000020

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

6 Networking

This section describes the Networking recommendations.

6.1 CSSMTP Recommendations

This section describes the CSSMTP recommendations.

6.1.1 Ensure CSSMTP started task user ID is PROTECTED (Automated)

Profile Applicability:

- Level 1

Description:

Protected user IDs are protected from being used to logon to the system and from being revoked through inactivity or unsuccessful attempts to access the system using incorrect passwords and password phrases. However, they can be revoked using the **ALTUSER REVOKE** command.

Rationale:

We recommend assigning protected user IDs to z/OS UNIX, and to the UNIX daemons, started procedures, applications, servers or subsystems associated with z/OS UNIX, to minimize their exposure to inadvertent or malicious misuse or revocation.

Impact:

A protected user ID cannot be used to enter the system by any method that uses, a supplied password, such as TSO logon, CICS signon, PassTicket authentication, z/OS UNIX rlogin, batch job submission when a password is specified using the **PASSWORD** parameter of the **JOB** statement, or by supplying a password phrase. Before assigning the **PROTECTED** attribute to a user ID, you should ensure that the user ID will not be used in any situation where specification of a password, PassTicket, or password phrase is required.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACSPT

Use the **ASSOCIATED USER** column to determine the user ID associated with CSSMTP.

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that the CSSMTP started task RACF user ID:

- Has the **PROTECTED** attribute

Remediation:

To make a user ID **PROTECTED** use the RACF **ALTUSER** command:

```
ALTUSER <user-id> +  
        NOPASSWORD +  
        NOPHRASE +  
        NOOIDCARD
```

Default Value:

When the **ADDUSER** command is issued to create a user ID and you specify **NOOIDCARD** (or you allow this option to default), do not specify **PHRASE**, and if you specify **NOPASSWORD** or you omit the **PASSWORD** keyword, by default the ID will be created with the **PROTECTED** attribute.

References:

1. IBM z/OS CSSMTP for RACF STIG: ZSMTR030

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Defining protected user IDs](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			

6.1.2 Ensure that the *STARTED* resource class is used to assign user IDs to CSSMTP started tasks (Automated)

Profile Applicability:

- Level 1

Description:

Started procedures have system generated job statements that do not contain the user, group, or password statements. To enable the started procedure to access the same protected resources that users and groups access, started procedures must have an associated user ID. If a user ID is not associated with the started procedure, the started procedure will not have access to the resources.

User ID can be assigned through the RACF **STARTED** class or through the **ICHRIN03** table. As it is easily auditable, does not require assembler knowledge or a system IPL for changes, we require the usage of the RACF **STARTED** class.

Rationale:

If a user ID is not associated with the started procedure, the started procedure will not have access to the resources. By default started procedures should be assigned a user ID with limited privileges to prevent otherwise undefined tasks from getting unintentional access to resources secured by RACF.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES** = section.

Verify that **STARTED** appears.

Review the command output in the **GENERIC PROFILE CLASSES** = section.

Verify that **STARTED** appears.

Review the command output in the **SETR RACLIST CLASSES** = section.

Verify that **STARTED** appears.

Request the following **DSMON** report:

```
FUNCTION SYSTEM RACSPT
```

Verify that the CSSMTP started task(s) appear in the **FROM PROFILES IN THE STARTED CLASS**: section **and not** the **FROM THE STARTED PROCEDURES TABLE (ICHRIN03)**: section.

Remediation:

To activate the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT (STARTED)
```

To enable generic profile checking for the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC (STARTED)
```

To RACLIST the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST (STARTED)
```

To create a **STARTED** profile use the RACF **RDEFINE** and **SETROPTS** commands:

```
RDEFINE STARTED CSSMTP.* +  
    UACC(NONE) +  
    DATA('COMM SERVER SIMPLE MAIL TRANSFER PROTOCOL (CSSMTP)') +  
    STDATA( +  
        USER(<cssmtp-user>) +  
        GROUP(<cssmtp-group>) +  
    )  
  
SETROPTS REFRESH RACLIST (STARTED)
```

Default Value:

- The **STARTED** class is **INACTIVE** when RACF is using a newly initialized database.
- The **ICHRIN03** started procedures table is used to associate the names of started procedures with user IDs.

References:

1. IBM z/OS CSSMTP for RACF STIG: ZSMTR032

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 <u>Allowlist Authorized Software</u> Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.			
v8	4.6 <u>Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			

6.1.3 Ensure AT-TLS protection is enabled for CSSMTP (Manual)

Profile Applicability:

- Level 1

Description:

During the TLS handshake process, mutually acceptable suite of cryptographic algorithms is selected by the server and client. The algorithms specified in the selected suite are used to cryptographically protect the data that subsequently flows between the two. To apply TLS protection of adequate strength, either the CSSMTP application must be configured to use AT-TLS protection, or the JES batch jobs that send mail through CSSMTP must use the **STARTTLS** command.

Rationale:

Failure to properly enforce adequate encryption strength could result in the loss of data privacy.

Impact:

The cryptographic operations involved in TLS do come with a CPU cost. Most of the recommended algorithms are optimized through the use of hardware acceleration. Depending on the number and frequency of TLS handshakes, the CPU impact could be noticeable.

Audit:

Refer to the CSSMTP configuration file specified on the **CONFIG DD** statement in the CSSMTP started task JCL.

Verify that each **TargetServer** statement specifies the **SECURE YES** parameter.

Note: For any **TargetServer** that does not specify **SECURE YES**, then **verify** that each JES batch job that sends mail through CSSMTP uses the **STARTTLS** command to specifically request TLS protection of its outbound mail to the target Message Transfer Agent (MTA).

Remediation:

The site will need to follow their standard change management process for updating CSSMTP configuration file statements with compliant values.

Default Value:

No TLS protection is applied.

Additional Information:

[z/OS Communications Server - IP Configuration Reference: TargetServer statement](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

6.1.4 Ensure that access to CSSMTP started task data sets is controlled (Automated)

Profile Applicability:

- Level 1

Description:

The IBM Communications Server Simple Mail Transfer Protocol (CSSMTP) STC uses privileged functions and accesses to sensitive data. The data sets CSSMTP relies upon for its configuration, runtime environment and operation must be properly protected from unauthorized modifications or retrieval to ensure system integrity and privacy of sensitive data.

Rationale:

Failure to properly restrict access to their data sets could result in violating the integrity of the base product which could result in compromising the operating system or sensitive data.

Audit:

The data sets to be protected are identified in the data set referenced in the **DD** statements of the CSSMTP started task(s) and/or batch job(s).

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE --** or **-- NO ENTRIES --** or contains no entries covering CSSMTP STC data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That CSSMTP STC data sets are secured by profiles in the **DATASET** class that:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** permits are restricted to:
 - Auditors
 - Systems Programmers
 - IDs authorized to access these resources at this level
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(FAILURES(READ)) +  
      DATA('CSSMTP')  
  
PERMIT '<profile>' GENERIC +  
      ACCESS(ALTER) ID(SYSprog)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<profile>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS CSSMTP for RACF STIG: ZSMTR001

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

6.2 FTP Recommendations

This section describes the FTP recommendations.

6.2.1 Ensure that the STARTED resource class is used to assign user IDs with proper parameters to FTP server started tasks (Automated)

Profile Applicability:

- Level 1

Description:

The FTP Server daemon requires special privileges and access to sensitive resources to provide its system services. As such, the data sets the FTP Server daemon relies upon for its configuration, runtime environment and operation must be properly protected from unauthorized modifications or retrieval to ensure system integrity and privacy of sensitive data.

Rationale:

Failure to properly define and control the FTP Server daemon could lead to unauthorized access. This exposure may result in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **STARTED** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **STARTED** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **STARTED** appears.

Request the following **DSMON** report:

```
FUNCTION SYSTEM RACSPT
```

Verify that the FTP Server daemon started task(s) appear in the **FROM PROFILES IN THE STARTED CLASS:** section **and not** the **FROM THE STARTED PROCEDURES TABLE (ICHRIN03):** section.

Use the **ASSOCIATED USER** column to determine the user ID associated with the FTP Server daemon.

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that the FTP Server daemon started task RACF user ID:

- Has the **PROTECTED** attribute
- Has the following **OMVS** segment attributes:
 - **UID** is 0
 - **HOME** is /
 - **PROGRAM** is /bin/sh

Remediation:

To activate the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(STARTED)
```

To enable generic profile checking for the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(STARTED)
```

To RACLIST the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(STARTED)
```

To create a **STARTED** profile use the RACF **RDEFINE** and **SETROPTS** commands:

```
RDEFINE STARTED FTPD*.* +  
    UACC(NONE) +  
    DATA('FTP SERVER DAEMON') +  
    STDATA( +  
        USER(<ftpd-user>) +  
        GROUP(<ftpd-group>) +  
    )  
  
SETROPTS REFRESH RACLIST(STARTED)
```

To make a user ID **PROTECTED** use the RACF **ALTUSER** command:

```
ALTUSER <ftpd-id> +  
    NOPASSWORD +  
    NOPHRASE +  
    NOOIDCARD
```

To modify the **OMVS** segment for a user ID use the RACF **ALTUSER** command:

```
ALTUSER <ftpd-id> +  
    OMVS( +  
        UID(0) +  
        HOME('/') +  
        PROGRAM('/bin/sh') +  
    )
```

Notes:

1. If the security administrator has defined the **SHARED.IDS** profile in the **UNIXPRIV** class, the **UID** value must be unique. Use the **SHARED** keyword in addition to **UID** to assign a value that is already in use.
2. **OMVS DIRECTORY** and **PROGRAM** values are case sensitive, so be sure they are entered as-is and not translated to upper case.

Default Value:

- When the **ADDUSER** command is issued to create a user ID and you specify **NOOIDCARD** (or you allow this option to default), do not specify **PHRASE**, and if you specify **NOPASSWORD** or you omit the **PASSWORD** keyword, by default the ID will be created with the **PROTECTED** attribute.
- When the **ADDUSER** command is issued to create a user ID and you omit the **OMVS** keyword, by default the ID will be created with **NOOMVS**.
- The **ICHRIN03** started procedures table is used to associate the names of started procedures with user IDs.

References:

1. IBM z/OS RACF STIG: RACF-FT-000100

Additional Information:

[z/OS Communications Server - IP Configuration Guide: Configuring the FTPD cataloged procedure](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	5.5 Establish and Maintain an Inventory of Service Accounts Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			

6.2.2 Ensure startup parameters for the FTP daemon do not allow ANONYMOUS or INACTIVE keywords (Manual)

Profile Applicability:

- Level 1

Description:

During initialization, the FTP daemon reads JCL keywords and configuration files to determine values for critical operational parameters. Because system security is impacted by some of these parameter settings, controlling these options through the configuration file only and explicitly specifying the file locations reduces ambiguity, enhances security auditing, and ensures proper operations.

Rationale:

Inappropriate values could result in undesirable operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Audit:

Request a copy of all JESJCL of all active site FTP server started tasks.

Note: If an FTP server is inactive, review the procedure libraries defined to JES2 and locate the FTP JCL member.

Verify that:

- The following DD statements appear:
 - SYSTCPD
 - SYSFTPD
- If a PARM parameter is specified on the EXEC statement, it must not contain:
 - The ANONYMOUS keyword or any of its combinations
 - The INACTIVE keyword

The following instructions are only applicable if a site uses AUTOLOG in any PROFILE.TCPIP TCP/IP profiles to start FTP servers.

Request a copy of all AUTOLOG statement blocks that start FTP server started tasks.

Verify that:

- If a PARMSTRING parameter is specified, it must not contain:
 - The ANONYMOUS keyword or any of its combinations
 - The INACTIVE keyword

Remediation:

The site will need to follow their standard change management process for updating started task procedures to to add **DD** statements or update non-compliant **PARM** parameters.

The site will need to follow their standard change management process for updating **PROFILE.TCPIP** TCP/IP profiles to remove non-compliant **PARMSTRING** parameters.

References:

1. IBM z/OS RACF STIG: RACF-FT-000120

Additional Information:

- [z/OS Communications Server - IP Configuration Reference: FTP server cataloged procedure \(FTPD\) parameters](#)
- [z/OS Communications Server - IP Configuration Reference: AUTOLOG statement](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

6.2.3 Ensure FTP.DATA configuration statements enforce secure configuration (Manual)

Profile Applicability:

- Level 1

Description:

The statements in the **FTP.DATA** configuration file specify the parameters and values that control the operation of the FTP Server components including the use of anonymous FTP. Several of the parameters must have specific settings to provide a secure configuration.

Rationale:

Inappropriate values could result in undesirable operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Impact:

Clients that were previously able to connect to the FTP server without TLS protection will no longer be able to do so. In addition, limiting the amount of server information will reduce the amount of server identification information that FTP clients may have previously had access to.

Audit:

Request a copy of the FTP server configuration statements in **FTP.DATA** for any active site FTP server started tasks.

Verify that:

- The **ACCESSERRORMSG** statement is omitted *or* is commented out *or* is coded with a value of **FALSE**
- The **ANONYMOUS** statement is omitted *or* is commented out
- The **BANNER** statement is coded
- The **INACTIVE** statement is coded with a value between 1 and 900
- The **PASSIVEDATACONN** statement is coded with a value of **NOREDIRECT**
- The **REPLYSECURITYLEVEL** statement is coded with a value of 1
- The **UMASK** statement is coded with a value of 077.

Remediation:

The site will need to follow their standard change management process for updating FTP server configuration statements in **FTP.DATA** with compliant values.

Default Value:

- The default **INACTIVE** value is 120
- The default **PASSIVEDATACONN** value is **UNRESTRICTED**
- The default **REPLYSECURITYLEVEL** value is 0

References:

1. IBM z/OS RACF STIG: RACF-FT-000070

Additional Information:

[z/OS Communications Server - IP Configuration Reference: FTP configuration statements in FTP.DATA](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v8	13.5 <u>Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			

6.2.4 Ensure FTP.DATA configuration statements enforce AT-TLS protection (Manual)

Profile Applicability:

- Level 1

Description:

During the TLS handshake process, mutually acceptable suite of cryptographic algorithms is selected by the server and client. The algorithms specified in the selected suite are used to cryptographically protect the data that subsequently flows between the two. To apply TLS protection of adequate strength, the FTP daemon must be configured to use AT-TLS protection. Though the FTP daemon was initially implemented to use System SSL directly, that level of support no longer meets acceptable protection standards and is therefore not adequate. In z/OS V2R5, the native support for System SSL was removed from the FTP daemon.

Rationale:

Failure to properly enforce adequate encryption strength could result in the loss of data privacy.

Impact:

The cryptographic operations involved in TLS do come with a CPU cost. Most of the recommended algorithms are optimized through the use of hardware acceleration. Depending on the number and frequency of TLS handshakes, the CPU impact could be noticeable.

Audit:

Request a copy of the FTP server configuration statements in **FTP.DATA** for any active site FTP server started tasks.

Verify that:

- The **EXTENSIONS** statement is coded with the **AUTH_TLS** value
- The **SECURE_CTRLCONN** statement is coded with the **PRIVATE** value
- The **SECURE_DATACONN** statement is coded with the **PRIVATE** or **SAFE** value
- The **SECURE_FTP** statement is coded with the **REQUIRED** value
- The **TLSCERTCROSSCHECK** statement is omitted or is commented out or is coded with the **TRUE** value
- The **TLSMECHANISM** statement is coded with the **ATTLS** value
- The **TLSRFCLEVEL** statement is coded with the **RFC4217** value

Note: if the z/OS version is V2R5 or higher the **TLSMECHANISM** statement may also be omitted or commented out.

Remediation:

The site will need to follow their standard change management process for updating FTP server configuration statements in **FTP.DATA** with compliant values.

Default Value:

No TLS protection is applied.

Additional Information:

[z/OS Communications Server - IP Configuration Reference: FTP configuration statements in FTP.DATA](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

6.2.5 Ensure user exits for the FTP server are not used without approval (Manual)

Profile Applicability:

- Level 1

Description:

Several user exit points in the FTP Server component are available to permit customization of its operating behavior. These exits can be used to modify functions such as FTP command usage, client connection controls, post processing tasks, and SMF record modifications. Proper review and documentation of these exit programs will avoid unintentional compromise of FTP and system security, integrity and availability.

Rationale:

Without proper review and adequate documentation of these exit programs, undesirable operations and degraded security may result. This exposure could lead to unauthorized access impacting data integrity or the availability of some system services or contribute to the loss of accountability and hamper security audit activities.

Impact:

If exits were previously in use, and the reviews find them to be insufficient from a security, integrity or availability point of view, the functions provided by those exits may become unavailable until the exit can be brought up to local standards.

Audit:

1. Refer to the Data configuration file specified on the **SYSFTPD DD** statement in the FTP started task JCL.
 - Refer to the file(s) allocated by the **STEPLIB** DD statement in the FTP started task JCL.
 - Refer to the libraries specified in the system **LINKLIST** and **LPA**. If any FTP Server exits are in use, identify them and validate that they were reviewed for integrity and approved by the site.
2. Ensure the following items are in effect for FTP Server user exits:
 - The **FTCHKCMD**, **FTCHKIP**, **FTCHKJES**, **FTCHKPWD**, **FTPSMFEX** and **FTPOSTPR** modules are not located in the FTP daemon's **STEPLIB**, **LINKLIST**, or **LPA**.
 - **Note:** The ISPF **ISRFIN**D utility can be used to search the system LINKLIST and LPA for specific modules.
 - If any FTP Server user exits are implemented, the site must have written approval from site ISSM to install and use the exits.
 - If any FTP Server user exits are implemented, the site must have the site systems programmer verify the exit was securely written and installed.

Remediation:

Review the configuration statements in the **FTP.DATA** file. Review the FTP daemon **STEPLIB**, system **LINKLIST**, and Link Pack Area libraries. If FTP Server exits are enabled or present and have not been approved by the site IAM and not securely written and implemented by the site systems programmer, they should not be installed. Verify that none of the following exits are installed unless they have met the requirements listed above:

- **FTCHKCMD**
- **FTCHKIP**
- **FTCHKJES**
- **FTCHKPWD**
- **FTPOSTPR**
- **FTPSMFEX**

References:

1. IBM z/OS RACF STIG: RACF-FT-000090

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.6 Allowlist Authorized Libraries Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.			

6.2.6 Ensure that access to the warning banner for the FTP server is controlled (Automated)

Profile Applicability:

- Level 1

Description:

A logon banner can be used to inform users about the environment during the initial logon. Logon banners are used to warn users against unauthorized entry and the possibility of legal action for unauthorized users and advise all users that system use constitutes consent to monitoring.

Rationale:

Failure to display a logon warning banner without this type of information could adversely impact the ability to prosecute unauthorized users and users who abuse the system.

Audit:

Request a copy of the FTP server configuration statements in **FTP.DATA** for any active site FTP server started tasks.

Verify that the **BANNER** statement is coded.

Verify that the logon banner(s) text(s) are in accordance with the company requirements.

Note: These requirements are only applicable to **BANNER** z/OS data sets.

Request the following DSMON report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering **BANNER** data sets

Request reports generated using IRRDBU00 output that will allow you to:

Verify that **BANNER** data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE** or **READ**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access higher than **READ**
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Note: These requirements are only applicable to **BANNER** UNIX files.

Verify that the permission bits and user audit bits for **BANNER** UNIX files match or are more restrictive than the specified settings listed in the table.

Permission Bits User Audit Bits

744	faf

Remediation:

The site will need to follow their standard change management process for updating FTP server configuration statements in **FTP.DATA** with a compliant **BANNER** value.

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +  
      UACC(READ) +  
      AUDIT(FAILURES(READ)) +  
      DATA('FTP SERVER LOGON BANNER')  
  
PERMIT '<profile>' GENERIC +  
      ACCESS(ALTER) ID(SYSPROG)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<profile>' GENERIC +  
      UACC(READ) +  
      AUDIT(FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<profile>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

To modify the audit flags for a UNIX file use the **chaudit** command:

```
chaudit w=sf,rx+f /etc/ftp.banner
```

To modify the access permissions for a UNIX file use the **chmod** command:

```
chmod 744 /etc/ftp.banner
```

Default Value:

The **BANNER** statement has no default value.

References:

1. IBM z/OS RACF STIG: RACF-FT-000040
2. IBM z/OS RACF STIG: RACF-FT-000050

Additional Information:

[z/OS Communications Server - IP Configuration Reference: BANNER \(FTP server\) statement](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

6.2.7 Ensure SMF recording options for the FTP Server are configured (Manual)

Profile Applicability:

- Level 1

Description:

The FTP Server can provide audit data in the form of SMF records. The SMF data produced by the FTP Server provides transaction information for both successful and unsuccessful FTP commands.

Rationale:

Failure to collect and retain audit data may contribute to the loss of accountability and hamper security audit activities.

Audit:

Request a copy of the FTP server configuration statements in **FTP.DATA** for any active site FTP server started tasks.

Verify that:

- The **SMF** statement is coded with the **TYPE119** value
- The **SMFJES** statement is coded with the **TYPE119** value
- The **SMFSQL** statement is coded with the **TYPE119** value
- The following statements are omitted or commented out:
 - **SMFAPPE**
 - **SMFDEL**
 - **SMFEXIT**
 - **SMFLOGN**
 - **SMFREN**
 - **SMFRETR**
 - **SMFSTOR**

Remediation:

The site will need to follow their standard change management process for updating FTP server configuration statements in **FTP.DATA** with compliant values.

Default Value:

- If the **SMF** statement is omitted, SMF recording occurs for only the events with a statement coded.
- Records for transfer actions when using **FILETYPE=JES** are not recorded unless the **SMFJES** statement is also specified.
- Records for transfer actions when using **FILETYPE=SQL** are not recorded unless the **SMFSQL** statement is also specified.

References:

1. IBM z/OS RACF STIG: RACF-FT-000010

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			

6.2.8 Ensure UNIX permission and user audit bits for FTP server are configured (Manual)

Profile Applicability:

- Level 1

Description:

The FTP Server daemon uses privileged functions and accesses sensitive data. The files and directories the FTP daemon relies upon for its configuration, runtime environment and operation must be properly protected from unauthorized modifications or retrieval to ensure system integrity and privacy of sensitive data.

Rationale:

Failure to properly secure these objects may lead to unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Audit:

Verify that the permission bits and user audit bits for FTP server UNIX files match or are more restrictive than the specified settings listed in the table:

File	Permission Bits	User Audit Bits
<code>/usr/sbin/ftpd</code>	740	fff
<code>/usr/sbin/ftpdns</code>	755	fff
<code>/etc/ftp.data</code>	744	faf

Notes:

- Some of the files listed above may not be used in every configuration. While the absence of a file is generally not a security issue, the existence of a file that has not been properly secured can often be an issue. Therefore, all files that do exist should have the specified permission and audit bit settings
- The `/usr/sbin/ftpd` and `/usr/sbin/ftpdns` objects are symbolic links to `/usr/lpp/tcpip/sbin/ftpd` and `/usr/lpp/tcpip/sbin/ftpdns` respectively. The permission and user audit bits on the targets of the symbolic links must have the required settings.

Remediation:

To modify the audit flags for a UNIX file use the **chaudit** command:

```
chaudit rwx=f /usr/lpp/tcpip/sbin/ftpd  
chaudit rwx=f /usr/lpp/tcpip/sbin/ftpdns  
chaudit w=sf,rx+f /etc/ftp.data
```

To modify the access permissions for a UNIX file use the **chmod** command:

```
chmod 740 /usr/lpp/tcpip/sbin/ftpd  
chmod 755 /usr/lpp/tcpip/sbin/ftpdns  
chmod 744 /etc/ftp.data
```

References:

1. IBM z/OS RACF STIG: RACF-FT-000020

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

6.2.9 Ensure access to FTP server FTP.DATA data sets is controlled (Manual)

Profile Applicability:

- Level 1

Description:

The FTP Server daemon uses privileged functions and accesses sensitive data. The data sets the FTP daemon relies upon for its configuration, runtime environment and operation must be properly protected from unauthorized modifications or retrieval to ensure system integrity and privacy of sensitive data.

Rationale:

Failure to properly secure these data sets may lead to unauthorized access resulting in the compromise of the integrity and availability of customer data and some system services.

Audit:

Request a list of the FTP server **FTP.DATA** data sets for any site FTP server started tasks.

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering FTP server **FTP.DATA** configuration data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That the FTP server **FTP.DATA** configuration data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access greater than **READ**
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      DATA('FTP SERVER CONFIGURATION')  
  
PERMIT '<profile>' GENERIC +  
      ACCESS(ALTER) ID(SYSprog)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<profile>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-FT-000030

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

6.2.10 Ensure access to FTP control card data sets is controlled (Manual)

Profile Applicability:

- Level 1

Description:

FTP control cards carry unencrypted information such as user IDs, passwords and remote IP Addresses. This sensitive credential information should be stored separate from the JCL in a secured file.

Rationale:

Without a requirement to store this information separate from the JCL and in-stream JCL, it allows a security exposure by allowing read exposure to this information from anyone having access to the JCL libraries.

Audit:

Verify that no FTP control cards are within in-stream JCL.

Request a list of all data sets containing FTP Control cards.

Request the following DSMON report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- -- GLOBAL INACTIVE -- or -- NO ENTRIES -- or contains no entries covering FTP control card data sets

Request reports generated using IRRDBU00 output that will allow you to:

Verify That the FTP control card data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(FAILURES(READ)) +  
      DATA('FTP CONTROL CARDS')  
  
PERMIT '<profile>' GENERIC +  
      ACCESS(READ) ID(<compliant-id>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<profile>' GENERIC +  
      UACC(NONE) +  
      AUDIT(FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<profile>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-FT-000030

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

6.3 OpenSSH

This section describes the OpenSSH recommendations.

6.3.1 Ensure SSH daemon is configured to only use the SSHv2 protocol (Manual)

Profile Applicability:

- Level 1

Description:

SSHv1 has many well-known vulnerability exploits, and SSH daemons should only use the SSHv2 protocol.

Note: Support for SSHv1 was removed from IBM z/OS OpenSSH in z/OS V2R4. This benchmark only applies to z/OS OpenSSH on releases prior to V2R4, or for installations that use a third party SSH implementation on z/OS.

Rationale:

Exploits of the SSH daemon using the SSHv1 protocol could provide immediate root access to the system.

Impact:

Any clients using SSHv1 (if any) will need to upgrade to SSHv2

Audit:

Review all active **sshd_config** (OpenSSH daemon configuration files).

Verify that the **Protocol** keyword specifies 2.

Remediation:

The site will need to follow their standard change management process for updating **sshd_config** configuration files with compliant values.

Default Value:

The default **Protocol** value is 2

References:

1. IBM z/OS RACF STIG: RACF-SH-000050

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

6.3.2 Ensure SSH daemon is configured to use FIPS 140-2 compliant cryptographic provider (Manual)

Profile Applicability:

- Level 2

Description:

Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. Cryptographic modules must adhere to the higher standards approved by the United States federal government since this provides assurance they have been tested and validated.

Rationale:

The FIPS-140 standard requires strict adherence to the use of strong cryptographic algorithms and keys and built-in integrity checks by compliant cryptographic modules.

Audit:

Review the active `sshd_config` (OpenSSH daemon configuration files).

Verify that:

- The `Ciphers` keyword list contains ciphers prefixed with `aes` and without the `@openssh.com` suffix.
- The `MACs` keyword list contains entries greater than `hmac-sha-256`

Review the active `zos_sshd_config` (z/OS-specific OpenSSH daemon configuration files).

Verify that:

- The `CiphersSource` keyword value is `ICSF`
- The `FIPSMODE` keyword value is `yes`
- The `HostKeyRingLabel` keyword is coded
- The `KexAlgorithmsSource` keyword value is `ICSF`
- The `MacSource` keyword value is `ICSF`

Remediation:

The site will need to follow their standard change management process for updating `sshd_config` configuration files with compliant values.

Default Value:

- **sshd_config**
 - The **Ciphers** default list is `aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc, aes256-cbc,arcfour`
 - The **MACs** default list is `hmac-md5-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-96-etm@openssh.com,hmac-md5,hmac-sha1,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160,hmac-ripemd16@openssh.com,hmac-sha1-96,hmac-md5-96`
- **zos_sshd_config**
 - The **CiphersSource** default value is **CPACF**
 - The **FIPSMODE** default value is **no**
 - The **HostKeyRingLabel** keyword has no default value
 - The **KexAlgorithmsSource** default value is **OpenSSL**
 - The **MacSource** default value is **CPACF**

References:

1. IBM z/OS RACF STIG: RACF-SH-000020

Additional Information:

- [z/OS OpenSSH User's Guide: Steps for setting up OpenSSH to run in FIPS mode](#)
- [z/OS OpenSSH User's Guide: Setting up OpenSSH to use ICSF cryptographic operations](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	12.6 <u>Use of Secure Network Management and Communication Protocols</u> Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).			

6.3.3 Ensure SSH daemon is configured with a logon banner (Manual)

Profile Applicability:

- Level 1

Description:

A logon banner can be used to inform users about the environment during the initial logon. Logon banners are used to warn users against unauthorized entry and the possibility of legal action for unauthorized users and advise all users that system use constitutes consent to monitoring.

Rationale:

Failure to display a logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.

Audit:

Review the active `sshd_config` (OpenSSH daemon configuration files).

Verify that the `Banner` keyword is coded.

Verify that the permission bits and user audit bits for OpenSSH `Banner` UNIX files match or are more restrictive than the specified settings listed in the table.

Permission Bits	User Audit Bits

744	faf

Remediation:

The site will need to follow their standard change management process for updating `sshd_config` configuration files with compliant values.

To modify the audit flags for a UNIX file use the `chaudit` command:

```
chaudit w=sf,rx+f /etc/ssh.banner
```

To modify the access permissions for a UNIX file use the `chmod` command:

```
chmod 744 /etc/ssh.banner
```

Default Value:

The `Banner` keyword has no default value

References:

1. IBM z/OS RACF STIG: RACF-SH-000020

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

6.3.4 Ensure SSH daemon is configured for SMF logging (Manual)

Profile Applicability:

- Level 1

Description:

The z/OS OpenSSH daemon can provide audit data in the form of SMF records. The SMF data produced by the OpenSSH daemon provides transaction information for both successful and unsuccessful SSH commands.

Rationale:

Failure to collect and retain audit data may contribute to the loss of accountability and hamper security audit activities and use of the SMF data in the execution of a contingency plan could be compromised.

Audit:

Review the active `zos_sshd_config` (z/OS-specific OpenSSH daemon configuration files).

Verify that the `ServerSMF` keyword value is `TYPE119_U83`.

Remediation:

Consult the [z/OS OpenSSH User's Guide](#) for guidance on configuring z/OS OpenSSH to collect SMF records.

Default Value:

The `ServerSMF` keyword default value is `none`

References:

1. IBM z/OS RACF STIG: RACF-SH-000010

Additional Information:

[z/OS OpenSSH User's Guide: Setting up OpenSSH to collect SMF records](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			

6.3.5 Ensure SSH daemon is configured to use SAF keyrings for key storage (Manual)

Profile Applicability:

- Level 1

Description:

The z/OS OpenSSH daemon supports the storage of asymmetric authentication keys in SAF key rings or z/OS UNIX file system files. The SSH keys should be stored in SAF key rings to ensure their protection and to provide for organization access control over the keys.

Rationale:

The use of SAF Key Rings for key storage enforces organizational access control policies and assures the protection of cryptographic keys in storage.

Audit:

Review the active **sshd_config** (OpenSSH daemon configuration files).

Verify that any **HostKey** keywords have been omitted *or* commented out.

Review the active **zos_sshd_config** (z/OS-specific OpenSSH daemon configuration files).

Verify that the **HostKeyRingLabel** keyword value is coded.

Remediation:

Consult the [z/OS OpenSSH User's Guide](#) for guidance on configuring z/OS OpenSSH to setup up server authentication where keys are stored in RACF key rings.

Default Value:

The **HostKeyRingLabel** keyword has no default value

Additional Information:

[z/OS OpenSSH User's Guide: Steps for setting up server authentication when keys are stored in key rings](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>16.11 Leverage Vetted Modules or Services for Application Security Components</u> Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.			

6.4 Syslogd Recommendations

This section describes the Syslogd recommendations.

6.4.1 Ensure syslog daemon is started at z/OS initialization (Manual)

Profile Applicability:

- Level 1

Description:

The Syslog daemon, known as **syslogd**, is a z/OS UNIX daemon that provides a central processing point for log messages issued by other z/OS UNIX processes. The messages may be of varying importance levels including general process information, diagnostic information, critical error notification, and audit-class information. It is important that **syslogd** be started during the initialization phase of the z/OS system to ensure that significant messages are not lost. Finally, **syslogd** should run in non-swappable mode and under a sufficiently high WLM service class to allow it to keep up with heavy logging loads. If **syslogd** falls behind, it can cause system instability.

Rationale:

Failure to collect and retain audit data may contribute to the loss of accountability and hamper security audit activities.

Audit:

Verify with the site that the syslog daemon (**syslogd**) is started automatically during the initialization for every z/OS system.

Note: **syslogd** may be started from the UNIX shell, a cataloged procedure (STC), or the **BPXBATCH** program. Additionally, other mechanisms (e.g., CONTROL-O) may be used to automatically start **syslogd**.

Verify that the WLM service class under which **syslogd** is classified, is of a high enough to ensure **syslogd** will not starve for dispatching priority.

Remediation:

Consult the [z/OS Communications Server - IP Configuration Guide](#) for guidance on starting and stopping **syslogd**.

References:

1. IBM z/OS RACF STIG: RACF-SL-000020

Additional Information:

[z/OS Communications Server - IP Configuration Guide: Starting and stopping syslogd](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

6.4.2 Ensure that the STARTED resource class is used to assign user IDs with proper parameters to syslog daemon started tasks (Manual)

Profile Applicability:

- Level 1

Description:

Syslog daemon, known as **syslogd**, is a zOS UNIX daemon that provides a central processing point for log messages issued by other zOS UNIX processes. It is also possible to receive log messages from other network-connected hosts. Some of the IBM Communications Server components that may send messages to syslog are the FTP and zOS UNIX Telnet servers, AT-TLS and the **IKED**, **NSSD** and **DMD** daemons. The messages may be of varying importance levels including general process information, diagnostic information, critical error notification, and audit-class information. Primarily because of the potential to use this information in an audit process, there is a security interest in protecting the **syslogd** process and its associated data. The Syslog daemon requires special privileges and access to sensitive resources to provide its system services.

Rationale:

Failure to properly define and control the Syslog daemon could lead to unauthorized access. This exposure may result in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **STARTED** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **STARTED** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **STARTED** appears.

Request the following **DSMON** report:

```
FUNCTION SYSTEM RACSPT
```

Verify that the **syslogd** started task(s) appear in the **FROM PROFILES IN THE STARTED CLASS:** section **and not** the **FROM THE STARTED PROCEDURES TABLE (ICHRIN03):** section.

Use the **ASSOCIATED USER** column to determine the user ID associated with the **syslogd** task.

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that the **syslogd** started task RACF user ID:

- Has the **PROTECTED** attribute
- Has the following **OMVS** segment attributes:
 - **UID** is 0
 - **HOME** is /
 - **PROGRAM** is /bin/sh
- Is permitted a minimum of **READ** to the **BPX.STOR.SWAP** resource in the **FACILITY** class.

Remediation:

To activate the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(STARTED)
```

To enable generic profile checking for the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(STARTED)
```

To RACLIST the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(STARTED)
```

To create a **STARTED** profile use the RACF **RDEFINE** and **SETROPTS** commands:

```
RDEFINE STARTED SYSLOGD.* +  
    UACC(NONE) +  
    DATA('UNIX SYSLOG DAEMON') +  
    STDATA( +  
        USER(<syslogd-user>) +  
        GROUP(<syslogd-group>) +  
    )  
  
SETROPTS REFRESH RACLIST(STARTED)
```

To make a user ID **PROTECTED** use the RACF **ALTUSER** command:

```
ALTUSER <syslogd-user> +  
    NOPASSWORD +  
    NOPHRASE +  
    NOOIDCARD
```

To modify the **OMVS** segment for a user ID use the RACF **ALTUSER** command:

```
ALTUSER <syslogd-user> +  
    OMVS( +  
        UID(0) +  
        HOME('/') +  
        PROGRAM('/bin/sh') +  
    )
```

Notes:

1. If the security administrator has defined the **SHARED.IDS** profile in the **UNIXPRIV** class, the **UID** value must be unique. Use the **SHARED** keyword in addition to **UID** to assign a value that is already in use.
2. **OMVS DIRECTORY** and **PROGRAM** values are case sensitive, so be sure they are entered as-is and not translated to upper case.

To add an access list entries use the RACF **PERMIT** command:


```
PERMIT BPX.STOR.SWAP CLASS(FACILITY) +  
    ACCESS(READ) ID(<syslogd-user>)  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

Default Value:

- When the **ADDUSER** command is issued to create a user ID and you specify **NOOIDCARD** (or you allow this option to default), do not specify **PHRASE**, and if you specify **NOPASSWORD** or you omit the **PASSWORD** keyword, by default the ID will be created with the **PROTECTED** attribute.
- When the **ADDUSER** command is issued to create a user ID and you omit the **OMVS** keyword, by default the ID will be created with **NOOMVS**.
- The **ICHRIN03** started procedures table is used to associate the names of started procedures with user IDs.

References:

1. IBM z/OS RACF STIG: RACF-SL-000030

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	●	●	●

6.4.3 Ensure permission and user audit bits for syslog daemon component are configured (Manual)

Profile Applicability:

- Level 1

Description:

Directories and files of the syslog daemon provide the configuration and executable properties of this product. These directories and files must be properly protected from unauthorized modifications or retrieval to ensure system integrity and privacy of sensitive data.

Rationale:

Failure to properly secure these objects could lead to unauthorized access. This exposure may result in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Audit:

Verify that the permission bits and user audit bits for syslog daemon UNIX files match or are more restrictive than the specified settings listed in the table:

File	Permission Bits	User Audit Bits
<code>/usr/sbin/syslogd</code>	740	fff
<code>/etc/syslog.conf</code>	744	faf

Notes:

- The `/usr/sbin/syslogd` object is a symbolic link to `/usr/lpp/tcpip/sbin/syslogd`. The permission and user audit bits on the target of the symbolic link must have the required settings.
- The `/etc/syslog.conf` file may not be the configuration file the daemon uses. It is necessary to check the script or JCL used to start the daemon to determine the actual configuration file.

Remediation:

To modify the audit flags for a UNIX file use the **chaudit** command:

```
chaudit rwx=f /usr/lpp/tcpip/sbin/syslogd  
chaudit w=sf,rx+f /etc/syslog.conf
```

To modify the access permissions for a UNIX file use the **chmod** command:

```
chmod 740 /usr/lpp/tcpip/sbin/syslogd  
chmod 744 /etc/syslog.conf
```

References:

1. IBM z/OS RACF STIG: RACF-SL-000010

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

6.4.4 Ensure that access to syslog daemon archive data sets is controlled (Manual)

Profile Applicability:

- Level 1

Description:

syslogd can be configured to automatically archive log files to sequential or Generation Data Group (**GDG**) data sets. These archive data sets contain log information from multiple z/OS system components and must be properly protected from unauthorized modifications or retrieval to ensure system integrity and privacy of sensitive data.

Rationale:

Failure to properly secure these data sets may lead to unauthorized access resulting in the compromise of sensitive log information from different z/OS system components.

Audit:

Request a list of all **syslogd** archive data set prefixes specified by the **BeginArchiveParms** keyword in **/etc/syslog.conf** configurations.

Note: the **/etc/syslog.conf** file may not be the configuration file the **syslogd** daemon uses. It is necessary to check the script or JCL used to start the daemon to determine the actual configuration file.

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entry covering **syslogd** archive data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that **syslogd** archive data sets are secured by RACF profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<syslogd-archive>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      DATA('UNIX SYSLOGD ARCHIVE')  
  
PERMIT '<syslogd-archive>' GENERIC +  
      ACCESS(ALTER) ID(SYSPROG)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<syslogd-archive>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<syslogd-archive>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

Additional Information:

[z/OS Communications Server - IP Configuration Reference: BeginArchiveParms statement](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

6.5 TCP/IP Recommendations

This section describes the TCP/IP recommendations.

6.5.1 Ensure configuration files for the TCP/IP stack are explicitly specified (Manual)

Profile Applicability:

- Level 1

Description:

The TCP/IP stack reads two configuration files to determine values for critical operational parameters. These file names are specified in multiple locations and, depending on the process, are referenced differently. Because system security is impacted by some of the parameter settings, specifying the file names explicitly in each location reduces ambiguity and ensures proper operations.

Rationale:

Inappropriate values could result in undesirable operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Audit:

Request a copy of all **JESJCL** of all active site TCP/IP stack started tasks.

Note: If a TCP/IP stack is inactive, review the procedure libraries defined to JES2 and locate the TCP/IP stack JCL member.

Verify that:

- The following **DD** statements appear:
 - **SYSTCPD**
 - **PROFILE**
- If a **PARM** parameter is specified on the **EXEC** statement *and* it includes an **ENVAR** keyword *and* it specifies the **RESOLVER_CONFIG** variable:
 - The **RESOLVER_CONFIG** value must be set to the **same** file name specified on the **SYSTCPD DD** statement.

Remediation:

The site will need to follow their standard change management process for updating started task procedures to add **DD** statements or update non-compliant **PARM** parameters.

References:

1. IBM z/OS RACF STIG: RACF-TC-000080

Additional Information:

- [z/OS Communications Server - IP Configuration Guide: Configuring TCPIP.DATA](#)
- [z/OS Communications Server - IP Configuration Guide: Configuring PROFILE.TCPIP](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

6.5.2 Ensure TCP/IP stack configuration defined in TCPIP.DATA meets minimum requirements (Manual)

Profile Applicability:

- Level 1

Description:

During the initialization of TCP/IP servers and clients, the **TCPIP.DATA** configuration file provides information that is essential for proper operations of TCP/IP applications. The **TCPIP.DATA** file acts as the anchor configuration data set for the TCP/IP stack and all TCP/IP servers and clients running in z/OS. During the initialization of TCP/IP servers and clients, the **TCPIP.DATA** file provides basic information that is essential for proper operation.

Rationale:

Inappropriate values could result in undesirable operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Audit:

Request a copy of all **JESJCL** of all active site TCP/IP stack started tasks.

Note: If an TCP/IP stack is inactive, review the procedure libraries defined to JES2 and locate the FTP JCL member.

Verify that the following parameters are coded in **TCPIP.DATA** files specified by **SYSTCPD DD** statements:

- **DATASETPREFIX**
- **DOMAINORIGIN**
- **HOSTNAME**
- **TCPIPJOBNAME**

Remediation:

The site will need to follow their standard change management process for updating **TCPIP.DATA** configuration files.

References:

1. IBM z/OS RACF STIG: RACF-TC-000100

Additional Information:

[z/OS Communications Server - IP Configuration Reference: Resolver setup and TCPIP.DATA configuration statements](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

6.5.3 Ensure hosts identified by the NSINTERADDR statement are protected (Manual)

Profile Applicability:

- Level 1

Description:

If the hosts identified by **NSINTERADDR** statement are not properly protected they can be stolen, damaged, or disturbed. Without adequate physical security, unauthorized users can access the host and the hosts' components. Therefore, they can interfere with the normal operations of the host.

Rationale:

Improper control of hosts and the hosts' components could compromise network operations.

Audit:

1. Refer to the Data configuration file specified on the **SYSTCPD DD** statement in the TCP/IP started task JCL.
2. Gather the following information for any **NSINTERADDR** statement coded in the TCP/IP Data configuration file:
 - Identify the physical location of the host running a DNS server (i.e., on-site or off-site at organization, city, state).
 - Obtain the description of the physical security controls used to limit access to the area where the host is located.

Remediation:

Verify that if the **NSINTERADDR** statements are not specified in the TCP/IP Data configuration file, this is not applicable. Verify that the **NSINTERADDR** statements specified in the TCP/IP Data configuration file.

- The **NSINTERADDR** statements refer to hosts connected directly to networks within the physical premises of the host site.
- The **NSINTERADDR** statements refer to hosts that are located in areas with physical access limited to authorized personnel.

Ensure that the hosts and the hosts components identified in the **NSINTERADDR** statement are protected. Ensure that any **NSINTERADDR** statements coded in the TCPIP.DATA file refer to hosts connected directly to networks within the physical premises of the host site and located in areas with physical access limited to authorized personnel.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

6.5.4 Ensure TCP/IP stack configuration defined in PROFILE.TCPIP meets minimum requirements (Manual)

Profile Applicability:

- Level 1

Description:

The **PROFILE.TCPIP** configuration file provides system operation and configuration parameters for the TCP/IP stack. Inappropriate values could result in undesirable operations and degraded security.

Rationale:

This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Audit:

This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Audit Procedure

Request a copy of all **JESJCL** of all active site TCP/IP stack started tasks.

Note: If an TCP/IP stack is inactive, review the procedure libraries defined to JES2 and locate the FTP JCL member.

Verify that the following parameters in **PROFILE.TCPIP** files specified by **PROFILE DD** statements:

- The **SMFPARMS** statement is omitted *or* commented out.
- The **DELETE** statement is omitted *or* commented out.
- The **SMFCONFIG** statement is coded with (at least) the **FTPCLIENT** and **TN3270CLIENT** operands. In addition:
 - One or more of the **ZERTDETAIL**, **ZERTSUMMARY** and (for z/OS V2R5 and later) **ZERTDETAILBYPOLICY** operands are coded.
 - Alternatively, one or more of the **ZERTSERVICE**, **ZERTSUMMARY**, and (for z/OS V2R5 and later) **ZERTSERVICEBYPOLICY** operands may be coded on the **NETMONITOR** statement if a network monitoring product is in use.
 - The **TCPSTACK** operand is coded.
 - The **PROFILE** and **DVIPA** operands are coded.
 - Alternatively **PROFILE** and **SMFSERVICE DVIPA** may be coded on the **NETMONITOR** statement if a network monitoring product is in use.

- If the IPsec protocol is used to protect any z/OS traffic, then **IPSECURITY** must be coded.
 - Alternatively, **SMFSERVICE IPSECURITY** may be coded on the **NETMONITOR** statement if a network monitoring product is in use.
- e. If SMC-D is in use the **SMCDLINKEVENT** operand must be coded.
- If SMC-R is in use the **SMCRLINKEVENT** operand must be coded.
- If CSSMTP is in use the **NETMONITOR** statement must be coded with the **SMFSERVICE CSMail CSSMTP** operands.
- The **TCPCONFIG** statement is coded with (at least) the **RESTRICTLOWPORTS** and **TTLS** operands.
 - If the **FINWAIT2TIME** operand is coded, it must have a value of 60 or less.
- The **UDPCONFIG** statement is coded with (at least) the **RESTRICTLOWPORTS** operand. In addition, the **NOUDPCHKSUM** and **NOUDPQUEUELIMIT** operands must be omitted or commented out.
- The **IPCONFIG** statement is coded with (at least) the **NODATAGRAMFWD** and **IGNOREREDIRECT** operands.
 - In some cases, there will be a legitimate reason for having **DATAGRAMFWD** coded, and the site must be able to provide proof of approval as well as any documented justification.
- The **GLOBALCONFIG** statement is coded with (at least) the **ZERT** operand.
- The **SACONFIG** statement is coded with (at least) a community name other than **public**.
 - In addition, the **SETENABLED** operand must be omitted or commented out.

Note: If the **INCLUDE** statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked as well.

Remediation:

The site will need to follow their standard change management process for updating **PROFILE.TCPIP** configuration files.

References:

1. IBM z/OS RACF STIG: RACF-TC-000010

Additional Information:

[z/OS Communications Server - IP Configuration Reference: TCP/IP profile \(PROFILE.TCPIP\) and configuration statements](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v8	<u>8.2 Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

6.5.5 Ensure permission and user audit bits for z/OS UNIX file system objects that are part of the base TCP/IP component are configured (Manual)

Profile Applicability:

- Level 1

Description:

z/OS UNIX directories and files of the Base TCP/IP component provide the configuration, operational, and executable properties of IBM's TCP/IP system product.

Rationale:

Failure to properly secure these objects may lead to unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Audit:

Verify that the permission bits and user audit bits for base TCP/IP components files match or are more restrictive than the specified settings listed in the table:

File	Permission Bits	User Audit Bits
/etc/hosts	744	faf
/etc/protocol	744	faf
/etc/resolv.conf	744	faf
/etc/services	740	faf
/usr/lpp/tcpip/bin	755	faf
/usr/lpp/tcpip/sbin	755	faf

Note: Some of the files listed above may not be used in every configuration.

Remediation:

To modify the audit flags for a UNIX file use the **chaudit** command:

```
chaudit w=sf,rx+f /etc/hosts
chaudit w=sf,rx+f /etc/protocol
chaudit w=sf,rx+f /etc/resolv.conf
chaudit w=sf,rx+f /etc/services
chaudit w=sf,rx+f /usr/lpp/tcpip/bin
chaudit w=sf,rx+f /usr/lpp/tcpip/sbin
```

To modify the access permissions for a UNIX file use the **chmod** command:

```
chmod 744 /etc/hosts
chmod 744 /etc/protocol
chmod 744 /etc/resolv.conf
chmod 740 /etc/services
chmod 755 /usr/lpp/tcpip/bin
chmod 755 /usr/lpp/tcpip/sbin
```

References:

1. IBM z/OS RACF STIG: RACF-TC-000030

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

6.5.6 Ensure access to TCP/IP SAF resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

The Communication Server access authorization is used to protect TCP/IP resources such as stack, network, port, and other **SERVAUTH** resources. These resources provide additional security checks for TCP/IP users.

Rationale:

Failure to properly secure these TCP/IP resources could lead to unauthorized user access resulting in the compromise of some system services and possible compromise of data.

Impact:

Initial deployment of these measures may cause some applications or users that have legitimate reasons to access a given resource, but were initially unrecognized as such, to be denied access. Once your access control lists are fully developed and verified, this impact will no longer be a factor.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES** = section.

Verify that **SERVAUTH** appears.

Review the command output in the **GENERIC PROFILE CLASSES** = section.

Verify that **SERVAUTH** appears.

Review the command output in the **SETR RACLIST CLASSES** = section.

Verify that **SERVAUTH** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that:

- The **SERVAUTH** entry has:
 - **-- GLOBAL INACTIVE -- or -- NO ENTRIES --**

Request reports generated using IRRDBU00 output that will allow you to:

Verify the following **GENERIC** catch-all profiles are defined in the **SERVAUTH** class:

- **EZA.** or EZA.* or EZA.*.****
- **EZB.** or EZB.* or EZB.*.****
- **IST.** or IST.* or IST.*.****

Verify that those **GENERIC** catch-all profiles defined in the **SERVAUTH** class:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers

Verify that any **EZB.INITSTACK** prefixed profiles defined in the **SERVAUTH** class:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Note: Access to **EZB.INITSTACK** prefixed profiles allows access to a TCP/IP stack during the period of time after the stack is active but before Application Transparent Transport Layer Security (AT-TLS) policies are loaded and enforced. This means an ID could potentially open a socket connection without an encryption policy being applied. It should strictly be limited to IDs associated with the TCP/IP stack bootstrap process.

Verify that any `EZB.FTP.*.*.ACCESS.HFS` profiles defined in the `SERVAUTH` class:

- Have `UACC` of `NONE`
- Are not in `WARNING` mode
- `AUDIT` a minimum of `FAILURES(READ)`
- `ID(*)` is not used to grant access
- `READ` and higher permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Note: Access should be limited to FTP users with specific written documentation showing a valid requirement exists to access z/OS UNIX files and directories via FTP.

Verify that any `EZB.FTP.*.*.ACCESS.JES` profiles defined in the `SERVAUTH` class:

- Have `UACC` of `NONE`
- Are not in `WARNING` mode
- `AUDIT` a minimum of `FAILURES(READ)`
- `ID(*)` is not used to grant access
- `READ` and higher permits are restricted to:
 - System programmers
 - Systems Programmers
 - IDs authorized to access these resources at this level

Note: Access should be limited to FTP users with specific written documentation showing a valid requirement exists to access FTP JES mode.

Remediation:

To activate RACF classes use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(SERVAUTH)
```

To enable generic profile checking for a RACF class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(SERVAUTH)
```

To RACLIST a RACF class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(SERVAUTH)
```

To create catch-all profiles use the RACF **RDEFINE** command:

```
RDEFINE SERVAUTH EZA.** +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('CATCH-ALL PROFILE')

RDEFINE SERVAUTH EZB.** +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('CATCH-ALL PROFILE')

RDEFINE SERVAUTH EZB.INITSTACK.** +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    DATA('ACCESS TCP/IP STACK BEFORE AT-TLS POLICIES HAVE BEEN
INSTALLED')

RDEFINE SERVAUTH EZB.FTP.*.*.ACCESS.HFS +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('ACCESS UNIX ENVIRONMENT VIA FTP')

RDEFINE SERVAUTH EZB.FTP.*.*.ACCESS.JES +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('ACCESS FTP JES MODE')

RDEFINE SERVAUTH IST.** +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('CATCH-ALL PROFILE')

SETROPTS REFRESH RACLIST(SERVAUTH)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** command:

```
RALTER SERVAUTH <profile> +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    NOWARNING  
  
SETROPTS REFRESH RACLIST(SERVAUTH)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(SERVAUTH) +  
    DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH RACLIST(SERVAUTH)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **SERVAUTH** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-TC-000040

Additional Information:

- [z/OS Communications Server - IP Configuration Guide: TCP/IP resource protection](#)
- [z/OS Communications Server - IP Configuration Guide: TCP/IP stack initialization access control](#)
- [z/OS Communications Server - IP Configuration Guide: \(Optional\) Steps for controlling user access to the z/OS UNIX file system](#)
- [z/OS Communications Server - IP Configuration Guide: \(Optional\) Steps for controlling user access to FTP JES mode](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

6.5.7 Ensure that the SERVAUTH resource class is enabled (Manual)

Profile Applicability:

- Level 1

Description:

IBM Provides the **SERVAUTH** Class for use in protecting a variety of TCP/IP features/functions/products both IBM and third-party. Failure to activate this class will result in unprotected resources.

Rationale:

This exposure may threaten the integrity of the operating system environment and compromise the confidentiality of customer data.

Impact:

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified below.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **SERVAUTH** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **SERVAUTH** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **SERVAUTH** appears.

Remediation:

To activate RACF classes use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT (SERVAUTH)
```

To enable generic profile checking for a RACF class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC (SERVAUTH)
```

To RACLIST a RACF class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST (SERVAUTH)
```

Default Value:

The **SERVAUTH** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-TC-000050

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

6.5.8 Ensure that the STARTED resource class is used to assign user IDs with proper parameters to base TCP/IP component started tasks (Manual)

Profile Applicability:

- Level 1

Description:

The TCP/IP started tasks require special privileges and access to sensitive resources to provide its system services. Failure to properly define and control these TCP/IP started tasks could lead to unauthorized access.

Rationale:

This exposure may result in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **STARTED** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **STARTED** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **STARTED** appears.

Request the following **DSMON** report:

```
FUNCTION SYSTEM RACSPT
```

Verify that the TCP/IP and **EZAZSSI** started task(s) appear in the **FROM PROFILES IN THE STARTED CLASS:** section **and not** the **FROM THE STARTED PROCEDURES TABLE (ICHRIN03):** section.

Use the **ASSOCIATED USER** column to determine the user ID associated with the started tasks.

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that the TCP/IP started task RACF user ID:

- Has the **PROTECTED** attribute
- Has the following OMVS segment attributes:
 - **UID** is **0**
 - **HOME** is **/**
 - **PROGRAM** is **/bin/sh**

Verify that the **EZAZSSI** started task RACF user ID:

- Has the **PROTECTED** attribute

Remediation:

To activate the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(STARTED)
```

To enable generic profile checking for the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(STARTED)
```

To RACLIST the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(STARTED)
```

To create a **STARTED** profile use the RACF **RDEFINE** and **SETROPTS** commands:

```
RDEFINE STARTED TCPIP.* +
    UACC(NONE) +
    DATA('TCP/IP STACK') +
    STDATA( +
        USER(<tcpip-user>) +
        GROUP(<tcpip-group>) +
        TRUSTED +
    )

RDEFINE STARTED EZAZSSI.* +
    UACC(NONE) +
    DATA('START VMCF AND TNF AS RESTARTABLE SUBSYSTEMS') +
    STDATA( +
        USER(<ezazssi-user>) +
        GROUP(<ezazssi-group>) +
    )

SETROPTS REFRESH RACLIST(STARTED)
```

To make a user ID **PROTECTED** use the RACF **ALTUSER** command:

```
ALTUSER <user-id> +
    NOPASSWORD +
    NOPHRASE +
    NOOIDCARD
```

To modify the **OMVS** segment for a user ID use the RACF **ALTUSER** command:

```
ALTUSER <tcpip-id> +
    OMVS( +
        UID(0) +
        HOME('/') +
        PROGRAM('/bin/sh') +
    )
```

Notes:

1. If the security administrator has defined the **SHARED.IDS** profile in the **UNIXPRIV** class, the **UID** value must be unique. Use the **SHARED** keyword in addition to **UID** to assign a value that is already in use.
2. **OMVS DIRECTORY** and **PROGRAM** values are case sensitive, so be sure they are entered as-is and not translated to upper case.

Default Value:

- When the **ADDUSER** command is issued to create a user ID and you specify **NOOIDCARD** (or you allow this option to default), do not specify **PHRASE**, and if you specify **NOPASSWORD** or you omit the **PASSWORD** keyword, by default the ID will be created with the **PROTECTED** attribute.
- When the **ADDUSER** command is issued to create a user ID and you omit the **OMVS** keyword, by default the ID will be created with **NOOMVS**.
- The **ICHRIN03** started procedures table is used to associate the names of started procedures with user IDs.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	5.5 <u>Establish and Maintain an Inventory of Service Accounts</u> Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			

6.5.9 Ensure access to data sets for the base TCP/IP component is controlled (Manual)

Profile Applicability:

- Level 1

Description:

MVS data sets of the Base TCP/IP component provide the configuration, operational, and executable properties of IBM's TCP/IP system product. The data sets TCP/IP relies upon for its configuration, runtime environment and operation must be properly protected from unauthorized modifications or retrieval to ensure system integrity and privacy of sensitive data.

Rationale:

Failure to properly secure these data sets may lead to unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering base TCP/IP component data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That the base TCP/IP component data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access greater than **READ**
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<tcpip-base>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      DATA('BASE TCP/IP COMPONENT')  
  
PERMIT '<tcpip-base>' GENERIC +  
      ACCESS(ALTER) ID(SYSprog)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<tcpip-base>' GENERIC +  
      UACC(NONE) +  
      AUDIT(SUCCESS(UPDATE), FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<tcpip-base>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-TC-000070

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

6.6 TN3270 Recommendations

This section describes the TN3270E Telnet Server recommendations.

6.6.1 Ensure configuration statements for the TN3270E telnet server are configured (Manual)

Profile Applicability:

- Level 1

Description:

The TN3270E Telnet Server profile (often called the "Telnet profile") configuration file provides system operation and configuration parameters for the TN3270E Telnet Server. Several of these parameters have potential impact to system security.

Rationale:

Failure to code the appropriate values could result in unexpected operations, degraded security, or unauthorized access impacting data integrity or the availability of some system services.

Audit:

Request a copy of all **JESJCL** of all active site TN3270E started tasks.

Note: If a TN3270E started task is inactive, review the procedure libraries defined to JES2 and locate the TN3270E JCL member.

Verify that the following parameters are coded in TN3270E configuration files specified by **PROFILE DD** statements:

- **TELNETGLOBAL** block (only one defined)
 - If the **TNSACONFIG** statement is coded, the **COMMUNITY** parameter must be specified with a value other than **public**.
- **TELNETPARMS** block (one defined for each port the server is listening to)
 - The **INACTIVE** and **KEEPINACTIVE** statements must be coded and must specify a value between 1 and 900.
 - The **TKOSPECLURECON** statement is omitted *or* commented out.
 - The **RESTRICTAPPL** statement is omitted *or* commented out.

Note: If the **INCLUDE** statement is coded in the Telnet profile, the data set specified on this statement must be checked for the following items as well.

Remediation:

The site will need to follow their standard change management process for updating TN3270E configuration files.

References:

1. IBM z/OS RACF STIG: RACF-TN-000060

Additional Information:

[z/OS Communications Server - IP Configuration Reference: TN3270E Telnet server](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v8	12.3 <u>Securely Manage Network Infrastructure</u> Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.			
v8	13.5 <u>Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			

6.6.2 Ensure VTAM session setup controls for the TN3270E telnet server are configured (Manual)

Profile Applicability:

- Level 1

Description:

After a connection from a Telnet client to the TN3270E Telnet Server has been established, the process of session setup with a VTAM application occurs. A number of **BEGINVTAM** statements must be coded in a specific configuration to ensure adequate control to VTAM applications is maintained. The appropriate statements must be coded to ensure adequate security of the established SNA sessions.

Rationale:

Failure to code the appropriate statements could result in unauthorized access to the host and application resources. This exposure may impact data integrity or the availability of some system services.

Audit:

Request a copy of all **JESJCL** of all active site TN3270E started tasks.

Note: If a TN3270E started task is inactive, review the procedure libraries defined to JES2 and locate the TN3270E JCL member.

Verify that the following parameters are coded in TN3270E configuration files specified by **PROFILE DD** statements:

1. Within each **BEGINVTAM** statement block, one **BEGINVTAM USSTCP** statement is coded that specifies only the table name operand. No client identifier, such as host name or IP address, is specified so the statement applies to all connections not otherwise controlled.
2. The Unformatted System Services (USS) table specified on each "backstop" **USSTCP** statement mentioned in Item (1) above is coded to allow access only to session manager applications and NC-PASS applications.
3. Within each **BEGINVTAM** statement block, additional **BEGINVTAM USSTCP** statements that specify an Unformatted System Services (USS) table that allows access to other applications may be coded only if the statements include a client identifier operand that references only secure terminals.
4. Any **BEGINVTAM DEFAULTAPPL** statement that does not specify a client identifier or specifies any type of client identifier that would apply to unsecured terminals, specifies a session manager application or an NC-PASS application as the application name.
5. Any **BEGINVTAM LUMAP** statement, if used with the **DEFAPPL** operand and applied to unsecured terminals, specifies only a session manager application or an NC-PASS application.

Notes:

- If the **INCLUDE** statement is coded in the Telnet profile, the data set specified on this statement must be checked for the following items as well.
- The **BEGINVTAM LINEMODEAPPL** requirements are not reviewed here. Further testing must be performed to determine how the CL/Supersession and NC-PASS applications work with line mode.

Remediation:

The site will need to follow their standard change management process for updating TN3270E configuration files.

References:

1. IBM z/OS RACF STIG: RACF-TN-000050

Additional Information:

[z/OS Communications Server - IP Configuration Reference: TN3270E Telnet server](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

6.6.3 Ensure a warning banner for the TN3270 telnet server is configured (Manual)

Profile Applicability:

- Level 1

Description:

A logon banner can be used to inform users about the environment during the initial logon. For example, the logon banners can be used to warn users against unauthorized entry and the possibility of legal action for unauthorized users and advise all users that system use constitutes consent to monitoring.

Rationale:

Failure to display a logon warning banner without this type of information could adversely impact the ability to prosecute unauthorized users and users who abuse the system.

Audit:

Request a copy of all **JESJCL** of all active site TN3270E started tasks.

Note: If a TN3270E started task is inactive, review the procedure libraries defined to JES2 and locate the TN3270E JCL member.

Verify that the following parameters are coded in TN3270E configuration files specified by **PROFILE DD** statements:

- All un-formatted System Services (USS) tables referenced in **BEGINVTAM USSTCP** statements include **MSG10** text that specifies a logon banner.

Note: If the **INCLUDE** statement is coded in the Telnet profile, the data set specified on this statement must be checked for the following items as well.

Remediation:

The site will need to follow their standard change management process for updating TN3270E configuration files.

References:

1. IBM z/OS RACF STIG: RACF-TN-000040

Additional Information:

[z/OS Communications Server - IP Configuration Reference: USSMSG macroinstruction](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

6.6.4 Ensure AT-TLS protection is enabled for the TN3270 telnet server (Manual)

Profile Applicability:

- Level 1

Description:

During the TLS handshake process, mutually acceptable suite of cryptographic algorithms is selected by the server and client. The algorithms specified in the selected suite are used to cryptographically protect the data that subsequently flows between the two. To apply TLS protection of adequate strength, the TN3270 Telnet server must be configured to use AT-TLS protection. Though the TN3270 Telnet server was initially implemented to use System SSL directly, that level of support no longer meets acceptable protection standards and is therefore not adequate.

Note: In z/OS V2R5 native support for System SSL was removed from the TN3270 Telnet server.

Rationale:

Failure to properly enforce adequate encryption strength could result in the loss of data privacy.

Impact:

The cryptographic operations involved in TLS do come with a CPU cost. Most of the recommended algorithms are optimized using hardware acceleration. Depending on the number and frequency of TLS handshakes, the CPU impact could be noticeable.

Audit:

Request a copy of all **JESJCL** of all active site TN3270E started tasks.

Note: If a TN3270E started task is inactive, review the procedure libraries defined to JES2 and locate the TN3270E JCL member.

Verify that the following parameters are coded in TN3270E configuration files specified by **PROFILE DD** statements:

- Each **TELNETPARMS** block specifies the **TTLSPORT** statement, and the **PORT** statement is not used.
- The **TELNETPARMS CONNTYPE** statement is coded within each **TELNETPARMS** block with either the **SECURE**, **NEGTSECURE** or **NONE** value.

Note: If the **INCLUDE** statement is coded in the Telnet profile, the data set specified on this statement must be checked for the following items as well.

Remediation:

The site will need to follow their standard change management process for updating TN3270E configuration files.

Additional Information:

- [z/OS Communications Server - IP Configuration Reference: PORT and TTLSPORT statements](#)
- [z/OS Communications Server - IP Configuration Reference: CONNTYPE statement](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

6.6.5 Ensure SMF recording options for the TN3270 telnet server are configured (Manual)

Profile Applicability:

- Level 1

Description:

The TN3270 Telnet Server can provide audit data in the form of SMF records. The SMF data produced provides information about individual sessions. This data includes the VTAM application, the remote and local IP addresses, and the remote and local IP port numbers.

Rationale:

Failure to collect and retain audit data may contribute to the loss of accountability and hamper security audit activities.

Audit:

Request a copy of all **JESJCL** of all active site TN3270E started tasks.

Note: If a TN3270E started task is inactive, review the procedure libraries defined to JES2 and locate the TN3270E JCL member.

Verify that the following parameters are coded in TN3270E configuration files specified by **PROFILE DD** statements:

- The **TELNETPARMS SMFINIT** statement is coded with the **TYPE119** operand within each **TELNETPARMS** statement block.
- The **TELNETPARMS SMFTERM** statement is coded with the **TYPE119** operand within each **TELNETPARMS** statement block.

Note: If the **INCLUDE** statement is coded in the Telnet profile, the data set specified on this statement must be checked for the following items as well.

Remediation:

The site will need to follow their standard change management process for updating TN3270E configuration files.

References:

1. IBM z/OS RACF STIG: RACF-OS-000030

Additional Information:

[z/OS Communications Server - IP Configuration Reference: SMFINIT and SMFTERM statements](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			

6.6.6 Ensure that access to the *otelnetd* and *EZATNTLE* programs is controlled (Manual)

Profile Applicability:

- Level 1

Description:

The z/OS Unix Telnet Server (*otelnetd*) provides remote access to the z/OS Unix command prompt. *otelnetd* does not provide any cryptographic protection of user connections. Due to this lack of security, the *otelnetd* server should not be used. Instead, use SSH for remote z/OS Unix command prompt access.

Note: *otelnetd* is an alias for the *EZATNTLE* program.

Rationale:

The inability to cryptographically protect *otelnetd* connections exposes all communications between telnet clients and the *otelnetd* server, including sensitive values like passwords, to network-based observers, resulting in a complete lack of data privacy.

Impact:

otelnetd users (if any) will no longer have access to *otelnetd* and must switch to a secure remote access mechanism such as SSH.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **PROGRAM** entry has:

- **-- GLOBAL INACTIVE --** or **-- NO ENTRIES --** or contains no entries covering the **EZATNTLE** and **OTELNETD** resources

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that a **EZATNTLE** profile in the **PROGRAM** class is defined and:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- No permits defined

Verify that a **OTELNETD** profile in the **PROGRAM** class is defined and:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- No permits defined

Remediation:

To create a **PROGRAM** profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE PROGRAM EZATNTLE +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    ADDMEM('SYS1.TCPIP.SEZALOAD'//NOPADCHK) +
    DATA("Z/OS UNIX TELNET SERVER")

RDEFINE PROGRAM OTELNETD +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    ADDMEM('SYS1.TCPIP.SEZALOAD'//NOPADCHK) +
    DATA("Z/OS UNIX TELNET SERVER ALIAS")

SETROPTS REFRESH WHEN(PROGRAM)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER PROGRAM <profile> +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    NOWARNING

SETROPTS REFRESH WHEN(PROGRAM)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(PROGRAM) +
    DELETE ID(<non-compliant>)

SETROPTS REFRESH WHEN(PROGRAM)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```


CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

6.7 VTAM Recommendations

This section describes the VTAM recommendations.

6.7.1 Ensure VTAM USSTAB definitions are being used for secured terminals (Manual)

Profile Applicability:

- Level 1

Description:

VTAM options and definitions are used to define VTAM operational capabilities. They must be strictly controlled. Unauthorized users could override or change start options or network definitions.

Rationale:

Failure to properly control VTAM resources could potentially compromise the network operations.

Audit:

VTAM Systems Programmer supplies the following information:

- Documentation regarding terminal naming standards.
- Documentation of all procedures controlling terminal logons to the system.
- A complete list of all USS commands used by terminal users to log on to the system.
- Members and data set names containing **USSTAB** and **LOGAPPL** definitions of all terminals that can log on to the system (e.g. **SYS1.VTAMLST**).
- Members and data set names containing logon mode parameters.

Check that the **USSTAB** definitions are only used for secure terminals (e.g., terminals that are locally attached to the host or connected to the host via secure leased lines).

Remediation:

The Systems programmer will verify that **USSTAB** definitions are only used for secure terminals.

Only terminals that are locally attached to the host or connected to the host via secure leased lines located in a secured area. Only authorized personnel may enter the area where secure terminals are located.

USSTAB or **LOGAPPL** definitions are used to control logon from secure terminals. These terminals can log on directly to any VTAM application (e.g., TSO, CICS, etc.) of their choice and bypass Session Manager services. Secure terminals are usually locally attached to the host or connected to the host via a private LAN without access to an external network. Only authorized personnel may enter the area where secure terminals are located.

References:

1. IBM z/OS RACF STIG: RACF-VT-000020

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

6.7.2 Ensure that access to the system data sets used to support the VTAM network is controlled (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that RACF data set rules for all VTAM system data sets restrict access to only network systems programming staff. These data sets include libraries containing VTAM load modules and exit routines, and VTAM start options and definition statements.

Rationale:

Failure to properly control VTAM datasets could potentially compromise the network operations.

Audit:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES -- or** contains no entries covering VTAM system data sets

Request reports generated using IRRDBU00 output that will allow you to:

Verify That VTAM system data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<vtam-dataset>' GENERIC +  
      UACC(NONE) +  
      AUDIT(FAILURES(READ)) +  
      DATA('MASTER CATALOG')  
  
PERMIT '<vtam-dataset>' GENERIC +  
      ACCESS(ALTER) ID(SYSPROG)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<vtam-dataset>' GENERIC +  
      UACC(NONE) +  
      AUDIT(FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<vtam-dataset>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-VT-000010

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

7 Cryptography and Encryption

Integrated Cryptographic Service Facility - ICSF - is a software element of z/OS that works with hardware cryptographic features and the Security Server to provide secure, high-speed cryptographic services in the z/OS environment. ICSF provides the application programming interfaces by which applications request the cryptographic services. As such, the protection of ICSF's resources is critical to a secure system.

7.1 ICSF Installation and Configuration

Once ICSF has been installed on a z/OS system, there are a minimal set of configuration tasks that need to be performed to make ICSF operational. This section expands upon the set of post-installation configuration tasks to ensure the resources associated with ICSF have been protected.

7.1.1 Ensure that access to ICSF installation data sets is controlled (Manual)

Profile Applicability:

- Level 1

Description:

The data sets installed by Integrated Crypto Service Facility (ICSF) need to be protected from unauthorized modifications or deletions.

Rationale:

ICSF can use privileged functions and/or have access to sensitive data. Failure to properly restrict access to their installed data sets could result in a loss of system integrity or customer data.

Audit:

Integrated Crypto Service Facility (ICSF) system data sets include, but are not limited to:

- CSF.SCSFCLI0
- CSF.SCSFHDRS
- CSF.SCSFMODE0
- CSF.SCSFMODE1
- CSF.SCSFMSG0
- CSF.SCSFOBJ
- CSF.SCSFPNL0
- CSF.SCSFSKL0
- CSF.SCSFTLIB

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- -- GLOBAL INACTIVE -- or -- NO ENTRIES -- or contains no entry covering ICSF system data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that ICSF system data sets are secured by RACF profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD 'CSF.**' GENERIC +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('ICSF SYSTEM DATA SETS')  
  
PERMIT 'CSF.**' GENERIC +  
      ACCESS(ALTER) ID(SYSprog)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD 'CSF.**' GENERIC +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT 'CSF.**' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-IC-000020

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

7.1.2 Ensure that the STARTED resource class is used to assign user IDs with proper parameters to ICSF started tasks (Automated)

Profile Applicability:

- Level 1

Description:

ICSF can be started via a started task. On z/OS, a started task should have a protection profile in the **STARTED** class that has neither the **PRIVILEGED** nor **TRUSTED** attribute, and the user ID identified in the **STDATA** field is neither **UID(0)** nor **SPECIAL**.

Rationale:

As a started task on a z/OS system, the ICSF started task must have a protection profile in the **STARTED** class to limit its abilities to impact other tasks running on the system. By ensuring the started task is neither **TRUSTED** nor **PRIVILEGED**, and ensuring the user ID associated with the started task is neither **UID(0)** nor **SPECIAL**, it ensures the ICSF address space is isolated from the rest.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **STARTED** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **STARTED** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **STARTED** appears.

Request the following **DSMON** report:

```
FUNCTION SYSTEM RACSPT
```

Verify that:

- The ICSF started task(s) appear in the **FROM PROFILES IN THE STARTED CLASS:** section **and not** the **FROM THE STARTED PROCEDURES TABLE (ICHRIN03):** section.
- The **TRUSTED** and **PRIVILEGED** column values are **NO** for ICSF started task(s).

Use the **ASSOCIATED USER** column to determine the user ID associated with the ICSF started task(s).

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that the FTP Server daemon started task RACF user ID:

- Has the **PROTECTED** attribute
- Does not have the **SPECIAL** attribute
- Has the following OMVS segment attributes:
 - **UID** that is not **0**

Remediation:

To activate the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(STARTED)
```

To enable generic profile checking for the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(STARTED)
```

To RACLIST the **STARTED** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(STARTED)
```

To create a **STARTED** profile use the RACF **RDEFINE** and **SETROPTS** commands:

```
RDEFINE STARTED CSF.* +  
    UACC(NONE) +  
    DATA('INTEGRATED CRYPTO SERVICE FACILITY') +  
    STDATA( +  
        USER(<icsf-user>) +  
    )  
  
SETROPTS REFRESH RACLIST(STARTED)
```

To modify a **STARTED** profile use the RACF **RALTER** and **SETROPTS** commands:

```
RALTER STARTED CSF.* +  
    STDATA( +  
        NOPRIVILEGED +  
        NOTRUSTED +  
    )  
  
SETROPTS REFRESH RACLIST(STARTED)
```

To make a user ID **PROTECTED** use the RACF **ALTUSER** command:

```
ALTUSER <icsf-id> +  
    NOPASSWORD +  
    NOPHRASE +  
    NOOIDCARD
```

To remove the **SPECIAL** attribute use the RACF **ALTUSER** command:

```
ALTUSER <icsf-id> NOSPECIAL
```

To modify the **OMVS** segment for a user ID use the RACF **ALTUSER** command:

```
ALTUSER <icsf-id> +  
    OMVS( +  
        UID(1) +  
    )
```


Notes:

1. If the security administrator has defined the **SHARED.IDS** profile in the **UNIXPRIV** class, the **UID** value must be unique. Use the **SHARED** keyword in addition to **UID** to assign a value that is already in use.
2. **OMVS DIRECTORY** and **PROGRAM** values are case sensitive, so be sure they are entered as-is and not translated to upper case.

Default Value:

- When the **ADDUSER** command is issued to create a user ID and you specify **NOOIDCARD** (or you allow this option to default), do not specify **PHRASE**, and if you specify **NOPASSWORD** or you omit the **PASSWORD** keyword, by default the ID will be created with the **PROTECTED** attribute.
- When the **ADDUSER** command is issued to create a user ID and you omit the **OMVS** keyword, by default the ID will be created with **NOOMVS**.
- The **ICHRIN03** started procedures table is used to associate the names of started procedures with user IDs.
- **NOTRUSTED** is the default for **STARTED** profiles.
- **NOPRIVILEGED** is the default for **STARTED** profiles.

References:

1. IBM z/OS RACF STIG: RACF-IC-000050

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	5.5 Establish and Maintain an Inventory of Service Accounts Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			

7.1.3 Ensure CSFINPV2 requires signature verification (Manual)

Profile Applicability:

- Level 1

Description:

Certain z/OS load modules can have an associated signature generated by IBM that is verified by the system when the module is loaded into system storage for execution. The way to ensure the signature verification occurs is by defining a profile in the **PROGRAM** class with the **SIGVER** segment.

Rationale:

By verifying the IBM generated signature when a module is loaded into storage, the integrity and authenticity of the module are guaranteed.

Audit:

Request reports generated using **IRRDBU00 output that will allow you to:**

Verify that a **CSFINPV2** profile in the **PROGRAM** class is defined and:

- Is not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- Has a **SIGVER** segment with the following values:
 - **FAILLOAD** is **ANYBAD**
 - **SIGAUDIT** is **ANYBAD**
 - **SIGREQUIRED** is **YES**

Remediation:

To create a **PROGRAM** profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE PROGRAM CSFINPV2 +
  AUDIT (FAILURES (READ) ) +
  ADDMEM ( 'SYS1.SIEALNKE' //NOPADCHK) +
  SIGVER ( +
    FAILLOAD (ANYBAD) +
    SIGAUDIT (ANYBAD) +
    SIGREQUIRED (YES) +
  )
SETROPTS REFRESH WHEN (PROGRAM)
```

To modify the **AUDIT**, **WARN**, or **SIGVER** segment settings for a general resource profile use the RACF **RALTER** command:

```
RALTER PROGRAM ICHDSM00 +
  AUDIT (FAILURES (READ) ) +
  NOWARNING +
  SIGVER ( +
    FAILLOAD (ANYBAD) +
    SIGAUDIT (ANYBAD) +
    SIGREQUIRED (YES) +
  )
SETROPTS REFRESH WHEN (PROGRAM)
```

Additional Information:

[z/OS Cryptographic Services ICSF System Programmer's Guide: Requiring signature verification for ICSF module CSFINPV2](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●

7.1.4 Ensure ICSF is configured to start during IPL (Manual)

Profile Applicability:

- Level 1

Description:

ICSF can be started in different ways, including manual via a **START** operator command. To ensure maximum availability of ICSF and crypto services, it is best to configure ICSF to be started during the z/OS IPL procedures.

This can be done by configuring ICSF to start early as described in Chapter 4. "Operating ICSF", Section "Starting ICSF during IPL-time" in the ICSF System Programmer's Guide. The **ICSF=xx** parameter should be specified in **IEASYSxx**.

Rationale:

By configuring ICSF to start during IPL, there is less operator manual intervention required, and more availability of crypto services and resources.

Audit:

Ensure the **IEASYSxx** parmlib member has **ICSFPROC** and **ICSF** system parameters, e.g.:

```
ICSFPROC=CSF2  
ICSF=00
```

Ensure the ICSF started procedure has been modified to accept the **PRM** procedure variable, e.g.:

```
//CSF      PROC PRM=00  
//CSF      EXEC PGM=CSFINIT,REGION=0M,TIME=1440,MEMLIMIT=NOLIMIT  
//CSFPARM DD DISP=SHR,DSN=USER.PARMLIB(CSFPRM&PRM)
```

Remediation:

Create the **ICSFPROC** and **ICSF** parameters in the **IEASYSxx PARMLIB** member and modify the ICSF started procedure to accept the **PRM** procedure variable.

Additional Information:

[z/OS Cryptographic Services ICSF System Programmer's Guide: Starting ICSF during IPL-time](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

7.1.5 Ensure that ICSF Master Keys are managed by a Trusted Key Entry (TKE) workstation (Manual)

Profile Applicability:

- Level 2

Description:

The z/OS Trusted Key Entry (TKE) workstation allows secure management of IBM Z host cryptographic modules running in (CCA) or IBM Enterprise PKCS#11 (EP11) mode, using hardware-based key management techniques.

Rationale:

Audit:

Verify that the site has a configured TKE workstation, and that ICSF master keys are loaded exclusively through a TKE workstation.

Remediation:

For an interactive starting point and access to a variety of technical resources about z/OS Trusted Key Entry, see [z/OS Trusted Key Entry Workstation content solution](#).

Additional Information:

[z/OS Trusted Key Entry Workstation](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

7.2 ICSF Component Configuration

ICSF has a multitude of ways it can be configured to operate, most of them specified in a dataset member referred to as the “ICSF Installation Options Dataset”. This section outlines recommendations and requirements for ICSF configuration options with an emphasis on security.

7.2.1 Ensure crypto usage statistics are enabled (Manual)

Profile Applicability:

- Level 1

Description:

ICSF can be configured to capture statistics related to the use of cryptographic resources, for example key material, cryptographic hardware engines, or even specific cryptographic algorithms.

Rationale:

By employing ICSF Crypto Usage Statistics, it is possible to detect the use of crypto resources that are not recommended, such as weak algorithms.

Audit:

Issue the following z/OS console command:

```
DISPLAY ICSF,OPTIONS
```

Look for the following message:

```
STATS:
```

Verify the following statistics are collected:

- ALG
- ENG
- SRV

Remediation:

The site will need to follow their standard change management process for updating parameters in the ICSF installation options data set to update non-compliant parameters.

Additional Information:

[z/OS Cryptographic Services ICSF System Programmer's Guide: Parameters in the installation options data set](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

7.2.2 Ensure crypto key lifecycle auditing is enabled (Manual)

Profile Applicability:

- Level 1

Description:

ICSF can be configured to audit the lifecycle of key material, for example, key creation, key activation, key deletion, etc. The lifecycle events are recorded using SMF Type 82 records.

Rationale:

By configuring ICSF to audit key lifecycle events, it is possible to preserve a record of all major events in a key's lifecycle.

Audit:

Issue the following z/OS console command:

```
DISPLAY ICSF,OPTIONS
```

Look for the following message:

```
AUDITKEYLIFECKDS: Audit CCA symmetric key lifecycle events
  SYSNAME    LABEL    TOKEN
```

Verify that the **LABEL** and **TOKEN** column values are **Yes**.

Look for the following message:

```
AUDITKEYLIFECPKDS: Audit CCA asymmetric key lifecycle events
  SYSNAME    LABEL    TOKEN
```

Verify that the **LABEL** and **TOKEN** column values are **Yes**.

Look for the following message:

```
AUDITKEYLIFETKDS: Audit PKCS #11 key lifecycle events
  SYSNAME    TOKOBJ    SESSOBJ
```

Verify that the **TOKOBJ** and **SESSOBJ** column values are **Yes**.

Remediation:

The site will need to follow their standard change management process for updating parameters in the ICSF installation options data set to update non-compliant parameters.

Default Value:

- If the **AUDITKEYLIFECKDS** option is not specified, the default is **AUDITKEYLIFECKDS (TOKEN(NO), LABEL(NO))**
- If the **AUDITKEYLIFEPKDS** option is not specified, the default is **AUDITKEYLIFEPKDS (TOKEN(NO), LABEL(NO))**
- If the **AUDITKEYLIFETKDS** option is not specified, the default is **AUDITKEYLIFETKDS (TOKENOBJ(NO), SESSIONOBJ(NO))**

Additional Information:

[z/OS Cryptographic Services ICSF System Programmer's Guide: Parameters in the installation options data set](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 Log Sensitive Data Access Log sensitive data access, including modification and disposal.			

7.2.3 Ensure crypto key usage auditing is enabled (Manual)

Profile Applicability:

- Level 1

Description:

ICSF can be configured to audit the use of key material, whether or not the key material is stored in an ICSF key data set.

Rationale:

By configuring ICSF to audit key usage events, it is possible to document which users and/or jobs are using key material.

Audit:

Issue the following z/OS console command:

```
DISPLAY ICSF,OPTIONS
```

Look for the following message:

```
AUDITKEYUSGCKDS: Audit CCA symmetric key usage events
  SYSNAME    LABEL      TOKEN      Interval Days/HH.MM.SS
```

Verify that the **LABEL** and **TOKEN** column values are **Yes**.

Look for the following message:

```
AUDITKEYUSGPKDS: Audit CCA asymmetric key usage events
  SYSNAME    LABEL      TOKEN      Interval Days/HH.MM.SS
```

Verify that the **LABEL** and **TOKEN** column values are **Yes**.

Look for the following message:

```
AUDITPKCS11USG: Audit PKCS #11 usage events
  SYSNAME    TOKOBJ     SESSOBJ    NOKEY    Interval Days/HH.MM.SS
```

Verify that the **TOKOBJ** and **SESSOBJ** column values are **Yes**.

Remediation:

The site will need to follow their standard change management process for updating parameters in the ICSF installation options data set to update non-compliant parameters.

Default Value:

- If the **AUDITKEYUSGCKDS** option is not specified, the default is **AUDITKEYUSGCKDS(TOKEN(NO), LABEL(NO), INTERVAL(24))**
- If the **AUDITKEYUSGPKDS** option is not specified, the default is **AUDITKEYUSGPKDS(TOKEN(NO), LABEL(NO), INTERVAL(24))**
- If the **AUDITPKCS11USG** option is not specified, the default is **AUDITPKCS11USG(TOKENOBJ(NO), SESSIONOBJ(NO), NOKEY(NO), INTERVAL(24))**

Additional Information:

[z/OS Cryptographic Services ICSF System Programmer's Guide: Parameters in the installation options data set](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 <u>Log Sensitive Data Access</u> Log sensitive data access, including modification and disposal.			

7.2.4 Ensure ICSF key data sets have a system backup (Manual)

Profile Applicability:

- Level 1

Description:

ICSF stores key material in data sets known as "Key Data Sets" (KDS). Symmetric keys (AES, DES, HMAC) are stored in the **CKDS**, asymmetric keys (RSA, ECC, QSA) are stored in the **PKDS**, and PKCS#11 tokens and objects are stored in the **TKDS**. These datasets need to be included in an installation's backup procedure.

Rationale:

To prevent the permanent loss of key material, and thus the loss of encrypted data, ICSF's key data sets must be backed up according to installation procedures.

Audit:

Issue the following z/OS console command:

```
DISPLAY ICSF,KDS
```

Verify that any KDS data sets listed are included in the system's backup procedure.

Remediation:

The site will need to follow their standard change management process for making updates to the system's backup procedure.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.1 Establish and Maintain a Data Recovery Process Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

7.2.5 Ensure ICSF master keys have a backup procedure (Manual)

Profile Applicability:

- Level 1

Description:

In the context of ICSF, a "master key" is a key that is loaded and stored on a Crypto Express Coprocessor, whether configured in **CCA** mode or **EP11** mode. This master key is used to encipher key material when it exists outside the boundary of the CEX coprocessor, and thus is required to make the key material usable. It is critical that the master key values can be recovered if needed.

Rationale:

ICSF's operational keys are enciphered using the Crypto Express master key, thus if the master key is lost or damaged, the key material stored in ICSF Key Data Sets are not usable. It is critical that the master key values be backed up such that if needed, the master key registered on the Crypto Express Coprocessor can be restored to their correct values so operational keys in ICSF can continue to be used.

Audit:

Issue the following z/OS console command:

```
DISPLAY ICSF,MKS
```

Verify that for any active master keys found there is a procedure in place to backup the value of that master key.

Remediation:

Create a procedure for backing up and restoring the Crypto Express master keys.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.1 Establish and Maintain a Data Recovery Process Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

7.2.6 Ensure all ICSF key data sets are in common record format (Manual)

Profile Applicability:

- Level 1

Description:

The format of ICSF Key Data Sets have evolved over time. The most recent format, referred to as "Common Record Format" or **KDSR**, is recommended as it enables features such as key reference date tracking.

Rationale:

The ICSF Key Data Sets must be in **KDSR** format in order to enable advanced security features such as key reference date tracking.

Audit:

Issue the following z/OS console command:

```
DISPLAY ICSF,KDS
```

Verify that for any KDS data sets listed the **FORMAT** value is **KDSRL**.

Remediation:

The [z/OS Cryptographic Services Integrated Cryptographic Service Facility Administrator's Guide](#) provides guidance on using the **xKDS CONVERSION** utility to convert the record format of a **KDS**.

Additional Information:

[z/OS Cryptographic Services ICSF Administrator's Guide: Converting a key data set to common record format](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●

7.2.7 Ensure all ICSF key data sets are enabled for sysplex sharing (Manual)

Profile Applicability:

- Level 1

Description:

When the ICSF Key Datasets are shared among members of a sysplex, it is critical that updates to the data sets are communicated across all members of the sysplex group. To enable the sysplex communication, the ICSF Installation Options Dataset must contain the appropriate sysplex enablement keywords.

Rationale:

Failure to specify **SYSPLEXCKDS(YES)**, **SYSPLEXPKDS(YES)**, or **SYSPLEXTKDS(YES)** when you are sharing a key data set can result in damage to the key data set.

Audit:

1. From the ICSF Primary Menu panel, select option 3 **OPSTAT**.
2. From the ICSF Installation Options panel, select option 1 **OPTIONS**.

Verify that:

- The **SYSPLEXCKDS** value is **YES, FAIL(YES)**
- The **SYSPLEXPKDS** value is **YES, FAIL(YES)**
- The **SYSPLEXTKDS** value is **YES, FAIL(YES)**

Remediation:

The site will need to follow their standard change management process for updating parameters in the ICSF installation options data set to update non-compliant parameters.

Additional Information:

- [z/OS Cryptographic Services ICSF Administrator's Guide: Running in a Sysplex Environment](#)
- [z/OS Cryptographic Services ICSF System Programmer's Guide: Parameters in the installation options data set](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	16.11 <u>Leverage Vetted Modules or Services for Application Security Components</u> Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.			

7.2.8 Ensure ICSF is running with FIPSMODE enabled (Manual)

Profile Applicability:

- Level 1

Description:

If **FIPSMODE(YES)** is specified in the ICSF Installation Options Dataset, the PKCS#11 services that ICSF provides will operate in compliance with Federal Information Processing Standard Security Requirements for Cryptographic Modules, referred to as FIPS 140-2.

Rationale:

By operating in compliance with FIPS 140-2, ICSF's PKCS#11 services will ensure the use of strong keys and FIPS 140-2 approved encryption algorithms.

Audit:

1. From the ICSF Primary Menu panel, select option 3 **OPSTAT**.
2. From the ICSF Installation Options panel, select option 1 **OPTIONS**.

Verify that the **FIPSMODE** value is **YES, FAIL(YES)**.

Remediation:

The site will need to follow their standard change management process for updating parameters in the ICSF installation options data set to update non-compliant parameters.

Default Value:

If the **FIPSMODE** option is not specified, the default is **FIPSMODE(NO, FAIL(NO))**

Additional Information:

- [z/OS Cryptographic Services ICSF Writing PKCS #11 Applications: Operating in compliance with FIPS 140-2](#)
- [z/OS Cryptographic Services ICSF System Programmer's Guide: Parameters in the installation options data set](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

7.2.9 Ensure CCA operational keys are created with WRAPENH3 key wrapping (Manual)

Profile Applicability:

- Level 1

Description:

When the Crypto Express Coprocessor is configured to run in **CCA** mode, keys generated by the coprocessor are enciphered using the coprocessor's master key (e.g. DES keys are enciphered by the DES master key). The way the keys are enciphered by the master key is referred to as the wrapping method. The most recent wrapping method, **WRAPENH3**, provides the first proprietary TDES key token (also known as a key block) to be independently reviewed and confirmed to be compliant with Payment Card Industry (PCI) Security Standard Council (SSC) PIN Security key block requirements as updated Sep 30, 2020.

Rationale:

Creating DES keys using **WRAPENH3** will ensure those key blocks are PCI compliant as noted above.

Audit:

1. From the ICSF Primary Menu panel, select option 3 **OPSTAT**.
2. From the ICSF Installation Options panel, select option 1 **OPTIONS**.

Verify that all **DEFAULTWRAP** values are **WRAPENH3**.

Remediation:

The site will need to follow their standard change management process for updating parameters in the ICSF installation options data set to update non-compliant parameters.

Default Value:

If the **DEFAULTWRAP** parameter is not specified, the default wrapping method is **ORIGINAL** for both internal and external tokens

Additional Information:

[z/OS Cryptographic Services ICSF System Programmer's Guide: Parameters in the installation options data set](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			

7.3 ICSF Security Configuration

ICSF offers many resources and services to users which can be protected using various RACF classes and resource profiles. This section provides recommendations for securing the ICSF resources

7.3.1 Ensure that the CSFSERV class is active (Manual)

Profile Applicability:

- Level 1

Description:

The **CSFSERV** SAF class is used to protect access to ICSF callable services and utilities.

Rationale:

Users can be permitted or restricted from using ICSF callable services and utilities by enabling profiles within the **CSFSERV** class.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **CSFSERV** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that:

- The **CSFSERV** entry has:
 - **-- GLOBAL INACTIVE -- or -- NO ENTRIES --**

Request reports generated using IRRDBU00 output that will allow you to:

Verify that all profiles in the **CSFSERV** class:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**

Remediation:

To activate the **CSFSERV** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(CSFSERV)
```

To modify the **UACC** setting for a profile use the RACF **RALTER** command:

```
RALTER CSFSERV <profile> +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    NOWARNING
```

Default Value:

The **CSFSERV** class is **INACTIVE** when RACF is using a newly initialized database.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

7.3.2 Ensure that the CSFKEYS class is active (Manual)

Profile Applicability:

- Level 1

Description:

The **CSFKEYS** SAF class is used to protect access to key material stored in an ICSF Key Data Set.

Rationale:

Users can be permitted or restricted from access key material by enabling profiles within the **CSFKEYS** class.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **CSFKEYS** appears.

Request the following **DSMON** report:

```
FUNCTION SYSTEM RACGAC
```

Verify that:

- The **CSFKEYS** entry has:
 - **-- GLOBAL INACTIVE -- or -- NO ENTRIES --**

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that all profiles in the **CSFKEYS** class:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**

Remediation:

To activate the **CSFKEYS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(CSFKEYS)
```

To modify the **UACC** setting for a profile use the RACF **RALTER** command:

```
RALTER CSFKEYS <profile> +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    NOWARNING
```

Default Value:

The **CSFKEYS** class is **INACTIVE** when RACF is using a newly initialized database.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

7.3.3 Ensure that the CRYPTOZ class is active (Manual)

Profile Applicability:

- Level 1

Description:

The **CRYPTOZ** class is used to protect tokens and objects stored in the ICSF Token Data Set (**TKDS**).

Rationale:

Users can be permitted or restricted from access tokens and objects in the **TKDS** by using resource profiles the **CRYPTOZ** class.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **CRYPTOZ** appears.

Request the following **DSMON** report:

```
FUNCTION SYSTEM RACGAC
```

Verify that:

- The **CRYPTOZ** entry has:
 - **-- GLOBAL INACTIVE -- or -- NO ENTRIES --**

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that all profiles in the **CRYPTOZ** class:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**

Remediation:

To activate the **CRYPTOZ** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(CRYPTOZ)
```

To modify the **UACC** setting for a profile use the RACF **RALTER** command:

```
RALTER CRYPTOZ <profile> +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    NOWARNING
```

Default Value:

The **CRYPTOZ** class is **INACTIVE** when RACF is using a newly initialized database.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

7.3.4 Ensure that the XCSFKEY class is active (Manual)

Profile Applicability:

- Level 1

Description:

While the **CSFKEYS** class controls who has access to key material, the **XCSFKEY** class provides additional controls regarding how the keys can be used. For example, it is possible to setup profiles in the **XCSFKEY** class to restrict a keys ability to be used as an exporter or importer key.

Rationale:

The **XCSFKEY** class provides usage control in addition to access permission provided by the **CSFKEYS** class.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **XCSFKEY** appears.

Request the following **DSMON** report:

```
FUNCTION SYSTEM RACGAC
```

Verify that:

- The **XCSFKEY** entry has:
 - **-- GLOBAL INACTIVE -- or -- NO ENTRIES --**

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that all profiles in the **XCSFKEY** class:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**

Remediation:

To activate the **XCSFKEY** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(XCSFKEY)
```

To modify the **UACC** setting for a profile use the RACF **RALTER** command:

```
RALTER XCSFKEY <profile> +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    NOWARNING
```

Default Value:

The **XCSFKEY** class is **INACTIVE** when RACF is using a newly initialized database.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

7.3.5 Ensure ICSF key store policy controls are enabled (Manual)

Profile Applicability:

- Level 1

Description:

ICSF Key Store Policy governs the use of key tokens in callable services. A key token is just a control block of key material that can be passed directly as an input parameter to an ICSF callable service - as opposed to specifying the label of a key stored in an ICSF Key Data Set. The Key Store Policy settings control how permission to use a key token is performed.

Rationale:

The ICSF Key Store Policy controls make it possible to provide protection profiles to key tokens in addition to key labels.

Audit:

Request reports generated using **IRRDBU00** output that will allow you to:

Verify the following fully qualified profiles are defined in the **XFACILIT** class:

- **CSF.CKDS.TOKEN.CHECK.LABEL.FAIL**
- **CSF.PKDS.TOKEN.CHECK.LABEL.FAIL**

Remediation:

To create general resource profiles use the RACF **RDEFINE** command:

```
RDEFINE XFACILIT CSF.CKDS.TOKEN.CHECK.LABEL.FAIL +  
DATA('ACTIVATES ICSF KEY STORE POLICY FOR CKDS IN FAIL MODE')  
  
RDEFINE XFACILIT CSF.PKDS.TOKEN.CHECK.LABEL.FAIL +  
DATA('ACTIVATES ICSF KEY STORE POLICY FOR PKDS IN FAIL MODE')
```

Note: Depending on the RACF class settings you may be required to issue a RACF **SETROPTS REFRESH** command for updates to be effective.

Default Value:

The **XFACILIT** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Cryptographic Services ICSF Administrator's Guide: Enabling access authority checking for key tokens](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

7.3.6 Ensure access to ICSF key data sets is controlled (Manual)

Profile Applicability:

- Level 1

Description:

ICSF has three key data sets (KDS) which are used to store cryptographic keys for application use. The three are the CKDS for CCA symmetric keys (AES, DES, HMAC), the PKDS for CCA asymmetric keys (RSA, ECC, QSA), and the TKDS for PKCS#11 tokens and key objects. These key data sets need to be protected to avoid damage or destruction to critical key material.

Rationale:

The ICSF key data sets are critical to the system and a RACF profile in the DATASET class is required to ensure no malicious or inadvertent damage can occur.

Audit:

Issue the following z/OS console command:

```
DISPLAY ICSF,KDS
```

Note the names of active ICSF Key Data Sets.

Request the following **DSMON** report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **DATASET** entry has:

- -- GLOBAL INACTIVE -- or -- NO ENTRIES -- or contains no entry covering ICSF key data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that ICSF key data sets are secured by RACF profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - The ICSF started task
 - The user ID used by any back up batch jobs

Note: Temporary **ALTER** access may be needed by administrators responsible for performing a coordinated master key change, converting KDS record formats, or other such maintenance tasks.

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD 'CSF.KDS.**' GENERIC +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('ICSF KEY DATA SETS')  
  
PERMIT 'CSF.KDS.**' GENERIC +  
      ACCESS(ALTER) ID(<icsf-id>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD 'CSF.KDS.**' GENERIC +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT 'CSF.KDS.**' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

Additional Information:

[z/OS Cryptographic Services ICSF Administrator's Guide: Setting up and maintaining cryptographic key data sets](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

7.3.7 Ensure access to ICSF administrative services is controlled (Manual)

Profile Applicability:

- Level 1

Description:

ICSF has an extensive ISPF panel architecture which can be used to administer ICSF and its resources. The use of these panels should be restricted from unauthorized use.

Rationale:

Since the ICSF ISPF panels can control ICSF resources and ICSF operating characteristics, it is critical that only authorized users have access to these panels to avoid outages or resource corruption.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **CSFSERV** appears.

Request the following **DSMON** report:

```
FUNCTION SYSTEM RACGAC
```

Verify that:

- The **CSFSERV** entry has:
 - **-- GLOBAL INACTIVE -- or -- NO ENTRIES --**

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that resources in the following table are secured by RACF profiles in the **CSFSERV** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - ICSF administrators

Resource	Description
CSFBRCK	CKDS Key Utility
CSFBRPK	PKDS Key Utility
CSFBRTK	TKDS Browser
CSFCMK	Change Master Key Utility
CSFCONF	PCF CKDS to ICSF CKDS conversion utility
CSFCRC	Coordinated KDS Administration
CSFDKCS	Master Key Entry Utility
CSFGKF	Generate Fingerprint Utility
CSFKGUP	Key Generator Utility Program
CSFOPKL	Operational Key Load
CSFPCAD	Cryptographic Processor Management (active/deactivate)
CSFPKDR	PKDS Reencipher and Refresh
CSFPMCI	Pass Phrase Initialization
CSFREFR	CKDS or PKDS Refresh
CSFRSWS	Administrator Control Functions Utility (ENABLE)
CSFRWP	CKDS Conversion2 Utility – Rewrap
CSFSMK	Set Master Key
CSFSSWS	Administrative Control Functions Utility (DISABLE)
CSFUDM	User Defined Extensions (UDX) management functions

Remediation:

To activate the **CSFSERV** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(CSFSERV)
```

To create general resource profiles use the RACF **RDEFINE** command:

```
RDEFINE CSFSERV <resource> +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    DATA('<description>')  
  
PERMIT <resource> CLASS(CSFSERV) +  
    ACCESS(ALTER) ID(<icsf-admin>)
```

Note: Depending on the RACF class settings you may be required to issue a RACF **SETROPTS REFRESH** command for updates to be effective.

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** command:

```
RALTER CSFSERV <profile> +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    NOWARNING
```

Note: Depending on the RACF class settings you may be required to issue a RACF **SETROPTS REFRESH** command for updates to be effective.

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(<class>) +  
    DELETE ID(<non-compliant>)
```

Note: Depending on the RACF class settings you may be required to issue a RACF **SETROPTS REFRESH** command for updates to be effective.

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **CSFSERV** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Cryptographic Services ICSF Administrator's Guide: Setting up profiles in the CSFSERV general resource class](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

7.3.8 Ensure access to ICSF operator commands is controlled (Manual)

Profile Applicability:

- Level 1

Description:

ICSF has two commands that can be issued at an operator console to display information about ICSF and ICSF resources or make changes to how ICSF is operating:

- **DISPLAY ICSF**
- **SETICSF**

Rationale:

Use of the ICSF operator commands must be restricted to authorized users.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **OPERCMDS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **OPERCMDS** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **OPERCMDS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **OPERCMDS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering the following resources:
 - **MVS.DISPLAY.ICSF**
 - **MVS.SETICSF**

Request reports generated using IRRDBU00 output that will allow you to:

Verify That the **MVS.DISPLAY.ICSF** and **MVS.SETICSF** resources are secured by profiles in the **OPERCMDS** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To activate the **OPERCMDS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(OPERCMDS)
```

To enable generic profile checking for the **OPERCMDS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(OPERCMDS)
```

To RACLIST the **OPERCMDS** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(OPERCMDS)
```

To create an **OPERCMDS** profile use the RACF **RDEFINE**, **PERMIT**, and **SETROPTS** commands:

```
RDEFINE OPERCMD MVS.DISPLAY.ICSF +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    DATA('DISPLAY ICSF COMMAND')  
  
PERMIT MVS.DISPLAY CLASS(OPERCMDS) +  
    ACCESS(READ) ID(SYSPROG)  
  
RDEFINE OPERCMD MVS.SETICSF +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    DATA('SETICSF COMMAND')  
  
PERMIT MVS.SETICSF CLASS(OPERCMDS) +  
    ACCESS(READ) ID(SYSPROG)  
  
SETROPTS REFRESH RACLIST(OPERCMDS)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** and **SETROPTS** commands:

```
RALTER OPERCMD <profile> +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    NOWARNING  
  
SETROPTS REFRESH RACLIST(OPERCMDS)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(OPERCMDS) +  
    DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH RACLIST(OPERCMDS)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **OPERCMDS** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

- [z/OS MVS System Commands: MVS commands, RACF access authorities, and resource names](#)
- [z/OS MVS System Commands: SETICSF command](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8 Job Management JES2

This section describes the Job Management JES2 recommendations.

8.1 JES2 Commands

This section describes the JES2 Commands recommendations.

8.1.1 Ensure that access to JES2 system commands is controlled (Manual)

Profile Applicability:

- Level 1

Description:

JES2 system commands are used to control JES2 resources and the operating system environment. Failure to properly control access to JES2 system commands could result in unauthorized personnel issuing sensitive JES2 commands.

Rationale:

If commands are not protected, this may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data. While JES2 operator commands cannot directly access sensitive data, it could change the routing of data such that it is available in an inappropriate environment.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **OPERCMDS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **OPERCMDS** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **OPERCMDS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **OPERCMDS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering:
 - resources prefixed by the JES2 subsystem IDs
 - resources prefixed by **JES2MON**

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named **<jesx>.**** has been defined for each JES2 subsystem ID in the **OPERCMDS** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers

Verify That the resources in the following table are secured by profiles in the **OPERCMDS** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access greater than **UPDATE**

Resource	JES2 Command
<jesx>.CANCEL.TSU	\$C T
<jesx>.CANCEL.TSUOUT	\$G D

Verify That the resources in the following table are secured by profiles in the **OPERCMDS** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access greater than **READ**
- **UPDATE** and higher permits are restricted to:
 - Systems Operators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Resource	JES2 Command
<jesx>.DISPLAY.<qualifier>	\$D <qualifier>
<jesx>.GDISPLAY.JOB	\$G D
JES2MON.DISPLAY.DETAIL	\$JD*
<jesx>.MODIFY.AUTOCMD	\$T A

Verify That <jesx>.UPDATE.JESNEWS resources are secured by profiles in the OPERCMDS class that:

- Have UACC of NONE
- Are not in WARNING mode
- AUDIT a minimum of SUCCESS(READ) and FAILURES(READ)
- ID(*) is not used to grant access
- READ and higher permits are restricted to:
 - Systems Programmers

Verify That any other command resources associated with the JES2 subsystem ID are secured by profiles in the OPERCMDS class that:

- Have UACC of NONE
- Are not in WARNING mode
- AUDIT a minimum of SUCCESS(READ) and FAILURES(READ)
- ID(*) is not used to grant access
- READ and higher permits are restricted to:
 - Systems Operators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Note: This covers profiles in the OPERCMDS class, associated with the JES2 subsystem ID, that are not the catch-all profile for the subsystem or profiles covering the resources in the above tables.

Remediation:

To activate the **OPERCMDS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(OPERCMDS)
```

To enable generic profile checking for the **OPERCMDS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(OPERCMDS)
```

To RACLIST the **OPERCMDS** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(OPERCMDS)
```

To create an **OPERCMDS** profile use the RACF **RDEFINE**, **PERMIT**, and **SETROPTS** commands:

```
RDEFINE OPERCMDS <jesx>.* * +
    UACC(NONE) +
    AUDIT(ALL(READ)) +
    DATA('CATCH-ALL COMMAND PROFILE FOR JES2 SUBSYSTEM NAMED <jesx>')

PERMIT <jesx>.* CLASS(OPERCMDS) +
    ACCESS(CONTROL) ID(SYSPROG)

SETROPTS REFRESH RACLIST(OPERCMDS)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** and **SETROPTS** commands:

```
RALTER OPERCMDS <profile> +
    UACC(NONE) +
    AUDIT(<audit>) +
    NOWARNING

SETROPTS REFRESH RACLIST(OPERCMDS)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(OPERCMDS) +
    DELETE ID(<non-compliant>)

SETROPTS REFRESH RACLIST(OPERCMDS)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **OPERCMDS** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-JS-000070
2. IBM z/OS RACF STIG: RACF-JS-000100

Additional Information:

- [z/OS JES2 Initialization and Tuning Guide: Authorizing the use of operator commands](#)
- [z/OS Security Server RACF Security Administrator's Guide: Protecting JESNEWS](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.2 JES2 SPOOL

This section describes the JES2 SPOOL recommendations.

8.2.1 Ensure that the JESSPOOL resource class is enabled (Manual)

Profile Applicability:

- Level 1

Description:

JESSPOOL resources control access to data stored on the JES spool data sets. This includes all **SYSOUT** and instream data set, **JCL**, **SYSLOG**, **JESTRACE**, and **JESNEWS** data sets stored on spool and the control blocks that represent those data set. Failure to properly control JES2 spool resources could result in unauthorized personnel accessing job output, system activity logs, and trace data containing user ID and password information.

Rationale:

If the **JESSPOOL** class is not active, the integrity and availability of the operating system environment is compromised, and potentially sensitive customer data is exposed. Failure to set the **JESSPOOL** class active and properly protect the resources covered by the **JESSPOOL** class could allow access to any data stored on the JES spool.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESSPOOL** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESSPOOL** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **JESSPOOL** appears.

Remediation:

To activate the **JESSPOOL** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT (JESSPOOL)
```

To enable generic profile checking for the **JESSPOOL** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC (JESSPOOL)
```

To RACLIST the **JESSPOOL** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST (JESSPOOL)
```

Default Value:

The **JESSPOOL** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-JS-000060

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Protecting data sets on spools](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

8.2.2 Ensure that access to JES2 spool resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

JESSPOOL resources controls access to data stored on the JES SPOOL data sets. This includes all SYSOUT and instream data set, JCL, SYSLOG, JESTRACE, and JESNEWS data sets stored on spool and the control blocks that represent those data set. Failure to properly control JES2 spool resources could result in unauthorized personnel accessing job output, system activity logs, and trace data containing user ID and password information. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Rationale:

Failure to manager access to resources in the **JESSPOOL** class may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data. Failure to set the **JESSPOOL** class active and properly protect the resources covered by the **JESSPOOL** class could allow access to any data stored on the JES spool.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESSPOOL** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESSPOOL** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **JESSPOOL** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESSPOOL** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --**

Note: The following specific entries can be considered compliant, but are not encouraged:

- ***.&RACUID.**/ALTER**
- ***.*.\$JESNEWS.**/READ**

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named ****** has been defined in the **JESSPOOL** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Operators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To activate the **JESSPOOL** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESSPOOL)
```

To enable generic profile checking for the **JESSPOOL** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESSPOOL)
```

To RACLIST the **JESSPOOL** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(JESSPOOL)
```

To create a **JESSPOOL** profile use the RACF **RDEFINE**, **PERMIT**, and **SETROPTS** commands:

```
RDEFINE JESSPOOL ** +
      UACC(NONE) +
      AUDIT(ALL(READ)) +
      DATA('CATCH-ALL PROFILE FOR JES SPOOL OUTPUT')

PERMIT ** CLASS(JESSPOOL) +
      ACCESS(ALTER) ID(OPERATOR SYSPROG)

SETROPTS REFRESH RACLIST(JESSPOOL)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** and **SETROPTS** commands:

```
RALTER JESSPOOL ** +
      UACC(NONE) +
      AUDIT(ALL(READ)) +
      NOWARNING

SETROPTS REFRESH RACLIST(JESSPOOL)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT ** CLASS(JESSPOOL) +
      DELETE ID(<non-compliant>)

SETROPTS REFRESH RACLIST(JESSPOOL)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESSPOOL** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-JS-000090

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling access to spool data](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.2.3 Ensure that access to JES2 trace resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

The JES2 tracing facility can be used to diagnose various problems that can occur in JES2. The data being logged may contain sensitive data and could include:

- Data from instream data set
- Data from **SYSOUT** data sets with PII data
- JCL statements including **JOB** cards potentially with passwords
- **NJE** headers including **JOB** headers potentially with passwords

SYSOUT containing this trace data is associated with the **\$TRCLOG** job and is protected by resources in the **JESSPOOL** class. Failure to protect this resource may compromise the confidentiality of customer data.

Rationale:

Since all trace data is intended to diagnose problems with how the system manages data, there are cases where that data may contain sensitive information. All trace diagnostic data should be treated as if it contains sensitive data and protected from unauthorized access.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESSPOOL** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESSPOOL** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **JESSPOOL** appears.

Request a list of all JES2 subsystem IDs used by the site.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESSPOOL** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --**

Note: The following specific entries can be considered compliant, but are not encouraged:

- ***.&RACUID.**/ALTER**
- ***.*.\$JESNEWS.**/READ**

Request reports generated using IRRDBU00 output that will allow you to:

Verify That all **<localnodeid>.<jesid>.\$TRCLOG.<jobid>.<dsnumber>.JESTRACE** resources are secured by profiles in the **JESSPOOL** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Operators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Note: **<localnodeid>** is the local **NJE** node, **<jesid>** is the user ID assigned to the JES2 address space, and **<jobid>** is the jobid of the **\$TRCLOG** job.

Remediation:

To activate the **JESSPOOL** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESSPOOL)
```

To enable generic profile checking for the **JESSPOOL** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESSPOOL)
```

To RACLIST the **JESSPOOL** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(JESSPOOL)
```

To create a **JESSPOOL** profile use the RACF **RDEFINE**, **PERMIT**, and **SETROPTS** commands:

```
RDEFINE JESSPOOL <localnodeid>.*.$TRCLOG.*.*.JESTRACE +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    DATA('CATCH-ALL JES2 TRACE OUTPUT')  
  
PERMIT <localnodeid>.*.$TRCLOG.*.*.JESTRACE CLASS(JESSPOOL) +  
    ACCESS(ALTER) ID(OPERATOR SYSPROG)  
  
SETROPTS REFRESH RACLIST(JESSPOOL)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** and **SETROPTS** commands:

```
RALTER JESSPOOL <localnodeid>.*.$TRCLOG.*.*.JESTRACE +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    NOWARNING  
  
SETROPTS REFRESH RACLIST(JESSPOOL)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(JESSPOOL) +  
    DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH RACLIST(JESSPOOL)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESSPOOL** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-JS-000090

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling access to spool data](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.2.4 Ensure that access to JESNEWS resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

JESNEWS is a spool data set that is added after the job separator when SYSOUT is printed. Installation use this facility to communicate information to their user community. Ensure that access authorization for updating **JESNEWS** is restricted to appropriate personnel (i.e. users responsible for maintaining the JES News data set).

Viewing the **JESNEWS** spool data set requires that the owner of the SPOOL data set being printed have access to the **JESNEWS** profile protected the **JESSPOOL** data set.

Rationale:

JESNEWS is intended to print information to a wide group of users of the system. The ability to create or delete a **JESNEWS** data set should be limited to system personnel.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESSPOOL** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESSPOOL** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **JESSPOOL** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESSPOOL** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --**

Note: The following specific entries can be considered compliant for **JESSPOOL**, but are not encouraged:

- ***.&RACUID.**/ALTER**
- ***.*.\$JESNEWS.**/READ**

Request reports generated using IRRDBU00 output that will allow you to:

Verify That all **<localnodeid>.<jesid>.\$JESNEWS.<jobid>.<dsnumber>.JESNEWS** resources are secured by profiles in the **JESSPOOL** class that:

- Have **UACC** of **NONE** or **READ**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access higher than **READ**
- **UPDATE** and higher permits are restricted to:
 - Systems Operators
 - Systems Programmers

Note: **<localnodeid>** is the local **NJE** node, **<jesid>** is the user ID assigned to the JES2 address space, and **<jobid>** is the jobid of the **\$TRCLOG** job.

Remediation:

To activate the **JESSPOOL** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESSPOOL)
```

To enable generic profile checking for the **JESSPOOL** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESSPOOL)
```

To RACLIST the **JESSPOOL** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(JESSPOOL)
```

To create a **JESSPOOL** profile use the RACF **RDEFINE**, **PERMIT**, and **SETROPTS** commands:

```
RDEFINE JESSPOOL <localnodeid>.*.$JESNEWS.*.*.JESNEWS +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    DATA('CATCH-ALL JES2 JESNEWS')  
  
PERMIT <localnodeid>.*.$JESNEWS.*.*.JESNEWS CLASS(JESSPOOL) +  
    ACCESS(READ) ID(*)  
  
PERMIT <localnodeid>.*.$JESNEWS.*.*.JESNEWS CLASS(JESSPOOL) +  
    ACCESS(ALTER) ID(OPERATOR SYSPROG)  
  
SETROPTS REFRESH RACLIST(JESSPOOL)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** and **SETROPTS** commands:

```
RALTER JESSPOOL <localnodeid>.*.$JESNEWS.*.*.JESNEWS +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    NOWARNING  
  
SETROPTS REFRESH RACLIST(JESSPOOL)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(JESSPOOL) +  
    DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH RACLIST(JESSPOOL)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESSPOOL** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling access to spool data](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.3 Job Level Protection

This section describes the Job Level Protection recommendations.

8.3.1 Ensure that the JESJOBS resource class is configured (Manual)

Profile Applicability:

- Level 1

Description:

The **JESJOBS** class controls access to job level resources. The high-level qualifier for entities in this class are used to specify which functions are being controlled. When defining resources in the **JESJOBS** class, avoid generic high-level qualifiers such as '*' as these could have impacts beyond the original intended purpose (especially as new resources are added to the class).

Note: If you created such profiles (ex. '*') on a system earlier than z/OS V2R1, the profiles only affected the ability of users to **CANCEL** or **SUBMIT** jobs. But on a z/OS V2R1 system, those profiles might have the unintended effect of allowing users to use the Job Modify SSI functions to modify the attributes of a job.

Rationale:

The **JESJOBS** class is used to control actions against jobs and the ability to access job related data. These types of actions and access should be restricted to appropriate personnel. Actions could be performed by unauthorized personnel that would disrupt normal processing.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESJOBS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESJOBS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESJOBS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --**

Note: The following specific entry can be considered compliant, but is not encouraged:

- **SUBMIT.*.&RACUID*&RACUID/READ**

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named *** or ** or *.* or *.*.*** is **not** defined in the **JESJOBS** class.

Verify That the following profiles have been defined in the **JESJOBS** class:

- **CANCEL.* or CANCEL.** or CANCEL.*.***
- **ENCRYPT.* or ENCRYPT.** or ENCRYPT.*.***
- **GROUPREG.* or GROUPREG.** or GROUPREG.*.***
- **HOLD.* or HOLD.** or HOLD.*.***
- **JOBCLASS.* or JOBCLASS.** or JOBCLASS.*.***
- **JOBNFY.* or JOBNFY.** or JOBNFY.*.***
- **MODIFY.* or MODIFY.** or MODIFY.*.***
- **PURGE.* or PURGE.** or PURGE.*.***
- **RELEASE.* or RELEASE.** or RELEASE.*.***
- **REROUTE.* or REROUTE.** or REROUTE.*.***
- **RESTART.* or RESTART.** or RESTART.*.***
- **SPIN.* or SPIN.** or SPIN.*.***
- **SPOOLIO.* or SPOOLIO.** or SPOOLIO.*.***
- **START.* or START.** or START.*.***
- **SUBMIT.* or SUBMIT.** or SUBMIT.*.***

Remediation:

To activate the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESJOBS)
```

To enable generic profile checking for the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESJOBS)
```

To create a **JESJOBS** profile use the RACF **RDEFINE**, **PERMIT**, and **SETROPTS** commands:

```
RDEFINE JESJOBS CANCEL.** +  
      DATA('CATCH-ALL PROFILE')  
RDEFINE JESJOBS ENCRYPT.** +  
      DATA('DEFAULT KEY LABEL TO USE TO ENCRYPT JES SPOOL DATA SETS')  
RDEFINE JESJOBS GROUPREG.** +  
      DATA('CATCH-ALL PROFILE')  
RDEFINE JESJOBS HOLD.** +  
      DATA('CATCH-ALL PROFILE')  
RDEFINE JESJOBS JOBCLASS.** +  
      DATA('CATCH-ALL PROFILE')  
RDEFINE JESJOBS JOBNFY.** +  
      DATA('CATCH-ALL PROFILE')  
RDEFINE JESJOBS MODIFY.** +  
      DATA('CATCH-ALL PROFILE')  
RDEFINE JESJOBS PURGE.** +  
      DATA('CATCH-ALL PROFILE')  
RDEFINE JESJOBS RELEASE.** +  
      DATA('CATCH-ALL PROFILE')  
RDEFINE JESJOBS REROUTE.** +  
      DATA('CATCH-ALL PROFILE')  
RDEFINE JESJOBS RESTART.** +  
      DATA('CATCH-ALL PROFILE')  
RDEFINE JESJOBS SPIN.** +  
      DATA('CATCH-ALL PROFILE')  
RDEFINE JESJOBS SPOOLIO.** +  
      DATA('CATCH-ALL PROFILE')  
RDEFINE JESJOBS START.** +  
      DATA('CATCH-ALL PROFILE')  
RDEFINE JESJOBS SUBMIT.** +  
      DATA('CATCH-ALL PROFILE')
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESJOBS** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling the use of job names](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

8.3.2 Ensure that access to JESJOBS CANCEL resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a **CANCEL** high-level qualifier in the **JESJOBS** resource class control the use of the cancel SSI 2 (used by the **CANCEL** TSO command) and the cancel function of the job modify SSI 85. Canceling jobs can cause the job to terminate the current phase of processing and optionally purge the job from the system.

Rationale:

Failure to properly control access to canceling jobs could result in unauthorized personnel disrupting normal system operations or unauthorized users terminate required jobs.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESJOBS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESJOBS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESJOBS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no **CANCEL** prefixed entries

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named **CANCEL.* or CANCEL.** or CANCEL.*.**** has been defined in the **JESJOBS** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **ALTER** permits are restricted to:
 - Systems Operators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Verify That any other **CANCEL** prefixed profiles have been defined in the **JESJOBS** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **ALTER** permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESJOBS)
```

To enable generic profile checking for the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESJOBS)
```

To create a **JESJOBS** profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE JESJOBS CANCEL.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('CATCH-ALL PROFILE')  
  
PERMIT CANCEL.** CLASS(JESJOBS) +  
      ACCESS(ALTER) ID(OPERATOR SYSPROG)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER JESJOBS CANCEL.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(JESJOBS) +  
      DELETE ID(<non-compliant>)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESJOBS** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling who can cancel jobs by job name](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.3.3 Ensure that access to JESJOBS GROUPREG resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

JCL writers can define dependencies between job using a structure called a **JOBGROUP**. A **JOBGROUP** is a set of JCL that defines the dependencies between jobs and a set of JCL jobs streams that are part of the **JOBGROUP**. **JESJOBS** resources with a high-level qualifier of **GROUPREG** control what jobs can be added to a **JOBGROUP** when the owner of the **JOBGROUP** is not the same as the owner of the **JOB**. Failure to protect this resource may allow unauthorized users to add jobs to a **JOBGROUP** that they do not own.

Rationale:

It is expected that all jobs in a job group run under the same user authority. Though this is not required. This resource prevents an unauthorized user from adding their job to an existing **JOBGROUP**.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESJOBS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESJOBS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESJOBS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no **GROUPREG** prefixed entries

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named **GROUPREG.* or GROUPREG.** or GROUPREG.*.**** has been defined in the **JESJOBS** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Production Control Specialists
 - Systems Programmers
 - IDs authorized to access these resources at this level

Verify That any other **GROUPREG** prefixed profiles have been defined in the **JESJOBS** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESJOBS)
```

To enable generic profile checking for the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESJOBS)
```

To create a **JESJOBS** profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE JESJOBS GROUPREG.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('CATCH-ALL PROFILE')  
  
PERMIT GROUPREG.** CLASS(JESJOBS) +  
      ACCESS(READ) ID(PRODCNTL SYSPROG)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER JESJOBS GROUPREG.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(JESJOBS) +  
      DELETE ID(<non-compliant>)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESJOBS** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling who can register a job to a job group](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.3.4 Ensure that access to JESJOBS HOLD resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a **HOLD** high-level qualifier in the **JESJOBS** resource class control the use of the hold function of the job modify SSI 85. Holding a job delays processing until the job is released.

Rationale:

Failure to properly control access to holding jobs could result in unauthorized personnel disrupting normal system operations.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESJOBS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESJOBS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESJOBS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no **HOLD** prefixed entries

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named **HOLD.* or HOLD.** or HOLD.*.**** has been defined in the **JESJOBS** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **UPDATE** and higher permits are restricted to:
 - Systems Operators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Verify That any other **HOLD** prefixed profiles have been defined in the **JESJOBS** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **UPDATE** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESJOBS)
```

To enable generic profile checking for the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESJOBS)
```

To create a **JESJOBS** profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE JESJOBS HOLD.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('CATCH-ALL PROFILE')  
  
PERMIT HOLD.** CLASS(JESJOBS) +  
      ACCESS(READ) ID(OPERATOR SYSPROG)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER JESJOBS HOLD.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(JESJOBS) +  
      DELETE ID(<non-compliant>)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESJOBS** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling who can modify job attributes using the Job Modify SSI 85](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.3.5 Ensure that access to JESJOBS JOBCLASS resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a **JOBCLASS** high-level qualifier in the **JESJOBS** resource class control the use of the job classes. Attributes of a job class such as bypass label processing (**BLP**) need to be restricted to appropriate users. Additionally, job classes can be associated with batch initiators that are reserved for appropriate applications.

Rationale:

Failure to properly control job class usage could result in unauthorized personnel disrupting normal system operations and using a job class reserved for a specific purpose.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES** = section.

Verify that **FACILITY** and **JESJOBS** appear.

Review the command output in the **GENERIC PROFILE CLASSES** = section.

Verify that **FACILITY** and **JESJOBS** appear.

Review the command output in the **SETR RACLIST CLASSES** = section.

Verify that **FACILITY** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESJOBS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no **JOBCLASS** prefixed entries

Request reports generated using IRRDBU00 output that will allow you to:

Verify That one or both of the following fully qualified profiles have been defined in the **FACILITY** class:

- **JES.JOBCLASS.OWNER**
- **JES.JOBCLASS.SUBMITTER**

Verify That a catch-all profile named **JOBCLASS.*** or **JOBCLASS.**** or **JOBCLASS.*.**** has been defined in the **JESJOBS** class that:

- Has a **UACC** of **READ**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access higher than **READ**

Verify That any other **JOBCLASS** prefixed profiles have been defined in the **JESJOBS** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate a class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FACILITY)
SETROPTS CLASSACT(JESJOBS)
```

To enable generic profile checking for the a class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FACILITY)
SETROPTS GENERIC(JESJOBS)
```

To RACLIST the a class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FACILITY)
```

To enable enforcement of **JOBCLASS** security use the RACF **RDEFINE** and **SETROPTS** commands:

```
RDEFINE FACILITY JES.JOBCLASS.OWNER +
    DATA('ENFORCE JESJOBS JOBCLASS PROFILES FOR JOB OWNERS')
RDEFINE FACILITY JES.JOBCLASS.SUBMITTER +
    DATA('ENFORCE JESJOBS JOBCLASS PROFILES FOR JOB SUBMITTERS')
SETROPTS REFRESH RACLIST(FACILITY)
```

To create a **JESJOBS** profile use the RACF **RDEFINE** command:

```
RDEFINE JESJOBS JOBCLASS.** +
    UACC(READ) +
    AUDIT(ALL(READ)) +
    DATA('CATCH-ALL PROFILE')
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER JESJOBS JOBCLASS.** +
    UACC(READ) +
    AUDIT(ALL(READ)) +
    NOWARNING
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(JESJOBS) +
    DELETE ID(<non-compliant>)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **FACILITY** and **JESJOBS** classes are **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling job class usage](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.3.6 Ensure that access to JESJOBS JOBNFY resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a **JOBNFY** high-level qualifier in the **JESJOBS** resource class control the use of the HTTP post notification of job status. Users of the **JOBS** REST API (and the internal reader) can specify an address where a HTTP **POST** notification is sent when certain job transitions occur (such as the job completes).

Rationale:

Use of HTTP **POST** function may need to be restricted to limit use of HTTP **POST** function.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESJOBS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESJOBS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESJOBS** entry has:

- **-- GLOBAL INACTIVE --** or **-- NO ENTRIES --** or contains no **JOBNFY** prefixed entries

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named **JOBNFY.*** or **JOBNFY.**** or **JOBNFY.*.**** has been defined in the **JESJOBS** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Verify That any other **JOBNFY** prefixed profiles have been defined in the **JESJOBS** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESJOBS)
```

To enable generic profile checking for the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESJOBS)
```

To create a **JESJOBS** profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE JESJOBS JOBNFY.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('CATCH-ALL PROFILE')  
  
PERMIT JOBNFY.** CLASS(JESJOBS) +  
      ACCESS(READ) ID(SYSPROG)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER JESJOBS JOBNFY.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(JESJOBS) +  
      DELETE ID(<non-compliant>)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESJOBS** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling job notifications](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.3.7 Ensure that access to JESJOBS MODIFY resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a **MODIFY** high-level qualifier in the **JESJOBS** resource class control the use of the modify job function of the job modify SSI 85. Modifying a job can change the attributes of a job such as the job class, service class, system affinity, and priority.

Rationale:

Failure to properly control access to modifying jobs could result in unauthorized personnel disrupting normal system operations by modifying critical jobs.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESJOBS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESJOBS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESJOBS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no **MODIFY** prefixed entries

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named **MODIFY.* or MODIFY.** or MODIFY.*.**** has been defined in the **JESJOBS** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **UPDATE** and higher permits are restricted to:
 - Production Control Specialists
 - Systems Operators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Verify That any other **MODIFY** prefixed profiles have been defined in the **JESJOBS** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **UPDATE** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESJOBS)
```

To enable generic profile checking for the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESJOBS)
```

To create a **JESJOBS** profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE JESJOBS MODIFY.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('CATCH-ALL PROFILE')  
  
PERMIT MODIFY.** CLASS(JESJOBS) +  
      ACCESS(UPDATE) ID(PRODCNTL OPERATOR SYSPROG)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER JESJOBS MODIFY.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(JESJOBS) +  
      DELETE ID(<non-compliant>)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESJOBS** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling who can modify job attributes using the Job Modify SSI 85](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.3.8 Ensure that access to JESJOBS PURGE resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a **PURGE** high-level qualifier in the **JESJOBS** resource class control the use of the purge function of the job modify SSI 85. Purging a job removes the job from the system.

Rationale:

Failure to properly control access to purging jobs could result in unauthorized personnel disrupting normal system operations by purging required jobs.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESJOBS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESJOBS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESJOBS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no **PURGE** prefixed entries

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named **PURGE.* or PURGE.** or PURGE.*.**** has been defined in the **JESJOBS** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **ALTER** permits are restricted to:
 - Production Control Specialists
 - Systems Operators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Verify That any other **PURGE** prefixed profiles have been defined in the **JESJOBS** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **ALTER** permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESJOBS)
```

To enable generic profile checking for the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESJOBS)
```

To create a **JESJOBS** profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE JESJOBS PURGE.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('CATCH-ALL PROFILE')  
  
PERMIT PURGE.** CLASS(JESJOBS) +  
      ACCESS(ALTER) ID(PRODCNTL OPERATOR SYSPROG)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER JESJOBS PURGE.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(JESJOBS) +  
      DELETE ID(<non-compliant>)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESJOBS** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling who can modify job attributes using the Job Modify SSI 85](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.3.9 Ensure that access to JESJOBS RELEASE resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a **RELEASE** high-level qualifier in the **JESJOBS** resource class control the use of the release function of the job modify SSI 85. Releasing a job could allow a job to begin processing prematurely.

Rationale:

Failure to properly control access to holding jobs could result in unauthorized personnel disrupting normal system operations.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESJOBS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESJOBS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESJOBS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES -- or** contains no **RELEASE** prefixed entries

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named **RELEASE.* or RELEASE.** or RELEASE.*.**** has been defined in the **JESJOBS** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **UPDATE** and higher permits are restricted to:
 - Production Control Specialists
 - Systems Operators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Verify That any other **RELEASE** prefixed profiles have been defined in the **JESJOBS** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **UPDATE** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESJOBS)
```

To enable generic profile checking for the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESJOBS)
```

To create a **JESJOBS** profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE JESJOBS RELEASE.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('CATCH-ALL PROFILE')  
  
PERMIT RELEASE.** CLASS(JESJOBS) +  
      ACCESS(UPDATE) ID(PRODCNTL OPERATOR SYSPROG)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER JESJOBS RELEASE.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(JESJOBS) +  
      DELETE ID(<non-compliant>)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESJOBS** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling who can modify job attributes using the Job Modify SSI 85](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.3.10 Ensure that access to JESJOBS REROUTE resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a **REROUTE** high-level qualifier in the **JESJOBS** resource class control the use of the reroute function of the job modify SSI 85. Rerouting a job sends a job (with any instream data) to another NJE node for execution (or could cause an NJE bound job to execute locally).

Rationale:

Failure to properly control access to rerouting jobs could result in unauthorized personnel disrupting normal system operations and potentially sending a job with sensitive instream data to a different NJE node. Unauthorized users rerouting a job could expose the contents of the job (and any instream data) to an unintended NJE node.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESJOBS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESJOBS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESJOBS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES -- or** contains no **REROUTE** prefixed entries

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named **REROUTE.* or REROUTE.** or REROUTE.*.**** has been defined in the **JESJOBS** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **UPDATE** and higher permits are restricted to:
 - Production Control Specialists
 - Systems Operators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Verify That any other **REROUTE** prefixed profiles have been defined in the **JESJOBS** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **UPDATE** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESJOBS)
```

To enable generic profile checking for the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESJOBS)
```

To create a **JESJOBS** profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE JESJOBS REROUTE.** +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    DATA('CATCH-ALL PROFILE')  
  
PERMIT REROUTE.** CLASS(JESJOBS) +  
    ACCESS(UPDATE) ID(PRODCNTL OPERATOR SYSPROG)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER JESJOBS REROUTE.** +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    NOWARNING
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(JESJOBS) +  
    DELETE ID(<non-compliant>)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESJOBS** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling who can modify job attributes using the Job Modify SSI 85](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.3.11 Ensure that access to JESJOBS SPIN resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a **SPIN** high-level qualifier in the **JESJOBS** resource class control the use of the spin function of the job modify SSI 85. Spinning a job caused all **SPIN** output of a job to be made available for immediate processing (rather than waiting for the job to end). **SPIN** output could include logs associated with the running job. Processing could include purging of the data sets that were spun.

Rationale:

Failure to properly control access to spinning jobs could result in unauthorized personnel making data available for processing (or purging) before the job completes.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESJOBS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESJOBS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESJOBS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no **SPIN** prefixed entries

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named **SPIN.* or SPIN.** or SPIN.*.**** has been defined in the **JESJOBS** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **CONTROL** and higher permits are restricted to:
 - Production Control Specialists
 - Systems Operators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Verify That any other **SPIN** prefixed profiles have been defined in the **JESJOBS** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **CONTROL** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESJOBS)
```

To enable generic profile checking for the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESJOBS)
```

To create a **JESJOBS** profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE JESJOBS SPIN.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('CATCH-ALL PROFILE')  
  
PERMIT SPIN.** CLASS(JESJOBS) +  
      ACCESS(CONTROL) ID(PRODCNTL OPERATOR SYSPROG)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER JESJOBS SPIN.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(JESJOBS) +  
      DELETE ID(<non-compliant>)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESJOBS** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling who can modify job attributes using the Job Modify SSI 85](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.3.12 Ensure that access to JESJOBS SPOOLIO resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a **SPOOLIO** high-level qualifier in the **JESJOBS** resource class control the use of the **SPOOL** I/O function of the job information SSI 71. The **SPOOL** I/O function is intended for application to access data on the JES2 spool for debugging purposes.

Most access to **SPOOL** control blocks is managed by the **JESSPOOL** resource class. However, that use requires that the data can be associated with a specific existing job. In the case where the data being accessed is not associated with a job or the job no longer exists, this **JESJOBS** resource class check is used.

Rationale:

Failure to properly control access to spool I/O could result in unauthorized personnel accessing sensitive or confidential data.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESJOBS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESJOBS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESJOBS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES -- or** contains no **SPOOLIO** prefixed entries

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named **SPOOLIO.* or SPOOLIO.** or SPOOLIO.*.**** has been defined in the **JESJOBS** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Verify That any other **SPOOLIO** prefixed profiles have been defined in the **JESJOBS** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESJOBS)
```

To enable generic profile checking for the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESJOBS)
```

To create a **JESJOBS** profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE JESJOBS SPOOLIO.** +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    DATA('CATCH-ALL PROFILE')  
  
PERMIT SPOOLIO.** CLASS(JESJOBS) +  
    ACCESS(READ) ID(SYSPROG)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER JESJOBS SPOOLIO.** +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    NOWARNING
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(JESJOBS) +  
    DELETE ID(<non-compliant>)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESJOBS** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS MVS Using the Subsystem Interface: SPOOL Read Service](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.3.13 Ensure that access to JESJOBS START resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a **START** high-level qualifier in the **JESJOBS** resource class control the use of the start function of the job modify SSI 85. Starting a job causes a job to begin processing immediately (starting an initiator if required). This could cause a job to begin processing prematurely.

Rationale:

Failure to properly control access to starting jobs could result in unauthorized personnel starting jobs prematurely or starting more jobs than the system has capacity to process.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESJOBS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESJOBS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESJOBS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no **START** prefixed entries

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named **START.* or START.** or START.*.**** has been defined in the **JESJOBS** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **CONTROL** and higher permits are restricted to:
 - Production Control Specialists
 - Systems Operators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Verify That any other **START** prefixed profiles have been defined in the **JESJOBS** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **CONTROL** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESJOBS)
```

To enable generic profile checking for the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESJOBS)
```

To create a **JESJOBS** profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE JESJOBS START.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('CATCH-ALL PROFILE')  
  
PERMIT START.** CLASS(JESJOBS) +  
      ACCESS(CONTROL) ID(PRODCNTL OPERATOR SYSPROG)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER JESJOBS START.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(JESJOBS) +  
      DELETE ID(<non-compliant>)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESJOBS** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling who can modify job attributes using the Job Modify SSI 85](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.3.14 Ensure that access to JESJOBS SUBMIT resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a **SUBMIT** high-level qualifier in the **JESJOBS** resource class control the submitting of batch jobs from all sources. By using these resources, you can control the combination of job names, owning user IDs, and submitting user IDs that can be used.

Rationale:

Typically, resources of this type are used when the use of job names must be restricted to certain owning user IDs or submitting user IDs. This would be the case if job names are used to control other concepts such as encryption. They can also be used to limit what jobs a user can submit or what user IDs can be used with batch jobs.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESJOBS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESJOBS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESJOBS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no **SUBMIT** prefixed entries

Note: The following specific entry can be considered compliant, but is not encouraged:

- **SUBMIT.*.&RACUID*&RACUID/READ**

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named **SUBMIT.*** or **SUBMIT.**** or **SUBMIT.*.**** has been defined in the **JESJOBS** class that:

- Has a **UACC** of **READ**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**

Note: Creating a catch-all profile that covers **SUBMIT** resources with a **UACC** of **NONE** blocks **all** batch job submission. Generally, a specific catch-all profile is created for **SUBMIT** resources with a **UACC** of **READ** and then more *specific* profiles are created with a **UACC** of **NONE** to restrict unauthorized job submissions.

Verify That any other **SUBMIT** prefixed profiles have been defined in the **JESJOBS** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

o activate the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESJOBS)
```

To enable generic profile checking for the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESJOBS)
```

To create a **JESJOBS** profile use the RACF **RDEFINE** commands:

```
RDEFINE JESJOBS SUBMIT.** +  
      UACC(READ) +  
      AUDIT(ALL(READ)) +  
      DATA('CATCH-ALL PROFILE')
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER JESJOBS SUBMIT.** +  
      UACC(READ) +  
      AUDIT(ALL(READ)) +  
      NOWARNING
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(JESJOBS) +  
      DELETE ID(<non-compliant>)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESJOBS** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling who can submit jobs by job name](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

8.3.15 Ensure that access to JESJOBS RESTART resources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a **RESTART** high-level qualifier in the **JESJOBS** resource class control the use of the restart function of the job modify SSI 85.

Rationale:

Failure to properly control access to holding jobs could result in unauthorized personnel disrupting normal system operations.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **JESJOBS** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **JESJOBS** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESJOBS** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no **RESTART** prefixed entries

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named **RESTART.* or RESTART.** or RESTART.*.**** has been defined in the **JESJOBS** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **CONTROL** and higher permits are restricted to:
 - Production Control Specialists
 - Systems Operators
 - Systems Programmers
 - IDs authorized to access these resources at this level

Verify That any other **RESTART** prefixed profiles have been defined in the **JESJOBS** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **CONTROL** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESJOBS)
```

To enable generic profile checking for the **JESJOBS** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESJOBS)
```

To create a **JESJOBS** profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE JESJOBS RESTART.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      DATA('CATCH-ALL PROFILE')  
  
PERMIT RESTART.** CLASS(JESJOBS) +  
      ACCESS(CONTROL) ID(PRODCNTL OPERATOR SYSPROG)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER JESJOBS RESTART.** +  
      UACC(NONE) +  
      AUDIT(ALL(READ)) +  
      NOWARNING
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(JESJOBS) +  
      DELETE ID(<non-compliant>)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESJOBS** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling who can modify job attributes using the Job Modify SSI 85](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.4 Enable Encryption of Data Set on SPOOL

This section describes the Enable Encryption of Data Set on SPOOL recommendations.

8.4.1 Ensure that data sets on SPOOL are encrypted (Manual)

Profile Applicability:

- Level 1

Description:

One way to encrypt data sets on SPOOL is to associate a KeyLabel with a **JESJOBS** resource with a high-level qualifier of **ENCRYPT**. This profile is not used to protect or audit use of KeyLabels, just to specify what KeyLabel is associated with a **SYSOUT** or instream data set.

Note: **ENCRYPT** resources are used to specify a KeyLabel to use to encrypt data and **are not** used to control *or* audit access.

Rationale:

Encrypting data sets on SPOOL provides an extra level of security for the data. Access to the data requires both access via the JESSPOOL class and access to the key label used to encrypt the data. It also limits the exposure to inadvertent access to SPOOL buffers.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **FACILITY** and **JESJOBS** appear.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **FACILITY** and **JESJOBS** appear.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **FACILITY** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **FACILITY** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries that would cover the following resources:
- **JES.ENCRIPT.OWNER**
- **JES.ENCRIPT.SUBMITTER**

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named **ENCRIPT.* or ENCRIPT.** or ENCRIPT.*.**** has been defined in the **JESJOBS** class that:

- Has a populated **KEYLABEL** in the **JES** segment

Verify That any other **ENCRIPT** prefixed profiles have been defined in the **JESJOBS** class:

- Have a populated **KEYLABEL** in the **JES** segment

Verify That fully qualified **JES.ENCRIPT.OWNER and JES.ENCRIPT.SUBMITTER** profiles have been defined in the **FACILITY** class that:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate a class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FACILITY)

SETROPTS CLASSACT(JESJOBS)
```

To enable generic profile checking for the a class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FACILITY)

SETROPTS GENERIC(JESJOBS)
```

To RACLIST the a class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FACILITY)
```

To create a **JESJOBS** profile use the RACF **RDEFINE** command:

```
RDEFINE JESJOBS ENCRYPT.** +
      UACC(NONE) +
      AUDIT(ALL(READ)) +
      DATA('DEFAULT KEY LABEL TO USE TO ENCRYPT JES SPOOL DATA SETS') +
      JES( +
          KEYLABEL(DEFAULTKEY)
      )
```

To modify the **KEYLABEL** settings for a general resource profile use the RACF **RALTER** command:

```
RALTER JESJOBS ENCRYPT.** +
      JES( +
          KEYLABEL(DEFAULTKEY)
      )
```

To create an **FACILITY** profile use the RACF **RDEFINE**, **PERMIT**, and **SETROPTS** commands:

```
RDEFINE FACILITY JES.ENCRYPT.OWNER +
      UACC(NONE) +
      AUDIT(FAILURES(READ)) +
      DATA('ALLOW DSKEYLBL=FOR OWNING USER ID')

RDEFINE FACILITY JES.ENCRYPT.SUBMITTER +
      UACC(NONE) +
      AUDIT(FAILURES(READ)) +
      DATA('ALLOW DSKEYLBL= FOR SUBMITTING USER ID')

PERMIT <profile> CLASS(FACILITY) +
      ACCESS(READ) ID(<compliant>)

SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(FACILITY) +  
    DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **FACILITY** and **JESJOBS** classes are **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling access to key labels for spool data sets](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			

8.5 Control Access to Data Sets Used by JES2

This section describes the Enable Encryption of Control Access to Data Sets Used by JES2 recommendations.

8.5.1 Ensure that access to the data sets used by JES2 is controlled (Automated)

Profile Applicability:

- Level 1

Description:

The JES2 System data sets are a common repository for all jobs submitted to the system and the associated printout and configuration of the JES2 environment. Initialization data sets can contain **NJE** and **RJE** signon passwords and need to be protected unintended access.

Rationale:

Allowing **READ** access to the **SPOOL** data set would allow an unauthorized user to access any data that resides on spool compromising the confidentiality of customer data.

Audit:

JES2 system data sets include:

- JES2 initialization parameters
- JES2 checkpoint data sets
- JES2 **SPOOL** data sets

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE --** or **-- NO ENTRIES --** or contains no entry covering JES2 system data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that JES2 system data sets are secured by RACF profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<jes-dataset>' GENERIC +  
      UACC(NONE) +  
      AUDIT(FAILURES(READ)) +  
      DATA('JES2 SYSTEM DATA SET')  
  
PERMIT '<jes-dataset>' GENERIC +  
      ACCESS(ALTER) ID(SYSPROG)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<jes-dataset>' GENERIC +  
      UACC(NONE) +  
      AUDIT(FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<jes-dataset>' GENERIC +  
      DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000420

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.5.2 Ensure that RACF is called for data sets opened by JES2 (Manual)

Profile Applicability:

- Level 1

Description:

The Program Property Table (PPT) provides an option to bypass password checking for data sets (NOPASS). This causes OPEN processing to bypass the call to RACF data set access authorization for the specified address space. JES2 is defined with the attribute PASS which requires that RACF be called for all data set access.

Rationale:

Specifying PASS for the PPT entry for JES2 (HASJES20) is required to ensure that access to JCLLIB data sets is properly authorized. Specifying NOPASS for HASJES20 would allow a JCLLIB JCL statement to access any data set. If the data set were a PDS with a record format of F and a record length of 80, during JCL conversion the data set would be read and its contents displayed as error message in the JCL listing. This could compromise the confidentiality of customer data.

Audit:

Request the following DSMON report:

FUNCTION SYSTEM SYSPPT

Verify that the BYPASS PASSWORD PROTECTION column value for HASJES20 is NO.

Remediation:

Update the SHEDxx PARMLIB member to remove the NOPASS specification for HASJES20.

Default Value:

No IBM-supplied default for SCHEDxx.

References:

1. IBM z/OS RACF STIG: RACF-OS-000290

Additional Information:

- [MVS Initialization and Tuning Reference: IBM-supplied program properties table \(PPT\) values](#)
- [MVS Initialization and Tuning Reference: Statements and parameters for SCHEDxx](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

8.6 Device Management

This section describes the Enable Encryption of Device Management recommendations.

8.6.1 Ensure that access to JES2 output devices is controlled (Manual)

Profile Applicability:

- Level 1

Description:

Profiles in the **WRITER** resource class can control what devices and destination a job can access. Most **WRITER** checks are made when the **SYSOUT** is selected to be printed. If the owner does not have access to the device (as defined by the **WRITER** resource class profile) then the output is not processed (and remains on **SPOOL**).

NJE destination checks (**JES2.NJE.nodename**) are performed at the time the **SYSOUT** is being allocated. If the owning user ID does not have access to the **NJE** node, the **SYSOUT** allocation is failed.

Rationale:

JES2 output devices provide a variety of channels to which output can be processed. Failure to properly control these output devices could result in unauthorized personnel accessing output.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES** = section.

Verify that **WRITER** appears.

Review the command output in the **GENERIC PROFILE CLASSES** = section.

Verify that **WRITER** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **WRITER** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --**

Request reports generated using IRRDBU00 output that will allow you to:

Verify That all profiles in the **WRITER** class:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access

Remediation:

To activate the **WRITER** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(WRITER)
```

To enable generic profile checking for the **WRITER** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(WRITER)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** and **SETROPTS** commands:

```
RALTER WRITER <profile> +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    NOWARNING
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **WRITER** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-JS-000040

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling where output can be processed](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.6.2 Ensure that bypass label processing is not set on any JOBCLASS (Manual)

Profile Applicability:

- Level 1

Description:

BLP=YES on a **JOBCLASS** statement allows certain security checks to be skipped when accessing certain tape data set. There are other ways to manage this setting than the **JOBCLASS** statement that allow for more granular authorization such as access via the RACF **TAPEVOL** resource class.

Rationale:

Using **BLP=YES** on a **JOBCLASS** statement could inadvertently expose data on tapes to unauthorized personnel.

Audit:

Issue the following JES command for each JES2 subsystem:

```
$D JOBCLASS (*),BLP
```

Verify that every **JOBCLASS** is defined with **BLP=NO**.

Remediation:

The site will need to follow their standard change management process to correct non-compliant JES2 initialization statement **JOBCLASS** entries.

Default Value:

BLP=NO

References:

1. IBM z/OS RACF STIG: RACF-JS-000040

Additional Information:

[z/OS JES2 Initialization and Tuning Reference: Parameter description for JOBCLASS\(class...|STC|TSU\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			

8.6.3 Ensure that access to JES2 input sources is controlled (Manual)

Profile Applicability:

- Level 1

Description:

JES2 input sources provide a variety of channels for job submission. Failure to properly control the use of these input sources could result in unauthorized submission of work into the operating system.

Rationale:

This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES** = section.

Verify that **JESINPUT** appears.

Review the command output in the **GENERIC PROFILE CLASSES** = section.

Verify that **JESINPUT** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **JESINPUT** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --**

Request reports generated using IRRDBU00 output that will allow you to:

Verify That a catch-all profile named ***** or ****** or ***.*** has been defined in the **JESINPUT** class that:

- Has **UACC** of **READ**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**

Verify That the resources in the following table are secured by profiles in the **JESINPUT** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access

Resource	Description
nodename	NJE node
OFF<n>.<qualifier>	Spool offload receiver
R<nnnn>.<qualifier>	RJE workstation
RDR<nn>	Local card reader

Note: The site will have to provide the specific resource names.

Verify That all other profiles in the **JESINPUT** class:

- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**

Remediation:

Note: If you activate the **JESINPUT** class and create no profiles for it, users cannot submit batch jobs.

To activate the **JESINPUT** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(JESINPUT)
```

To enable generic profile checking for the **JESINPUT** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(JESINPUT)
```

To create a **JESINPUT** catch-all profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE JESINPUT ** +  
      UACC(READ) +  
      AUDIT(ALL(READ)) +  
      DATA('CATCH-ALL PROFILE')
```

To modify the **WARN**, or **AUDIT** settings for a general resource profile use the RACF **RALTER** and **SETROPTS** commands:

```
RALTER JESINPUT <profile> +  
      AUDIT(FAILURES(READ)) +  
      NOWARNING
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **JESINPUT** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-JS-000030

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Authorizing the use of input sources](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

8.7 JES2 Networking

This section describes the JES2 Networking recommendations.

8.7.1 Ensure that RJE workstations and NJE nodes enforce password protection (Manual)

Profile Applicability:

- Level 1

Description:

JES2 **RJE** workstations and **NJE** nodes provide a method of sending and receiving data (e.g. jobs, job output, and commands) from remote locations.

Rationale:

Failure to properly identify and control these remote facilities could result in unauthorized sources transmitting data to and from the operating system. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **FACILITY** appears.

Request reports generated using **IRRDBU00 output that will allow you to:**

Verify That the following profiles have been defined in the FACILITY class:

- **NJE.* or NJE.****
- **RJE.* or RJE.****

Note: Defining these profiles will force user ID and password protection of all NJE and RJE connections respectively. A site may choose to use fully qualified profiles but this introduces the possibility of stale or missing definitions.

Remediation:

To activate the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FACILITY)
```

To enable generic profile checking for the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FACILITY)
```

To RACLIST the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FACILITY)
```

To create a the profiles use the RACF **RDEFINE** and **SETROPTS** commands:

```
RDEFINE FACILITY NJE.** +  
    DATA('ENFORCE USER ID AND PASSWORD PROTECTION FOR NJE NODES')  
RDEFINE FACILITY RJE.** +  
    DATA('ENFORCE USER ID AND PASSWORD PROTECTION FOR RJE WORKSTATIONS')  
  
SETROPTS REFRESH FACLIST(FACILITY)
```

Default Value:

The **FACILITY** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-JS-000010

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Authorizing the use of input sources](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

8.7.2 Ensure that RJE workstations have paired user IDs (Manual)

Profile Applicability:

- Level 1

Description:

JES2 **RJE** workstations and **NJE** nodes provide a method of sending and receiving data (e.g. jobs, job output, and commands) from remote locations. Failure to properly identify and control these remote facilities could result in unauthorized sources transmitting data to and from the operating system.

Rationale:

This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

This guidance addresses **RJE** Workstations that are "Dedicated". If an **RJE** workstation is dedicated, the assumption is that the **RJE** to host connection is hard-wired between the **RJE** and host. In this case the **RMT** definition statement will contain the keyword **LINE=** which specifies that this **RJE** is only connected via that one **LINE** statement.

Request a list of **RMT<nnnn> entries that are "dedicated".**

Request reports generated using **IRRDBU00 output that will allow you to:**

Verify that any "dedicated" **RMT<nnnn> entry has matching RACF **USER** ID that:**

- Has the **RESTRICTED** attribute
- Has the **UAUDIT** attribute
- Does not have any segments beyond base (ex. no **OMVS** segment)
- Does not have any extra system or group privileges (ex. **ROAUDIT**, **CLAUTH**, **group-JOIN**, etc.)
- Has **READ** access to a fully qualified **RMT<nnnn>** profile in the **JESINPUT** class

Remediation:

To create user IDs for "dedicated" **RMT<nnnn>** entries use the RACF **ADDGROUP**, **ADDUSER**, and **CONNECT** commands:

```
ADDGROUP RMTGRP +
    OWNER(<group>) +
    SUPGROUP(<group>) +
    DATA('DEFAULT DEDICATED RJE WORKSTATION ID OWNING GROUP')

ADDUSER RMT<nnnn> +
    OWNER(RMTGRP) +
    DFLTGRP(RMTGRP) +
    RESTRICTED +
    UAUDIT +
    DATA('DEDICATED RJE WORKSTATION ID')

CONNECT RMT<nnnn> +
    GROUP(RMTGRP) +
    OWNER(RMTGRP)
```

To create a paired profiles in the **JESINPUT** class use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE JESINPUT RMT<nnnn> +
    UACC(NONE) +
    AUDIT(FAILURES(READ)) +
    DATA('DEDICATED RJE WORKSTATION')

PERMIT JESINPUT RMT<nnnn> +
    ACCESS(READ) ID(RMT<nnnn>)
```

Default Value:

- **IBMUSER** is the only **USER** profile when RACF is using a newly initialized database.
- The **JESINPUT** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-JS-000120

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Authorizing the use of input sources](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.5 <u>Establish and Maintain an Inventory of Service Accounts</u> Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			

8.8 Require User Identification

This section describes the requirements for User identification.

8.8.1 Ensure that the SETROPTS JES(BATCHALLRACF) is enabled (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS BATCHALLRACF specifies that JES is to test for the presence of a user ID and password on the job statement or for propagated RACF identification information for all batch jobs. The system-wide option controls the default settings for determining how RACF will function when handling requests for access to the operating system environment, RACF, and customer data.

Rationale:

For proper logging and verification of batch job, all jobs must have a validated user ID. Failure to set this option will allow jobs to run on the system without being identified and verified by RACF.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Verify the following message appears:

```
JES-BATCHALLRACF OPTION IS ACTIVE
```

Alternatively, if IBM Health Checker for z/OS is installed and active, you can request the **HZSPRINT** output for:

```
CHECK(IBMRA CF, RACF_BATCHALLRACF)
```

Verify that the message returned is:

```
IRRH331E SETROPTS JES(BATCHALLRACF) is in effect.
```

Remediation:

To modify the **JES** parameter use the RACF **SETROPTS** command:

```
SETROPTS JES(BATCHALLRACF)
```

Default Value:

NOBATCHALLRACF is in effect when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000440

Additional Information:

- [z/OS Security Server RACF Security Administrator's Guide: Forcing batch users to identify themselves to RACF](#)
- [IBM Health Checker for z/OS: RACF_BATCHALLRACF](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

8.8.2 Ensure that the SETROPTS JES(XBMALLRACF) is enabled (Automated)

Profile Applicability:

- Level 1

Description:

XBM (Execution Batch Monitor) is a function that allows jobs to be submitted that only provide instream data to a pre-defined JCL **PROC**. The classic use of this is to perform student compiles in an educational environment. Even though the JCL **PROC** is pre-defined, proper auditing of what the JCL is accessing requires that a RACF identity exists for all jobs. **XBM** is configured by specifying a value for **XBM=** on a **JOBCLASS** statement. Use the command **\$DJOBCLASS(*),XBM!=,XBM** to determine if **XBM** is in use.

SETROPTS XBMALLRACF ensures that (assuming you have JES configured to support **XBM** jobs) any **XBM** job submitted by a user must have a RACF identity or the job will fail.

Note: This is used only in JES2.

Rationale:

Failure to set **XBMALLRACF** will allow **XBM** jobs run on a system without a proper RACF identity.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Verify the following message appears:

```
JES-XBMALLRACF OPTION IS ACTIVE
```

Remediation:

To modify the **JES** parameter use the RACF **SETROPTS** command:

```
SETROPTS JES (XBMALLRACF)
```

Default Value:

NOXBMALLRACF is in effect when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-ES-000440

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Support for execution batch monitor \(XBM\) \(JES2 Only\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

9 UNIX System Services

This section describes the UNIX System Services recommendations.

9.1 Ensure that access to z/OS UNIX SURROGAT resources is controlled (Automated)

Profile Applicability:

- Level 1

Description:

Resources in the **SURROGAT** class that start with **BPX.SRV** protect the ability to switch to another identity without providing an authenticator. Servers do this programmatically to run under the identity of their clients, and users can issue the shell **su** command to switch to another identity. These are sensitive functions that must be protected and logged, and must be used only by servers, not humans.

Rationale:

Improper protection of **BPX.SRV SURROGAT** resources can result in unintended privilege escalation and loss of accountability.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **SURROGAT** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **SURROGAT** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **SURROGAT** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **SURROGAT** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering **BPX.SRV** prefixed resources

Request reports generated using IRRDBU00 output that will allow you to:

Verify that **BPX.SRV** prefixed profiles in the **SURROGAT** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher access is restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate the **SURROGAT** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(SURROGAT)
```

To enable generic profile checking for the **SURROGAT** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(SURROGAT)
```

To RACLIST the **SURROGAT** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(SURROGAT)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** command:

```
RALTER SURROGAT BPX.SRV.<qualifier> +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    NOWARNING
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **SURROGAT** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-US-000070

Additional Information:

[z/OS UNIX System Services Planning: Defining servers to process users without passwords or password phrases](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

9.2 Ensure that access to superuser resources in the UNIXPRIV class is controlled (Automated)

Profile Applicability:

- Level 1

Description:

Resources in the **UNIXPRIV** class that start with **SUPERUSER** protect the various capabilities granted to a user with **UID(0)**. By defining profiles in the **UNIXPRIV** class, you can avoid assigning **UID(0)** to users by specifically granting certain superuser privileges with a high degree of granularity. This allows you to minimize the number of assignments of superuser authority at your installation and reduces your security risk.

Rationale:

UID(0) generally provides too much authority and presents a separation of duties issue, especially for human users. **UNIXPRIV** can be used to implement Least Privilege for UNIX superuser authorities.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **UNIXPRIV** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **UNIXPRIV** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **UNIXPRIV** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **UNIXPRIV** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering **SUPERUSER** prefixed resources

Request reports generated using IRRDBU00 output that will allow you to:

Verify that **SUPERUSER** prefixed profiles in the **UNIXPRIV** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher access is restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To activate the **UNIXPRIV** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT (UNIXPRIV)
```

To enable generic profile checking for the **UNIXPRIV** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC (UNIXPRIV)
```

To RACLIST the **UNIXPRIV** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST (UNIXPRIV)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** command:

```
RALTER UNIXPRIV SUPERUSER.<qualifiers> +  
      UACC (NONE) +  
      AUDIT (ALL (READ) ) +  
      NOWARNING
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **UNIXPRIV** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-US-000010

Additional Information:

[z/OS UNIX System Services Planning: Using UNIXPRIV class profiles](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

9.3 Ensure that general users are not allowed to change their file ownership (Automated)

Profile Applicability:

- Level 1

Description:

By default, only superusers can change the ownership of any file to any **UID** or **GID** on the system, and general users can only change the group ownership of files that they own, and only to one of their own associated **GID**. However, by defining a profile called **CHOWN.UNRESTRICTED** in the **UNIXPRIV** class, selected users can be permitted to transfer ownership of files they own to any UID or GID on the system. This is a less secure configuration.

Rationale:

Only highly trusted users should be allowed to change UNIX file ownership.

Audit:

Request reports generated using **IRRDBUG00 output that will allow you to:**

Verify that a fully qualified profile named **CHOWN.UNRESTRICTED** is **absent** in the **UNIXPRIV** class.

Remediation:

To remove a **UNIXPRIV** profile use the RACF **RDELETE** command:

```
RDELETE UNIXPRIV CHOWN.UNRESTRICTED
```

Default Value:

The **UNIXPRIV** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-US-000010

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Allowing z/OS UNIX users to change file ownerships](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			

9.4 Ensure that RESTRICTED users cannot access UNIX files to which they are not explicitly permitted (Automated)

Profile Applicability:

- Level 1

Description:

A user with the **RESTRICTED** attribute cannot access RACF protected resources by default mechanisms: the universal access of a profile (**UACC**), **ID(*)** in an access list, or the global access table. However, this restriction does not automatically apply to UNIX files.

Rationale:

RESTRICTED users may be able to access information they are not intended to have, by virtue of a file's **other** permission bits.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **UNIXPRIV** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **UNIXPRIV** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **UNIXPRIV** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **UNIXPRIV** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering the **RESTRICTED.FILESYS.ACCESS** resource

Request reports generated using IRRDBU00 output that will allow you to:

Verify that a fully qualified profile named **RESTRICTED.FILESYS.ACCESS** is **present** in the **UNIXPRIV** class and:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- Has no access permits

Remediation:

To activate the **UNIXPRIV** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT (UNIXPRIV)
```

To enable generic profile checking for the **UNIXPRIV** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC (UNIXPRIV)
```

To RACLIST the **UNIXPRIV** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST (UNIXPRIV)
```

To create a **UNIXPRIV** profile use the RACF **RDEFINE** command:

```
RDEFINE UNIXPRIV RESTRICTED.FILESYS.ACCESS +  
    UACC (NONE) +  
    AUDIT (ALL (READ) ) +  
    DATA ('PREVENT ACCESS VIA UNIX OTHER FOR RESTRICTED USER IDS')  
  
SETROPTS REFRESH RACLIST (UNIXPRIV)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** command:

```
RALTER UNIXPRIV RESTRICTED.FILESYS.ACCESS +  
    UACC (NONE) +  
    AUDIT (ALL (READ) ) +  
    NOWARNING  
  
SETROPTS REFRESH RACLIST (UNIXPRIV)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **UNIXPRIV** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling access to file system resources for restricted users](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

9.5 Ensure that newly assigned UID and GID are unique values (Automated)

Profile Applicability:

- Level 1

Description:

When users and groups share **UID** and **GID** respectively, they are essentially the same entity to the UNIX kernel.

Rationale:

Sharing IDs can result in unintended file access and a loss of accountability. Reverse mapping to a user ID or group name does not yield a consistent or predictable result (with the exception of **UID(0)**) which can lead to confusion in displays such as the output of an **ls** command. The only value that should ever be shared is **UID(0)**, which is often required by different daemons and servers.

Impact:

Administrators will need to know that the **SHARED** keyword must be specified when assigning a value, such as **UID(0)**, that is already in use. They will require **READ** access to **SHARED.IDS** in order to do so.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **UNIXPRIV** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **UNIXPRIV** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **UNIXPRIV** appears.

Request reports generated using IRRDBU00 output that will allow you to:

Verify that a fully qualified profile named **SHARED.IDS** is **present** in the **UNIXPRIV** class.

Remediation:

To activate the **UNIXPRIV** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT (UNIXPRIV)
```

To enable generic profile checking for the **UNIXPRIV** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC (UNIXPRIV)
```

To RACLIST the **UNIXPRIV** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST (UNIXPRIV)
```

To create a **UNIXPRIV** profile use the RACF **RDEFINE** command:

```
RDEFINE UNIXPRIV SHARED.IDS +  
DATA('CONTROL THE USE OF SHARED UNIX UID OR GID')
```

Default Value:

The **UNIXPRIV** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Controlling the use of shared UNIX identities](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 <u>Establish and Maintain an Inventory of Accounts</u> Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			

9.6 Ensure that z/OS UNIX user accounts are defined with compliant values (Automated)

Profile Applicability:

- Level 1

Description:

User IDs, groups, and started tasks that use z/OS UNIX facilities are defined to RACF with an **OMVS** segment containing attributes such as **UID** and **GID**.

Rationale:

If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Audit:

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that a **USER** profile with an **OMVS** segment has the following attributes:

- If specified, the **UID** value must be unique (excluding user IDs assigned **UID(0)**)
- If specified, the **HOME** value must be unique (excluding user IDs assigned **UID(0)**)
- The **PROGRAM** value must be **/bin/sh** or **/bin/tcsh** or **/bin/echo** or **/bin/false** or other approved value

Remediation:

To modify a **USER** profile use the RACF **ALTUSER** command:

```
ALTUSER <profile> +  
    OMVS ( +  
        AUTOUID +  
        HOME ('</unique/directory>') +  
        PROGRAM ('/bin/sh') +  
    )
```

Notes:

1. **AUTOUID** is only available if the site has enabled automatic assignment of unique UNIX identities.
2. The **HOME** and **PROGRAM** values are case sensitive.

Default Value:

USER profiles do not have an **OMVS** segment by default.

References:

1. IBM z/OS RACF STIG: RACF-US-000250

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 <u>Establish and Maintain an Inventory of Accounts</u> Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			

9.7 Ensure that RACF Classes required to secure the z/OS UNIX environment are active (Automated)

Profile Applicability:

- Level 1

Description:

The **FACILITY**, **SURROGAT**, and **UNIXPRIV** resource classes support profiles used to secure the z/OS UNIX (**OMVS**) environment.

- **UNIXPRIV** class profiles are used to manage certain system privileges that are typically associated with z/OS UNIX superuser authority. By defining **UNIXPRIV** class profiles, certain individual superuser privileges can be granted to users who do not have superuser authority. This reduces the security risks associated with assigning full superuser authority to users.
- **SURROGAT** class profiles are only needed if there are servers (e.g., a web server) running in the z/OS UNIX environment that must be able to act with the security context of a client and that client does not supply a password or other authenticator for RACF.
- **FACILITY** class profiles are used by a variety of IBM components including UNIX System Services (**OMVS**). **BPX** prefixed profiles in this class are critical to the proper security of the z/OS UNIX environment.

Rationale:

Without these classes being in active, system integrity can be compromised.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that:

- **FACILITY** appears
- **SURROGAT** appears
- **UNIXPRIV** appears

Remediation:

To activate the classes use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT (FACILITY SURROGAT UNIXPRIV)
```

Default Value:

The **FACILITY**, **SURROGAT**, and **UNIXPRIV** classes are **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-US-000130

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

9.8 Ensure that RACF Classes required to secure the z/OS UNIX environment are RACLISTed (Automated)

Profile Applicability:

- Level 1

Description:

RACF provides the ability to load certain classes of profiles into memory for better performance with the **SETROPTS RACLIST** command. For some classes **RACLIST** is required, but it does not happen automatically.

- **UNIXPRIV** class profiles are used to manage certain system privileges that are typically associated with z/OS UNIX superuser authority. By defining **UNIXPRIV** class profiles, certain individual superuser privileges can be granted to users who do not have superuser authority. This reduces the security risks associated with assigning full superuser authority to users.
- **SURROGAT** class profiles are only needed if there are servers (e.g., a web server) running in the z/OS UNIX environment that must be able to act with the security context of a client and that client does not supply a password or other authenticator for RACF.
- **FACILITY** class profiles are used by a variety of IBM components including UNIX System Services (**OMVS**). **BPX** prefixed profiles in this class are critical to the proper security of the z/OS UNIX environment.

Rationale:

Without these classes being **RACLIST**ed, system integrity can be compromised.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that:

- **FACILITY** appears
- **SURROGAT** appears
- **UNIXPRIV** appears

Remediation:

To activate the classes use the RACF **SETROPTS** command:

```
SETROPTS RACLIST (FACILITY SURROGAT UNIXPRIV)
```

Default Value:

The **FACILITY**, **SURROGAT**, and **UNIXPRIV** classes are **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-US-000130

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

9.9 Ensure that the user account for the z/OS UNIX kernel is defined with compliant attributes (Automated)

Profile Applicability:

- Level 1

Description:

User identifiers (RACF user IDs), groups, and started tasks that use z/OS UNIX facilities are defined to a RACF with attributes including **UID** and **GID**. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Rationale:

The z/OS UNIX kernel user ID must be defined with only the required UNIX system services attributes and prevented to access online z/OS facilities (ex. TSO, CICS, etc.).

Impact:

If compromised, without the proper attributes, the **OMVS** Kernel address space user might be used to access z/OS resources.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACSPT

Use the **ASSOCIATED USER** column to determine the user ID associated with OMVS started task.

Request reports generated using **IRRDBU00 output that will allow you to:**

Verify that the RACF user ID associated with the OMVS started task:

- Has the **PROTECTED** attribute
- Does not appear on any RACF data set or general resource access list
- Does not have any segments beyond **BASE** and **OMVS**
- Does not have any extra system or group privileges (ex. **ROAUDIT**, **CLAUTH**, **group-JOIN**, etc.)
- Has the following **OMVS** segment values:
 - **UID** value of **0**
 - **HOME** value of **/**
 - **PROGRAM** value of **/bin/sh**

Remediation:

To create a compliant UNIX kernel ID use the RACF **ADDGROUP**, **ADDUSER**, and **CONNECT** commands:

```
ADDGROUP OMVSGRP +
    OWNER(<group>) +
    SUPGROUP(<group>) +
    DATA('OMVS KERNEL') +
    OMVS(AUTOGID)

ADDUSER OMVSKERN +
    OWNER(OMVSGRP) +
    DFLTGRP(OMVSGRP) +
    NOPASSWORD +
    DATA('OMVS KERNEL') +
    OMVS( +
        UID(0) SHARED +
        HOME('/') +
        PROGRAM('/bin/sh') +
    )

CONNECT OMVSKERN +
    GROUP(OMVSGRP) +
    OWNER(OMVSGRP)
```

Notes:

1. **AUTOGID** is only available if the site has enabled automatic assignment of unique UNIX identities.
2. The **HOME** and **PROGRAM** values are case sensitive.

Default Value:

IBMUSER is the only defined **USER** profile when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-US-000220

Additional Information:

[z/OS UNIX System Services Planning: Steps for preparing RACF](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<u>5.5 Establish and Maintain an Inventory of Service Accounts</u> Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			

9.10 Ensure that z/OS UNIX automount configuration files are configured with compliant values (Automated)

Profile Applicability:

- Level 1

Description:

Parameter settings in **PARMLIB** and **/etc** specify values for z/OS UNIX security controls, in particular, the automount facility. The automount facility can automatically mount file systems at the time they are accessed, and also unmount them later. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of some system services.

Rationale:

The parameters of the automount facility should be set so they are securely mounted by the automount facility, and the users prevented to execute any file from a file-system using the user of the UNIX user or group owner other than that file. If not set, these parameters would allow a user to elevate their rights.

Audit:

Review the logical **PARMLIB** data sets (ex. **SYS1.PARMLIB(BPXPRMxx)**) for the following type of **FILESYSTYPE** entry:

<code>FILESYSTYPE TYPE(AUTOMNT) ENTRYPPOINT(BPXTAMD)</code>

Verify that for any **TYPE(AUTOMNT)** entries:

- Each **MapName** file specifies **setuid NO** and **security YES**

Remediation:

The site will need to follow their standard change process for updating non-compliant entries.

References:

1. IBM z/OS RACF STIG: RACF-US-000170

Additional Information:

[z/OS UNIX System Services Planning: Setting up the automount facility](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

9.11 Ensure that entries in `/etc/inetd.conf` are active and secure (Automated)

Profile Applicability:

- Level 1

Description:

Parameter settings in `PARMLIB` and `/etc` specify values for z/OS UNIX security controls. The UNIX services are controlled in `/etc/inetd.conf` and non-essential and potentially non-secure services must be disabled. The parameters impact HFS data access and operating system services. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of some system services.

Rationale:

The `/etc/inetd.conf` file determines if every entry in the file represents a service that is actually in use. Services that are not in use must be disabled to reduce potential security exposures. Some non-essential services can potentially give remote access to attackers and must be disabled.

Audit:

Verify that every entry in `/etc/inetd.conf` represents a service that is actually in use.

Verify that the following services have been disabled in `/etc/inetd.conf`:

Service	Port
chargen	19
daytime	13
discard	9
echo	7
exec	512
finger	79
login	513
nameserver	42
netstat	15
qotd	17
shell	514
smtp	25
systat	11
talk	517
tftp	69
time	37
timed	525
uucp	540

Remediation:

The site will need to follow their standard change process for updating non-compliant entries.

References:

1. IBM z/OS RACF STIG: RACF-US-000180

Additional Information:

[z/OS UNIX System Services Planning: Customizing the inetd daemon](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

9.12 Ensure that z/OS UNIX OMVS parameters in IEASYSxx are configured (Automated)

Profile Applicability:

- Level 1

Description:

This is a setting in **IEASYSxx PARMLIB** member to state which **BPXPRMxx** to use to configure UNIX system services. Parameter settings in **PARMLIB** and **/etc** specify values for z/OS UNIX security controls.

Rationale:

The parameters impact ZFS data access and operating system services. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of some system services.

Audit:

The parameter is specified as **OMVS=xx** or **OMVS=(xx,xx,...)** in the **IEASYSxx** member.

Note: If the **OMVS** statement is not specified, **OMVS=DEFAULT** is used. In minimum mode there is no access to permanent file systems or to the shell, and IBM's Communication Server TCP/IP will not run.

Verify that OMVS settings are not defaulting with the **OMVS=(xx,xx)** parameter set.

Remediation:

The site will need to follow their standard change process for updating non-compliant entries.

References:

1. IBM z/OS RACF STIG: RACF-US-000140

Additional Information:

[z/OS UNIX System Services Planning: Setting up kernel services in full function mode](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

9.13 Ensure that z/OS UNIX BPXPRMxx parameters in PARMLIB are configured for security (Automated)

Profile Applicability:

- Level 1

Description:

Parameter settings in **PARMLIB** member **BPXPRMxx** and **/etc** specify values for z/OS UNIX security controls.

Rationale:

The parameters in **BPXPRMxx** and **/etc** impact data access and operating system services.

Impact:

Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of some system services.

Audit:

Review the logical **PARMLIB** data sets (ex. **SYS1.PARMLIB(BPXPRMxx)**).

Verify the UNIX parameters are set according to the following table:

Keyword	Value
MOUNT	NOSETUID
ROOT	SETUID
SETUID (for Vendor-provided files)	SECURITY
STARTUP_PROC	OMVS
STEPLIBLIST	/etc/steplib
SUPERUSER	BPXROOT
TTYGROUP	TTY
UMASK	specify that other write bits are not ON
USERIDALIASTABLE	omitted or commented out

Remediation:

The site will need to follow their standard change process for updating non-compliant entries.

References:

1. IBM z/OS RACF STIG: RACF-US-000150

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

9.14 Ensure that z/OS UNIX permission bits and audit bits are configured to audit sensitive file access (Automated)

Profile Applicability:

- Level 1

Description:

With z/OS UNIX a file owner or a security auditor can specify if auditing is turned on or off, and when audit records should be written for a directory or a file: for successful accesses, failed accesses, or for all accesses. Sensitive files or directories access should be audited. The permissions bits also set access permissions for three classes: **owner**, **group**, and **other**. Sensitive files access must be restricted.

Rationale:

Sensitive configuration files or logs must be restricted to authorized personnel and audited for system integrity. If not audited, uncontrolled modifications to sensitive configuration files or logs would not be detected.

Audit:

Verify that the permission bits and user audit bits for sensitive files or directories match or are more restrictive than the specified settings listed in the table:

File	Permission Bits	User Audit Bits
/usr/lpp/tcpip/sbin/syslogd	740	rwX=f
/etc/syslog.conf	744	w=sf,rx+f
/etc/hosts	744	w=sf,rx+f
/etc/protocol	744	w=sf,rx+f
/etc/resolv.conf	744	w=sf,rx+f
/etc/services	740	w=sf,rx+f
/usr/lpp/tcpip/bin	755	w=sf,rx+f
/usr/lpp/tcpip/sbin	755	w=sf,rx+f

Remediation:

To modify the audit flags for a UNIX file use the **chaudit** command:

```
chaudit rwx=f /usr/lpp/tcpip/sbin/syslogd
chaudit w=sf,rx+f /etc/syslog.conf
chaudit w=sf,rx+f /etc/hosts
chaudit w=sf,rx+f /etc/protocol
chaudit w=sf,rx+f /etc/resolv.conf
chaudit w=sf,rx+f /etc/services
chaudit w=sf,rx+f /usr/lpp/tcpip/bin
chaudit w=sf,rx+f /usr/lpp/tcpip/sbin
```

To modify the access permissions for a UNIX file use the **chmod** command:

```
chmod 740 /usr/lpp/tcpip/sbin/syslogd
chmod 744 /etc/syslog.conf
chmod 744 /etc/hosts
chmod 744 /etc/protocol
chmod 744 /etc/resolv.conf
chmod 740 /etc/services
chmod 755 /usr/lpp/tcpip/bin
chmod 755 /usr/lpp/tcpip/sbin
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

9.15 Ensure that access to BPX resources in the FACILITY class is controlled (Automated)

Profile Applicability:

- Level 1

Description:

The RACF **FACILITY** class profiles prefixed with **BPX** are protecting sensitive UNIX System Services capabilities and must be protected.

Rationale:

z/OS UNIX RACF-defined resources, prefixed with **BPX** in the **FACILITY** class consist of sensitive capabilities including **SUPERUSER**, daemon, and numerous file manipulation privileges.

Impact:

Missing or inaccurate protection of these resources could allow a user to access sensitive data, modify or delete data and operating system controls, or issue commands that could negatively impact system availability.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **FACILITY** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **FACILITY** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering **BPX** prefixed resources

Request reports generated using IRRDBU00 output that will allow you to:

Verify that a fully-qualified profile named **BPX.SAFFASTPATH** is **not** defined in the **FACILITY** class.

Verify that a catch-all profile named **BPX.** or BPX.* or BPX.*.**** is defined in the **FACILITY** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access

Verify that **BPX** prefixed profiles in the **FACILITY** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher access is restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FACILITY)
```

To enable generic profile checking for the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FACILITY)
```

To RACLIST the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FACILITY)
```

To remove a **BPX.SAFFASTPATH** profile use the RACF **RDELETE** command:

```
RDELETE FACILITY BPX.SAFFASTPATH
```

To create catch-all profiles use the RACF **RDEFINE** command:

```
RDEFINE FACILITY BPX.** +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    DATA('UNIX SYSTEM SERVICES CATCH-ALL PROFILE')  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** command:

```
RALTER FACILITY BPX.<qualifiers> +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    NOWARNING  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **FACILITY** class is **INACTIVE** when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-US-000020

Additional Information:

[z/OS UNIX System Services Planning: Setting up the UNIX-related FACILITY and SURROGAT class profiles](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

9.16 Ensure that security parameters in /etc/profile are configured (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/profile` file is the system-wide profile for the z/OS UNIX System Services shell users. It contains environment variables and commands used by most shell users. Some variables and commands in a secure system.

Rationale:

When users are using UNIX System Services through a shell, we must ensure that specific variables are set and specific commands are issued.

Impact:

If the variables are not set or the commands not executed, the system security can be compromised.

Audit:

Verify that the following entries have been defined in all active zOS UNIX system services `/etc/profile` files:

- `umask` with a value of `077`
- `readonly` with a value of `LOGNAME`

Remediation:

The site will follow their standard change management process for updating `/etc/profile` to set compliant values.

References:

1. IBM z/OS RACF STIG: RACF-US-000050

Additional Information:

[z/OS UNIX System Services Planning: Customizing /etc/profile](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

9.17 Ensure that security commands in /etc/rc are safe (Automated)

Profile Applicability:

- Level 1
- Level 2

Description:

The `/etc/rc` file contains customization commands for z/OS UNIX System Services Application Services. Part of these commands are changing files authorization bits and might change auditing options.

Rationale:

Sensitive configuration files or logs must be restricted to authorized personnel and audited for system integrity. Text and must not be changed by application services customization commands.

Audit:

Verify that any any `chmod` or `chaudit` commands targeting sensitive files in active `/etc/rc` are either removed or configured to set the following values:

File	Permission Bits	User Audit Bits
<code>/</code>	755	faf
<code>/bin</code>	755	fff
<code>/bin/sh</code>	755	faf
<code>/dev</code>	755	fff
<code>/dev/console</code>	740	fff
<code>/dev/null</code>	666	fff
<code>/etc</code>	755	faf
<code>/etc/auto.master</code>	740	faf
<code>/etc/inetd.conf</code>	740	faf

File	Permission Bits	User Audit Bits
/etc/init.options	740	faf
/etc/log	744	fff
/etc/profile	755	faf
/etc/rc	744	faf
/etc/steplib	740	faf
/etc/tablename	740	faf
/lib	755	fff
/samples	755	fff
/tmp	777	fff
/u	755	fff
/usr	755	fff
/usr/lib/cron/at.allow	700	faf
/usr/lib/cron/at.deny	700	faf
/usr/lib/cron/cron.allow	700	faf
/usr/lib/cron/cron.deny	700	faf
/var	775	fff

Remediation:

The site will follow their standard change management process for updating `/etc/rc` to compliant values.

References:

1. IBM z/OS RACF STIG: RACF-US-000060

Additional Information:

[z/OS UNIX System Services Planning: Customizing /etc/rc](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

9.18 Ensure that the BPXROOT user account is configured with compliant values (Manual)

Profile Applicability:

- Level 1

Description:

The z/OS UNIX System Services function **setuid** can be used to change the **UID** of the process. When the **UID** requested is **UID=0**, the user set as **SUPERUSER** in **BPXPRMxx** is used. The default user is **BPXROOT**.

Rationale:

The **BPXROOT** user must be defined with the correct attributes so the **setuid** function can be securely used. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Audit:

Request a list of **BPXROOT** user ID values for the **SUPERUSER** statement in **BPXPRMxx** members.

Request reports generated using IRRDBU00 output that will allow you to:

Verify that the RACF user ID defined as **BPXROOT** in a **SUPERUSER** statement:

- Has the **PROTECTED** attribute
- Does not appear on any RACF data set or general resource access list
- Does not have any segments beyond base and **OMVS**
- Does not have any extra system or group privileges (ex. **ROAUDIT**, **CLAUTH**, **group-JOIN**, etc.)
- Has the following **OMVS** segment values:
 - **UID** value of **0**
 - **HOME** value of **/**
 - **PROGRAM** value of **/bin/sh**
- Does **not** have access to the **BPX.DAEMON** resource secured by the **FACILITY** class.

Remediation:

To create a compliant **BPXROOT** user ID use the RACF **ADDGROUP**, **ADDUSER**, and **CONNECT** commands:

```
ADDUSER BPXROOT +
  OWNER(OMVSGRP) +
  DFLTGRP(OMVSGRP) +
  NOPASSWORD +
  DATA('USER IS DEFINED AS SUPERUSER IN BPXPRMXX') +
  OMVS( +
    UID(0) SHARED +
    HOME('/') +
    PROGRAM('/bin/sh') +
  )

CONNECT OMVSKERN +
  GROUP(OMVSGRP) +
  OWNER(OMVSGRP)
```

Note: The **HOME** and **PROGRAM** values are case sensitive.

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT BPX.DAEMON CLASS(FACILITY) +
  DELETE ID(BPXROOT)

SETROPTS RACFLIST GENERIC(FACILITY)
```

Default Value:

- If you do not specify the **SUPERUSER** statement in **BPXPRMxx** the default is **BPXROOT**.
- **IBMUUSER** is the only defined **USER** profile when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-US-000230

Additional Information:

[z/OS UNIX System Services Planning: Steps for preparing the security program for daemons](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.5 <u>Establish and Maintain an Inventory of Service Accounts</u> Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			

9.19 Ensure that each RACF group for UNIX is defined with a unique GID (Automated)

Profile Applicability:

- Level 1

Description:

When groups share **GIDs**, they are essentially the same entity to the UNIX kernel.

Rationale:

Sharing **GIDs** can result in unintended file access and a loss of accountability. Reverse mapping to a group name does not yield a consistent or predictable result, which can lead to confusion in displays such as the output of an **ls** command.

Audit:

Request reports generated using **IRRDBU00 output that will allow you to:**

Verify that the RACF groups with **OMVS** segment values have unique **GID** values.

Remediation:

To modify the GID value of a RACF group use the **ALTGROUP** command:

```
ALTGROUP <group-id> OMVS(AUTOGID)
```

Note: **AUTOGID** is only available if the site has enabled automatic assignment of unique UNIX identities.

Default Value:

GROUP profiles do not have an **OMVS** segment by default.

References:

1. IBM z/OS RACF STIG: RACF-US-000200

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Enabling automatic assignment of unique UNIX identities](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 <u>Establish and Maintain an Inventory of Accounts</u> Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			

9.20 Ensure that access to data sets used as step libraries in /etc/steplib is controlled (Automated)

Profile Applicability:

- Level 1

Description:

The **STEPLIBLIST** parameter specifies the pathname of the HFS file that contains the list of MVS data sets that are used as step libraries for programs that have the set user id or set group id permission bit set. The use of **STEPLIBLIST** is at the site's discretion, but if used the value of **STEPLIBLIST** should be **/etc/steplib**. All update and alter access to the MVS data sets in the list will be logged and only systems programming personnel should be authorized to update the data sets.

Rationale:

Insufficient protection of these data sets can cause the environment to become compromised.

Audit:

Request a list of data sets defined in active **/etc/steplib**.

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entry covering data sets defined in **/etc/steplib**

Request reports generated using **IRRDBU00** output that will allow you to:

Verify that data sets defined in **/etc/steplib** are secured by RACF profiles in the **DATASET** class that:

- Have **UACC** of **NONE** or **READ**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(UPDATE)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access higher than **READ**
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<steplib-dataset>' GENERIC +
      UACC(NONE) +
      AUDIT(SUCCESS(UPDATE),FAILURES(READ)) +
      DATA('CAN BE USED AS STEPLIB LIBRARY FOR SETUID PROGRAMS')

PERMIT '<steplib-dataset>' GENERIC +
      ACCESS(READ) ID(*)

PERMIT '<steplib-dataset>' GENERIC +
      ACCESS(ALTER) ID(SYSPROG)

SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<steplib-dataset>' GENERIC +
      UACC(NONE) +
      AUDIT(SUCCESS(UPDATE),FAILURES(READ)) +
      NOWARNING

SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<steplib-dataset>' GENERIC +
      DELETE ID(<non-compliant>)

SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

References:

1. IBM z/OS RACF STIG: RACF-US-000120

Additional Information:

[z/OS UNIX System Services Planning: STEPLIBLIST](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

9.21 Ensure that ability to switch into superuser mode is controlled (Automated)

Profile Applicability:

- Level 1

Description:

When a user switches into superuser mode (for example, by issuing the **su** command in the shell) they operate with an effective **UID** of **0**. That is, they are as privileged as if they were assigned **UID(0)** in their **OMVS** segment.

Rationale:

Granting access to **BPX.SUPERUSER** should be viewed to be as sensitive as explicitly assigning **UID(0)**. Erroneous access to **BPX.SUPERUSER** can result in complete compromise of the system.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **FACILITY** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **FACILITY** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering the **BPX.SUPERUSER** resource

Request reports generated using IRRDBU00 output that will allow you to:

Verify that the **BPX.SUPERUSER** resource is secured by a fully-qualified profile in the **FACILITY** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits is restricted to:
 - Systems Programmers
 - IDs authorized to access these resources at this level

Remediation:

To activate the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FACILITY)
```

To enable generic profile checking for the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FACILITY)
```

To RACLIST the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FACILITY)
```

To create a fully-qualified profile use the RACF **RDEFINE** command:

```
RDEFINE FACILITY BPX.SUPERUSER +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    DATA('PERMISSION TO USE THE SU COMMAND TO OBTAIN SUPERUSER  
AUTHORITY')  
  
PERMIT BPX.SUPERUSER CLASS(FACILITY) +  
    ACCESS(READ) ID(SYSPROG)  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** command:

```
RALTER FACILITY BPX.SUPERUSER +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    NOWARNING  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **FACILITY** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS UNIX System Services Planning: Using the BPX.SUPERUSER resource in the FACILITY class](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

9.22 Ensure access to zFS data sets is controlled (Automated)

Profile Applicability:

- Level 1

Description:

z/OS zFS datasets contains z/OS UNIX file systems data. If not protected these datasets can be modified, hindering system security.

Rationale:

z/OS zFS datasets contains the files from the z/OS UNIX file systems along with the UNIX attributes controlling security.

Audit:

Request the following **DSMON** report:

FUNCTION SYSTEM RACGAC

Verify that the **DATASET** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering zFS data sets

Request reports generated using **IRRDBU00** output that will allow you to:

Verify That the zFS data sets are secured by profiles in the **DATASET** class that:

- Have **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **UPDATE** and higher permits are restricted to:
 - Systems Programmers

Remediation:

To create a **DATASET** profile use the RACF **ADDSD** and **PERMIT** commands:

```
ADDSD '<zfs-dataset>' GENERIC +  
      UACC(NONE) +  
      AUDIT(FAILURES(READ)) +  
      DATA('UNIX FILE SYSTEM')  
  
PERMIT '<zfs-dataset>' GENERIC +  
      ACCESS(ALTER) ID(SYSprog)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a **DATASET** profile use the RACF **ALTDSD** command:

```
ALTDSD '<zfs-dataset>' GENERIC +  
      UACC(NONE) +  
      AUDIT(FAILURES(READ)) +  
      NOWARNING  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT '<zfs-dataset>' GENERIC +  
      DELETE ID(*)  
  
SETROPTS REFRESH GENERIC(DATASET)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

SETROPTS NOPROTECTALL is in effect for data sets when RACF is using a newly initialized database.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

9.23 Ensure USS Telnet server is not active (Automated)

Profile Applicability:

- Level 1

Description:

Running the USS Telnet server is a security concern as telnet data flow is not encrypted. SSH is recommended.

Rationale:

Using an unencrypted network protocol results in clear text passwords being sent across the network connection.

Audit:

The `otelnetd` server should not be activated through the `inet daemon` (through `/etc/inetd.conf`) or permitted in the list of TCPIP services (`/etc/services` or `<hlq>.ETC.SERVICES`).

Remediation:

The site will have to follow their standard change management procedure for disabling non-compliant z/OS UNIX daemons.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

9.24 Ensure rlogin is not active (Manual)

Profile Applicability:

- Level 1

Description:

The **rlogin** command enables log in to a remote system and navigate through the remote file system and manipulate its contents, copy files, or execute remote commands.

Rationale:

rlogin server processing operates in clear text and therefore should be disabled.

Audit:

The **rlogind** server should not be activated through the **inet daemon** (through **/etc/inetd.conf**) or permitted in the list of TCPIP services (**/etc/services** or **<hlq>.ETC.SERVICES**).

Remediation:

The site will have to follow their standard change management procedure for disabling non-compliant z/OS UNIX daemons.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

9.25 Ensure that the FSSEC resource class is enabled (Manual)

Profile Applicability:

- Level 1

Description:

By default, UNIX security attribute (e.g. owner, permission bits) changes are not logged in SMF Type 80 records. These changes should be logged, just as changes to RACF profiles should be logged.

Rationale:

In the absence of SMF Type 80 records for UNIX file security attribute changes, it is more difficult to debug authorization problems and investigate potential attacks. Enabling logging for security changes provides a historical record of security changes and allows for **ICH408I** violation messages to be sent to the security console when an unauthorized person attempts to change security attributes.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES** = section.

Verify that **FSSEC** appears.

Review the command output in the **LOGOPTIONS "ALWAYS" CLASSES** = section.

Verify that **FSSEC** appears.

Remediation:

To activate the **FSSEC** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT (FSSEC)
```

Note: Activating the FSSEC class enables the use of ACLs in authorization checking.

To enforce logging in the **FSSEC** class use the RACF **SETROPTS** command:

```
SETROPTS LOGOPTIONS (ALWAYS (FSSEC) )
```

Default Value:

The **FSSEC** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Auditing for z/OS UNIX System Services](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

9.26 Ensure that programs cannot execute from the /tmp directory (Automated)

Profile Applicability:

- Level 1

Description:

By default, programs and scripts can be run from within any file system in the hierarchy. This ability should be restricted from within the `/tmp` directory. The `FSEEXEC` class can be used to prevent file execution from an individual file system regardless of permission bits, file ownership, or even superuser privilege.

Note: `FSEEXEC` restriction does not apply to file systems mounted with the `-s nosecurity` option.

Rationale:

When an attacker gains access to UNIX, their first action is often to run a script to detect system vulnerabilities. The `/tmp` directory is often used for this purpose because all users, by necessity, can typically create files in this directory.

Impact:

An additional access check is performed whenever a UNIX file is opened for execute access.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **FSEEXEC** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **FSEEXEC** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **FSEEXEC** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering **/tmp**

Request reports generated using IRRDBU00 output that will allow you to:

Verify that a fully qualified **/tmp** profile is defined in the **FSEEXEC** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access

Remediation:

To activate the **FSEEXEC** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FSEEXEC)
```

To RACLIST the **FSEEXEC** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FSEEXEC)
```

To create catch-all profiles use the RACF **RDEFINE** command:

```
RDEFINE FSEEXEC /tmp +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    DATA('CONTROL EXECUTE FROM UNIX TMP DIRECTORY')  
  
SETROPTS REFRESH RACLIST(FSEEXEC)
```

Note: Profile names in the **FSEEXEC** class are case sensitive.

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** command:

```
RALTER FSEEXEC /tmp +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    NOWARNING  
  
SETROPTS REFRESH RACLIST(FSEEXEC)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>  
SETROPTS REFRESH GLOBAL(<class>)  
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **FSEEXEC** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS Security Server RACF Security Administrator's Guide: Restricting execute access in a zFS or TFS file system](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			

9.27 Ensure that data sets containing user file systems do not have the user ID as the high-level qualifier (Manual)

Profile Applicability:

- Level 1

Description:

A naming convention is generally established when allocating new zFS user file systems for a UNIX user to have as their home directory. If the high-level qualifier for this data set is the user's RACF user ID, then the user has read and write access to it outside of the UNIX environment where UNIX authorization checks are not made.

Rationale:

A user can set sensitive file attributes from the traditional MVS environment, and they will be honored within the UNIX environment. This can lead to full compromise of your system.

Audit:

Check the names of the zFS aggregates used for user file systems. The shell **df** command displays all file systems by path name and by zFS data set name.

Verify that the data sets in the **Filesystem** column containing user file systems do not have the user ID as the high-level qualifier.

Remediation:

Establish a plan by which to replace these file systems. Modify your provisioning steps (for example, your automount policy) to discontinue the user ID-based naming convention in the high-level qualifier.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

9.28 Ensure that daemons are running with z/OS UNIX level security (Automated)

Profile Applicability:

- Level 1

Description:

Running with z/OS UNIX level security ensures that system programmers with **UID(0)** cannot switch identity to any other z/OS UNIX user without authentication. This capability should be restricted to daemon user IDs with **READ** access to **BPX.DAEMON** in the **FACILITY** class.

Rationale:

In contrast, with UNIX level security, anyone with **UID(0)** or access to **BPX.SUPERUSER** in the **FACILITY** class can switch identity to any other z/OS UNIX user without authentication. This violates separation of duties and least privilege.

Impact:

Implementing z/OS UNIX level security requires daemons to be running in a clean address space. This requires additional setup and maintenance to identify programs that are allowed to execute in the daemon address space and define them to RACF program control.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **FACILITY** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **FACILITY** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering the **BPX.DAEMON** resource

Request reports generated using IRRDBU00 output that will allow you to:

Verify that a fully qualified **BPX.DAEMON** profile is defined in the **FACILITY** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher access is restricted to:
 - User IDs associated with daemons

Remediation:

To activate the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FACILITY)
```

To enable generic profile checking for the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FACILITY)
```

To RACLIST the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FACILITY)
```

To create a **BPX.DAEMON** profile use the RACF **RDEFINE** command:

```
RDEFINE FACILITY BPX.DAEMON +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    DATA('ACCESS TO UNIX DAEMON SYSTEM CALLS')  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** command:

```
RALTER FACILITY BPX.DAEMON +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    NOWARNING  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT BPX.DAEMON CLASS(FACILITY) +  
    DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **FACILITY** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS UNIX System Services Planning: BPX.DAEMON](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

9.29 Ensure that servers are running with z/OS UNIX level security (Automated)

Profile Applicability:

- Level 1

Description:

Running with z/OS UNIX level security ensures that system programmers with **UID(0)** cannot establish thread-level security under any other z/OS UNIX user without authentication. This capability is restricted to server user IDs with **READ** or **UPDATE** access to **BPX.SERVER** in the **FACILITY** class.

Rationale:

In contrast, with UNIX level security, anyone with **UID(0)** or access to **BPX.SUPERUSER** in the **FACILITY** class can establish thread-level security under any other z/OS UNIX user without authentication. This violates separation of duties and least privilege.

Impact:

Implementing z/OS UNIX level security requires servers to be running in a clean address space. This requires additional setup and maintenance to identify programs that are allowed to execute in the server address space and define them to RACF program control.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **FACILITY** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **FACILITY** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **FACILITY** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering the **BPX.SERVER** resource

Request reports generated using IRRDBU00 output that will allow you to:

Verify that a fully qualified **BPX.SERVER** profile is defined in the **FACILITY** class that:

- Has a **UACC** of **NONE**
- Is not in **WARNING** mode
- **AUDIT** a minimum of **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher access is restricted to:
 - User IDs associated with servers

Remediation:

To activate the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FACILITY)
```

To enable generic profile checking for the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FACILITY)
```

To RACLIST the **FACILITY** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FACILITY)
```

To create a **BPX.SERVER** profile use the RACF **RDEFINE** command:

```
RDEFINE FACILITY BPX.SERVER +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    DATA('ACCESS TO UNIX SERVER SYSTEM CALLS')  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** command:

```
RALTER FACILITY BPX.SERVER +  
    UACC(NONE) +  
    AUDIT(FAILURES(READ)) +  
    NOWARNING  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT BPX.SERVER CLASS(FACILITY) +  
    DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH RACLIST(FACILITY)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETROPTS REFRESH GLOBAL(<class>)
SETROPTS NOGLOBAL(<class>)
```

Default Value:

The **FACILITY** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS UNIX System Services Planning: Establishing the correct level of security for servers](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

9.30 Ensure that access to file systems containing critical data is controlled (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Critical data can be stored within zFS file systems. Access to files and directories is controlled by z/OS UNIX mechanisms such as **UID(0)**, file ownership, file permission and access control lists. Using profiles in the **FSACCESS** class, you can restrict the ability to cross a mount point into a zFS file system to only those explicitly permitted in the profile. This overrides even **UID(0)** authority. Once you have crossed the mount point, UNIX rules apply when accessing files and directories within that file system.

File systems containing critical data should be protected with an **FSACCESS** profile.

Rationale:

Access at the mount point level is controlled only by RACF security administrators. This provides a clear separation of duties in the event that you have **UID(0)** users. It also provides protection against overly permissive access rules in z/OS UNIX made outside the scope of control of the security administrator.

Impact:

Use of the **FSACCES** class can cause increased CPU usage in some environments.

Audit:

Issue the following TSO command:

```
SETROPTS LIST
```

Review the command output in the **ACTIVE CLASSES =** section.

Verify that **FSACCES** appears.

Review the command output in the **GENERIC PROFILE CLASSES =** section.

Verify that **FSACCES** appears.

Review the command output in the **SETR RACLIST CLASSES =** section.

Verify that **FSACCES** appears.

Request the following DSMON report:

```
FUNCTION SYSTEM RACGAC
```

Verify that the **FSACCES** entry has:

- **-- GLOBAL INACTIVE -- or -- NO ENTRIES --** or contains no entries covering file systems containing critical data

Request reports generated using IRRDBU00 output that will allow you to:

Verify that profiles covering file systems containing critical data are defined in the **FSACCES** class:

- Have a **UACC** of **NONE**
- Are not in **WARNING** mode
- **AUDIT** a minimum of **SUCCESS(READ)** and **FAILURES(READ)**
- **ID(*)** is not used to grant access
- **READ** and higher permits are restricted to:
 - IDs authorized to access these resources at this level

Remediation:

To activate the **FSACCES** class use the RACF **SETROPTS** command:

```
SETROPTS CLASSACT(FSACCES)
```

To enable generic profile checking for the **FSACCES** class use the RACF **SETROPTS** command:

```
SETROPTS GENERIC(FSACCES)
```

To RACLIST the **FSACCES** class use the RACF **SETROPTS** command:

```
SETROPTS RACLIST(FSACCES)
```

To create an **FSACCES** profile use the RACF **RDEFINE** and **PERMIT** commands:

```
RDEFINE FSACCES <dataset-mask> +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    DATA('CROSS A MOUNT POINT INTO ZFS FILE SYSTEM')  
  
PERMIT <dataset-mask> CLASS(FSACCES) +  
    ACCESS(READ) ID(<compliant>)
```

To modify the **UACC**, **WARN**, or **AUDIT** settings for a profile use the RACF **RALTER** command:

```
RALTER FSACCES <profile> +  
    UACC(NONE) +  
    AUDIT(ALL(READ)) +  
    NOWARNING  
  
SETROPTS REFRESH RACLIST(FSACCES)
```

To remove a non-compliant access list entries use the RACF **PERMIT** command:

```
PERMIT <profile> CLASS(FSACCES) +  
    DELETE ID(<non-compliant>)  
  
SETROPTS REFRESH RACLIST(FSACCES)
```

To remove a non-compliant GAC entry you need to use both RACF **RALTER** and **SETROPTS** commands:

```
RALTER GLOBAL <class> DELMEM(<entry>)  
SETROPTS REFRESH GLOBAL(<class>)
```

Note: Access gained via global access checking is not logged, so caution must be used when making changes to GAC entries.

To disable GAC for a class you will need to use both RACF **RDELETE** to remove the associated **GLOBAL** profile and RACF **SETROPTS** to fully disable GAC for the class:

```
RDELETE GLOBAL <class>
SETOPTS REFRESH GLOBAL(<class>)
SETOPTS NOGLOBAL(<class>)
```

Default Value:

The **FSACCES** class is **INACTIVE** when RACF is using a newly initialized database.

Additional Information:

[z/OS UNIX System Services Planning: Restricting access to a zFS file system](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

9.31 Ensure that file systems are mounted Read Only wherever possible (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Some zFS file systems contain data that is not expected to change. For example, a file system may be dedicated to containing the binary executables of a specific application. You generally do not expect this data to change until the next time you apply service.

Rationale:

Mounting a file system in read-only mode protects against accidental or malicious changes to the data within.

Audit:

Mounting a file system in read-only mode protects against accidental or malicious changes to the data within.

Audit Procedure

The UNIX shell command named **df** displays a list of the currently mounted file systems, by mount point (UNIX directory path) and data set name. Using the verbose option, yields additional information, including the mount mode.

Issue the following shell command:

```
df -v
```

The mount mode will be displayed as **Read Only** or **Read/Write**.

Verify that zFS file systems containing data that is not expected to change are mounted as **Read Only**.

Remediation:

For each **Read/Write**-mounted file system in which you don't expect data to change, plan to remount it in **Read Only** mode as application availability allows, and update the **BPXPRMxx** member of **SYS1.PARMLIB** to make the change effective at the next IPL.

Default Value:

There is no default **BPXPRMxx** parmlib member.

Additional Information:

[z/OS MVS Initialization and Tuning Reference: BPXPRMxx \(z/OS UNIX System Services parameters\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			

9.32 Ensure that file systems are mounted with set-id files disabled wherever possible (Manual)

Profile Applicability:

- Level 1

Description:

set-user-ID and **set-group-ID** files are those containing executables that run under the identity of the file owner rather than the person running the executable. These are often the target of attackers. On the other hand, some applications rely on these types of files to operate as expected. Any file system that is not expected to contain set-id files should be mounted in **NOSETUID** mode. In this mode, the **set-user-ID** and **set-group-ID** bits in the file mode are ignored.

Rationale:

Mounting a file system in **NOSETUID** mode reduces the attack surface of your zFS file systems.

Audit:

The UNIX shell command named **df** displays a list of the currently mounted file systems, by mount point (UNIX directory path) and data set name. Using the verbose option, yields additional information, including the mount mode.

Issue the following shell command:

```
df -v
```

The presence of the string **No SUID** indicates the file system is mounted with the **NOSETUID** option. If it is mounted with the default of **SETUID**, no option is displayed.

Verify that zFS file systems mounted with **SETUID** have a business justification.

Note: Examples of **SETUID** justification includes, but is not limited to:

- Being the root (/) filesystem.
- It is listed as a requirement by product documentation.

Remediation:

The shell **find** command can be used to search for occurrences of **set-user-ID** and **set-group-ID** files starting at the path name specified. For example, to see if any **set-id** files exist in the file system mounted on the **/usr/lpp/appx** directory:

```
find /usr/lpp/appx -type f \( -perm -4000 -o -perm -2000 \)
```

Note: The spaces within the parentheses are significant.

For each file system in which you don't expect set-id files to exist, plan to remount it with the **NOSETUID** option as application availability allows, and update the **BPXPRMxx** member of **SYS1.PARMLIB** to make the change effective at the next IPL.

Default Value:

SETUID

Additional Information:

[z/OS MVS Initialization and Tuning Reference: BPXPRMxx \(z/OS UNIX System Services parameters\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			

9.33 Ensure that no file systems are mounted with security disabled (Automated)

Profile Applicability:

- Level 1

Description:

If a file system is mounted with the **NOSECURITY** option, everyone has all access to every object in the file system. In a production environment, no file system should be mounted with this option.

Rationale:

Mounting a file system in **NOSECURITY** mode completely nullifies any access control established within it, opening the data for reading and writing to everyone.

Audit:

The UNIX shell command named **df** displays a list of the currently mounted file systems, by mount point (UNIX directory path) and data set name. Using the verbose option, yields additional information, including the mount mode.

Issue the following shell command:

```
df -v
```

The presence of the string **No Security** indicates the file system is mounted with the **NOSECURITY** option. If it is mounted with the default of **SECURITY**, no option is displayed.

Verify that zFS file systems are mounted with **SECURITY**.

Remediation:

For each file system mounted with the **NOSECURITY** option, plan to remount it without the **NOSECURITY** option as application availability allows and update the **BPXPRMxx** member of **SYS1.PARMLIB** to make the change effective at the next IPL.

Default Value:

SECURITY

Additional Information:

[z/OS MVS Initialization and Tuning Reference: BPXPRMxx \(z/OS UNIX System Services parameters\)](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	Identification and Authentication		
1.1	Password Control		
1.1.1	Ensure that the SETROPTS PASSWORD(INTERVAL and PHRASEINT) values are set to a maximum of 365 (Automated)	☐	☐
1.1.2	Ensure that the SETROPTS PASSWORD(HISTORY) value is set to a minimum of 5 (Automated)	☐	☐
1.1.3	Ensure that at least one SETROPTS PASSWORD(RULE) is defined with (LENGTH(8) MIXEDALL(1:8)) (Automated)	☐	☐
1.1.4	Ensure that the SETROPTS PASSWORD(MINCHANGE) value is set to a minimum of 1 (Automated)	☐	☐
1.1.5	Ensure that the SETROPTS PASSWORD(REVOKE) value is set to a maximum of 6 (Automated)	☐	☐
1.1.6	Ensure that the SETROPTS PASSWORD(ALGORITHM) value is set to KDFAES (Automated)	☐	☐
1.1.7	Ensure that the SETROPTS PASSWORD(WARNING) value is set to a minimum of 5 (Automated)	☐	☐
1.1.8	Ensure that the SETROPTS RVARYPW values are secured with KDFAES (Automated)	☐	☐
1.1.9	Ensure SETROPTS PASSWORD(MIXEDCASE) is in effect (Automated)	☐	☐
1.1.10	Ensure SETROPTS PASSWORD(SPECIALCHARS) is in effect (Automated)	☐	☐
1.2	System Settings		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.2.1	Ensure that the SETROPTS INACTIVE value is set to a maximum of 45 (Automated)	☐	☐
1.2.2	Ensure that the STARTED resource class is used to assign user IDs to started tasks (Automated)	☐	☐
1.2.3	Ensure user propagation is controlled (Automated)	☐	☐
1.2.4	Ensure that started tasks defined with the TRUSTED attribute are justified (Manual)	☐	☐
1.2.5	Ensure that the OPERCMDS resource class is enabled (Automated)	☐	☐
1.2.6	Ensure that the CONSOLE resource class is enabled (Automated)	☐	☐
1.2.7	Ensure that the FACILITY resource class is enabled (Automated)	☐	☐
1.2.8	Ensure that inapplicable PPT entries have been invalidated (Manual)	☐	☐
1.2.9	Ensure that LNKAUTH=APFTAB is specified in the IEASYSxx members currently active parmlib data sets (Automated)	☐	☐
1.2.10	Ensure that the CONSOLxx members are configured (Manual)	☐	☐
1.2.11	Ensure that no expired digital certificates are used (Automated)	☐	☐
1.2.12	Ensure that the SETROPTS RVARYPW are set to non-default values (Automated)	☐	☐
1.2.13	Ensure that RACF default user ID IBMUSER is disabled (Automated)	☐	☐
1.3	User Attributes		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.3.1	Ensure that the use of RACF SPECIAL attribute is justified (Manual)	☐	☐
1.3.2	Ensure that SYS1.UADS contains only recovery user IDs (Manual)	☐	☐
1.3.3	Ensure that MCS console user IDs are protected (Manual)	☐	☐
1.3.4	Ensure that STARTED resource class profiles assign PROTECTED user IDs (Automated)	☐	☐
1.3.5	Ensure that the assignment of RACF CLAUTH authority is justified (Automated)	☐	☐
2	Authorization and Access Control Management		
2.1	Data Protection		
2.1.1	Ensure that access to DASDVOL and STGADMIN resources are controlled (Automated)	☐	☐
2.1.2	Ensure that access to active SMF collection files is controlled (Automated)	☐	☐
2.1.3	Ensure that the SETROPTS WHEN(PROGRAM) value is active (Automated)	☐	☐
2.1.4	Ensure that access to the ICHDSM00 (DSMON) program is controlled (Automated)	☐	☐
2.1.5	Ensure that access to the IRRDPI00 program is controlled (Automated)	☐	☐
2.1.6	Ensure that the SETROPTS ERASE value is set to ALL (Automated)	☐	☐
2.1.7	Ensure that the TEMPDSN class is active (Automated)	☐	☐
2.1.8	Ensure that access to RACF database data sets is controlled (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.1.9	Ensure that access to the RACF remote sharing facility data sets is controlled (Automated)	☐	☐
2.1.10	Ensure that access to the RACF parameter library is controlled (Automated)	☐	☐
2.1.11	Ensure that RACF remote sharing connections use the TCP/IP protocol (Automated)	☐	☐
2.1.12	Ensure that access to memory and privileged program dumps is controlled (Automated)	☐	☐
2.1.13	Ensure that access to system TRACE data sets is controlled (Automated)	☐	☐
2.1.14	Ensure that access to system backup data sets is controlled (Automated)	☐	☐
2.1.15	Ensure that access to system DUMP data sets is controlled (Automated)	☐	☐
2.1.16	Ensure that access to SMF collection offload data sets is controlled (Automated)	☐	☐
2.2	Resource Protection		
2.2.1	Ensure that the access to update system dynamic lists is controlled (Automated)	☐	☐
2.2.2	Ensure that access to IEASYMUP resources is controlled (Manual)	☐	☐
2.2.3	Ensure that PASSWORD protection for data sets is not used (Manual)	☐	☐
2.2.4	Ensure that access to data sets in the PARMLIB concatenation is controlled (Automated)	☐	☐
2.2.5	Ensure that access to all LPA libraries is controlled (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.6	Ensure that access to system MASTER catalogs is controlled (Manual)	☐	☐
2.2.7	Ensure that access to all APF-authorized objects is controlled (Manual)	☐	☐
2.2.8	Ensure that access to the SYS1.SVCLIB data set is controlled (Automated)	☐	☐
2.2.9	Ensure that access to the SYS1.IMAGELIB data set is controlled (Manual)	☐	☐
2.2.10	Ensure that access to libraries that contain PPT modules is controlled (Automated)	☐	☐
2.2.11	Ensure that access to the SYS1.NUCLEUS data set is controlled (Automated)	☐	☐
2.2.12	Ensure that access to all system PROCLIB data sets is controlled (Automated)	☐	☐
2.2.13	Ensure that access to System REXX IRRPWREX exit is controlled (Automated)	☐	☐
2.2.14	Ensure that access to the SYS1.LINKLIB data set is controlled (Automated)	☐	☐
2.2.15	Ensure that access to all system-level product installation libraries is controlled (Automated)	☐	☐
2.2.16	Ensure that access to RACF resources in the FACILITY class is controlled (Automated)	☐	☐
2.2.17	Ensure that access to VTAMAPPL resources is controlled (Manual)	☐	☐
2.2.18	Ensure that access to IBM Health Checker resources is controlled (Automated)	☐	☐
2.3	System Settings		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.1	Ensure that the SETROPTS TERMINAL value is set to NONE (Automated)	☐	☐
2.3.2	Ensure that the SETROPTS GENERIC is enabled for ACTIVE classes (Automated)	☐	☐
2.3.3	Ensure that the SETROPTS PROTECTALL value is set to FAIL (Automated)	☐	☐
2.3.4	Ensure that ALTER access authority in DISCRETE profiles is limited (Automated)	☐	☐
2.3.5	Ensure that the ACEECHK resource class is enabled (Automated)	☐	☐
2.3.6	Ensure that SETROPTS ENHANCEDGENERICOWNER is in effect (Automated)	☐	☐
2.3.7	Ensure that SETROPTS NOADDCREATOR is in effect (Automated)	☐	☐
2.4	User Privilege		
2.4.1	Ensure that the assignment of the RACF OPERATIONS attribute is justified (Automated)	☐	☐
2.4.2	Ensure that access to TSOAUTH resources is controlled (Automated)	☐	☐
2.4.3	Ensure that access to SURROGAT resources is controlled (Automated)	☐	☐
2.4.4	Ensure that the assignment of the UNIX uid(0) is justified (Automated)	☐	☐
2.4.5	Ensure that started tasks defined with the PRIVILEGED attribute is justified (Automated)	☐	☐
2.4.6	Ensure that access to libraries containing EXIT modules is controlled (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.4.7	Ensure that access to LINKLIST libraries is controlled (Automated)	☐	☐
2.4.8	Ensure that access to the SYS1.UADS data set is controlled (Automated)	☐	☐
2.4.9	Ensure that access to system page data sets is controlled (Automated)	☐	☐
2.4.10	Ensure that MCS console access is controlled through profiles in the CONSOLE resource class (Manual)	☐	☐
2.4.11	Ensure that access to system USER catalogs is controlled (Automated)	☐	☐
2.4.12	Ensure that access to Libraries containing EXIT modules is controlled (Automated)	☐	☐
3	Logging and Auditing		
3.1	Ensure that SETROPTS CMDVIOL is in effect (Automated)	☐	☐
3.2	Ensure that SETROPTS SAUDIT is in effect (Automated)	☐	☐
3.3	Ensure that SETROPTS AUDIT is enabled for ACTIVE classes (Automated)	☐	☐
3.4	Ensure that SETROPTS OPERAUDIT is in effect (Automated)	☐	☐
3.5	Ensure that SETROPTS INITSTATS is in effect (Automated)	☐	☐
3.6	Ensure that the assignment of the RACF AUDITOR or ROAUDIT attribute is justified (Automated)	☐	☐
3.7	Ensure that effective SMF records collection options are set (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.8	Ensure that an automated process is in place to collect and retain SMF data (Manual)	☐	☐
3.9	Ensure that required SMF data record types are collected (Automated)	☐	☐
3.10	Ensure that RACF audit logs is reviewed on a regular basis (Manual)	☐	☐
3.11	Ensure regular audits of AC=1 modules in APF authorized libraries are conducted (Manual)	☐	☐
3.12	Ensure that only supported software is installed and active on the system (Manual)	☐	☐
3.13	Ensure all OS software on your system is supported (Manual)	☐	☐
3.14	Implement sensitive z/OS data set monitoring (Manual)	☐	☐
3.15	Ensure that SETROPTS REALDSN is in effect (Automated)	☐	☐
4	System Resilience		
4.1	Ensure that RACF database is backed up on a scheduled basis (Manual)	☐	☐
4.2	Ensure that the RACF PRIM and BACK databases are isolated (Manual)	☐	☐
4.3	Ensure sensitive data sets are encrypted with z/OS data set encryption (Manual)	☐	☐
4.4	Ensure that RACF application identity mapping (AIM) is at stage 3 (Manual)	☐	☐
4.5	Ensure that RACF ENQ names are not in the Global Resource Serialization (GRS) Resource Name List (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.6	Ensure that SETROPTS GRPLIST is in effect (Automated)	☐	☐
4.7	Ensure that SETROPTS NOSTATISTICS(*) is in effect (Automated)	☐	☐
4.8	Ensure that RACF is enabled for Sysplex communication (Automated)	☐	☐
4.9	Ensure that Validated Boot for z/OS is in effect (Manual)	☐	☐
4.10	Ensure that the site is registered to the IBM Z and IBM LinuxONE Security Portal (Manual)	☐	☐
5	Storage Management		
5.1	Ensure that DFSMS is configured (Manual)	☐	☐
5.2	Ensure that access to the Tape Bypass Label Processing (BLP) resource is controlled (Automated)	☐	☐
5.3	Ensure that SETROPTS ADSP is disabled (Automated)	☐	☐
5.4	Ensure that access to DFSMS control data sets is controlled (Automated)	☐	☐
6	Networking		
6.1	CSSMTP Recommendations		
6.1.1	Ensure CSSMTP started task user ID is PROTECTED (Automated)	☐	☐
6.1.2	Ensure that the STARTED resource class is used to assign user IDs to CSSMTP started tasks (Automated)	☐	☐
6.1.3	Ensure AT-TLS protection is enabled for CSSMTP (Manual)	☐	☐
6.1.4	Ensure that access to CSSMTP started task data sets is controlled (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.2	FTP Recommendations		
6.2.1	Ensure that the STARTED resource class is used to assign user IDs with proper parameters to FTP server started tasks (Automated)	☐	☐
6.2.2	Ensure startup parameters for the FTP daemon do not allow ANONYMOUS or INACTIVE keywords (Manual)	☐	☐
6.2.3	Ensure FTP.DATA configuration statements enforce secure configuration (Manual)	☐	☐
6.2.4	Ensure FTP.DATA configuration statements enforce AT-TLS protection (Manual)	☐	☐
6.2.5	Ensure user exits for the FTP server are not used without approval (Manual)	☐	☐
6.2.6	Ensure that access to the warning banner for the FTP server is controlled (Automated)	☐	☐
6.2.7	Ensure SMF recording options for the FTP Server are configured (Manual)	☐	☐
6.2.8	Ensure UNIX permission and user audit bits for FTP server are configured (Manual)	☐	☐
6.2.9	Ensure access to FTP server FTP.DATA data sets is controlled (Manual)	☐	☐
6.2.10	Ensure access to FTP control card data sets is controlled (Manual)	☐	☐
6.3	OpenSSH		
6.3.1	Ensure SSH daemon is configured to only use the SSHv2 protocol (Manual)	☐	☐
6.3.2	Ensure SSH daemon is configured to use FIPS 140-2 compliant cryptographic provider (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.3.3	Ensure SSH daemon is configured with a logon banner (Manual)	☐	☐
6.3.4	Ensure SSH daemon is configured for SMF logging (Manual)	☐	☐
6.3.5	Ensure SSH daemon is configured to use SAF keyrings for key storage (Manual)	☐	☐
6.4	Syslogd Recommendations		
6.4.1	Ensure syslog daemon is started at z/OS initialization (Manual)	☐	☐
6.4.2	Ensure that the STARTED resource class is used to assign user IDs with proper parameters to syslog daemon started tasks (Manual)	☐	☐
6.4.3	Ensure permission and user audit bits for syslog daemon component are configured (Manual)	☐	☐
6.4.4	Ensure that access to syslog daemon archive data sets is controlled (Manual)	☐	☐
6.5	TCP/IP Recommendations		
6.5.1	Ensure configuration files for the TCP/IP stack are explicitly specified (Manual)	☐	☐
6.5.2	Ensure TCP/IP stack configuration defined in TCPIP.DATA meets minimum requirements (Manual)	☐	☐
6.5.3	Ensure hosts identified by the NSINTERADDR statement are protected (Manual)	☐	☐
6.5.4	Ensure TCP/IP stack configuration defined in PROFILE.TCPIP meets minimum requirements (Manual)	☐	☐
6.5.5	Ensure permission and user audit bits for z/OS UNIX file system objects that are part of the base TCP/IP component are configured (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.5.6	Ensure access to TCP/IP SAF resources is controlled (Manual)	☐	☐
6.5.7	Ensure that the SERVAUTH resource class is enabled (Manual)	☐	☐
6.5.8	Ensure that the STARTED resource class is used to assign user IDs with proper parameters to base TCP/IP component started tasks (Manual)	☐	☐
6.5.9	Ensure access to data sets for the base TCP/IP component is controlled (Manual)	☐	☐
6.6	TN3270 Recommendations		
6.6.1	Ensure configuration statements for the TN3270E telnet server are configured (Manual)	☐	☐
6.6.2	Ensure VTAM session setup controls for the TN3270E telnet server are configured (Manual)	☐	☐
6.6.3	Ensure a warning banner for the TN3270 telnet server is configured (Manual)	☐	☐
6.6.4	Ensure AT-TLS protection is enabled for the TN3270 telnet server (Manual)	☐	☐
6.6.5	Ensure SMF recording options for the TN3270 telnet server are configured (Manual)	☐	☐
6.6.6	Ensure that access to the otelnetd and EZATNTLE programs is controlled (Manual)	☐	☐
6.7	VTAM Recommendations		
6.7.1	Ensure VTAM USSTAB definitions are being used for secured terminals (Manual)	☐	☐
6.7.2	Ensure that access to the system data sets used to support the VTAM network is controlled (Manual)	☐	☐
7	Cryptography and Encryption		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
7.1	ICSF Installation and Configuration		
7.1.1	Ensure that access to ICSF installation data sets is controlled (Manual)	☐	☐
7.1.2	Ensure that the STARTED resource class is used to assign user IDs with proper parameters to ICSF started tasks (Automated)	☐	☐
7.1.3	Ensure CSFINPV2 requires signature verification (Manual)	☐	☐
7.1.4	Ensure ICSF is configured to start during IPL (Manual)	☐	☐
7.1.5	Ensure that ICSF Master Keys are managed by a Trusted Key Entry (TKE) workstation (Manual)	☐	☐
7.2	ICSF Component Configuration		
7.2.1	Ensure crypto usage statistics are enabled (Manual)	☐	☐
7.2.2	Ensure crypto key lifecycle auditing is enabled (Manual)	☐	☐
7.2.3	Ensure crypto key usage auditing is enabled (Manual)	☐	☐
7.2.4	Ensure ICSF key data sets have a system backup (Manual)	☐	☐
7.2.5	Ensure ICSF master keys have a backup procedure (Manual)	☐	☐
7.2.6	Ensure all ICSF key data sets are in common record format (Manual)	☐	☐
7.2.7	Ensure all ICSF key data sets are enabled for sysplex sharing (Manual)	☐	☐
7.2.8	Ensure ICSF is running with FIPSMODE enabled (Manual)	☐	☐
7.2.9	Ensure CCA operational keys are created with WRAPENH3 key wrapping (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
7.3	ICSF Security Configuration		
7.3.1	Ensure that the CSFSERV class is active (Manual)	☐	☐
7.3.2	Ensure that the CSFKEYS class is active (Manual)	☐	☐
7.3.3	Ensure that the CRYPTOZ class is active (Manual)	☐	☐
7.3.4	Ensure that the XCSFKEY class is active (Manual)	☐	☐
7.3.5	Ensure ICSF key store policy controls are enabled (Manual)	☐	☐
7.3.6	Ensure access to ICSF key data sets is controlled (Manual)	☐	☐
7.3.7	Ensure access to ICSF administrative services is controlled (Manual)	☐	☐
7.3.8	Ensure access to ICSF operator commands is controlled (Manual)	☐	☐
8	Job Management JES2		
8.1	JES2 Commands		
8.1.1	Ensure that access to JES2 system commands is controlled (Manual)	☐	☐
8.2	JES2 SPOOL		
8.2.1	Ensure that the JESSPOOL resource class is enabled (Manual)	☐	☐
8.2.2	Ensure that access to JES2 spool resources is controlled (Manual)	☐	☐
8.2.3	Ensure that access to JES2 trace resources is controlled (Manual)	☐	☐
8.2.4	Ensure that access to JESNEWS resources is controlled (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
8.3	Job Level Protection		
8.3.1	Ensure that the JESJOBS resource class is configured (Manual)	☐	☐
8.3.2	Ensure that access to JESJOBS CANCEL resources is controlled (Manual)	☐	☐
8.3.3	Ensure that access to JESJOBS GROUPREG resources is controlled (Manual)	☐	☐
8.3.4	Ensure that access to JESJOBS HOLD resources is controlled (Manual)	☐	☐
8.3.5	Ensure that access to JESJOBS JOBCLASS resources is controlled (Manual)	☐	☐
8.3.6	Ensure that access to JESJOBS JOBNFY resources is controlled (Manual)	☐	☐
8.3.7	Ensure that access to JESJOBS MODIFY resources is controlled (Manual)	☐	☐
8.3.8	Ensure that access to JESJOBS PURGE resources is controlled (Manual)	☐	☐
8.3.9	Ensure that access to JESJOBS RELEASE resources is controlled (Manual)	☐	☐
8.3.10	Ensure that access to JESJOBS REROUTE resources is controlled (Manual)	☐	☐
8.3.11	Ensure that access to JESJOBS SPIN resources is controlled (Manual)	☐	☐
8.3.12	Ensure that access to JESJOBS SPOOLIO resources is controlled (Manual)	☐	☐
8.3.13	Ensure that access to JESJOBS START resources is controlled (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
8.3.14	Ensure that access to JESJOBS SUBMIT resources is controlled (Manual)	☐	☐
8.3.15	Ensure that access to JESJOBS RESTART resources is controlled (Manual)	☐	☐
8.4	Enable Encryption of Data Set on SPOOL		
8.4.1	Ensure that data sets on SPOOL are encrypted (Manual)	☐	☐
8.5	Control Access to Data Sets Used by JES2		
8.5.1	Ensure that access to the data sets used by JES2 is controlled (Automated)	☐	☐
8.5.2	Ensure that RACF is called for data sets opened by JES2 (Manual)	☐	☐
8.6	Device Management		
8.6.1	Ensure that access to JES2 output devices is controlled (Manual)	☐	☐
8.6.2	Ensure that bypass label processing is not set on any JOBCLASS (Manual)	☐	☐
8.6.3	Ensure that access to JES2 input sources is controlled (Manual)	☐	☐
8.7	JES2 Networking		
8.7.1	Ensure that RJE workstations and NJE nodes enforce password protection (Manual)	☐	☐
8.7.2	Ensure that RJE workstations have paired user IDs (Manual)	☐	☐
8.8	Require User Identification		
8.8.1	Ensure that the SETROPTS JES(BATCHALLRACF) is enabled (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
8.8.2	Ensure that the SETROPTS JES(XBMALLRACF) is enabled (Automated)	☐	☐
9	UNIX System Services		
9.1	Ensure that access to z/OS UNIX SURROGAT resources is controlled (Automated)	☐	☐
9.2	Ensure that access to superuser resources in the UNIXPRIV class is controlled (Automated)	☐	☐
9.3	Ensure that general users are not allowed to change their file ownership (Automated)	☐	☐
9.4	Ensure that RESTRICTED users cannot access UNIX files to which they are not explicitly permitted (Automated)	☐	☐
9.5	Ensure that newly assigned UID and GID are unique values (Automated)	☐	☐
9.6	Ensure that z/OS UNIX user accounts are defined with compliant values (Automated)	☐	☐
9.7	Ensure that RACF Classes required to secure the z/OS UNIX environment are active (Automated)	☐	☐
9.8	Ensure that RACF Classes required to secure the z/OS UNIX environment are RACLISTed (Automated)	☐	☐
9.9	Ensure that the user account for the z/OS UNIX kernel is defined with compliant attributes (Automated)	☐	☐
9.10	Ensure that z/OS UNIX automount configuration files are configured with compliant values (Automated)	☐	☐
9.11	Ensure that entries in /etc/inetd.conf are active and secure (Automated)	☐	☐
9.12	Ensure that z/OS UNIX OMVS parameters in IEASYSxx are configured (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
9.13	Ensure that z/OS UNIX BPXPRMxx parameters in PARMLIB are configured for security (Automated)	☐	☐
9.14	Ensure that z/OS UNIX permission bits and audit bits are configured to audit sensitive file access (Automated)	☐	☐
9.15	Ensure that access to BPX resources in the FACILITY class is controlled (Automated)	☐	☐
9.16	Ensure that security parameters in /etc/profile are configured (Automated)	☐	☐
9.17	Ensure that security commands in /etc/rc are safe (Automated)	☐	☐
9.18	Ensure that the BPXROOT user account is configured with compliant values (Manual)	☐	☐
9.19	Ensure that each RACF group for UNIX is defined with a unique GID (Automated)	☐	☐
9.20	Ensure that access to data sets used as step libraries in /etc/steplib is controlled (Automated)	☐	☐
9.21	Ensure that ability to switch into superuser mode is controlled (Automated)	☐	☐
9.22	Ensure access to zFS data sets is controlled (Automated)	☐	☐
9.23	Ensure USS Telnet server is not active (Automated)	☐	☐
9.24	Ensure rlogin is not active (Manual)	☐	☐
9.25	Ensure that the FSSEC resource class is enabled (Manual)	☐	☐
9.26	Ensure that programs cannot execute from the /tmp directory (Automated)	☐	☐
9.27	Ensure that data sets containing user file systems do not have the user ID as the high-level qualifier (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
9.28	Ensure that daemons are running with z/OS UNIX level security (Automated)	☐	☐
9.29	Ensure that servers are running with z/OS UNIX level security (Automated)	☐	☐
9.30	Ensure that access to file systems containing critical data is controlled (Manual)	☐	☐
9.31	Ensure that file systems are mounted Read Only wherever possible (Manual)	☐	☐
9.32	Ensure that file systems are mounted with set-id files disabled wherever possible (Manual)	☐	☐
9.33	Ensure that no file systems are mounted with security disabled (Automated)	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	Ensure that the SETROPTS PASSWORD(INTERVAL and PHRASEINT) values are set to a maximum of 365	☐	☐
1.1.2	Ensure that the SETROPTS PASSWORD(HISTORY) value is set to a minimum of 5	☐	☐
1.1.3	Ensure that at least one SETROPTS PASSWORD(RULE) is defined with (LENGTH(8) MIXEDALL(1:8))	☐	☐
1.1.4	Ensure that the SETROPTS PASSWORD(MINCHANGE) value is set to a minimum of 1	☐	☐
1.1.5	Ensure that the SETROPTS PASSWORD(REVOKE) value is set to a maximum of 6	☐	☐
1.1.7	Ensure that the SETROPTS PASSWORD(WARNING) value is set to a minimum of 5	☐	☐
1.1.9	Ensure SETROPTS PASSWORD(MIXEDCASE) is in effect	☐	☐
1.1.10	Ensure SETROPTS PASSWORD(SPECIALCHARS) is in effect	☐	☐
1.2.1	Ensure that the SETROPTS INACTIVE value is set to a maximum of 45	☐	☐
1.2.2	Ensure that the STARTED resource class is used to assign user IDs to started tasks	☐	☐
1.2.3	Ensure user propagation is controlled	☐	☐
1.2.4	Ensure that started tasks defined with the TRUSTED attribute are justified	☐	☐
1.2.5	Ensure that the OPERCMDS resource class is enabled	☐	☐
1.2.6	Ensure that the CONSOLE resource class is enabled	☐	☐
1.2.7	Ensure that the FACILITY resource class is enabled	☐	☐
1.2.9	Ensure that LNKAUTH=APFTAB is specified in the IEASYSxx members currently active parmlib data sets	☐	☐
1.2.10	Ensure that the CONSOLxx members are configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.2.11	Ensure that no expired digital certificates are used	☐	☐
1.2.12	Ensure that the SETROPTS RVARYPW are set to non-default values	☐	☐
1.2.13	Ensure that RACF default user ID IBMUSER is disabled	☐	☐
1.3.1	Ensure that the use of RACF SPECIAL attribute is justified	☐	☐
1.3.2	Ensure that SYS1.UADS contains only recovery user IDs	☐	☐
1.3.3	Ensure that MCS console user IDs are protected	☐	☐
1.3.4	Ensure that STARTED resource class profiles assign PROTECTED user IDs	☐	☐
1.3.5	Ensure that the assignment of RACF CLAUTH authority is justified	☐	☐
2.1.1	Ensure that access to DASDVOL and STGADMIN resources are controlled	☐	☐
2.1.2	Ensure that access to active SMF collection files is controlled	☐	☐
2.1.3	Ensure that the SETROPTS WHEN(PROGRAM) value is active	☐	☐
2.1.4	Ensure that access to the ICHDSM00 (DSMON) program is controlled	☐	☐
2.1.5	Ensure that access to the IRRDPI00 program is controlled	☐	☐
2.1.6	Ensure that the SETROPTS ERASE value is set to ALL	☐	☐
2.1.7	Ensure that the TEMPDSN class is active	☐	☐
2.1.8	Ensure that access to RACF database data sets is controlled	☐	☐
2.1.9	Ensure that access to the RACF remote sharing facility data sets is controlled	☐	☐
2.1.10	Ensure that access to the RACF parameter library is controlled	☐	☐
2.1.12	Ensure that access to memory and privileged program dumps is controlled	☐	☐
2.1.13	Ensure that access to system TRACE data sets is controlled	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.1.14	Ensure that access to system backup data sets is controlled	☐	☐
2.1.15	Ensure that access to system DUMP data sets is controlled	☐	☐
2.1.16	Ensure that access to SMF collection offload data sets is controlled	☐	☐
2.2.1	Ensure that the access to update system dynamic lists is controlled	☐	☐
2.2.2	Ensure that access to IEASYMUP resources is controlled	☐	☐
2.2.3	Ensure that PASSWORD protection for data sets is not used	☐	☐
2.2.4	Ensure that access to data sets in the PARMLIB concatenation is controlled	☐	☐
2.2.5	Ensure that access to all LPA libraries is controlled	☐	☐
2.2.6	Ensure that access to system MASTER catalogs is controlled	☐	☐
2.2.7	Ensure that access to all APF-authorized objects is controlled	☐	☐
2.2.8	Ensure that access to the SYS1.SVCLIB data set is controlled	☐	☐
2.2.9	Ensure that access to the SYS1.IMAGELIB data set is controlled	☐	☐
2.2.10	Ensure that access to libraries that contain PPT modules is controlled	☐	☐
2.2.11	Ensure that access to the SYS1.NUCLEUS data set is controlled	☐	☐
2.2.12	Ensure that access to all system PROCLIB data sets is controlled	☐	☐
2.2.13	Ensure that access to System REXX IRRPWREX exit is controlled	☐	☐
2.2.14	Ensure that access to the SYS1.LINKLIB data set is controlled	☐	☐
2.2.15	Ensure that access to all system-level product installation libraries is controlled	☐	☐
2.2.16	Ensure that access to RACF resources in the FACILITY class is controlled	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.2.17	Ensure that access to VTAMAPPL resources is controlled	☐	☐
2.2.18	Ensure that access to IBM Health Checker resources is controlled	☐	☐
2.3.1	Ensure that the SETROPTS TERMINAL value is set to NONE	☐	☐
2.3.2	Ensure that the SETROPTS GENERIC is enabled for ACTIVE classes	☐	☐
2.3.3	Ensure that the SETROPTS PROTECTALL value is set to FAIL	☐	☐
2.3.4	Ensure that ALTER access authority in DISCRETE profiles is limited	☐	☐
2.3.6	Ensure that SETROPTS ENHANCEDGENERICOWNER is in effect	☐	☐
2.3.7	Ensure that SETROPTS NOADDCREATOR is in effect	☐	☐
2.4.1	Ensure that the assignment of the RACF OPERATIONS attribute is justified	☐	☐
2.4.2	Ensure that access to TSOAUTH resources is controlled	☐	☐
2.4.3	Ensure that access to SURROGAT resources is controlled	☐	☐
2.4.4	Ensure that the assignment of the UNIX uid(0) is justified	☐	☐
2.4.5	Ensure that started tasks defined with the PRIVILEGED attribute is justified	☐	☐
2.4.6	Ensure that access to libraries containing EXIT modules is controlled	☐	☐
2.4.7	Ensure that access to LINKLIST libraries is controlled	☐	☐
2.4.8	Ensure that access to the SYS1.UADS data set is controlled	☐	☐
2.4.9	Ensure that access to system page data sets is controlled	☐	☐
2.4.10	Ensure that MCS console access is controlled through profiles in the CONSOLE resource class	☐	☐
2.4.11	Ensure that access to system USER catalogs is controlled	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.4.12	Ensure that access to Libraries containing EXIT modules is controlled	☐	☐
3.1	Ensure that SETROPTS CMDVIOL is in effect	☐	☐
3.2	Ensure that SETROPTS SAUDIT is in effect	☐	☐
3.3	Ensure that SETROPTS AUDIT is enabled for ACTIVE classes	☐	☐
3.4	Ensure that SETROPTS OPERAUDIT is in effect	☐	☐
3.5	Ensure that SETROPTS INITSTATS is in effect	☐	☐
3.6	Ensure that the assignment of the RACF AUDITOR or ROAUDIT attribute is justified	☐	☐
3.7	Ensure that effective SMF records collection options are set	☐	☐
3.8	Ensure that an automated process is in place to collect and retain SMF data	☐	☐
3.9	Ensure that required SMF data record types are collected	☐	☐
3.10	Ensure that RACF audit logs is reviewed on a regular basis	☐	☐
3.11	Ensure regular audits of AC=1 modules in APF authorized libraries are conducted	☐	☐
3.12	Ensure that only supported software is installed and active on the system	☐	☐
3.13	Ensure all OS software on your system is supported	☐	☐
3.14	Implement sensitive z/OS data set monitoring	☐	☐
4.1	Ensure that RACF database is backed up on a scheduled basis	☐	☐
4.2	Ensure that the RACF PRIM and BACK databases are isolated	☐	☐
4.10	Ensure that the site is registered to the IBM Z and IBM LinuxONE Security Portal	☐	☐
5.1	Ensure that DFSMS is configured	☐	☐
5.2	Ensure that access to the Tape Bypass Label Processing (BLP) resource is controlled	☐	☐
5.3	Ensure that SETROPTS ADSP is disabled	☐	☐
5.4	Ensure that access to DFSMS control data sets is controlled	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.1.1	Ensure CSSMTP started task user ID is PROTECTED	☐	☐
6.1.2	Ensure that the STARTED resource class is used to assign user IDs to CSSMTP started tasks	☐	☐
6.1.4	Ensure that access to CSSMTP started task data sets is controlled	☐	☐
6.2.1	Ensure that the STARTED resource class is used to assign user IDs with proper parameters to FTP server started tasks	☐	☐
6.2.2	Ensure startup parameters for the FTP daemon do not allow ANONYMOUS or INACTIVE keywords	☐	☐
6.2.3	Ensure FTP.DATA configuration statements enforce secure configuration	☐	☐
6.2.6	Ensure that access to the warning banner for the FTP server is controlled	☐	☐
6.2.7	Ensure SMF recording options for the FTP Server are configured	☐	☐
6.2.8	Ensure UNIX permission and user audit bits for FTP server are configured	☐	☐
6.2.9	Ensure access to FTP server FTP.DATA data sets is controlled	☐	☐
6.2.10	Ensure access to FTP control card data sets is controlled	☐	☐
6.3.3	Ensure SSH daemon is configured with a logon banner	☐	☐
6.3.4	Ensure SSH daemon is configured for SMF logging	☐	☐
6.4.1	Ensure syslog daemon is started at z/OS initialization	☐	☐
6.4.2	Ensure that the STARTED resource class is used to assign user IDs with proper parameters to syslog daemon started tasks	☐	☐
6.4.3	Ensure permission and user audit bits for syslog daemon component are configured	☐	☐
6.4.4	Ensure that access to syslog daemon archive data sets is controlled	☐	☐
6.5.1	Ensure configuration files for the TCP/IP stack are explicitly specified	☐	☐
6.5.2	Ensure TCP/IP stack configuration defined in TCPIP.DATA meets minimum requirements	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.5.3	Ensure hosts identified by the NSINTERADDR statement are protected	☐	☐
6.5.4	Ensure TCP/IP stack configuration defined in PROFILE.TCPIP meets minimum requirements	☐	☐
6.5.5	Ensure permission and user audit bits for z/OS UNIX file system objects that are part of the base TCP/IP component are configured	☐	☐
6.5.6	Ensure access to TCP/IP SAF resources is controlled	☐	☐
6.5.7	Ensure that the SERVAUTH resource class is enabled	☐	☐
6.5.8	Ensure that the STARTED resource class is used to assign user IDs with proper parameters to base TCP/IP component started tasks	☐	☐
6.5.9	Ensure access to data sets for the base TCP/IP component is controlled	☐	☐
6.6.1	Ensure configuration statements for the TN3270E telnet server are configured	☐	☐
6.6.2	Ensure VTAM session setup controls for the TN3270E telnet server are configured	☐	☐
6.6.3	Ensure a warning banner for the TN3270 telnet server is configured	☐	☐
6.6.5	Ensure SMF recording options for the TN3270 telnet server are configured	☐	☐
6.7.1	Ensure VTAM USSTAB definitions are being used for secured terminals	☐	☐
6.7.2	Ensure that access to the system data sets used to support the VTAM network is controlled	☐	☐
7.1.1	Ensure that access to ICSF installation data sets is controlled	☐	☐
7.1.2	Ensure that the STARTED resource class is used to assign user IDs with proper parameters to ICSF started tasks	☐	☐
7.1.3	Ensure CSFINPV2 requires signature verification	☐	☐
7.1.4	Ensure ICSF is configured to start during IPL	☐	☐
7.1.5	Ensure that ICSF Master Keys are managed by a Trusted Key Entry (TKE) workstation	☐	☐
7.2.1	Ensure crypto usage statistics are enabled	☐	☐

Recommendation		Set Correctly	
		Yes	No
7.2.4	Ensure ICSF key data sets have a system backup	☐	☐
7.2.5	Ensure ICSF master keys have a backup procedure	☐	☐
7.2.6	Ensure all ICSF key data sets are in common record format	☐	☐
7.2.7	Ensure all ICSF key data sets are enabled for sysplex sharing	☐	☐
7.3.1	Ensure that the CSFSERV class is active	☐	☐
7.3.2	Ensure that the CSFKEYS class is active	☐	☐
7.3.3	Ensure that the CRYPTOZ class is active	☐	☐
7.3.4	Ensure that the XCSFKEY class is active	☐	☐
7.3.5	Ensure ICSF key store policy controls are enabled	☐	☐
7.3.6	Ensure access to ICSF key data sets is controlled	☐	☐
7.3.7	Ensure access to ICSF administrative services is controlled	☐	☐
7.3.8	Ensure access to ICSF operator commands is controlled	☐	☐
8.1.1	Ensure that access to JES2 system commands is controlled	☐	☐
8.2.1	Ensure that the JESSPOOL resource class is enabled	☐	☐
8.2.2	Ensure that access to JES2 spool resources is controlled	☐	☐
8.2.3	Ensure that access to JES2 trace resources is controlled	☐	☐
8.2.4	Ensure that access to JESNEWS resources is controlled	☐	☐
8.3.1	Ensure that the JESJOBS resource class is configured	☐	☐
8.3.2	Ensure that access to JESJOBS CANCEL resources is controlled	☐	☐
8.3.3	Ensure that access to JESJOBS GROUPREG resources is controlled	☐	☐
8.3.4	Ensure that access to JESJOBS HOLD resources is controlled	☐	☐
8.3.5	Ensure that access to JESJOBS JOBCLASS resources is controlled	☐	☐
8.3.6	Ensure that access to JESJOBS JOBNFY resources is controlled	☐	☐
8.3.7	Ensure that access to JESJOBS MODIFY resources is controlled	☐	☐

Recommendation		Set Correctly	
		Yes	No
8.3.8	Ensure that access to JESJOBS PURGE resources is controlled	☐	☐
8.3.9	Ensure that access to JESJOBS RELEASE resources is controlled	☐	☐
8.3.10	Ensure that access to JESJOBS REROUTE resources is controlled	☐	☐
8.3.11	Ensure that access to JESJOBS SPIN resources is controlled	☐	☐
8.3.12	Ensure that access to JESJOBS SPOOLIO resources is controlled	☐	☐
8.3.13	Ensure that access to JESJOBS START resources is controlled	☐	☐
8.3.14	Ensure that access to JESJOBS SUBMIT resources is controlled	☐	☐
8.3.15	Ensure that access to JESJOBS RESTART resources is controlled	☐	☐
8.5.1	Ensure that access to the data sets used by JES2 is controlled	☐	☐
8.5.2	Ensure that RACF is called for data sets opened by JES2	☐	☐
8.6.1	Ensure that access to JES2 output devices is controlled	☐	☐
8.6.2	Ensure that bypass label processing is not set on any JOBCLASS	☐	☐
8.6.3	Ensure that access to JES2 input sources is controlled	☐	☐
8.7.1	Ensure that RJE workstations and NJE nodes enforce password protection	☐	☐
8.8.1	Ensure that the SETROPTS JES(BATCHALLRACF) is enabled	☐	☐
8.8.2	Ensure that the SETROPTS JES(XBMALLRACF) is enabled	☐	☐
9.1	Ensure that access to z/OS UNIX SURROGAT resources is controlled	☐	☐
9.2	Ensure that access to superuser resources in the UNIXPRIV class is controlled	☐	☐
9.3	Ensure that general users are not allowed to change their file ownership	☐	☐

Recommendation		Set Correctly	
		Yes	No
9.4	Ensure that RESTRICTED users cannot access UNIX files to which they are not explicitly permitted	☐	☐
9.5	Ensure that newly assigned UID and GID are unique values	☐	☐
9.6	Ensure that z/OS UNIX user accounts are defined with compliant values	☐	☐
9.7	Ensure that RACF Classes required to secure the z/OS UNIX environment are active	☐	☐
9.8	Ensure that RACF Classes required to secure the z/OS UNIX environment are RACLISTed	☐	☐
9.9	Ensure that the user account for the z/OS UNIX kernel is defined with compliant attributes	☐	☐
9.10	Ensure that z/OS UNIX automount configuration files are configured with compliant values	☐	☐
9.12	Ensure that z/OS UNIX OMVS parameters in IEASYSxx are configured	☐	☐
9.13	Ensure that z/OS UNIX BPXPRMxx parameters in PARMLIB are configured for security	☐	☐
9.14	Ensure that z/OS UNIX permission bits and audit bits are configured to audit sensitive file access	☐	☐
9.15	Ensure that access to BPX resources in the FACILITY class is controlled	☐	☐
9.16	Ensure that security parameters in /etc/profile are configured	☐	☐
9.17	Ensure that security commands in /etc/rc are safe	☐	☐
9.19	Ensure that each RACF group for UNIX is defined with a unique GID	☐	☐
9.20	Ensure that access to data sets used as step libraries in /etc/steplib is controlled	☐	☐
9.21	Ensure that ability to switch into superuser mode is controlled	☐	☐
9.22	Ensure access to zFS data sets is controlled	☐	☐
9.25	Ensure that the FSSEC resource class is enabled	☐	☐
9.26	Ensure that programs cannot execute from the /tmp directory	☐	☐

Recommendation		Set Correctly	
		Yes	No
9.27	Ensure that data sets containing user file systems do not have the user ID as the high-level qualifier	☐	☐
9.28	Ensure that daemons are running with z/OS UNIX level security	☐	☐
9.29	Ensure that servers are running with z/OS UNIX level security	☐	☐
9.30	Ensure that access to file systems containing critical data is controlled	☐	☐
9.31	Ensure that file systems are mounted Read Only wherever possible	☐	☐
9.32	Ensure that file systems are mounted with set-id files disabled wherever possible	☐	☐
9.33	Ensure that no file systems are mounted with security disabled	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	Ensure that the SETROPTS PASSWORD(INTERVAL and PHRASEINT) values are set to a maximum of 365	☐	☐
1.1.2	Ensure that the SETROPTS PASSWORD(HISTORY) value is set to a minimum of 5	☐	☐
1.1.3	Ensure that at least one SETROPTS PASSWORD(RULE) is defined with (LENGTH(8) MIXEDALL(1:8))	☐	☐
1.1.4	Ensure that the SETROPTS PASSWORD(MINCHANGE) value is set to a minimum of 1	☐	☐
1.1.5	Ensure that the SETROPTS PASSWORD(REVOKE) value is set to a maximum of 6	☐	☐
1.1.6	Ensure that the SETROPTS PASSWORD(ALGORITHM) value is set to KDFAES	☐	☐
1.1.7	Ensure that the SETROPTS PASSWORD(WARNING) value is set to a minimum of 5	☐	☐
1.1.8	Ensure that the SETROPTS RVARYPW values are secured with KDFAES	☐	☐
1.1.9	Ensure SETROPTS PASSWORD(MIXEDCASE) is in effect	☐	☐
1.1.10	Ensure SETROPTS PASSWORD(SPECIALCHARS) is in effect	☐	☐
1.2.1	Ensure that the SETROPTS INACTIVE value is set to a maximum of 45	☐	☐
1.2.2	Ensure that the STARTED resource class is used to assign user IDs to started tasks	☐	☐
1.2.3	Ensure user propagation is controlled	☐	☐
1.2.4	Ensure that started tasks defined with the TRUSTED attribute are justified	☐	☐
1.2.5	Ensure that the OPERCMDS resource class is enabled	☐	☐
1.2.6	Ensure that the CONSOLE resource class is enabled	☐	☐
1.2.7	Ensure that the FACILITY resource class is enabled	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.2.8	Ensure that inapplicable PPT entries have been invalidated	☐	☐
1.2.9	Ensure that LNKAUTH=APFTAB is specified in the IEASYSxx members currently active parmlib data sets	☐	☐
1.2.10	Ensure that the CONSOLxx members are configured	☐	☐
1.2.11	Ensure that no expired digital certificates are used	☐	☐
1.2.12	Ensure that the SETROPTS RVARYPW are set to non-default values	☐	☐
1.2.13	Ensure that RACF default user ID IBMUSER is disabled	☐	☐
1.3.1	Ensure that the use of RACF SPECIAL attribute is justified	☐	☐
1.3.2	Ensure that SYS1.UADS contains only recovery user IDs	☐	☐
1.3.3	Ensure that MCS console user IDs are protected	☐	☐
1.3.4	Ensure that STARTED resource class profiles assign PROTECTED user IDs	☐	☐
1.3.5	Ensure that the assignment of RACF CLAUTH authority is justified	☐	☐
2.1.1	Ensure that access to DASDVOL and STGADMIN resources are controlled	☐	☐
2.1.2	Ensure that access to active SMF collection files is controlled	☐	☐
2.1.3	Ensure that the SETROPTS WHEN(PROGRAM) value is active	☐	☐
2.1.4	Ensure that access to the ICHDSM00 (DSMON) program is controlled	☐	☐
2.1.5	Ensure that access to the IRRDPI00 program is controlled	☐	☐
2.1.6	Ensure that the SETROPTS ERASE value is set to ALL	☐	☐
2.1.7	Ensure that the TEMPDSN class is active	☐	☐
2.1.8	Ensure that access to RACF database data sets is controlled	☐	☐
2.1.9	Ensure that access to the RACF remote sharing facility data sets is controlled	☐	☐
2.1.10	Ensure that access to the RACF parameter library is controlled	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.1.11	Ensure that RACF remote sharing connections use the TCP/IP protocol	☐	☐
2.1.12	Ensure that access to memory and privileged program dumps is controlled	☐	☐
2.1.13	Ensure that access to system TRACE data sets is controlled	☐	☐
2.1.14	Ensure that access to system backup data sets is controlled	☐	☐
2.1.15	Ensure that access to system DUMP data sets is controlled	☐	☐
2.1.16	Ensure that access to SMF collection offload data sets is controlled	☐	☐
2.2.1	Ensure that the access to update system dynamic lists is controlled	☐	☐
2.2.2	Ensure that access to IEASYMUP resources is controlled	☐	☐
2.2.3	Ensure that PASSWORD protection for data sets is not used	☐	☐
2.2.4	Ensure that access to data sets in the PARMLIB concatenation is controlled	☐	☐
2.2.5	Ensure that access to all LPA libraries is controlled	☐	☐
2.2.6	Ensure that access to system MASTER catalogs is controlled	☐	☐
2.2.7	Ensure that access to all APF-authorized objects is controlled	☐	☐
2.2.8	Ensure that access to the SYS1.SVCLIB data set is controlled	☐	☐
2.2.9	Ensure that access to the SYS1.IMAGELIB data set is controlled	☐	☐
2.2.10	Ensure that access to libraries that contain PPT modules is controlled	☐	☐
2.2.11	Ensure that access to the SYS1.NUCLEUS data set is controlled	☐	☐
2.2.12	Ensure that access to all system PROCLIB data sets is controlled	☐	☐
2.2.13	Ensure that access to System REXX IRRPWREX exit is controlled	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.2.14	Ensure that access to the SYS1.LINKLIB data set is controlled	☐	☐
2.2.15	Ensure that access to all system-level product installation libraries is controlled	☐	☐
2.2.16	Ensure that access to RACF resources in the FACILITY class is controlled	☐	☐
2.2.17	Ensure that access to VTAMAPPL resources is controlled	☐	☐
2.2.18	Ensure that access to IBM Health Checker resources is controlled	☐	☐
2.3.1	Ensure that the SETROPTS TERMINAL value is set to NONE	☐	☐
2.3.2	Ensure that the SETROPTS GENERIC is enabled for ACTIVE classes	☐	☐
2.3.3	Ensure that the SETROPTS PROTECTALL value is set to FAIL	☐	☐
2.3.4	Ensure that ALTER access authority in DISCRETE profiles is limited	☐	☐
2.3.5	Ensure that the ACEECHK resource class is enabled	☐	☐
2.3.6	Ensure that SETROPTS ENHANCEDGENERICOWNER is in effect	☐	☐
2.3.7	Ensure that SETROPTS NOADDCREATOR is in effect	☐	☐
2.4.1	Ensure that the assignment of the RACF OPERATIONS attribute is justified	☐	☐
2.4.2	Ensure that access to TSOAUTH resources is controlled	☐	☐
2.4.3	Ensure that access to SURROGAT resources is controlled	☐	☐
2.4.4	Ensure that the assignment of the UNIX uid(0) is justified	☐	☐
2.4.5	Ensure that started tasks defined with the PRIVILEGED attribute is justified	☐	☐
2.4.6	Ensure that access to libraries containing EXIT modules is controlled	☐	☐
2.4.7	Ensure that access to LINKLIST libraries is controlled	☐	☐
2.4.8	Ensure that access to the SYS1.UADS data set is controlled	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.4.9	Ensure that access to system page data sets is controlled	☐	☐
2.4.10	Ensure that MCS console access is controlled through profiles in the CONSOLE resource class	☐	☐
2.4.11	Ensure that access to system USER catalogs is controlled	☐	☐
2.4.12	Ensure that access to Libraries containing EXIT modules is controlled	☐	☐
3.1	Ensure that SETROPTS CMDVIOL is in effect	☐	☐
3.2	Ensure that SETROPTS SAUDIT is in effect	☐	☐
3.3	Ensure that SETROPTS AUDIT is enabled for ACTIVE classes	☐	☐
3.4	Ensure that SETROPTS OPERAUDIT is in effect	☐	☐
3.5	Ensure that SETROPTS INITSTATS is in effect	☐	☐
3.6	Ensure that the assignment of the RACF AUDITOR or ROAUDIT attribute is justified	☐	☐
3.7	Ensure that effective SMF records collection options are set	☐	☐
3.8	Ensure that an automated process is in place to collect and retain SMF data	☐	☐
3.9	Ensure that required SMF data record types are collected	☐	☐
3.10	Ensure that RACF audit logs is reviewed on a regular basis	☐	☐
3.11	Ensure regular audits of AC=1 modules in APF authorized libraries are conducted	☐	☐
3.12	Ensure that only supported software is installed and active on the system	☐	☐
3.13	Ensure all OS software on your system is supported	☐	☐
3.14	Implement sensitive z/OS data set monitoring	☐	☐
3.15	Ensure that SETROPTS REALDSN is in effect	☐	☐
4.1	Ensure that RACF database is backed up on a scheduled basis	☐	☐
4.2	Ensure that the RACF PRIM and BACK databases are isolated	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.3	Ensure sensitive data sets are encrypted with z/OS data set encryption	☐	☐
4.4	Ensure that RACF application identity mapping (AIM) is at stage 3	☐	☐
4.5	Ensure that RACF ENQ names are not in the Global Resource Serialization (GRS) Resource Name List	☐	☐
4.6	Ensure that SETROPTS GRPLIST is in effect	☐	☐
4.7	Ensure that SETROPTS NOSTATISTICS(*) is in effect	☐	☐
4.8	Ensure that RACF is enabled for Sysplex communication	☐	☐
4.9	Ensure that Validated Boot for z/OS is in effect	☐	☐
4.10	Ensure that the site is registered to the IBM Z and IBM LinuxONE Security Portal	☐	☐
5.1	Ensure that DFSMS is configured	☐	☐
5.2	Ensure that access to the Tape Bypass Label Processing (BLP) resource is controlled	☐	☐
5.3	Ensure that SETROPTS ADSP is disabled	☐	☐
5.4	Ensure that access to DFSMS control data sets is controlled	☐	☐
6.1.1	Ensure CSSMTP started task user ID is PROTECTED	☐	☐
6.1.2	Ensure that the STARTED resource class is used to assign user IDs to CSSMTP started tasks	☐	☐
6.1.3	Ensure AT-TLS protection is enabled for CSSMTP	☐	☐
6.1.4	Ensure that access to CSSMTP started task data sets is controlled	☐	☐
6.2.1	Ensure that the STARTED resource class is used to assign user IDs with proper parameters to FTP server started tasks	☐	☐
6.2.2	Ensure startup parameters for the FTP daemon do not allow ANONYMOUS or INACTIVE keywords	☐	☐
6.2.3	Ensure FTP.DATA configuration statements enforce secure configuration	☐	☐
6.2.4	Ensure FTP.DATA configuration statements enforce AT-TLS protection	☐	☐
6.2.5	Ensure user exits for the FTP server are not used without approval	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.2.6	Ensure that access to the warning banner for the FTP server is controlled	☐	☐
6.2.7	Ensure SMF recording options for the FTP Server are configured	☐	☐
6.2.8	Ensure UNIX permission and user audit bits for FTP server are configured	☐	☐
6.2.9	Ensure access to FTP server FTP.DATA data sets is controlled	☐	☐
6.2.10	Ensure access to FTP control card data sets is controlled	☐	☐
6.3.1	Ensure SSH daemon is configured to only use the SSHv2 protocol	☐	☐
6.3.2	Ensure SSH daemon is configured to use FIPS 140-2 compliant cryptographic provider	☐	☐
6.3.3	Ensure SSH daemon is configured with a logon banner	☐	☐
6.3.4	Ensure SSH daemon is configured for SMF logging	☐	☐
6.3.5	Ensure SSH daemon is configured to use SAF keyrings for key storage	☐	☐
6.4.1	Ensure syslog daemon is started at z/OS initialization	☐	☐
6.4.2	Ensure that the STARTED resource class is used to assign user IDs with proper parameters to syslog daemon started tasks	☐	☐
6.4.3	Ensure permission and user audit bits for syslog daemon component are configured	☐	☐
6.4.4	Ensure that access to syslog daemon archive data sets is controlled	☐	☐
6.5.1	Ensure configuration files for the TCP/IP stack are explicitly specified	☐	☐
6.5.2	Ensure TCP/IP stack configuration defined in TCPIP.DATA meets minimum requirements	☐	☐
6.5.3	Ensure hosts identified by the NSINTERADDR statement are protected	☐	☐
6.5.4	Ensure TCP/IP stack configuration defined in PROFILE.TCPIP meets minimum requirements	☐	☐
6.5.5	Ensure permission and user audit bits for z/OS UNIX file system objects that are part of the base TCP/IP component are configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.5.6	Ensure access to TCP/IP SAF resources is controlled	☐	☐
6.5.7	Ensure that the SERVAUTH resource class is enabled	☐	☐
6.5.8	Ensure that the STARTED resource class is used to assign user IDs with proper parameters to base TCP/IP component started tasks	☐	☐
6.5.9	Ensure access to data sets for the base TCP/IP component is controlled	☐	☐
6.6.1	Ensure configuration statements for the TN3270E telnet server are configured	☐	☐
6.6.2	Ensure VTAM session setup controls for the TN3270E telnet server are configured	☐	☐
6.6.3	Ensure a warning banner for the TN3270 telnet server is configured	☐	☐
6.6.4	Ensure AT-TLS protection is enabled for the TN3270 telnet server	☐	☐
6.6.5	Ensure SMF recording options for the TN3270 telnet server are configured	☐	☐
6.6.6	Ensure that access to the otelnetd and EZATNTLE programs is controlled	☐	☐
6.7.1	Ensure VTAM USSTAB definitions are being used for secured terminals	☐	☐
6.7.2	Ensure that access to the system data sets used to support the VTAM network is controlled	☐	☐
7.1.1	Ensure that access to ICSF installation data sets is controlled	☐	☐
7.1.2	Ensure that the STARTED resource class is used to assign user IDs with proper parameters to ICSF started tasks	☐	☐
7.1.3	Ensure CSFINPV2 requires signature verification	☐	☐
7.1.4	Ensure ICSF is configured to start during IPL	☐	☐
7.1.5	Ensure that ICSF Master Keys are managed by a Trusted Key Entry (TKE) workstation	☐	☐
7.2.1	Ensure crypto usage statistics are enabled	☐	☐
7.2.4	Ensure ICSF key data sets have a system backup	☐	☐
7.2.5	Ensure ICSF master keys have a backup procedure	☐	☐

Recommendation		Set Correctly	
		Yes	No
7.2.6	Ensure all ICSF key data sets are in common record format	☐	☐
7.2.7	Ensure all ICSF key data sets are enabled for sysplex sharing	☐	☐
7.2.8	Ensure ICSF is running with FIPSMODE enabled	☐	☐
7.2.9	Ensure CCA operational keys are created with WRAPENH3 key wrapping	☐	☐
7.3.1	Ensure that the CSFSERV class is active	☐	☐
7.3.2	Ensure that the CSFKEYS class is active	☐	☐
7.3.3	Ensure that the CRYPTOZ class is active	☐	☐
7.3.4	Ensure that the XCSFKEY class is active	☐	☐
7.3.5	Ensure ICSF key store policy controls are enabled	☐	☐
7.3.6	Ensure access to ICSF key data sets is controlled	☐	☐
7.3.7	Ensure access to ICSF administrative services is controlled	☐	☐
7.3.8	Ensure access to ICSF operator commands is controlled	☐	☐
8.1.1	Ensure that access to JES2 system commands is controlled	☐	☐
8.2.1	Ensure that the JESSPOOL resource class is enabled	☐	☐
8.2.2	Ensure that access to JES2 spool resources is controlled	☐	☐
8.2.3	Ensure that access to JES2 trace resources is controlled	☐	☐
8.2.4	Ensure that access to JESNEWS resources is controlled	☐	☐
8.3.1	Ensure that the JESJOBS resource class is configured	☐	☐
8.3.2	Ensure that access to JESJOBS CANCEL resources is controlled	☐	☐
8.3.3	Ensure that access to JESJOBS GROUPREG resources is controlled	☐	☐
8.3.4	Ensure that access to JESJOBS HOLD resources is controlled	☐	☐
8.3.5	Ensure that access to JESJOBS JOBCLASS resources is controlled	☐	☐
8.3.6	Ensure that access to JESJOBS JOBNFY resources is controlled	☐	☐

Recommendation		Set Correctly	
		Yes	No
8.3.7	Ensure that access to JESJOBS MODIFY resources is controlled	☐	☐
8.3.8	Ensure that access to JESJOBS PURGE resources is controlled	☐	☐
8.3.9	Ensure that access to JESJOBS RELEASE resources is controlled	☐	☐
8.3.10	Ensure that access to JESJOBS REROUTE resources is controlled	☐	☐
8.3.11	Ensure that access to JESJOBS SPIN resources is controlled	☐	☐
8.3.12	Ensure that access to JESJOBS SPOOLIO resources is controlled	☐	☐
8.3.13	Ensure that access to JESJOBS START resources is controlled	☐	☐
8.3.14	Ensure that access to JESJOBS SUBMIT resources is controlled	☐	☐
8.3.15	Ensure that access to JESJOBS RESTART resources is controlled	☐	☐
8.4.1	Ensure that data sets on SPOOL are encrypted	☐	☐
8.5.1	Ensure that access to the data sets used by JES2 is controlled	☐	☐
8.5.2	Ensure that RACF is called for data sets opened by JES2	☐	☐
8.6.1	Ensure that access to JES2 output devices is controlled	☐	☐
8.6.2	Ensure that bypass label processing is not set on any JOBCCLASS	☐	☐
8.6.3	Ensure that access to JES2 input sources is controlled	☐	☐
8.7.1	Ensure that RJE workstations and NJE nodes enforce password protection	☐	☐
8.7.2	Ensure that RJE workstations have paired user IDs	☐	☐
8.8.1	Ensure that the SETROPTS JES(BATCHALLRACF) is enabled	☐	☐
8.8.2	Ensure that the SETROPTS JES(XBMALLRACF) is enabled	☐	☐
9.1	Ensure that access to z/OS UNIX SURROGAT resources is controlled	☐	☐

Recommendation		Set Correctly	
		Yes	No
9.2	Ensure that access to superuser resources in the UNIXPRIV class is controlled	☐	☐
9.3	Ensure that general users are not allowed to change their file ownership	☐	☐
9.4	Ensure that RESTRICTED users cannot access UNIX files to which they are not explicitly permitted	☐	☐
9.5	Ensure that newly assigned UID and GID are unique values	☐	☐
9.6	Ensure that z/OS UNIX user accounts are defined with compliant values	☐	☐
9.7	Ensure that RACF Classes required to secure the z/OS UNIX environment are active	☐	☐
9.8	Ensure that RACF Classes required to secure the z/OS UNIX environment are RACLISTed	☐	☐
9.9	Ensure that the user account for the z/OS UNIX kernel is defined with compliant attributes	☐	☐
9.10	Ensure that z/OS UNIX automount configuration files are configured with compliant values	☐	☐
9.11	Ensure that entries in /etc/inetd.conf are active and secure	☐	☐
9.12	Ensure that z/OS UNIX OMVS parameters in IEASYSxx are configured	☐	☐
9.13	Ensure that z/OS UNIX BPXPRMxx parameters in PARMLIB are configured for security	☐	☐
9.14	Ensure that z/OS UNIX permission bits and audit bits are configured to audit sensitive file access	☐	☐
9.15	Ensure that access to BPX resources in the FACILITY class is controlled	☐	☐
9.16	Ensure that security parameters in /etc/profile are configured	☐	☐
9.17	Ensure that security commands in /etc/rc are safe	☐	☐
9.18	Ensure that the BPXROOT user account is configured with compliant values	☐	☐
9.19	Ensure that each RACF group for UNIX is defined with a unique GID	☐	☐

Recommendation		Set Correctly	
		Yes	No
9.20	Ensure that access to data sets used as step libraries in /etc/steplib is controlled	☐	☐
9.21	Ensure that ability to switch into superuser mode is controlled	☐	☐
9.22	Ensure access to zFS data sets is controlled	☐	☐
9.23	Ensure USS Telnet server is not active	☐	☐
9.24	Ensure rlogin is not active	☐	☐
9.25	Ensure that the FSSEC resource class is enabled	☐	☐
9.26	Ensure that programs cannot execute from the /tmp directory	☐	☐
9.27	Ensure that data sets containing user file systems do not have the user ID as the high-level qualifier	☐	☐
9.28	Ensure that daemons are running with z/OS UNIX level security	☐	☐
9.29	Ensure that servers are running with z/OS UNIX level security	☐	☐
9.30	Ensure that access to file systems containing critical data is controlled	☐	☐
9.31	Ensure that file systems are mounted Read Only wherever possible	☐	☐
9.32	Ensure that file systems are mounted with set-id files disabled wherever possible	☐	☐
9.33	Ensure that no file systems are mounted with security disabled	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	Ensure that the SETROPTS PASSWORD(INTERVAL and PHRASEINT) values are set to a maximum of 365	☐	☐
1.1.2	Ensure that the SETROPTS PASSWORD(HISTORY) value is set to a minimum of 5	☐	☐
1.1.3	Ensure that at least one SETROPTS PASSWORD(RULE) is defined with (LENGTH(8) MIXEDALL(1:8))	☐	☐
1.1.4	Ensure that the SETROPTS PASSWORD(MINCHANGE) value is set to a minimum of 1	☐	☐
1.1.5	Ensure that the SETROPTS PASSWORD(REVOKE) value is set to a maximum of 6	☐	☐
1.1.6	Ensure that the SETROPTS PASSWORD(ALGORITHM) value is set to KDFAES	☐	☐
1.1.7	Ensure that the SETROPTS PASSWORD(WARNING) value is set to a minimum of 5	☐	☐
1.1.8	Ensure that the SETROPTS RVARYPW values are secured with KDFAES	☐	☐
1.1.9	Ensure SETROPTS PASSWORD(MIXEDCASE) is in effect	☐	☐
1.1.10	Ensure SETROPTS PASSWORD(SPECIALCHARS) is in effect	☐	☐
1.2.1	Ensure that the SETROPTS INACTIVE value is set to a maximum of 45	☐	☐
1.2.2	Ensure that the STARTED resource class is used to assign user IDs to started tasks	☐	☐
1.2.3	Ensure user propagation is controlled	☐	☐
1.2.4	Ensure that started tasks defined with the TRUSTED attribute are justified	☐	☐
1.2.5	Ensure that the OPERCMDS resource class is enabled	☐	☐
1.2.6	Ensure that the CONSOLE resource class is enabled	☐	☐
1.2.7	Ensure that the FACILITY resource class is enabled	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.2.8	Ensure that inapplicable PPT entries have been invalidated	☐	☐
1.2.9	Ensure that LNKAUTH=APFTAB is specified in the IEASYSxx members currently active parmlib data sets	☐	☐
1.2.10	Ensure that the CONSOLxx members are configured	☐	☐
1.2.11	Ensure that no expired digital certificates are used	☐	☐
1.2.12	Ensure that the SETROPTS RVARYPW are set to non-default values	☐	☐
1.2.13	Ensure that RACF default user ID IBMUSER is disabled	☐	☐
1.3.1	Ensure that the use of RACF SPECIAL attribute is justified	☐	☐
1.3.2	Ensure that SYS1.UADS contains only recovery user IDs	☐	☐
1.3.3	Ensure that MCS console user IDs are protected	☐	☐
1.3.4	Ensure that STARTED resource class profiles assign PROTECTED user IDs	☐	☐
1.3.5	Ensure that the assignment of RACF CLAUTH authority is justified	☐	☐
2.1.1	Ensure that access to DASDVOL and STGADMIN resources are controlled	☐	☐
2.1.2	Ensure that access to active SMF collection files is controlled	☐	☐
2.1.3	Ensure that the SETROPTS WHEN(PROGRAM) value is active	☐	☐
2.1.4	Ensure that access to the ICHDSM00 (DSMON) program is controlled	☐	☐
2.1.5	Ensure that access to the IRRDPI00 program is controlled	☐	☐
2.1.6	Ensure that the SETROPTS ERASE value is set to ALL	☐	☐
2.1.7	Ensure that the TEMPDSN class is active	☐	☐
2.1.8	Ensure that access to RACF database data sets is controlled	☐	☐
2.1.9	Ensure that access to the RACF remote sharing facility data sets is controlled	☐	☐
2.1.10	Ensure that access to the RACF parameter library is controlled	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.1.11	Ensure that RACF remote sharing connections use the TCP/IP protocol	☐	☐
2.1.12	Ensure that access to memory and privileged program dumps is controlled	☐	☐
2.1.13	Ensure that access to system TRACE data sets is controlled	☐	☐
2.1.14	Ensure that access to system backup data sets is controlled	☐	☐
2.1.15	Ensure that access to system DUMP data sets is controlled	☐	☐
2.1.16	Ensure that access to SMF collection offload data sets is controlled	☐	☐
2.2.1	Ensure that the access to update system dynamic lists is controlled	☐	☐
2.2.2	Ensure that access to IEASYMUP resources is controlled	☐	☐
2.2.3	Ensure that PASSWORD protection for data sets is not used	☐	☐
2.2.4	Ensure that access to data sets in the PARMLIB concatenation is controlled	☐	☐
2.2.5	Ensure that access to all LPA libraries is controlled	☐	☐
2.2.6	Ensure that access to system MASTER catalogs is controlled	☐	☐
2.2.7	Ensure that access to all APF-authorized objects is controlled	☐	☐
2.2.8	Ensure that access to the SYS1.SVCLIB data set is controlled	☐	☐
2.2.9	Ensure that access to the SYS1.IMAGELIB data set is controlled	☐	☐
2.2.10	Ensure that access to libraries that contain PPT modules is controlled	☐	☐
2.2.11	Ensure that access to the SYS1.NUCLEUS data set is controlled	☐	☐
2.2.12	Ensure that access to all system PROCLIB data sets is controlled	☐	☐
2.2.13	Ensure that access to System REXX IRRPWREX exit is controlled	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.2.14	Ensure that access to the SYS1.LINKLIB data set is controlled	☐	☐
2.2.15	Ensure that access to all system-level product installation libraries is controlled	☐	☐
2.2.16	Ensure that access to RACF resources in the FACILITY class is controlled	☐	☐
2.2.17	Ensure that access to VTAMAPPL resources is controlled	☐	☐
2.2.18	Ensure that access to IBM Health Checker resources is controlled	☐	☐
2.3.1	Ensure that the SETROPTS TERMINAL value is set to NONE	☐	☐
2.3.2	Ensure that the SETROPTS GENERIC is enabled for ACTIVE classes	☐	☐
2.3.3	Ensure that the SETROPTS PROTECTALL value is set to FAIL	☐	☐
2.3.4	Ensure that ALTER access authority in DISCRETE profiles is limited	☐	☐
2.3.5	Ensure that the ACEECHK resource class is enabled	☐	☐
2.3.6	Ensure that SETROPTS ENHANCEDGENERICOWNER is in effect	☐	☐
2.3.7	Ensure that SETROPTS NOADDCREATOR is in effect	☐	☐
2.4.1	Ensure that the assignment of the RACF OPERATIONS attribute is justified	☐	☐
2.4.2	Ensure that access to TSOAUTH resources is controlled	☐	☐
2.4.3	Ensure that access to SURROGAT resources is controlled	☐	☐
2.4.4	Ensure that the assignment of the UNIX uid(0) is justified	☐	☐
2.4.5	Ensure that started tasks defined with the PRIVILEGED attribute is justified	☐	☐
2.4.6	Ensure that access to libraries containing EXIT modules is controlled	☐	☐
2.4.7	Ensure that access to LINKLIST libraries is controlled	☐	☐
2.4.8	Ensure that access to the SYS1.UADS data set is controlled	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.4.9	Ensure that access to system page data sets is controlled	☐	☐
2.4.10	Ensure that MCS console access is controlled through profiles in the CONSOLE resource class	☐	☐
2.4.11	Ensure that access to system USER catalogs is controlled	☐	☐
2.4.12	Ensure that access to Libraries containing EXIT modules is controlled	☐	☐
3.1	Ensure that SETROPTS CMDVIOL is in effect	☐	☐
3.2	Ensure that SETROPTS SAUDIT is in effect	☐	☐
3.3	Ensure that SETROPTS AUDIT is enabled for ACTIVE classes	☐	☐
3.4	Ensure that SETROPTS OPERAUDIT is in effect	☐	☐
3.5	Ensure that SETROPTS INITSTATS is in effect	☐	☐
3.6	Ensure that the assignment of the RACF AUDITOR or ROAUDIT attribute is justified	☐	☐
3.7	Ensure that effective SMF records collection options are set	☐	☐
3.8	Ensure that an automated process is in place to collect and retain SMF data	☐	☐
3.9	Ensure that required SMF data record types are collected	☐	☐
3.10	Ensure that RACF audit logs is reviewed on a regular basis	☐	☐
3.11	Ensure regular audits of AC=1 modules in APF authorized libraries are conducted	☐	☐
3.12	Ensure that only supported software is installed and active on the system	☐	☐
3.13	Ensure all OS software on your system is supported	☐	☐
3.14	Implement sensitive z/OS data set monitoring	☐	☐
3.15	Ensure that SETROPTS REALDSN is in effect	☐	☐
4.1	Ensure that RACF database is backed up on a scheduled basis	☐	☐
4.2	Ensure that the RACF PRIM and BACK databases are isolated	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.3	Ensure sensitive data sets are encrypted with z/OS data set encryption	☐	☐
4.4	Ensure that RACF application identity mapping (AIM) is at stage 3	☐	☐
4.5	Ensure that RACF ENQ names are not in the Global Resource Serialization (GRS) Resource Name List	☐	☐
4.6	Ensure that SETROPTS GRPLIST is in effect	☐	☐
4.7	Ensure that SETROPTS NOSTATISTICS(*) is in effect	☐	☐
4.8	Ensure that RACF is enabled for Sysplex communication	☐	☐
4.9	Ensure that Validated Boot for z/OS is in effect	☐	☐
4.10	Ensure that the site is registered to the IBM Z and IBM LinuxONE Security Portal	☐	☐
5.1	Ensure that DFSMS is configured	☐	☐
5.2	Ensure that access to the Tape Bypass Label Processing (BLP) resource is controlled	☐	☐
5.3	Ensure that SETROPTS ADSP is disabled	☐	☐
5.4	Ensure that access to DFSMS control data sets is controlled	☐	☐
6.1.1	Ensure CSSMTP started task user ID is PROTECTED	☐	☐
6.1.2	Ensure that the STARTED resource class is used to assign user IDs to CSSMTP started tasks	☐	☐
6.1.3	Ensure AT-TLS protection is enabled for CSSMTP	☐	☐
6.1.4	Ensure that access to CSSMTP started task data sets is controlled	☐	☐
6.2.1	Ensure that the STARTED resource class is used to assign user IDs with proper parameters to FTP server started tasks	☐	☐
6.2.2	Ensure startup parameters for the FTP daemon do not allow ANONYMOUS or INACTIVE keywords	☐	☐
6.2.3	Ensure FTP.DATA configuration statements enforce secure configuration	☐	☐
6.2.4	Ensure FTP.DATA configuration statements enforce AT-TLS protection	☐	☐
6.2.5	Ensure user exits for the FTP server are not used without approval	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.2.6	Ensure that access to the warning banner for the FTP server is controlled	☐	☐
6.2.7	Ensure SMF recording options for the FTP Server are configured	☐	☐
6.2.8	Ensure UNIX permission and user audit bits for FTP server are configured	☐	☐
6.2.9	Ensure access to FTP server FTP.DATA data sets is controlled	☐	☐
6.2.10	Ensure access to FTP control card data sets is controlled	☐	☐
6.3.1	Ensure SSH daemon is configured to only use the SSHv2 protocol	☐	☐
6.3.2	Ensure SSH daemon is configured to use FIPS 140-2 compliant cryptographic provider	☐	☐
6.3.3	Ensure SSH daemon is configured with a logon banner	☐	☐
6.3.4	Ensure SSH daemon is configured for SMF logging	☐	☐
6.3.5	Ensure SSH daemon is configured to use SAF keyrings for key storage	☐	☐
6.4.1	Ensure syslog daemon is started at z/OS initialization	☐	☐
6.4.2	Ensure that the STARTED resource class is used to assign user IDs with proper parameters to syslog daemon started tasks	☐	☐
6.4.3	Ensure permission and user audit bits for syslog daemon component are configured	☐	☐
6.4.4	Ensure that access to syslog daemon archive data sets is controlled	☐	☐
6.5.1	Ensure configuration files for the TCP/IP stack are explicitly specified	☐	☐
6.5.2	Ensure TCP/IP stack configuration defined in TCPIP.DATA meets minimum requirements	☐	☐
6.5.3	Ensure hosts identified by the NSINTERADDR statement are protected	☐	☐
6.5.4	Ensure TCP/IP stack configuration defined in PROFILE.TCPIP meets minimum requirements	☐	☐
6.5.5	Ensure permission and user audit bits for z/OS UNIX file system objects that are part of the base TCP/IP component are configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.5.6	Ensure access to TCP/IP SAF resources is controlled	☐	☐
6.5.7	Ensure that the SERVAUTH resource class is enabled	☐	☐
6.5.8	Ensure that the STARTED resource class is used to assign user IDs with proper parameters to base TCP/IP component started tasks	☐	☐
6.5.9	Ensure access to data sets for the base TCP/IP component is controlled	☐	☐
6.6.1	Ensure configuration statements for the TN3270E telnet server are configured	☐	☐
6.6.2	Ensure VTAM session setup controls for the TN3270E telnet server are configured	☐	☐
6.6.3	Ensure a warning banner for the TN3270 telnet server is configured	☐	☐
6.6.4	Ensure AT-TLS protection is enabled for the TN3270 telnet server	☐	☐
6.6.5	Ensure SMF recording options for the TN3270 telnet server are configured	☐	☐
6.6.6	Ensure that access to the otelnetd and EZATNTLE programs is controlled	☐	☐
6.7.1	Ensure VTAM USSTAB definitions are being used for secured terminals	☐	☐
6.7.2	Ensure that access to the system data sets used to support the VTAM network is controlled	☐	☐
7.1.1	Ensure that access to ICSF installation data sets is controlled	☐	☐
7.1.2	Ensure that the STARTED resource class is used to assign user IDs with proper parameters to ICSF started tasks	☐	☐
7.1.3	Ensure CSFINPV2 requires signature verification	☐	☐
7.1.4	Ensure ICSF is configured to start during IPL	☐	☐
7.1.5	Ensure that ICSF Master Keys are managed by a Trusted Key Entry (TKE) workstation	☐	☐
7.2.1	Ensure crypto usage statistics are enabled	☐	☐
7.2.2	Ensure crypto key lifecycle auditing is enabled	☐	☐
7.2.3	Ensure crypto key usage auditing is enabled	☐	☐

Recommendation		Set Correctly	
		Yes	No
7.2.4	Ensure ICSF key data sets have a system backup	☐	☐
7.2.5	Ensure ICSF master keys have a backup procedure	☐	☐
7.2.6	Ensure all ICSF key data sets are in common record format	☐	☐
7.2.7	Ensure all ICSF key data sets are enabled for sysplex sharing	☐	☐
7.2.8	Ensure ICSF is running with FIPSMODE enabled	☐	☐
7.2.9	Ensure CCA operational keys are created with WRAPENH3 key wrapping	☐	☐
7.3.1	Ensure that the CSFSERV class is active	☐	☐
7.3.2	Ensure that the CSFKEYS class is active	☐	☐
7.3.3	Ensure that the CRYPTOZ class is active	☐	☐
7.3.4	Ensure that the XCSFKEY class is active	☐	☐
7.3.5	Ensure ICSF key store policy controls are enabled	☐	☐
7.3.6	Ensure access to ICSF key data sets is controlled	☐	☐
7.3.7	Ensure access to ICSF administrative services is controlled	☐	☐
7.3.8	Ensure access to ICSF operator commands is controlled	☐	☐
8.1.1	Ensure that access to JES2 system commands is controlled	☐	☐
8.2.1	Ensure that the JESSPOOL resource class is enabled	☐	☐
8.2.2	Ensure that access to JES2 spool resources is controlled	☐	☐
8.2.3	Ensure that access to JES2 trace resources is controlled	☐	☐
8.2.4	Ensure that access to JESNEWS resources is controlled	☐	☐
8.3.1	Ensure that the JESJOBS resource class is configured	☐	☐
8.3.2	Ensure that access to JESJOBS CANCEL resources is controlled	☐	☐
8.3.3	Ensure that access to JESJOBS GROUPREG resources is controlled	☐	☐
8.3.4	Ensure that access to JESJOBS HOLD resources is controlled	☐	☐
8.3.5	Ensure that access to JESJOBS JOBCLASS resources is controlled	☐	☐

Recommendation		Set Correctly	
		Yes	No
8.3.6	Ensure that access to JESJOBS JOBNFY resources is controlled	☐	☐
8.3.7	Ensure that access to JESJOBS MODIFY resources is controlled	☐	☐
8.3.8	Ensure that access to JESJOBS PURGE resources is controlled	☐	☐
8.3.9	Ensure that access to JESJOBS RELEASE resources is controlled	☐	☐
8.3.10	Ensure that access to JESJOBS REROUTE resources is controlled	☐	☐
8.3.11	Ensure that access to JESJOBS SPIN resources is controlled	☐	☐
8.3.12	Ensure that access to JESJOBS SPOOLIO resources is controlled	☐	☐
8.3.13	Ensure that access to JESJOBS START resources is controlled	☐	☐
8.3.14	Ensure that access to JESJOBS SUBMIT resources is controlled	☐	☐
8.3.15	Ensure that access to JESJOBS RESTART resources is controlled	☐	☐
8.4.1	Ensure that data sets on SPOOL are encrypted	☐	☐
8.5.1	Ensure that access to the data sets used by JES2 is controlled	☐	☐
8.5.2	Ensure that RACF is called for data sets opened by JES2	☐	☐
8.6.1	Ensure that access to JES2 output devices is controlled	☐	☐
8.6.2	Ensure that bypass label processing is not set on any JOBCLASS	☐	☐
8.6.3	Ensure that access to JES2 input sources is controlled	☐	☐
8.7.1	Ensure that RJE workstations and NJE nodes enforce password protection	☐	☐
8.7.2	Ensure that RJE workstations have paired user IDs	☐	☐
8.8.1	Ensure that the SETROPTS JES(BATCHALLRACF) is enabled	☐	☐
8.8.2	Ensure that the SETROPTS JES(XBMALLRACF) is enabled	☐	☐

Recommendation		Set Correctly	
		Yes	No
9.1	Ensure that access to z/OS UNIX SURROGAT resources is controlled	☐	☐
9.2	Ensure that access to superuser resources in the UNIXPRIV class is controlled	☐	☐
9.3	Ensure that general users are not allowed to change their file ownership	☐	☐
9.4	Ensure that RESTRICTED users cannot access UNIX files to which they are not explicitly permitted	☐	☐
9.5	Ensure that newly assigned UID and GID are unique values	☐	☐
9.6	Ensure that z/OS UNIX user accounts are defined with compliant values	☐	☐
9.7	Ensure that RACF Classes required to secure the z/OS UNIX environment are active	☐	☐
9.8	Ensure that RACF Classes required to secure the z/OS UNIX environment are RACLISTed	☐	☐
9.9	Ensure that the user account for the z/OS UNIX kernel is defined with compliant attributes	☐	☐
9.10	Ensure that z/OS UNIX automount configuration files are configured with compliant values	☐	☐
9.11	Ensure that entries in /etc/inetd.conf are active and secure	☐	☐
9.12	Ensure that z/OS UNIX OMVS parameters in IEASYSxx are configured	☐	☐
9.13	Ensure that z/OS UNIX BPXPRMxx parameters in PARMLIB are configured for security	☐	☐
9.14	Ensure that z/OS UNIX permission bits and audit bits are configured to audit sensitive file access	☐	☐
9.15	Ensure that access to BPX resources in the FACILITY class is controlled	☐	☐
9.16	Ensure that security parameters in /etc/profile are configured	☐	☐
9.17	Ensure that security commands in /etc/rc are safe	☐	☐
9.18	Ensure that the BPXROOT user account is configured with compliant values	☐	☐

Recommendation		Set Correctly	
		Yes	No
9.19	Ensure that each RACF group for UNIX is defined with a unique GID	☐	☐
9.20	Ensure that access to data sets used as step libraries in /etc/steplib is controlled	☐	☐
9.21	Ensure that ability to switch into superuser mode is controlled	☐	☐
9.22	Ensure access to zFS data sets is controlled	☐	☐
9.23	Ensure USS Telnet server is not active	☐	☐
9.24	Ensure rlogin is not active	☐	☐
9.25	Ensure that the FSSEC resource class is enabled	☐	☐
9.26	Ensure that programs cannot execute from the /tmp directory	☐	☐
9.27	Ensure that data sets containing user file systems do not have the user ID as the high-level qualifier	☐	☐
9.28	Ensure that daemons are running with z/OS UNIX level security	☐	☐
9.29	Ensure that servers are running with z/OS UNIX level security	☐	☐
9.30	Ensure that access to file systems containing critical data is controlled	☐	☐
9.31	Ensure that file systems are mounted Read Only wherever possible	☐	☐
9.32	Ensure that file systems are mounted with set-id files disabled wherever possible	☐	☐
9.33	Ensure that no file systems are mounted with security disabled	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8	☐	☐

Appendix: Change History

Date	Version	Changes for this version
10/08/2025	1.0.0	Published