



Using Vanguard Security Solutions to Complete DISA STIG SRR Review Procedures

z/OS SDSF for RACF Analysis Process and Checklist

Modeled After:
SRR REVIEW PROCEDURES
z/OS SDSF Checklist for RACF
Developed by Vanguard Integrity Professionals
Version 6 Release 8
August 2016

Using Vanguard Security Solutions™ to Complete DISA STIG SRR Review Procedures

DISA Version 6.28

Document Number RACF_STIG-08012016-153500-628A

August, 2016

Copyright

© 1989-2013 Vanguard Integrity Professionals-Nevada.

All rights reserved. Printed in the USA.

No part of this publication may be copied, reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, for any purpose other than the Licensee's personal use, without express written permission from Vanguard Integrity Professionals-Nevada.

Trademarks

Vanguard Integrity Professionals, Vanguard Administrator, Vanguard Advisor, Vanguard Analyzer, Vanguard Authenticator, Vanguard Cleanup, Vanguard Configuration Manager, Vanguard Enforcer, Vanguard ez/AccessControl, Vanguard ez/SignOn, Vanguard ez/SignOn Deploy, Vanguard ez/Integrator, Vanguard ez/Token, Vanguard GRC, Vanguard IAM, Vanguard Identity Manager, Vanguard Identity & Access Management, Vanguard Governance, Risk Management and Compliance, Vanguard inCompliance, Vanguard Offline, Vanguard OPID Manager, Vanguard PasswordReset, Vanguard Policy Manager, Vanguard Registration Manager, Vanguard SecurityCenter, Vanguard Security Conference, Vanguard Security on Demand, Vanguard Security Solutions, Vanguard Security Suite, AutoPilot, eDistribution, Enterprise-Wise, Vanguard Deploy, Vanguard ez/Security on Demand, Find-it-Fix-it-Fast, Knowledge Expo, Pathway to Profitability, QS/390, QuickGen, Quality Security Framework, Quality Security/390 Suite, Registration Manager, RioVision, RiskMinder, Security on Demand, SmartAssist, SmartLink, SmartPanel, and Vanguard Tokenless Authentication are trademarks or service marks of Vanguard Integrity Professionals-Nevada.

AIX, AS/400, IBM logo and the Business Partner emblem, CICS, DB2, IMS, MVS/ESA, OS/400, RACF, and z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT and Windows Server are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. All other products mentioned in this publication, including Linux, Red Hat, SUSE, UNIX, Solaris and HP-UX, are trademarks or registered trademarks of their respective owners.

About This Product

Any software products accompanying this publication are copyrighted and owned by Vanguard Integrity Professionals-Nevada. Use of the software product is governed by the provisions of your License Agreement or the Terms of Use on the envelope in which the software product was sent to you. **Warranty and Limitation of Liability:** VANGUARD warrants that the licensed software products as delivered do not infringe any patent or copyright held by any third party and enforceable under U.S. law. THE FOREGOING WARRANTY IS THE SOLE AND EXCLUSIVE WARRANTY PROVIDED BY VANGUARD UNDER OR IN CONNECTION WITH THE LICENSED SOFTWARE PRODUCTS AND IS IN LIEU OF ALL OTHER WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NONINFRINGEMENT. UNDER NO CIRCUMSTANCES WILL VANGUARD BE LIABLE TO CUSTOMER FOR ANY OF THE FOLLOWING: (I) ANY DAMAGES CAUSED BY THE FAILURE OF CUSTOMER TO PERFORM ITS RESPONSIBILITIES; (II) ANY THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES; OR (III) ANY LOST PROFITS,

LOSS OF BUSINESS, LOST SAVINGS OR OTHER CONSEQUENTIAL, SPECIAL,
INCIDENTAL, INDIRECT, EXEMPLARY OR PUNITIVE DAMAGES, EVEN IF INFORMED OF
THEIR POSSIBILITY.

Table of Contents

___STIG ID: ZISF0040	5
___STIG ID: ZISFR000	6
___STIG ID: ZISFR002	8
___STIG ID: ZISFR020	10
___STIG ID: ZISFR021	11
___STIG ID: ZISFR030	13
___STIG ID: ZISFR032	15
___STIG ID: ZISFR038	16

UNCLASSIFIED
z/OS IBM SDSF for RACF Analysis and Checklist
Version 6 Release 8

___**STIG ID: ZISF0040**

Default Severity: Category II

- a) Use TSO option 3.4 to review SDSFPARM DD statement in the SDSF STC..
- b) If no SDSDFPARM DD statement was used look at ISFPRMxx member in the Parmlib.
(Find the applicable Parmlib by issuing F SDSF, D command).
- c) Ensure the following GROUP ISFSPROG Parameters are **NOT** specified in the GROUP statements:

AUTH
CMDAUTH
CMDLEV
DSPAUTH

- 1.. Ensure a value is specified for NAME as follows:
Name(xxxxxxxx)
- 2.. If
AUTH, CMDAUTH, CMDLEV, DSPAUTH are not specified in the GROUP statements
and
a value is specified for NAME
there is NO FINDING.
- 3. If
AUTH, CMDAUTH, CMDLEV or DSPAUTH are specified in the GROUP statements defined in the ISFPRMxx member
or
NAME is not specified with a value
there is a FINDING

NOTE: AUPDT is a parameter for Auto Update and allows overriding of terminal lockout times. All GROUP statements that specify a value greater than 0 for AUPDT will require justification for the setting.

CCI: CCI-000035

UNCLASSIFIED
z/OS IBM SDSF for RACF Analysis and Checklist
Version 6 Release 8

___ **STIG ID: ZISFR000**

Default Severity: Category II

- a) Consult with your systems programmer to identify the names of the SDSF product datasets and the data set that contains the ISFPARMS statements.
- b) Ensure the following data set controls are in effect for the SDSF product data sets and the data set that contains the ISFPARMS statements:
 - UPDATE or higher access to the SDSF product data sets (ISF.AISF* and ISF.SISF*) are restricted to systems programming personnel.
 - UPDATE or higher access to the data sets that contains the ISFPARMS statements (identified in the SDSFPARM DD statement of the SDSF stc) is restricted to systems programming personnel.
 - UACC (None) and NOWARNING are specified for the SDSF product data sets and for the data set that contains the ISFPARMS statements.
 - The RACF data set rules for the SDSF data sets specify that all accesses of UPDATE or higher(i.e., failures and successes) will be logged.
 - 1. From the Administrator main menu, select 3.3 (Dataset Profile Reports) and press <ENTER>
 - 2. Tab down to "Data SET" row, type LV next to the data set that contains the ISFPARMS statement and press <ENTER>.
 - 3. Review the Universal Access and Access List.
 - 4. Repeat steps 1-3 above for each of the SDSF product datasets.
- c) If UPDATE and ALLOCATE (e.g. ALTER) access to the SDSF product data sets are restricted to systems programming personnel, there is NO FINDING.
- d) If UPDATE and ALLOCATE (e.g. ALTER) access to the data sets that contain the ISFPARMS statements (identified in the SDSFPARM DD statement of the SDSF stc) are restricted to systems programming personnel, there is NO FINDING.
- e) If UPDATE and ALLOCATE (ALTER) access to the SDSF product data sets **is not** restricted to systems programming personnel, this is a FINDING.

UNCLASSIFIED
z/OS IBM SDSF for RACF Analysis and Checklist
Version 6 Release 8

- f) If UPDATE and ALLOCATE (ALTER) access to the data sets that contain the ISFPARMS statements (identified in the SDSFPARM DD statement of the SDSF stc) **is not** restricted to systems programming personnel, this is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS IBM SDSF for RACF Analysis and Checklist
Version 6 Release 8

STIG ID: ZISFR002

Default Severity: Category II

- a) Use TSO option 3.4 to browse the library/member below.
- b) Ensure the following data set controls are in effect for the HASPINDEX data set specified on the INDEX control statement in the ISFPARMS member (ex.SYS1.PARMLIB(ISFPRMxx)):

All access to the HASPINDEX is restricted as follows:

- 1. Read access is restricted to auditors.
- 2. Update access is restricted to SDSF started tasks.
- 3. Write access is restricted to systems programming personnel.
- 4. UACC(None) and NOWARNING is set.

c). To Verify:

- 1.From the Administrator main menu, review the access list for the HASPINDEX dataset. Type **3;3** and press <ENTER> to go to Data Set Reports.
- 2. Type in a 1 for DATA SET PROFILE SUMMARY, and type in the high level qualifier of the ISF profile, (e.g. ISF*), and press <ENTER>.
- 3. Tab down to the Data Set field and type in LRD and press <ENTER>. and press <ENTER>.
- 4.Make sure you find the name of the HASPINDEX dataset, (e.g. ISF.HASPINDEX).
- 5. Review the profile UACC and Access List.

- d). If (Read access is restricted to auditors
and
Update access is restricted to SDSF started tasks
and
Write access is restricted to systems programming personnel
and
UACC(NONE) and NOWARNING are specified)
for the HASPINDEX dataset, then there is NO FINDING.

UNCLASSIFIED
z/OS IBM SDSF for RACF Analysis and Checklist
Version 6 Release 8

- e) If access to the HASPINDEX is not restricted to auditors, SDSF started task and systems programming personnel as specified above, there is a FINDING.

NOTE: If running z/OS V1R11 or above, with the use of a new JES logical log, the HASPINDEX may not exist and may make this vulnerability not applicable (N/A). However if used the HASPINDEX dataset must be restricted.

If running z/OS V1R11 systems or above and NOT using JES logical log, the HASPINDEX data set must be protected.

CCI: CCI-001499

UNCLASSIFIED
z/OS IBM SDSF for RACF Analysis and Checklist
Version 6 Release 8

___**STIG ID: ZISFR020**

Default Severity: Category II

- a) From the Administrator main menu, select 3;4 (Security Server Reports, General Resource Profiles) and press <ENTER>
- b) Tab down to “CLASS: “, type SDSF and press <ENTER>
 1. Review the profiles in the “Profile Name” column that are listed in the SDSF SAF resource table in the z/OS STIG Addendum.
 2. Ensure that they are defined with a UACC=NONE in the UACC column:
 3. If all UACCs are NONE, there is NO FINDING on this point.
 4. If any UACC is not equal to NONE, this is a FINDING.
 5. Check that the RACF resource logging is specified for each resource as specified in the SDSF SAF resource table referenced above.
- c) Type **LR** in the CMD column of each resource name listed in the table above and check that.
 1. Warning = NO
 2. The Auditing options are set as defined in the SDSF SAF resource table for the resource.
 3. The access list showing list of user groups, only includes valid users per the SDSF SAF resources table.
 4. The users only have the level of access permitted per the SDSF SAF resource table
- d) If
 - WARNING is not set to NO or
 - the AUDIT options for each resource are not as defined in the SDSF SAF resource table
 - or any user groups are granted access who are not in the SDSF SAF resource Table
 - or any users are granted access that is not permitted to them per the SDSF SAF resource tablethere is a FINDING.
- e). If none of the conditions in d. above are true and UACC = NONE for all resources, then there is NO FINDING.

NOTE: The RACF resource access authorizations for SDSF GROUP.group-name will require additional analysis to justify access.

CCI: CCI-000035

CCI: CCI-002234

UNCLASSIFIED
z/OS IBM SDSF for RACF Analysis and Checklist
Version 6 Release 8

___**STIG ID: ZISFR021**

Default Severity: Category II

- a) From the Administrator main menu, select 3;4 (Security Server Reports - General Resource Reports) and press <ENTER>
- b) Type 1 for General Resource Profile Summary and Tab down to “CLASS: “, type OPERCMDS and press <ENTER>
- c) Find profiles that begin with a prefix of “server.”** and “server.MODIFY.mod-parm” in the “Profile Name” column, review the corresponding UACC column
 1. If all UACC’s are equal to NONE, there is NO FINDING
 2. If any UACC is not equal to NONE, this is a FINDING** “server” here means the name of the SDSF server (likely SDSF, you can find it by going to SDSF and looking for the JOBID of the SDSF started task)
- d) Type **LR** in the CMD column of each “server.MODIFY.DISPLAY.” prefixed resource and review the access list.
 1. If the access list is restricted to systems programming personnel, auditors or operations personnel and their access is READ, there is NO FINDING
 2. If any other user/group is on the access list, this is a FINDING
- e) Type **LR** in the CMD column of each “server.MODIFY.mod-parm.” prefixed resource and review the access list.
 - a. If the access list is restricted to systems programming personnel and their access is CONTROL, there is NO FINDING
 - b. If any other user/group is on the access list, this is a FINDING
- f) Review the audit values.
 1. If the audit “access attempts / access level” value is “ALL”, or “SUCCESS,UPDATE” there is NO FINDING
 2. If the audit “access attempts / access level” value is any other value, this is a FINDING

Note:

- *server* is the name of the SDSF server specified either by the ISFPMAC macro or SDSF command.

UNCLASSIFIED

z/OS IBM SDSF for RACF Analysis and Checklist
Version 6 Release 8

- *mod-parm* is one of the following parameters specified on the MVS MODIFY command: DEBUG, FOLDMSG, LOGCLASS, LOGTYPE, REFRESH, START, STOP, TRACE, and TRCLASS.

CCI: CCI-000035

CCI: CCI-002234

UNCLASSIFIED
z/OS IBM SDSF for RACF Analysis and Checklist
Version 6 Release 8

___ **STIG ID: ZISFR030**

Default Severity: Category II

- a) From the Administrator main menu, select 3;4 (Security Server Reports - General Resource Reports) and press ENTER
- b) Type 1 for General Resource Profile Summary and Tab down to “CLASS: “, type ‘STARTED’ for class name.
- c).Find the SDSF General Resource profile. If not found go to step k. below.
- d). Find the userid associated with the SDSF started task under the STDATA segment information of the SDSF general resource profile.
- e). Go back to Administrator main menu, select 3;1 (Security Server Reports – User Profile) and press ENTER
- f) Tab down to User ID and enter the User ID found in Step d) above and hit enter
- g). Page down till the Attributes section of the profile.
- h) Verify that “Protected = Yes”
- i) If Protected = Yes, there is no FINDING
- j). If Protected = No, there is a FINDING
- k) If SDSF is NOT found as a General Resource profile under the STARTED class in c. above, then check if is defined in the Started Procedures Table (ICHRIN03) as follows:
 - 1, From Analyzer main Menu, go to 3;4 (Online Displays – Started Procedures Analysis) and Press ENTER
 - 2. Look for STARTED in the Source column and SDSF in the Procname column.
 - 3. If the SDSF started procedure does not have an R in the “M” column there is NO FINDING (an R in the “M” column indicates that either the STARTED TASK USER ID does not have the protected attribute or is not defined (these are both findings)

UNCLASSIFIED
z/OS IBM SDSF for RACF Analysis and Checklist
Version 6 Release 8

4..If there is an R in the “M” column, there is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS IBM SDSF for RACF Analysis and Checklist
Version 6 Release 8

___**STIG ID: ZISFR032**

Default Severity: Category II

- a) From the Administrator main menu, select 3;4 (Security Server Reports - General Resource Profiles) and press ENTER
- b) Type 1 for General Resource Profile Summary and Tab down to “CLASS: “; enter ‘STARTED’ for class name.
- c). Find the SDSF General Resource profile.
- d). If SDSF is found as a General Resource profile under the STARTED class, there is no FINDING. .
- e) If SDSF is NOT found as a General Resource profile under the STARTED class in d. above, then check if is defined in the Started Procedures Table (ICHRIN03) as follows:
 - 1, From Analyzer main Menu, go to 3;4 (Online Displays – Started Procedures Analysis) and Press ENTER
 - 2. Look for STARTED in the Source column and SDSF in the Procname column..
 - 3. If SDSF is not found either as a General Resource Profile under STARTED class in e. above AND not found in the Started Procedures Table, this is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS IBM SDSF for RACF Analysis and Checklist
Version 6 Release 8

___**STIG ID: ZISFR038**

Default Severity: Category II

- a) From the Analyzer main Menu, select 3 (Online Displays), press ENTER
- b) Select 7 (SETROPTS Analysis) and press ENTER
- c) Tab down and type an S next to “Audit for CDT Classes”, press ENTER
- d) Review the row for the SDSF class:
 - 1. If the STATUS is active, there is NO FINDING.
 - 2. If the STATUS is inactive, this is a FINDING

CCI: CCI-000336

CCI: CCI-002358