



Using Vanguard Security Solutions to Complete DISA STIG SRR Review Procedures

z/OS BMC Control-D for RACF Analysis Process and Checklist

Modeled After:
SRR REVIEW PROCEDURES
z/OS Control-D for RACF Checklist
Developed by DISA for the DOD
Version 6 Release 7
October 2018

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

DISA Version 6.28

Document Number CTD_STIG-08012016-115500-628A

October, 2018

Copyright

© 1989-2012 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: ZCTD0040	5
___STIG ID: ZCTDR060	6
___STIG ID: ZCTDR000	7
___STIG ID: ZCTDR001	7
___STIG ID: ZCTDR002	9
___STIG ID: ZCTDR020	10
___STIG ID: ZCTDR030	11
___STIG ID: ZCTDR032	12

___**STIG ID: ZCTD0040**

Default Severity: Category II

- A. Ensure the following keywords are specified in the BMC CONTROL-D security parameter member:

Keyword	Value
DEFMCHKD	\$\$CTDEDM
SECTOLD	NO
DFMD01	EXTEND
DFMD04	EXTEND
DFMD08	EXTEND
DFMD19	EXTEND
DFMD23	EXTEND
DFMD24	EXTEND
DFMD26	EXTEND
DFMD27	EXTEND

- B. If the keywords and values are as required above, there is NO FINDING.
- C. If the keywords and values are NOT as required above, there is a FINDING.

CCI: CCI-000035

___**STIG ID: ZCTDR060**

Default Severity: Category II

- A. Interview the systems programmer responsible for the BMC CONTROL-D. Determine if the site has modified the following security exit(s):
- CTDSE01
 - CTDSE04
 - CTDSE08
 - CTDSE19
 - CTDSE24
 - CTDSE28
1. Ensure the above security exit(s) has (have) not been modified.
 2. If the above security exit(s) has (have) been modified, ensure that the security exit(s) has (have) been approved by the site systems programmer and the approval is on file for examination.
- B. If the exits have not been modified, or were modified with system programmer approval on file, then there is NO FINDING.
- C. If the exits have been modified and NO system programmer approval is on file, then there is FINDING.

CCI: CCI-000035

- A. Check with your IOA or Systems Programming personnel and compile the list of BMC CONTROL-D Installation Datasets. Most likely they are similar to:SYS2.IOA.*.CTD*,** or SYS3.IOA.*.CTDI.**
1. From the Administrator Main Menu Choose Option 2 Security Server Commands.
 2. Choose Option 3 Data Set.
 3. Type the resource names collected in option A) above into: "Enter fully qualified (without quotes) data set or profile name:".
 4. Hit enter.
 5. Enter Y for Display covering profile?
 6. Verify that the UACC is NONE.
 7. Verify that Audit Successes and Failures specify UPDATE or READ.
 8. Tab down to Standard Access Permits and place an E next to it and hit enter and verify that UPDATE or higher access is limited to Systems Programming personnel. Verify Read access is given to:
 - a. Auditors
 - b. BMC Users
 - c. Security Personnel (Centralized)
 - d. Security Personnel (De-centralized)
 - e. BMC STCs
 - f. Batch Users.
 9. If Conditional Access Permits: _ (E to edit data) has *data is present* next to it, place an E next to it and validate that conditional access permits of Update or higher are limited to Systems Programming personnel as well. Verify Read access is given to Authorized Users if applicable.
 10. Repeat steps 2 through 10 for all datasets in option A).above.
- B. If A.7, A.8, A.9 and A.10 are all true, there is NO FINDING.
- C. If A.7, A.8, A.9 and A.10 are not true, this is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

- A. Check with your IOA or Systems Programming personnel and compile the list of BMC Control-D STC and/or batch datasets. Most likely they are similar to SYS3.IOA.*.CTDO.*.
1. From the Administrator Main Menu Choose Option 2 Security Server Commands
 2. Choose Option 3 Data Set
 3. Type the resource names collected in option A) above into: Enter fully qualified (without quotes) data set or profile name.
 4. Hit enter.
 5. Enter Y for Display covering profile?
 6. Verify that the UACC is NONE.
 7. Verify that Audit Successes and Failures specify UPDATE or READ.
 8. Tab down to Standard Access Permits and place an E next to it (hit enter). Validate that UPDATE or higher access is limited to Systems Programming personnel, BMC STCs and/or Batch users. Validate that UPDATE access is permitted to centralized and decentralized users. Verify Read access is permitted to Auditors and Control-D end-users.
 9. If Conditional Access Permits: _ (E to edit data) has *data is present* next to it, place an E next to it and hit enter. Validate that UPDATE or higher access is limited to Systems Programming personnel, BMC STCs and/or Batch users. Validate that UPDATE access is permitted to centralized and decentralized users. Verify Read access is permitted to Auditors and Control-D end-users.
 10. Repeat steps 1 through 9 for all datasets in option A) above.
- B. If A.7, A.8, A.9 and A.10 are all true, there is NO FINDING.
- C. If A.7, A.8, A.9 and A.10 are not true, this is a FINDING.

- A. Check with your IOA or Systems Programming personnel and compile the list of CONTROL-D user data sets. Most likely: they are similar to:
- SYS3.IOA.*.CTDR.**
 - CTRUSR.**
 - CTDSRV.**
 - CTDJB1.**
- From the Administrator Main Menu Choose Option 2 Security Server Commands
 - Choose Option 3 Data Set
 - Type the resource names collected in option A) above into: "Enter fully qualified (without quotes) data set or profile name:".
 - Hit enter.
 - Enter Y for Display covering profile?
 - Verify that the UACC is NONE.
 - Verify that Audit Successes and Failures specify UPDATE or READ.
 - Tab down to Standard Access Permits and place an E next to it (hit enter).
 - Validate Read access is limited to Auditors and any of the rest of the users below.
 - Validate that UPDATE access is permitted to centralized and decentralized security personnel, and CONTROL-D end users and any of the rest of the users below.
 - Validate that UPDATE or higher access is permitted to Systems Programming personnel AND BMC STCs AND Batch Users.
 - If Conditional Access Permits: _ (E to edit data) has *data is present* next to it, place an E next to it and hit enter.
 - Validate Read access is limited to Auditors and any of the rest of the users below.
 - Validate that UPDATE access is permitted to centralized and decentralized security personnel, and CONTROL-D end users and any of the rest of the users below.
 - Validate that UPDATE or higher access is permitted to Systems Programming personnel AND BMC STCs AND Batch Users.
 - Repeat steps 1 through 9 for all datasets in option A) above.
- B. If A.7, A.8, A.9 and A.10 are all true, there is NO FINDING.
- C. If A.7, A.8, A.9 and A.10 are not true, this is a FINDING.

Verify that the access to resources in the BMC CONTROL-D Resources table in the z/OS STIG Addendum are properly restricted.

NOTE: To determine what resource class is used review the IOACCLASS setting in SECPARM to determine the resource class to use. Refer to ZIOA0040 for this setting.

- A. Verify the resources identified in the BMC CONTROL-D Resources table in the z/OS STIG Addendum are properly defined and access is restricted to the appropriate personnel. For all the PROFILES found in BMC CONTROL-D Resources table in the z/OS STIG Addendum:
 1. From the Administrator Main Menu Choose Option 3 Security Server Reports
 2. Choose Option: 4 General Resource Profile
 3. On the command line choose option 4 AND then Put (* or \$\$*) next to PROFILE: and (class name from ZIOA0040) next to CLASS:
 - Profile: from table (or specify \$\$* as all profile start with a \$\$)
 - Class: from ZIOA0040
 4. Hit enter.
 5. Verify that the UACC for all profiles listed is NONE
 6. Place an S next to the profile and validate that the access list is appropriate (as defined or more restrictive than the BMC CONTROL-D Resources table in the z/OS STIG Addendum. If TYPE is GROUP, place an S in the CMD line and hit enter to explode the GROUP.
 7. For all resources with logging requirements place an LR next to the profile (hit enter and review the output) and validate that it specifies ALL(READ).
- B. If all profiles, access lists, and Auditing are defined like or more restrictive than the BMC CONTROL-D Resources table in the z/OS STIG Addendum, then there is NO FINDING.
- C. If any Profile, Access list or Auditing is more permissive than the BMC CONTROL-D Resources table in the z/OS STIG Addendum, then there is a FINDING.

CCI: CCI-000035

CCI: CCI-002234

- A. Verify that the BMC CONTROL-D Started Task name is properly identified / defined to the system ACP.
1. From Analyzer main Menu, go to 3;4; Press ENTER
 2. Key in SORT PROCNAME; Press ENTER
 3. Key in L CONTROLD; Press ENTER
 4. If not found then CONTROLD; is not defined to RACF as a STC user.
 5. If found then use the U line command to determine if the userid is defined to RACF.
 6. The userid is defined to RACF if a userid display appears. If not defined you should see the message No data to display.
 7. Now press f3 to go back to the previous display. If no R is next to the entry then the user is protected.
 8. If an R is next to the entry, place an M on the command line and validate the following is NOT displayed:
 - VSA346R The user ID does not have the protected attribute.
- B. If the userid for the CONTROL-D started task is defined to the security database and is protected, there is NO FINDING.
- C. If the userid for the CONTROL-D started task is not defined to the security database, or is defined but does not have the protected attribute, this is a FINDING.

- A. Use Vanguard's Analyzer product to look at the Started Procedures Analysis report:
 - 1. From Analyzer main Menu, go to 3;4; Press ENTER
 - 2. Key in SORT PROCNAME; Press ENTER
 - 3. Key in L CONTROLD; Press ENTER
 - 4. Look at the source column. It will indicate STARTED class profile or ICHRIN03 entry.
 - 5. If not found then CONTROLD is not defined to RACF as a STC user.
- B. If a STARTED resource class profile exists for the CONTROLD STC, there is NO FINDING.
- C. If neither a STARTED resource class profile or an ICHRIN03 entry exists for the CONTROLD STC, this is a FINDING.

CCI: CCI-000764