



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

### **z/OS CA VTape for RACF STIG Analysis Process and Checklist**

*Modeled After:  
SRR REVIEW PROCEDURES  
z/OS VTape for RACF Checklist  
Developed by DISA for the DOD  
Version 6 Release 4  
January 2015*

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

DISA Version 6.28

Document Number VTA\_STIG-08012016-105400-628A

August, 2016

## 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: ZVTAR000 ..... 4

\_\_\_STIG ID: ZVTAR001 ..... 5

\_\_\_STIG ID: ZVTAR030 ..... 5

\_\_\_STIG ID: ZVTAR032 ..... 7

**UNCLASSIFIED**  
z/OS CA VTAPE for RACF Analysis and Checklist  
*Version 6 Release 4*

\_\_\_**STIG ID: ZVTAR000**

**Default Severity:** Category II

- a. Check with your IOA or Systems Programming personnel and compile the list of CA VTAPE Installation Datasets, Likely:
  1. SYS2.VTAPE.\*\*  
SYS3.VTAPE.\*\*
  2. From the Administrator Main Menu Choose Option 2 Security Server Commands
  3. then choose Option: 3 Data Set
  4. Type the resource names collected in option a.1 above into: Enter fully qualified (without quotes) data set or profile name:
  5. Hit enter.
  6. Enter Y for Display covering profile? Y
  7. Verify that the UACC is NONE
  8. Verify that Audit Successes and Failures specifies UPDATE or READ.
  9. Tab down to Standard Access Permits and place an E next to it (hit enter) and validate that UPDATE or higher access is limited to Systems Programming personnel.  
Restrict Read access to only authorized users (ie, not UACC(READ) but ID(\*) is permitted.
  10. 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. Restrict Read access to only authorized users (ie, not UACC(READ) but ID(\*) is permitted.
  11. Repeat steps 2 through 10 for all datasets in option a.1.
- 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

**UNCLASSIFIED**  
z/OS CA VTAPE for RACF Analysis and Checklist  
*Version 6 Release 4*

\_\_\_**STIG ID: ZVTAR001**

**Default Severity:** Category II

- a. Check with your IOA or Systems Programming personnel and compile the list of CA VTAPE product installation data sets. Likely these data set names will start with SYS3.VTAPE.
- b. Do the following:
  1. From the Administrator Main Menu Choose Option 2 - Security Server Commands
  2. Then choose Option 3 - Data Set
  3. Tab to 'Enter fully qualified (without quotes) data set or profile name:' and enter the name of the first CA VTAPE product installation data set found in a. above.
  4. Hit Enter.
  5. For the resulting pop-up, select 'Y' when prompted with 'Display covering profile?'.
  6. On the next screen ,
    - a) Verify that the UACC is NONE
    - b) Verify that all accesses of UPDATE or higher (i.e., failures and successes) will be logged. Look at the section of the screen under 'Audit:'. Next to 'Successes' and 'Failures' you should see 'Update'.
    - c) Tab down to 'Standard Access Permits' and type an 'E' and hit Enter.
    - d) On the next screen verify that UPDATE, and/or ALTER access is permitted to systems programming personnel, tape management personnel (tape librarians and any other users that perform control, initialization, and maintenance of the systems tape library) and CA VTAPE STCs and/or CA VTAPE batch userids.
    - e) Check if the 'Conditional Access Permits:' section on the screen has the phrase "\*data is present\*" next to it. If so, enter an 'E' on the line and hit 'Enter' to get a list of who has Conditional Access Permits.
    - f) Verify that Conditional Access Permits of UPDATE, and/or ALTER access are restricted to systems programming personnel, tape management personnel (tape librarians and any other users that perform control initialization and maintenance of the systems tape library) and CA VTAPE STCs and/or CA VTAPE batch userids.
    - g) Repeat steps 3 through 6 for all the CA VTAPE datasets found in a. above.
- c. If 6a, 6b, 6d and 6f above are all true, there is NO FINDING.
- d. If 6a, 6b, 6d and 6f above are NOT all true, there is a FINDING

**CCI:** CCI:-001499

**UNCLASSIFIED**  
z/OS CA VTape for RACF Analysis and Checklist  
*Version 6 Release 4*

\_\_\_**STIG ID: ZVTAR030**

**Default Severity:** Category II

- a. Use Vanguard's Analyzer product to look at the Started Procedures Analysis report: Do the following for the VTape started task, likely called SVSTS or SVTSAS
  1. From Analyzer main Menu, go to 3;4; Press <ENTER>
  2. Key in SORT PROCNAME; Press <ENTER>
  3. Key in L **SVSTS or SVTSAS (or the name of the Vtape Started task)**; Press <ENTER>
  4. If not found then **the VTape Started Task** is not defined to RACF as a STC user.
  5. If found but has a R in the M column, review the message and ensure that the following does not appear: VSA346R The user ID does not have the protected attribute. If message exists, then user does not have the PROTECTED attribute. This is a finding.
  6. If found then you would use the "U" line command to determine if the userid is defined to RACF.
  7. Key the "U" line command for the **SVSTS or SVTSAS or VTape started task entry**; Press <ENTER>
  8. The userid is defined to RACF if a userid display appears. If not defined you should see the message "Unable to display".
- b. If the userid for the VTape started task is defined to the security database with the PROTECTED attribute, there is NO FINDING.
- c. If the userid for the VTape started task is not defined to the security database or does not have the PROTECTED attribute, this is a FINDING.

**CCI:** CCI-000764

**UNCLASSIFIED**  
z/OS CA VTape for RACF Analysis and Checklist  
*Version 6 Release 4*

\_\_\_**STIG ID: ZVTAR032**

**Default Severity:** Category II

- a. Use Vanguard's Analyzer product to look at the Started Procedures Analysis report: The name of the VTape started task is likely SVTS or SVTSAS.
  1. From Analyzer main Menu, go to 3;4; Press <ENTER>
  2. Key in SORT PROCNAME; Press <ENTER>
  3. Key in L SVTS or SVTSAS ; Press <ENTER>
  4. Look at the source column. It will indicate STARTED class profile or ICHRIN03 entry.
  5. If not found then the VTape started task is not defined to RACF as a STC user.
- b. If a **STARTED** resource class profile exists for the started tasks SVTS or SVTSAS, there is NO FINDING.
- c. If neither a **STARTED** resource class profile or an ICHRIN03 entry exists for the started task for VTape, this is a FINDING.

**CCI:** CCI-000764