

Beyond Best Practices: The DISA STIGs

Jim McNeill
Vanguard Integrity Professionals

Outline

Terms and Terminology
History of the STIGS
Categories of STIG Checks
Individual STIGS
Anatomy of a STIG

Terms and Terminology

Terms and Terminology

Defense Information Systems Agency (DISA)

A United States Department of Defense combat support agency with the goal of providing real-time information technology (IT) and communications support to the President, Vice President, Secretary of Defense, the military Services, and the Combatant Commands.

National Institute of Standards and Technology (NIST)

Publishes configuration controls that must be used by each Federal Agency and by all contractors processing data for a federal agency.

Security Technical Implementation Guide (STIG)

A configuration document used to standardized security controls for software and hardware systems. Each **STIG** check in the SRR checklist is mapped to IA Controls defined in **DoD Directive 8500.2**.

Information Assurance (IA)

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Department of Defense (DoD)

The U.S. federal department charged with coordinating and supervising all agencies and functions of the government relating directly to national security and the United States armed forces.

DoD Directive 8500.1

Requires that “all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines” and tasks **DISA** to “develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA.”

DoD IA Controls

The Department of Defense Information Assurance (IA) program establishes a baseline set of controls to be applied to all DoD information systems. Each control is uniquely named and can be referenced, measured, and reported against throughout the life cycle of a DoD information system.

Security Readiness Review (SRR)

The audit performed at designated sites to review compliance with the **DISA STIGs**.

SRRAUDIT

The name assigned to the **SSR** audit process to validate compliance with the **DISA STIGs**.

DHS

Department of Homeland Security

Checks

A specific vulnerability test or configuration control. Each Check gets its first few characters from the category of checks it is in.

For example, ACP00282 – Access Control Program (ACP)

Checklist

Refers to the list of **checks** that are to be performed as part of the **SRR**

Checklist Result

Outcome of a check - Open, Not A Finding, Not Reviewed, Not Applicable

Finding Severities

Category I - Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.

Category II - Vulnerabilities that provide information that have a high potential of giving access to an intruder.

Category III - Vulnerabilities that provide information that potentially could lead to compromise.

NCP

National Checklist Program (Part of the NVD)

NVD

National Vulnerability Database (hosted by NIST and DHS)

Vulid

Vulnerability Identification

XCCDF

eXtensible Configuration Checklist Description Format

SCAP

Security Content Automation Protocol

OMB

Office of Management and Budget

VANGUARD
INTEGRITY PROFESSIONALS, INC.
enterprise security software

History of the STIGS

©2010 Vanguard Integrity Professionals, Inc. 9 IBM Business Partner Server Proven

History of the STIGS

VANGUARD
INTEGRITY PROFESSIONALS, INC.
enterprise security software

DOD issues Directive 8500.1 (OCT 2002)

Its purpose is to establish policy and assign responsibilities in order to achieve Department of Defense (DoD) information assurance (IA).

DISA created the STIGS in response to DoD 8500.1

The term STIGS was coined by DISA who creates configuration documents in support of the United States Department of Defense (DoD). The implementation guidelines include recommended administrative processes and span over the lifecycle of the device.

10 IBM Business Partner Server Proven

NIST Publishes Security Configuration Controls.

They do not include mainframe configuration controls.

NIST controls lead to the SCAP standard.

NIST Co-hosts with DHS a security configuration checklist at the NVD.

NIST 800-53 rev 3 included security controls in its catalog for both national security and non-national security systems.

DISA converts STIGS to SCAP format

DISA converts the STIGS to XCCDF format, the first step toward SCAP.
SP 800-126

NIST adopts STIGS

The NVD now contains checklist for the mainframe in the NCP.

OMB mandate

If NIST has a standard, all Federal agencies and all contractors processing data for a federal agency must conform to those standards.

History of the STIGS

VANGUARD
INTEGRITY PROFESSIONALS, INC.
enterprise security software

Version 4, Release 1.3, Feb. 2004

Version 4, Release 1.4, Oct. 2004

Version 4, Release 1.5, July 2005

Version 5, Release 1.1, April 2006

Version 5, Release 2.1, Nov. 2006

Version 5, Release 2.2, March 2007

Version 5, Release 2.3, May 2007

Version 5, Release 2.6, Nov. 2007

Version 5, Release 2.10, Dec. 2008

13

IBM Business Partner Server Proven

History of the STIGS

VANGUARD
INTEGRITY PROFESSIONALS, INC.
enterprise security software

Version 5.2.10

The last release of the STIG Guideline (1000 page booklet that contained all the rationale behind the configuration control).

Version 6.1

This release and all subsequent released as SRR checklists only.

Version 6.2

XCCDF expressed checklist in line with Security Content Automation Protocol (SCAP). NIST 800-126

Version 6.14

Released on Jan 25, 2013 is the current release.

14

IBM Business Partner Server Proven

VANGUARD
INTEGRITY PROFESSIONALS, INC.
enterprise security software

Categories of STIG Checks

©2010 Vanguard Integrity Professionals, Inc. 15 IBM Business Partner Server Proven

VANGUARD
INTEGRITY PROFESSIONALS, INC.
enterprise security software

Categories of STIG Checks

- z/OS Data Analysis (AAMV)
- Security Server (RACF) Data Analysis (ACP, RACF)
- CA-1 (Tape Management System) Data Analysis (ZCA1)
- CICS Data Analysis (ZCIC)
- CL/Supersession Data Analysis (ZCLS)
- DBMS Data Analysis (ZDBM)
- Front End Processor Data Analysis (ZFEP)
- IBM Communications Server Data Analysis (IFTP,ISLG,ITCP,ITNT,IUTN)
- Integrated Cryptographic Services Facility (ZICS)
- Integrated Database Management System (IDMS) Data Analysis (ZIDM)
- BMC Control-D, Control-M, Control-O and IOA checks (ZCDT, ZCDM, ZCDO,ZIOA)
- CA – Auditor checks (ZADT)
- JES2 Data Analysis (ZJES)
- NC-Pass Data Analysis (ZNCP)

16 IBM Business Partner Server Proven

Categories of STIG Checks

SDSF Data Analysis (ZISF)
DFSMS Data Analysis (ZSMS)
TSO Data Analysis (ZTSO)
UNIX System Services Data Analysis (ZUSS)
VTAM Data Analysis (ZVTM)
WebSphere Application Server for z/OS Analysis (ZWAS)
WebSphere MQSeries for z/OS Analysis (ZWMQ)
Hardware Configuration Definition (ZHCD)
Tivoli Asset Discovery (ZTAD)
Catalog Solutions (ZCSL)
Roscoe (ZROS)
SRR Audit (ZSRR)
Transparent Data Migration Facility Data Analysis (ZTDM)
NetView Data Analysis (ZNET)
Vanguard Security Solutions (ZVSS)

17

Categories of STIG Checks

CA Common Services (ZCCS)
CA MIM (ZMIM)
CA VTape (ZVTA)
Compuware Abend-AID (ZAID)
IBM CSSMTP (ZSMT)
IBM Health Checker (ZHCK)
IBM SDSF (SDSF)
QWEST NC-PASS (ZNCP)

18

Individual STIGS

OS/390 & z/OS Data Analysis (AAMV)

- AAMV0010** A CMP (Change Management Process) is not being utilized on this system
- AAMV0012** Unsupported system software is installed and active on the system
- AAMV0014** Site does not have a formal migration plan for removing or upgrading OS systems software prior to the date the vendor drops security patch support
- AAMV0016** The IAO or Site does not subscribe to the DOD-CERT/VCTS (Vulnerability Compliance Tracking System) bulletin mailing list.
- AAMV0018** Site does not maintain documented procedures to apply security related software patches to their system and does not maintain a log of when these patches were applied
- AAMV0030** LNKAUTH=APFTAB is not specified in the IEASYSxx member(s) in the currently active parmlib data set(s).
- AAMV0040** Inaccessible APF libraries defined
- AAMV0050** Duplicated sensitive utilities and/or programs exist in APF libraries
- AAMV0160** Inapplicable PPT entries have not been invalidated
- AAMV0325** Non-existent or inaccessible Link Pack Area (LPA) libraries
- AAMV0350** Non-existent or inaccessible LINKLIST libraries
- AAMV0370** Non-standard SMF data collection options specified
- AAMV0380** Required SMF data record types not being collected
- AAMV0400** An automated process is not in place to collect and retain SMF data
- AAMV0410** ACP database is not on a separate physical volume from its backup and recovery datasets.
- AAMV0420** ACP database is not backed up on a scheduled basis documented correctly

- AAMV0430** System DASD backups are not performed on a regularly scheduled basis
- AAMV0440** PASSWORD data set and OS passwords are utilized
- AAMV0450** System programs (e.g., exits, SVCs, etc.) are in use without DAA approval and/or are not documented correctly
- AAMV0500** Sensitive and critical system data sets exist on shared DASD

- ACP00010** SYS1.PARMLIB is not limited to only system programmers.
- ACP00020** Access to SYS1.LINKLIB is not properly protected
- ACP00030** Update and Allocate access to SYS1.SVCLIB is not limited to system programmers only
- ACP00040** Update and allocate access to SYS1.IMAGELIB is not limited to system programmers only.
- ACP00050** Update and allocate access to SYS1.LPALIB is not limited to system programmers only
- ACP00060** Update and allocate access to all APF authorized libraries are not limited to system programmers only
- ACP00070** Update and allocate access to all LPA libraries are not limited to system programmers only.
- ACP00080** Update and allocate access to SYS1.NUCLEUS is not limited to system programmers only.
- ACP00100** Update and allocate access to libraries that contain PPT modules are not limited to system programmers only
- ACP00110** Update and allocate access to LINKLIST libraries are not limited to system programmers only
- ACP00120** Update and allocate access to ACP files and/or databases are not limited to system programmers and/or security personnel
- ACP00130** Access Greater than Read to the System Master Catalog is not limited to system programmers only.
- ACP00135** Allocate access to system user catalogs are not limited to system programmers only.
- ACP00140** Update and allocate access to all system-level product installation libraries are not limited to system programmers only

- ACP00150** Update and allocate access to the JES2 System data sets (e.g., Spool, Checkpoint, and Initialization parameters) are not limited to system programmers only
- ACP00170** Allocate access to SYS1.UADS is not limited to system programmers only and read and update access is not limited to system programmer personnel and/or security personnel
- ACP00180** Update and allocate access to SMF collection files (i.e., SYS1.MANx) are not limited to system programmers and/or batch jobs that perform SMF dump processing.
- ACP00190** Update and allocate access to data sets used to backup and/or dump SMF collection files are not limited to system programmers and/or batch jobs that perform SMF dump processing.
- ACP00200** Access to SYSTEM DUMP data sets are not limited to system programmers only
- ACP00210** Update and allocate access to System backup files are not limited to system programmers and/or batch jobs that perform DASD backups.
- ACP00220** Access to SYS(x) TRACE is not limited to system programmers only
- ACP00230** Access to System page data sets (i.e., PLPA, COMMON, and LOCALx) are not limited to system programmers.
- ACP00240** Update and allocate access to Libraries containing EXIT modules are not limited to system programmers only
- ACP00250** Update and alter access to all system proclib datasets are limited to system programmers only
- ACP00260** Memory and privileged program dumps are not protected in accordance with proper security requirements
- ACP00270** Dynamic lists are not protected in accordance with proper security requirements.

- ACP00282** z/OS system commands are improperly protected.
- ACP00291** The system programmer will ensure that the CONSOLxx members are properly configured.
- ACP00292** MCS consoles userid(s) are improperly protected
- ACP00293** MCS consoles access authorization(s) for CONSOLE resource(s) is (are) improperly protected.
- ACP00294** Users that have access to the CONSOLE resource in the TSOAUTH resource class are not properly defined
- ACP00320** The ACP audit logs are not reviewed on a regular basis
- ACP00330** User accounts defined to the ACP do not uniquely identify system users
- ACP00340** z/OS Baseline reports are not reviewed and validated to ensure only authorized changes have been made within the z/OS operating system. This is a current DISA requirement for change management to system libraries.
- ACP00350** IEASYMUP resource will be protected in accordance with proper security requirements

Security Server Data Analysis (RACF)

- RACF0244** FACILITY resource class is inactive
- RACF0246** The OPERCMDS resource class is not active.
- RACF0248** MCS consoles are not active
- RACF0250** The Automatic Data Set Protection (ADSP) SETROPTS value is not set to NOADSP
- RACF0260** The AUDIT SETROPTS value is improperly set.
- RACF0270** The CLASSACT SETROPTS has not been specified for the DATASET, USER, and GROUP Classes.
- RACF0280** The CMDVIOL SETROPTS value is not set to CMDVIOL
- RACF0290** The EGN SETROPTS value specified is not set to EGN
- RACF0300** The ERASE ALL SETROPTS value is not set to ERASE() on unclassified systems and ERASE(ALL) on Classified systems
- RACF0310** The GENCMD SETROPTS value is not enabled for ACTIVE classes
- RACF0320** The GENERIC SETROPTS value is not enabled for ACTIVE classes
- RACF0330** The TERMINAL SETROPTS value is not set to READ
- RACF0350** The GRPLIST SETROPTS value is not set to ACTIVE
- RACF0360** The INACTIVE SETROPTS value is not set to 35 days
- RACF0370** The INITSTATS SETROPTS value is not set to INITSTATS.
- RACF0380** The JES(BATCHALLRACF) SETROPTS value is not set to JES(BATCHALLRACF)
- RACF0400** The JES(XBMALLRACF) SETROPTS value is not set to JES(XBMALLRACF).
- RACF0420** The OPERAUDIT SETROPTS value is not set to OPERAUDIT.
- RACF0430** The PASSWORD(HISTORY) SETROPTS value is not set to 10
- RACF0440** The PASSWORD(INTERVAL) SETROPTS value is not set to 60 days

Security Server Data Analysis (RACF)

- RACF0450** The PASSWORD(REVOKE) SETROPTS value specified is not in accordance with security requirements
- RACF0460** The PASSWORD(RULEn) SETROPTS value(s) specified is/are improperly set
- RACF0470** The PASSWORD(WARNING) SETROPTS value is improperly set
- RACF0480** The PROTECTALL SETROPTS value specified is improperly set
- RACF0490** The REALDSN SETROPTS value specified is improperly set
- RACF0500** The RETPD SETROPTS value specified is improperly set
- RACF0510** The RVARYPW SETROPTS value specified is improperly set
- RACF0520** The SAUDIT SETROPTS value specified is improperly set
- RACF0530** The SECLEVELAUDIT SETROPTS value specified is improperly set
- RACF0550** The TAPEDSN SETROPTS value specified is improperly set
- RACF0560** The WHEN(PROGRAM) SETROPTS value specified is not active
- RACF0570** RACF users do not have the required default fields
- RACF0580** There are interactive USERIDs defined to RACF that do not have the required fields completed
- RACF0590** RACF batch jobs are improperly secured
- RACF0595** Batch jobs are improperly defined
- RACF0600** RACF batch jobs are not protected with propagation control
- RACF0620** Started Tasks are not properly identified to RACF
- RACF0650** Started Tasks are improperly defined to RACF.
- RACF0660** There are started tasks defined to RACF with the trusted attribute that are not justified.

Security Server Data Analysis (RACF)

- RACF0680** Maintenance USERIDs are improperly controlled
- RACF0690** Emergency USERIDs are improperly defined.
- RACF0710** The use of the RACF SPECIAL Attribute is not justified
- RACF0720** Assignment of the RACF OPERATIONS attribute to individual usersids is not fully justified
- RACF0730** The use of the RACF AUDITOR privilege is not justified
- RACF0740** The number of USERIDs possessing the Tape Bypass Label Processing (BLP) privilege is not justified
- RACF0760** DASD Volume level protection does not exist or is improperly defined
- RACF0770** Access to sensitive utilities is not properly protected by RACF

CA-1 (Tape Management System) Data Analysis (ZCA1)

- ZCA10041** CA 1 Tape Management system password will be changed from the default.
- ZCA10060** CA 1 Tape Management exits when in use will be reviewed and/or approved.
- ZCA1R000** CA 1 Tape Management installation data sets will be properly protected
- ZCA1R003** CA 1 Tape Management TMC, AUDIT and optional RDS and VPD data sets will be properly protected
- ZCA1R020** CA 1 Tape Management command resources will be properly defined and protected.
- ZCA1R021** CA 1 Tape Management function and password resources will be properly defined and protected
- ZCA1R030** CA 1 Tape Management Started Task name will be properly identified and/or defined to the system ACP.
- ZCA1R032** CA 1 Tape Management Started task will be properly defined to the STARTED resource class for RACF.
- ZCA1R038** CA 1 Tape Management Resource Class will be defined or active in the ACP.
- ZCA1R040** CA 1 Tape Management external security options will be specified properly

ZDBM0010 Database management systems do not interface with the access control product to perform identification and authentication

ZFDR0000 Fast Dump Restore (FDR) install data sets are not properly protected.

ZFDR0040 FDR (Fast Dump Restore) security options are improperly specified.

CICS Data Analysis (ZCIC)

- ZCIC0010** CICS system data sets are not properly protected
- ZCIC0020** Sensitive CICS transactions are not protected in accordance with security requirements.
- ZCIC0030** CICS System Initialization Table (SIT) parameter values are not specified in accordance with proper security requirements
- ZCIC0040** CICS region logonid(s) are not defined and/or controlled in accordance with the security requirements
- ZCIC0041** CICS default logonid(s) are not defined and/or controlled in accordance with the security requirements
- ZCIC0042** CICS logonid(s) do not have time-out limit set to 15 minutes
- ZCICR021** External RACF Classes are not active for CICS transaction checking
- ZCICR021** IBM CICS Transaction Server SPI command resources will be properly defined and protected.
- ZCICR041** CICS regions are improperly protected to prevent unauthorized propagation of the region userid

Front End Processor (FEP) Data Analysis (ZFEP)

- ZFEP0011** All hardware components of the FEPs are not placed in secure locations where they cannot be stolen, damaged, or disturbed
- ZFEP0012** Procedures are not in place to restrict access to FEP functions of the service subsystem from operator consoles (local and/or remote), and to restrict access to the diskette drive of the service subsystem.
- ZFEP0013** A documented procedure is not available instructing how to load and dump the FEP NCP (Network Control Program)
- ZFEP0014** An active log is not available to keep track of all hardware upgrades and software changes made to the FEP (Front End Processor ZFEP0015 NCP Dataset Analysis)
- ZFEP0015** NCP (Net Work Control Program) Data set access authorization does not restricts UPDATE and/or ALLOCATE access to appropriate personnel
- ZFEP0016** A password control is not in place to restrict access to the service subsystem via the operator consoles (local and/or remote) and a key-lock switch is not used to protect the modem supporting the remote console of the service subsystem.

Hardware Configuration Definition (ZHCD)

- ZHCDR000** IBM Hardware Configuration Definition (HCD) install data sets are not properly protected.
- ZHCDR002** IBM Hardware Configuration Definition (HCD) User data sets are not properly protected.
- ZHCDR020** IBM Hardware Configuration Definition (HCD) resources are not properly defined and protected.

IBM Communications Server Data (IFTP)

- IFTP0010** The FTP Server daemon is not defined with proper security parameters
- IFTP0020** The startup parameters for the FTP include the ANONYMOUS, ANONYMOUS=, or INACTIVE keywords. The FTP daemon's started task JCL does not specify the SYSTCPD and SYSFTPD DD statements for configuration files.
- IFTP0030** FTP.DATA configuration statements for the FTP Server are not specified in accordance with requirements
- IFTP0040** User exits for the FTP Server are in use without proper approval or proper documentation
- IFTP0050** The warning banner for the FTP Server is not specified properly
- IFTP0060** SMF recording options for the FTP Server are not configured to write SMF records for all eligible events
- IFTP0070** The permission bits and user audit bits for HFS objects that are part of the FTP Server component are not properly configured IFTP0080 Configuration Files Access and Audit
- IFTP0080** MVS data sets for the FTP Server are not properly protected.
- IFTP0090** The TFTP Server program is not properly protected
- IFTP0100** FTP / Telnet unencrypted transmissions require Acknowledgement of Risk Letter (AORL)
- IFTP0110** FTP Control cards will be properly stored in a secure PDS file.

IBM Communications Server Data (ISLG)

VANGUARD
INTEGRITY PROFESSIONALS, INC.
enterprise security software

- ISLG0010** The Syslog daemon is not started at z/OS initialization.
- ISLG0020** The Syslog daemon is improperly defined and secured
- ISLG0030** The permission bits and user audit bits for HFS objects that are part of the Syslog daemon component are not configured properly

35

IBM Business Partner **Server Proven**

IBM Communications Server Data (ITCP)

VANGUARD
INTEGRITY PROFESSIONALS, INC.
enterprise security software

- ITCP0010** Configuration files for the TCP/IP stack are not properly specified.
- ITCP0020** TCPIP.DATA configuration statements for the TCP/IP stack are not properly specified.
- ITCP0025** The hosts identified by the NSINTERADDR statement are not properly protected.
- ITCP0030** PROFILE.TCPIP configuration statements for the TCP/IP stack are not coded properly.
- ITCP0040** The permission bits and user audit bits for HFS objects that are part of the Base TCP/IP component are not configured properly
- ITCP0050** Resources for the Base TCP/IP component are improperly protected.
- ITCP0060** Started tasks for the Base TCP/IP component are not defined in accordance with security requirements
- ITCP0070** MVS data sets for the Base TCP/IP component are not properly protected

36

IBM Business Partner **Server Proven**

IBM Communications Server Data (ITNT)

- ITNT0010** PROFILE.TCPIP configuration statements for the TN3270 Telnet Server are not properly specified.

- ITNT0020** VTAM session setup controls for the TN3270 Telnet Server are not properly specified

- ITNT0030** The warning banner for the TN3270 Telnet Server is not specified or properly specified.

- ITNT0040** The use of Digital Certificates is not implemented in accordance with security requirements

- ITNT0050** SSL encryption options for the TN3270 Telnet Server are not specified or specified properly for each statement that defines a SECUREPORT

- ITNT0060** SMF recording options for the TN3270 Telnet Server are not properly specified

IBM Communications Server Data (IUTN)

- IUTN0010** The startup user account for the z/OS UNIX Telnet Server is not defined properly

- IUTN0020** Startup parameters for the z/OS UNIX Telnet Server are not specified properly

- IUTN0030** The warning banner for the z/OS UNIX Telnet Server is not specified or not properly specified.

- IUTN0040** HFS objects for the z/OS UNIX Telnet Server are not properly protected

Integrated Cryptographic Services Facility (ZICS)

- ZICSR000** IBM Integrated Crypto Service Facility (ICSF) install data sets are not properly protected.
- ZICSR001** IBM Integrated Crypto Service Facility (ICSF) STC data sets are not properly protected.
- ZICSR030** IBM Integrated Crypto Service Facility (ICSF) Started Task name is not properly identified / defined to the system ACP.
- ZICSR032** IBM Integrated Crypto Service Facility (ICSF) Started task is not properly defined to the STARTED resource class for RACF.

Integrated Database Management System (ZIDM)

- ZIDM0010** IDMS is not using external security and/or the resource class is not configured properly to the IDMS-CV
- ZIDM0014** Each IDMS CV is not uniquely defined to the ACP IDMS resource class
- ZIDM0020** IDMS data set access authorization does not restricts UPDATE and/or ALLOCATE access to systems programming personnel
- ZIDM0030** IDMS regions (central versions) STC and or batch jobs are not defined in accordance with the proper security requirements
- ZIDM0032** IDMS regions (central versions) Userids/ACIDs are not defined to the PROPCNTL resource class

BMC IOA for RACF STIG (ZIOA)

- ZIOAR000** BMC IOA installation data sets will be properly protected
- ZIOAR001** BMC IOA STC data sets will be properly protected.
- ZIOAR002** BMC IOA User data sets will be properly protected
- ZIOAR020** BMC IOA resources will be properly defined and protected.
- ZIOAR030** BMC IOA Started Task name is not properly identified / defined to the system ACP.
- ZIOAR032** BMC IOA Started task(s) must be properly defined to the STARTED resource class for RACF
- ZIOAR040** BMC IOA configuration/parameter values are not specified properly.
- ZIOA0060** BMC IOA security exits are not installed or configured properly

BMC CONTROL-D for RACF STIG (ZCDT)

- ZCTD0040** BMC CONTROL-D configuration/parameter values are not specified properly
- ZCTD0060** BMC CONTROL-D security exits are not installed or configured properly
- ZCTDR000** BMC CONTROL-D installation data sets are not properly protected
- ZCTDR001** BMC CONTROL-D STC data sets are not properly protected
- ZCTDR002** BMC CONTROL-D User data sets are not properly protected
- ZCTDR020** BMC CONTROL-D resources are not properly defined and protected
- ZCTDR030** BMC CONTROL-D Started Task name is not properly identified / defined to the system ACP
- ZCTDR032** BMC CONTROL-D Started task is not properly defined to the STARTED resource class for RACF.

BMC CONTROL-O for RACF STIG (ZCTO)

- ZCTO0040** BMC CONTROL-O configuration/parameter values are not specified properly.
- ZCTO0041** BMC CONTROL-O configuration/parameter values are not specified properly.
- ZCTO0060** BMC CONTROL-O security exits are not installed or configured properly
- ZCTOR000** BMC CONTROL-O installation data sets are not properly protected
- ZCTOR001** BMC CONTROL-O STC data sets are not properly protected
- ZCTOR020** BMC CONTROL-O resources are not properly defined and protected.
- ZCTOR030** BMC CONTROL-O Started Task name is not properly identified / defined to the system ACP.
- ZCTOR032** BMC CONTROL-O Started task is not properly defined to the STARTED resource class for RACF.

BMC CONTROL-M for RACF STIG (ZCTM)

- ZCTM0060** BMC CONTROL-M security exits are not installed or configured properly.
- ZCTMR000** BMC CONTROL-M installation data sets are not properly protected.
- ZCTMR001** BMC CONTROL-M STC data sets are not properly protected.
- ZCTMR002** BMC CONTROL-M User data sets are not properly protected.
- ZCTMR003** BMC CONTROL-M User/Application JCL data sets are not properly protected
- ZCTMR020** BMC CONTROL-M resources are not properly defined and protected.
- ZCTMR030** BMC CONTROL-M Started Task name is not properly identified / defined to the system ACP.
- ZCTMR032** BMC CONTROL-M Started task is not properly defined to the STARTED resource class for RACF.
- ZCTMR040** BMC CONTROL-M configuration/parameter values are not specified properly

ZCTR000 BMC CONTROL-M/Restart installation data sets are not properly protected.

ZCTR002 BMC CONTROL-M/Restart Archived Sysout data sets are not properly protected.

ZADTR000 CA Auditor installation data sets are not properly protected.

ZADTR002 CA Auditor User data sets are not properly protected

ZADTR020 CA Auditor resources are not properly defined and protected

JES2 Data Analysis (ZJES)

- ZJES0011** RJE workstations and NJE nodes are not controlled in accordance with security requirements.
- ZJES0012** NJE nodes are not controlled in accordance with security requirements
- ZJES0014** RJE workstations and NJE nodes are not controlled in accordance with STIG requirements.

- ZJES0021** JES2 input sources are not controlled in accordance with the proper security requirements.
- ZJES0022** JES2 input sources are not properly controlled.

- ZJES0031** JES2 output devices are not controlled in accordance with the proper security requirements.

- ZJES0032** JES2 output devices are not properly controlled.

- ZJES0041** JESSPOOL resources are not protected in accordance with security requirements.

- ZJES0042** JESNEWS resources are not protected in accordance with security requirements.

- ZJES0044** JESTRACE and/or SYSLOG resources are not protected in accordance with security requirements.
- ZJES0046** JES2 spool resources are not controlled in accordance with security requirements.

- ZJES0052** JES2 system commands are not protected in accordance with security requirements.

- ZJES0060** Surrogate users are not controlled in accordance with proper security requirements.

NC-Pass Data Analysis (ZNCPR)

- ZNCPR000** Quest NC-Pass installation data sets will be properly protected.

- ZNCPR001** Quest NC-Pass STC data sets will be properly protected.

- ZNCPR020** Quest NC-Pass will be used by Highly-Sensitive users.

- ZNCPR030** Quest NC-Pass Started Task name will be properly identified and/or defined to the system ACP.

- ZNCPR032** Quest NC-Pass Started task will be properly defined to the STARTED resource class for RACF.

- ZISF0005** SDSF product data sets do not restrict all update and alter access to systems programming personnel.
- ZISFR000** IBM System Display and Search Facility (SDSF) installation data sets will be properly protected
- ZISFR002** IBM System Display and Search Facility (SDSF) HASPINDEX data set identified in the INDEX parameter must be properly protected.
- ZISFR020** IBM System Display and Search Facility (SDSF) resources will be properly defined and protected.
- ZISFR021** IBM System Display and Search Facility (SDSF) resources will be properly defined and protected.
- ZISFR030** IBM System Display and Search Facility (SDSF) Started Task name will be properly identified and/or defined to the system ACP.
- ZISFR032** IBM System Display and Search Facility (SDSF) Started task will be properly defined to the STARTED resource class for RACF.
- ZISFR038** IBM System Display and Search Facility (SDSF) Resource Class will be active in the RACF.
- ZISF0040** IBM System Display and Search Facility (SDSF) Configuration parameters will be correctly specified.

- ZSMSR008** Active and Raclisted Classes Analysis
- ZSMS0010** DFSMS STGADMIN Class resources are not protected in accordance with security requirements
- ZSMS0012** DFSMS DGT resource in the PROGRAM resource class is not protected in accordance with security requirements
- ZSMS0014** DFSMS DFP Resource Ownership is not configured in accordance with security requirements
- ZSMS0020** DFSMS control data sets are not protected in accordance with security requirements
- ZSMS0022** DFSMS control data sets are not properly protected.
- ZSMS0030** SYS(x).Parmlib(IEFSSNxx) SMS configuration parameter settings are not properly specified
- ZSMS0032** SYS(x).PARMLIB(IGDSMSxx), SMS parameter settings are not properly specified

- ZTSO0020** There are LOGONIDs defined to SYS1.UADS for non-emergency use
- ZTSO0030** Unauthorized users possess access to the resource TSOAUTH

UNIX System Services Data Analysis (ZUSS)

- ZUSS0011** z/OS UNIX OMVS parameters in PARMLIB are not properly specified.
- ZUSS0012** z/OS UNIX BPXPRMxx security parameters in PARMLIB are not properly specified.
- ZUSS0013** z/OS UNIX HFS MapName files security parameters are not properly specified
- ZUSS0014** z/OS UNIX security parameters for restricted network service(s) in /etc/inetd.conf are not properly specified.
- ZUSS0015** z/OS UNIX security parameters in etc/profile are not properly specified
- ZUSS0016** z/OS UNIX security parameters in /etc/rc not properly specified
- ZUSS0021** BPX resource(s) is (are) not protected in accordance with security requirements.
- ZUSS0022** z/OS UNIX resources are not protected in accordance with security requirements.
- ZUSS0023** z/OS UNIX SUPERUSER resource is not protected in accordance with guidelines
- ZUSS0031** z/OS UNIX MVS data sets or HFS objects are not properly protected
- ZUSS0032** z/OS UNIX MVS data sets WITH z/OS UNIX COMPONENTS are not properly protected
- ZUSS0033** z/OS UNIX MVS data sets used as step libraries in /etc/steplib are not properly protected
- ZUSS0034** z/OS UNIX HFS permission bits and audit bits for each directory are not properly protected or specified.
- ZUSS0035** z/OS UNIX SYSTEM FILE SECURITY SETTINGS are not properly protected or specified.
- ZUSS0036** z/OS UNIX MVS HFS directory(s) with "other" write permission bit set are not properly defined.
- ZUSS0041** Attributes of z/OS UNIX user accounts are not defined properly
- ZUSS0042** z/OS UNIX each group is not defined with a unique GID.

UNIX System Services Data Analysis (ZUSS) (continued)

- ZUSS0043** The user account for the z/OS UNIX kernel (OMVS) is not properly defined to the security database.
- ZUSS0044** The user account for the z/OS UNIX BPXROOT is not properly defined.
- ZUSS0045** The user account for the z/OS UNIX (RMFGAT) is not properly defined.
- ZUSS0046** UID(0) is improperly assigned.
- ZUSS0047** z/OS UNIX user accounts are not properly defined.
- ZUSS0048** Attributes of z/OS UNIX user accounts are not defined in accordance with security requirements.
- ZUSSR050** The z/OS Default Userid is not properly defined with the corresponding FACILITY Class Profile.
- ZUSSR060** The RACF Classes required to properly security the z/OS UNIX environment are not ACTIVE.
- ZUSSR070** RACF Classes required to support z/OS UNIX security are not properly implemented with the SETROPTS RACLIST command.
- ZUSS0080** z/OS USS Software owning Shared accounts do not meet strict security and creation restrictions.

- ZVTM0011** The VTAM USSTAB definitions are being used for unsecured terminals
- ZVTM0018** The System datasets used to support the VTAM network are not properly secured

- ZVTAR000** CA VTAPE installation data sets are not properly protected.
- ZVTAR001** CA VTAPE STC data sets will be properly protected.
- ZVTAR030** CA VTAPE Started Task name is not properly identified/defined to the system ACP.
- ZVTAR032** CA VTAPE Started task(s) must be properly defined to the STARTED resource class for RACF.

- ZWMQ0011** WebSphere MQ channel security is not implemented in accordance with security requirements.
- ZWMQ0012** WebSphere MQ channel security is not implemented in accordance with security requirements
- ZWMQ0014** Production WebSphere MQ Remotes will utilize Certified Name Filters (CNF).
- ZWMQ0020** User timeout parameter values for WebSphere MQ queue managers are not specified in accordance with security requirements.
- ZWMQ0030** WebSphere MQ started tasks are not defined in accordance with the proper security requirements
- ZWMQ0040** WebSphere MQ all update and alter access to MQSeries/WebSphere MQ product and system data sets are not properly restricted
- ZWMQ0049** WebSphere MQ resource classes are not properly activated for security checking by the ACP.
- ZWMQ0051** WebSphere MQ "switch" profiles are improperly defined to the MQADMIN class.
- ZWMQ0052** WebSphere MQ MQCONN Class (Connection) resource definitions are not protected in accordance with security.
- ZWMQ0053** WebSphere MQ dead letter and alias dead letter queues are not properly defined.
- ZWMQ0054** WebSphere MQ MQQUEUE (Queue) resource profiles defined to the MQQUEUE class are not protected in accordance with security requirements.
- ZWMQ0055** WebSphere MQ Process resource profiles defined in the MQPROC Class are not protected in accordance with security requirements.

- ZWMQ0056** WebSphere MQ Namelist resource profiles defined in the MQNLIST Class are not protected in accordance with security requirements.
- ZWMQ0057** WebSphere MQ Alternate User resources defined to MQADMIN resource class are not protected in accordance with security requirements.
- ZWMQ0058** WebSphere MQ context resources defined to the MQADMIN resource class are not protected in accordance with security requirements.
- ZWMQ0059** WebSphere MQ command resources defined to MQCMDS resource class are not protected in accordance with security requirements.
- ZWMQ0060** WebSphere MQ RESLEVEL resources in the MQADMIN resource class are not protected in accordance with security requirements.

- ZWAS0010** MVS data sets for the WebSphere Application Server are not protected in accordance with the proper security requirements
- ZWAS0020** HFS objects for the WebSphere Application Server are not protected in accordance with the proper security requirements.
- ZWAS0030** The CBIND Resource Class for the WebSphere Application Server is not configured in accordance with security requirements
- ZWAS0040** Vendor-supplied user accounts for the WebSphere Application Server are defined to the ACP
- ZWAS0050** The WebSphere Application Server plug-in is not specified in accordance with the proper security requirements.

Tivoli Asset Discovery (ZTAD)

ZTADR000 Tivoli Asset Discovery for z/OS (TADz) Install data sets are not properly protected.

ZTADR001 Tivoli Asset Discovery for z/OS (TADz) STC and/or batch data sets are not properly protected.

ZTADR030 Tivoli Asset Discovery for z/OS (TADz) Started Task name(s) is not properly identified / defined to the system ACP

ZTADR032 The Tivoli Asset Discovery for z/OS (TADz) Started task is not properly defined to the STARTED resource class for RACF

Catalog Solutions (ZCSL)

ZCSLR000 Catalog Solutions Install data sets are not properly protected.

ZCSLR020 Catalog Solutions resources are not properly defined and protected.

ROSCOE (ZROS)

- ZROSR000** ROSCOE Install data sets are not properly protected.
- ZROSR001** ROSCOE STC data sets are not properly protected.
- ZROSR020** ROSCOE resources are not properly defined and protected.
- ZROSR030** ROSCOE Started Task name is not properly identified / defined to the system ACP.
- ZROSR032** The ROSCOE Started task is not properly defined to the STARTED resource class for RACF
- ZROSR038** The Product's Resource Class for Roscoe is not defined or active in the ACP.
- ZROSR040** Product configuration/parameter values are not specified properly.

SRR Audit (ZSRR)

- ZSRRR000** SRRAUDIT Install data sets are not properly protected.
- ZSRRR002** SRRAUDIT User data sets are not properly protected.

Transparent Data Migration Facility (TDMF)

VANGUARD
INTEGRITY PROFESSIONALS, INC.
enterprise security software

- ZTDMR000** Transparent Data Migration Facility (TDMF) Install data sets are not properly protected.
- ZTDM0040** Transparent Data Migration Facility (TDMF) configuration/parameter/option values are not specified properly.

61

IBM Business Partner Server Proven

NetView (ZNET)

VANGUARD
INTEGRITY PROFESSIONALS, INC.
enterprise security software

- ZNET0040** NetView configuration/parameter values are not specified properly.
- ZNETR000** NetView install data sets are not properly protected.
- ZNETR001** NetView STC data sets are not properly protected.
- ZNETR030** NetView Started Task name(s) is not properly identified / defined to the system ACP.
- ZNETR032** NetView Started Task name(s) is not properly identified / defined to the system ACP.

62

IBM Business Partner Server Proven

- ZVSSR000** Vanguard Security Solutions (VSS) Install data sets are not properly protected.
- ZVSSR002** Vanguard Security Solutions (VSS) User data sets are not properly protected.
- ZVSSR020** Vanguard Security Solutions' resources for the FACILITY resource class are not properly defined and protected.

- ZHCKR001** IBM Health Checker STC data sets will be properly protected.
- ZHCKR030** IBM Health Checker Started Task name will be properly identified and/or defined to the system ACP.
- ZHCKR032** IBM Health Checker Started task will be properly defined to the STARTED resource class for RACF.
- ZSMTR030** IBM CSSMTP Started Task name is not properly identified and/or defined to the system ACP.
- ZSMTR032** IBM CSSMTP Started task(s) must be properly defined to the STARTED resource class for RACF.

VANGUARD
INTEGRITY PROFESSIONALS, INC.
enterprise security software

Anatomy of a STIG Check

©2010 Vanguard Integrity Professionals, Inc. 65 IBM Business Partner Server Proven

VANGUARD
INTEGRITY PROFESSIONALS, INC.
enterprise security software

Anatomy of a STIG

Group ID (Vulid): V-3895
Group Title: ZSMS0020
Rule ID: SV-7357r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZSMS0020

Rule Title: DFSMS control data sets are not protected in accordance with security requirements

Vulnerability Discussion: DFSMS control data sets provide the configuration and operational characteristics of the system-managed storage environment. Failure to properly protect these data sets may result in unauthorized access. This exposure could compromise the availability and integrity of some system services and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD

66 IBM Business Partner Server Proven

Check Content:

Review the logical parmlib data sets, example: SYS1.PARMLIB(IGDSMSxx), to identify the fully qualified file names for the following SMS data sets:

- Source Control Data Set (SCDS)
- Active Control Data Set (ACDS)
- Communications Data Set (COMMDS)
- ACDS Backup
- Automatic Class Selection Routine Source Data Sets (ACS)
- COMMDS Backup

If the RACF data set rules for the SCDS, ACDS, COMMDS, and ACS data sets restrict UPDATE and ALTER access to only systems programming personnel, there is **NO FINDING**.

If the RACF data set rules for the SCDS, ACDS, COMMDS, and ACS data sets do not restrict UPDATE and ALTER access to only systems programming personnel, this is a **FINDING**

Fix Text:

Review the SYS1.PARMLIB(IGDSMS00) data set to identify the fully qualified file names for the following SMS data sets:

- Source Control Data Set (SCDS)
- Active Control Data Set (ACDS)
- Communications Data Set (COMMDS)
- Automatic Class Selection Routine Source Data Sets (ACS)
- ACDS Backup
- COMMDS Backup

The RACF data set rules for the SCDS, ACDS, COMMDS, and ACS data sets must restrict UPDATE and ALTER access to only z/OS systems programming personnel.

Some example commands to implement the proper controls are shown here:

```
AD 'sys3.dfsms.mmd.commnds.***' UACC(NONE) OWNER(SYS3) AUDIT(ALL(READ)) DATA('PROTECTED PER ZSMS0020')
```

```
PE 'sys3.dfsms.mmd.commnds.***' ID(<syspaut>) ACC(A)
```

Summary & Questions