

## IBM Education Assistance for z/OS V2R3

“New and changed health checks for V2R3”

Element/Component: Multiple across z/OS

# Agenda

- .Trademarks
- .Overview
- .Usage & Invocation
- .Migration & Coexistence Considerations
- .Installation
- .Health Check Details
- .Appendix

# Trademarks

- See url <http://www.ibm.com/legal/copytrade.shtml> for a list of trademarks.
- The term Health Checker is used as short form of “IBM Health Checker for z/OS” in this presentation.
- The term “health check” or just “check” is used as short form of “health check for the IBM Health Checker for z/OS” in this presentation.

# Session Objectives

- Very briefly describe what Health Checker, a health check, and a migration check is
- Present an overview of new and changed health checks developed in z/OS V2R3

# Overview

## **.Problem Statement / Need Addressed:**

–Continued need for programmatic approach to ensuring component best practices and to providing migration assistance

## **.Solution:**

–Provide additional health checks for existing and new best practices, and for migration actions

## **.Benefit:**

–Improved system health and smoother release migration

# Overview – What is Health Checker?

**.IBM Health Checker for z/OS is a system component that identifies potential problems before they impact your installation's availability or, in worst cases, would cause outages.**

**.It checks the currently active settings and definitions for a system and compares the values to those suggested by IBM or defined by you.**

**.It produces output in the form of detailed messages to let you know of both potential problems and suggested actions to take.**

# Overview – What are health checks?

- A health check is doing the actual “inspection of settings...”, as a “plug-in” to the Health Checker framework
- There are health checks from different sources
  - from individual IBM components, ISVs, and general users
  - each check is supposed to focus on one scenario only
- Health checks are named (*CheckOwner*, *CheckName*)
  - *CheckOwner* is typically *CompanyName\_ComponentName*
  - *CheckName* is typically *ComponentName\_CheckPurpose*
- For example: (IBMASM, ASM\_PLPA\_COMMON\_USAGE)
  - An IBM Auxiliary Storage Manager (ASM) check, which "Looks at the slot usage of the PLPA and Common page data sets"

# Overview – What are migration checks?

- Migration checks are health checks which help with the task of identifying the need for migration actions
- Migration checks are shipped inactive and are manually activated on demand, typically before an actual migration
- A common naming convention for migration checks is (CheckOwner, ZOSMIGxyz\_RestOfCheckName) and ICSF (Cryptographic Facility) also uses ICSFMIG as prefix. The xyz can be
  - VxRy, for migration actions required for a specific release (e.g. “V2R3”)
  - VxRy\_NEXT and VxRy\_NEXT2, for recommended migrations which will be come required in one or two releases after VxRy
  - “REC”, for recommended migration actions without a specific release for the foreseeable future
  - (“REQ”, for recommended actions which become required soon, but which have no release attached to them yet)
- For example:
  - (IBMCNZ, ZOSMIGV1R13\_CNZ\_Cons\_Oper\_Mode)
  - (IBMZFS, ZOSMIGREC\_ZFS\_RM\_MULTIFS)



## Overview – List of new (or updated\*) health checks in V2R3

- (IBMCICS,CICS\_CEDA\_ACCESS)
- (IBMCICS,CICS\_JOB SUB\_SPOOL)
- (IBMCICS,CICS\_JOB SUB\_TDQINTRDR)
- (IBMCS,CSAPP\_FTPD\_ANONYMOUS\_JES)
- (IBMCS,CSAPP\_MVRSHD\_RHOSTS\_DATA)
- (IBMCS,CSAPP\_SMTPD\_MAIL\_RELAY)
- (IBMCS,CSAPP\_SNMPAGENT\_PUBLIC\_COMMUNITY)
- (IBMICSF,ICSF\_OPTIONS\_CHECKS)
- (IBMICSF,ICSF\_UNSUPPORTED\_CCA\_KEYS)

## Overview – List of new (or updated\*) health checks in V2R3

- (IBMIXGLOGR,ZOSMIGV2R2\_NEXT\_IXG\_REMOVE\_DRXRC)
- (IBMJES,JES\_NJE\_SECURITY[\_ssname])
- (IBMRACF,RACF\_AUDIT\_CONTROLS)
- (IBMRACF,RACF\_BATCHALLRACF)
- (IBMRACF,RACF\_JESJOBS\_ACTIVE)
- (IBMRACF,RACF\_JESSPOOL\_ACTIVE)
- (IBMTDS,TDS\_DB2\_MAINTENANCE)

## Overview – List of new (or updated\*) health checks in V2R3

- (IBMUSS,USS\_INETD\_UNSECURE\_SERVICES)
- (IBMUSS,USS\_SUPERUSER)
- (IBMVSAM,VSAM\_CA\_RECLAIM)
- (IBMXCF,XCF\_CF\_STR\_ENCRYPT)
- (IBMXCF,XCF\_SYSSTATDET\_PARTITIONING)\*
- (IBMZFS,ZFS\_VERIFY\_COMPRESSION\_HEALTH)

# Usage & Invocation

**.Most checks** are shipped **ACTIVE** and do not require manual interaction to run. Just monitor their output in form of check exception messages and with further details in a check's message buffer (inspect it for example via the SDSF CK panel).

**.Migration checks** are a set of checks which are shipped **INACTIVE**.

–Look for them on the SDSF CK panel or via operator command, for example  
MODIFY HZSPROC,DISPLAY,CHECK(\*,\*MIG\*)

–Activate them for example via SDSF or operator commands like MODIFY  
HZSPROC,UPDATE,CHECK(\*,\*MIG\*),ACTIVE

# Migration & Coexistence Considerations

- .Updated/Changed checks are sometimes shipped with a new DATE
- The DATE is used as a “version” ID
- If updated, the check owner recommends that you re-evaluate any custom HZSPRMxx parmlib member POLICY statements for those changed checks
- ...and Health Checker will enforce such inspection by rejecting such custom statements until the POLICY statement's DATE has been updated

# Migration & Coexistence Considerations, cont...

.Some checks have been rolled back to previous releases or even specifically implemented just for those in-service releases (migration checks)

–Check for HOLDDATA/PTFs tagged with SMP/E FIXCAT IBM.Function.HealthChecker

.Look in particular for the following pre-V2R3 APARs:

–(IBMCS,CSAPP\_FTPD\_ANONYMOUS\_JES) **PI47637, OA49668**

–(IBMCS,CSAPP\_MVRSHD\_RHOSTS\_DATA) **PI51640, OA50122**

–(IBMCS,CSAPP\_SMTPD\_MAIL\_RELAY) **PI51640, OA50122**

–(IBMCS,CSAPP\_SNMPAGENT\_PUBLIC\_COMMUNITY) **PI51640, OA50122**

–(IBMICSF,ICSF\_OPTIONS\_CHECKS) **OA48452**

–(IBMJES,JES\_NJE\_SECURITY[\_ssname]) **OA49171**

–(IBMXGLOGR,ZOSMIGV2R2\_NEXT\_IXG\_REMOVE\_DRXRC) **OA49507**

–(IBMRACF,RACF\_BATCHALLRACF) **OA48716**

–(IBMRACF,RACF\_JESJOBS\_ACTIVE) **OA48716**

–(IBMRACF,RACF\_JESSPOOL\_ACTIVE) **OA48716**

–(IBMUSS,USS\_INETD\_UNSECURE\_SERVICES) **OA50999**

–(IBMVSAM,VSAM\_CA\_RECLAIM) **OA51002, OA51393, OA51394**

# Installation

- Most IBM health checks are automatically installed with their associated product or component, or are shipped with the base operation system for the new release
- In addition, some checks, in particular migration checks, will have APARs available for previous releases

## Check Details – (IBMCICS,CICS\_CEDA\_ACCESS)

- .Checks if the default user has access to install CICS resources using CEDA (CICS Execute Definition and Administration)
- .This kind of access can, depending on configuration details, comprise system security.
- .Parameters: None
- .INTERVAL is 00:30 (minutes), SEVERITY is LOW
- .for CICS TS 4.2-5.4



## Check Details – (IBMCICS,CICS\_JOBSUB\_SPOOL)

- .Checks if the default user can use CECI (command level interpreter) to submit jobs under the region userid using the SPOOLWRITE command
- .This kind of access can, depending on configuration details, comprise system security.

.Parameters: None

.INTERVAL is 00:30 (minutes), SEVERITY is LOW

.for CICS TS 4.2-5.4

## Check Details – (IBMCICS,CICS\_JOBSUB\_TDQINTRDR)

- .Checks if the default user can use CECI (command level interpreter) to submit jobs under the region userid using a TDQ (Transient Data Queue) defined to write to the internal reader.
- .This kind of definition can, depending on configuration details, comprise system security.

- .Parameters: None
- .INTERVAL is 00:30 (minutes), SEVERITY is LOW
- .for CICS TS 4.2-5.4

## Check Details – (IBMCS,CSAPP\_FTPD\_ANONYMOUS\_JES)

- .Checks to see whether ANONYMOUS users can submit jobs.
- .When ANONYMOUS FTP is allowed on the FTP server, set ANONYMOUSLEVEL to 3 and ANONYMOUSFILETYPEJES to FALSE to prevent anonymous users from submitting jobs.

.Parameters: None

.INTERVAL is ONETIME, SEVERITY is MEDIUM

.Lineitem: n/a; APAR: PI47637, OA49668 (V2R1, V2R2)

## Check Details – (IBMCS,CSAPP\_MVRSHD\_RHOSTS\_DATA)

- .Checks to see if the MVRSHD server is active and detects if a RSH client uses a RHOSTS.DATA dataset for authentication.
- .The MVRSHD server supports the RSH and REXEC protocols that transfer user ID and password information in the clear. There is also the potential of weak authentication for RSH clients that use RHOSTS.DATA datasets. This authentication method allows remote command execution without requiring the RSH client to supply a password.
- .Parameters: None
- .INTERVAL is ONETIME, SEVERITY is MEDIUM
- .Lineitem: n/a; APAR: PI51640 and OA50122 (V2R1, V2R2)

## Check Details – (IBMCS,CSAPP\_SMTPD\_MAIL\_RELAY)

- Checks the INBOUNDOPENLIMIT.

- IBM recommends to set the INBOUNDOPENLIMIT to zero. Specifying a valid non-zero value or allowing it to default to the value of 256 causes the SMTP server to open a listening port and implicitly become exploitable by remote users as a mail relay.

- Parameters: None

- INTERVAL is ONETIME, SEVERITY is MEDIUM

- Lineitem: n/a; APAR: PI51640,OA50122 (V2R1, V2R2)

## Check Details – (IBMCS,CSAPP\_SNMPAGENT\_PUBLIC\_COMMUNITY)

- Checks to see if the SNMP agent has been configured with a community name of “public”.
- IBM recommends not to use the well-known community name of public with community-based security because of security considerations.

•Parameters: None

•INTERVAL is ONETIME, SEVERITY is MEDIUM

•Lineitem: n/a; APAR: PI51640, OA50122 (V2R1, V2R2)

## Check Details – (IBMICSF,ICSF\_OPTIONS\_CHECKS)

- Examines the value of some of the ICSF installation options that can affect performance.

- Parameters: CHECKAUTH(NO|YES),CKTAUTH(NO|YES),KEYAUTH(NO|YES), to identify installation option values to expect

- INTERVAL is ONETIME, SEVERITY is MEDIUM

- Lineitem: n/a; APAR: OA48452 (V1R9-V2R2/HCR7780-HCR77B1)

## Check Details – (IBMXGLOGR,ZOSMIGV2R2\_NEXT\_IXG\_REMOVE\_DRXRC)

- Checks for the DRXRC duplex mode option being specified for any log streams in the sysplex.
  - z/OS V2R2 is the last release to support the log stream DRXRC duplex mode option, defined in the LOGR CDS, for example.
  - IBM recommends to use a different logger duplex option along with the appropriate DASD mirroring capabilities and configurations.
- 
- Parameters: None
  - INTERVAL is ONETIME, SEVERITY is LOW
  - Lineitem: n/a; APAR OA49507 (V1R13, V2R1, V2R2)



## Check Details – (IBMJES,JES\_NJE\_SECURITY[\_ssname])

.Examines the various NJE (Network Job Entry) parameters associated with the primary, and with any additional, JES subsystem and verifies that the subsystem is configured using best practices.

.In particular, the check ensures that any node that is considered trusted by the installation security product (allowed to submit jobs without additional authentication) is configured with appropriate parameters.

### .Parameters:

-NJEEEXEC(*execname*|NONE) – The name of the security product REXX exec that should be used to determine what nodes are trusted. It should be set based on the security product used on the system. Default: 'IRRNJECK' for RACF.

-DEBUG(ALL|YES|NO|JES|SEC) – to activate additional diagnostic messages

.INTERVAL is 06:00 (hours), SEVERITY is DYNAMIC

.Lineitem: n/a; APAR: OA49171 (V2R1, V2R2)

## Check Details – (IBMRACF,RACF\_AUDIT\_CONTROLS)

- .The check examines AUDIT related RACF options (SETROPTS):
  - SAUDIT – audit admin commands allowed via SPECIAL attribute
  - OPERAUDIT – audit dataset open allowed only via OPERATIONS attribute
  - CMDVIOL – audit admin command failures due to missing authority
- .IBM recommends to enable these options to have an (SMF-) audit trace of the security sensitive items that these options refer to.
- .Parameters: SAUDIT(YES|NO),OPERAUDIT(YES|NO),CMDVIOL(YES|NO), specifying the expected enablement state for these options
- .INTERVAL is 24:00 (hours), SEVERITY is MEDIUM
- .Lineitem: n/a; APAR: n/a (V2R3 only)

## Check Details – (IBMRACF,RACF\_BATCHALLRACF)

- .The check examines the SETROPTS JES(BATCHALLRACF) setting.
- .SETROPTS JES(BATCHALLRACF) ensures that all batch jobs have a RACF-identified user ID.

.Parameters: None

.INTERVAL is 24:00 (hours), SEVERITY is MEDIUM

.Lineitem: n/a; APAR: OA48716 (V1R13, V2R1, V2R2)

## Check Details – (IBMRACF,RACF\_JESJOBS\_ACTIVE)

- Examines the status of the RACF general resource class RACF\_JESJOBS\_ACTIVE.
- An effective RACF implementation requires that the baseline group of this RACF general resource class be active.

- Parameters: None
- INTERVAL is 24:00 (hours), SEVERITY is MEDIUM
- Lineitem: n/a; APAR: OA48716 (V1R13, V2R1, V2R2)

## Check Details – (IBMRACF,RACF\_JESSPOOL\_ACTIVE)

- Examines the status of the RACF general resource class RACF\_JESSPOOL\_ACTIVE.
- An effective RACF implementation requires that the baseline group of this RACF general resource class be active.

- Parameters: None
- INTERVAL is 24:00 (hours), SEVERITY is MEDIUM
- Lineitem: n/a; APAR: OA48716 (V1R13, V2R1, V2R2)

## Check Details – (IBMTDS,TDS\_DB2\_MAINTENANCE)

- The check alerts users when a DB2 database REORG or RUNSTATS is recommended for DB2-backed backend-stores TDBM and GDBM of the IBM Tivoli Directory Server (TDS) for z/OS.
- IBM recommends to run REORG and RUNSTATS periodically to avoid general performance degradation and for better optimization of DB2 queries.
- NOTE: Additional TDS configuration is necessary before this health check can run successfully (see next page)
- Parameters: (via TDS backend)
- INTERVAL is ONETIME (and on-demand by TDS), SEVERITY is LOW
- Lineitem FP1181; APAR: n/a (V2R3, only)

## Check Details – (IBMTDS,TDS\_DB2\_MAINTENANCE)...

.The separate slide-deck for FP1811 – “TDBM Health Check” and the TDS publications referenced in there list some configuration requirements:

–Requires at least one TDBM or GDBM, DB2 backed backend to be configured for TDS

–Required additions to the server configuration file:

.Global section: healthcheck DB2 TOD

.TDBM/GDBM section: db2CheckHealth on

–Also has more, optional parameters to override check defaults

.... as well as additional information on how to handle any reported health check exceptions

.... as well as some dependencies:

–z/OS DB2 v10 or higher (or v9 with PTF UK32795), WLM, RRS, System Logger

## Check Details – (IBMUSS,USS\_INETD\_UNSECURE\_SERVICES)

- .Reports any unsecure services that are configured for the inetd daemon.
- .The inetd daemon can be configured to accept connections for services that are considered unsecure because they require user authentication via clear-text (unencrypted) sockets.

- .Parameters: IGNORE\_SERVICES(*service\_list*)
- .INTERVAL is ONETIME (and automatically after inetd.conf updates)
- .SEVERITY is MEDIUM
- .Lineitem: n/a; APAR: OA50999



## Check Details – (IBMUSS,USS\_SUPERUSER)

- .Checks the user ID specified via the SUPERUSER option in BPXPRMxx
- .This user ID needs to be defined to the security product and have an OMVS segment with a UID of 0.
- .Parameters: None
- .INTERVAL is ONETIME (and automatically when the SUPERUSER option is changed dynamically)
- .SEVERITY is HIGH
- .Lineitem: n/a; APAR: n/a (V2R3 only)

## Check Details – (IBMVSAM,VSAM\_CA\_RECLAIM)

- .Checks for VSAM CA (Control Area) reclaim being enabled.
- .IBM recommends running with CA reclaim enabled to provide improved DASD space usage and performance enhancements.
- .See CA\_RECLAIM option for IGDSMSxx and SETSMS.

.Parameters: n/a

.INTERVAL is ONETIME & on-demand, SEVERITY is MEDIUM

.Lineitem: n/a; APAR: OA51002, OA51393, OA51394 (V2R1, V2R2)

## Check Details – (IBMXCF,XCF\_CF\_STR\_ENCRYPT)

.Checks the current resident data format of structure data (encrypted or non-encrypted) in allocated structures to be consistent with the effective ENCRYPT parameter and the cryptographic encryption key (when the structure is encrypted) for the structure in the CFRM policy.

.Parameters: None

.INTERVAL is 01:00 (hour), SEVERITY MEDIUM

.Lineitem: FP0944; APAR: n/a (V2R3 only)

## Check Details – (IBMXCF,XCF\_SYSSTATDET\_PARTITIONING) - updated

.Checks that the system status detection (SSD) partitioning protocol is enabled to ensure that failed systems are removed from the sysplex expeditiously and with a minimum of operator involvement.

.Updates:

–Include detection of “missing services (BCPii and other APIs) which are required by the SSD protocol” in the list of environmental factors that can trigger a check exception

–Check is now also more responsive to environmental changes occurring in the sysplex

–Additional VERBOSE information lists SSD partitioning protocol status for local and all remote systems in the sysplex

.Parameters: ENABLED(YES|NO) – what SSD enablement state to check for

.INTERVAL is 4:00 (hours), SEVERITY is MEDIUM

.Lineitem 1864; APAR: n/a (V2R3 only)

## Check Details – (IBMZFS,ZFS\_VERIFY\_COMPRESSION\_HEALTH)

- .Checks for user cache pages being registered with the zEDC Express service when there are compressed file systems.
- .To improve performance of the compression I/O, IBM recommends that you specify the **edcfixed** option in the IOEFSPRM parameter **user\_cache\_size**
- .Parameters: None
- .INTERVAL is ONETIME, SEVERITY is LOW
- .References: Lineitem F1327; APAR: n/a (new in V2R3, only)

# Session Summary

.The list of “regular” health checks and migration checks is growing, helping to keep your system healthy and to ease the migration to new z/OS releases.

# Appendix

## .Related Publications

- “IBM Health Checker for z/OS User's Guide” (SC23-6843)

- .Includes an inventory of all IBM health checks known at publication time, with quarterly check refreshes as needed

- “Exploiting the Health Checker for z/OS infrastructure”

- .Redpaper 4590