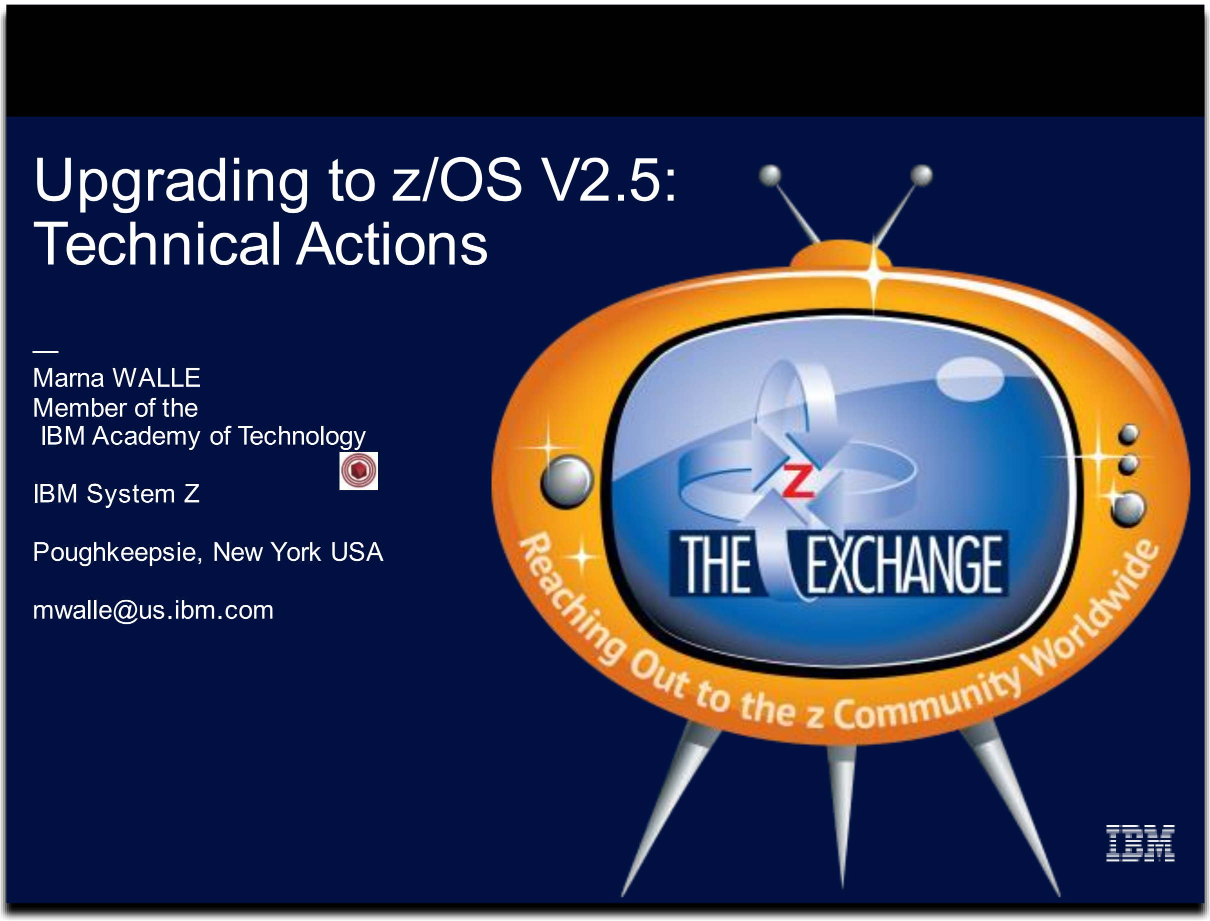


Upgrading to z/OS V2.5: Technical Actions

—

Marna WALLE
Member of the
IBM Academy of Technology

IBM System Z

Poughkeepsie, New York USA

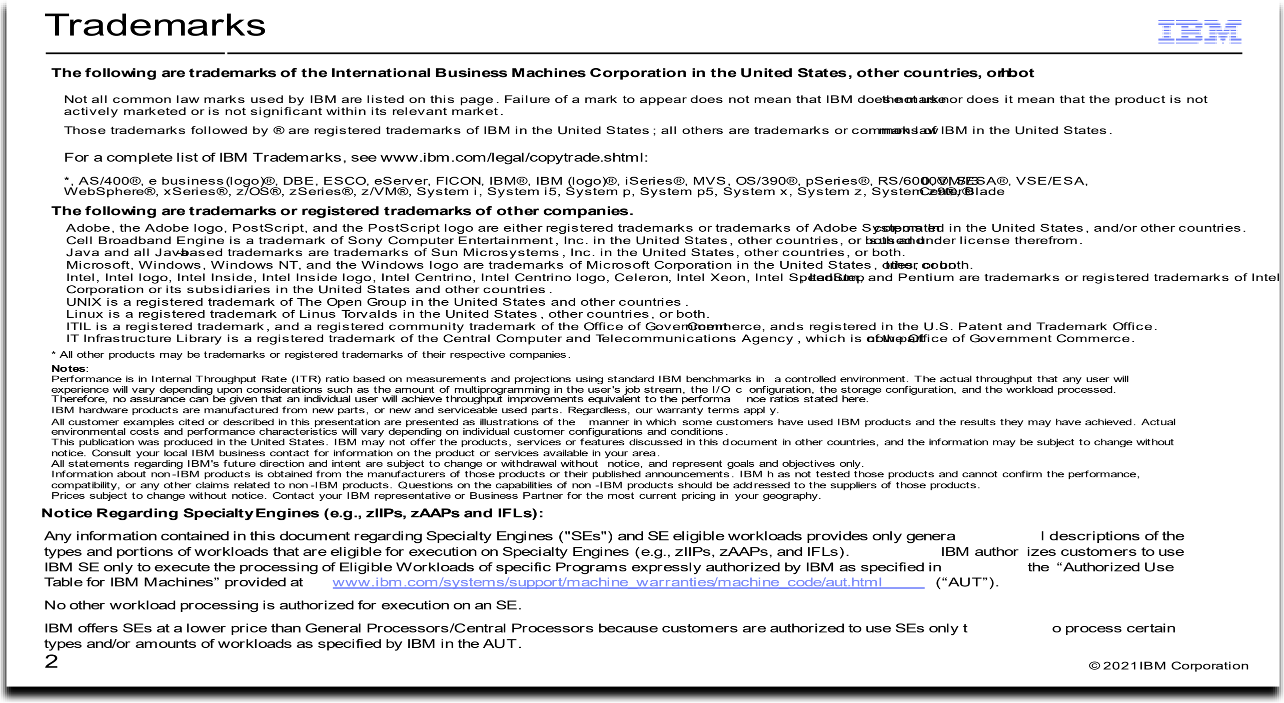
mwalle@us.ibm.com

THE EXCHANGE
Reaching Out to the z Community Worldwide
IBM

Abstract:

Yes, "upgrade" is the new name for these traditional "migration" sessions! This is part one of a two-part session that will be of interest to System Programmers and their managers who are upgrading to z/OS V2.5 from either z/OS V2.3 or V2.4. It is strongly recommended that you review sessions for a complete upgrade picture.

The general availability date for z/OS V2.5 was September 30, 2021.



Trademarks

The following are trademarks of the International Business Machines Corporation in the United States, other countries, or both

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:
Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Notice Regarding Specialty Engines (e.g., zIIPs, zAAPs and IFLs):

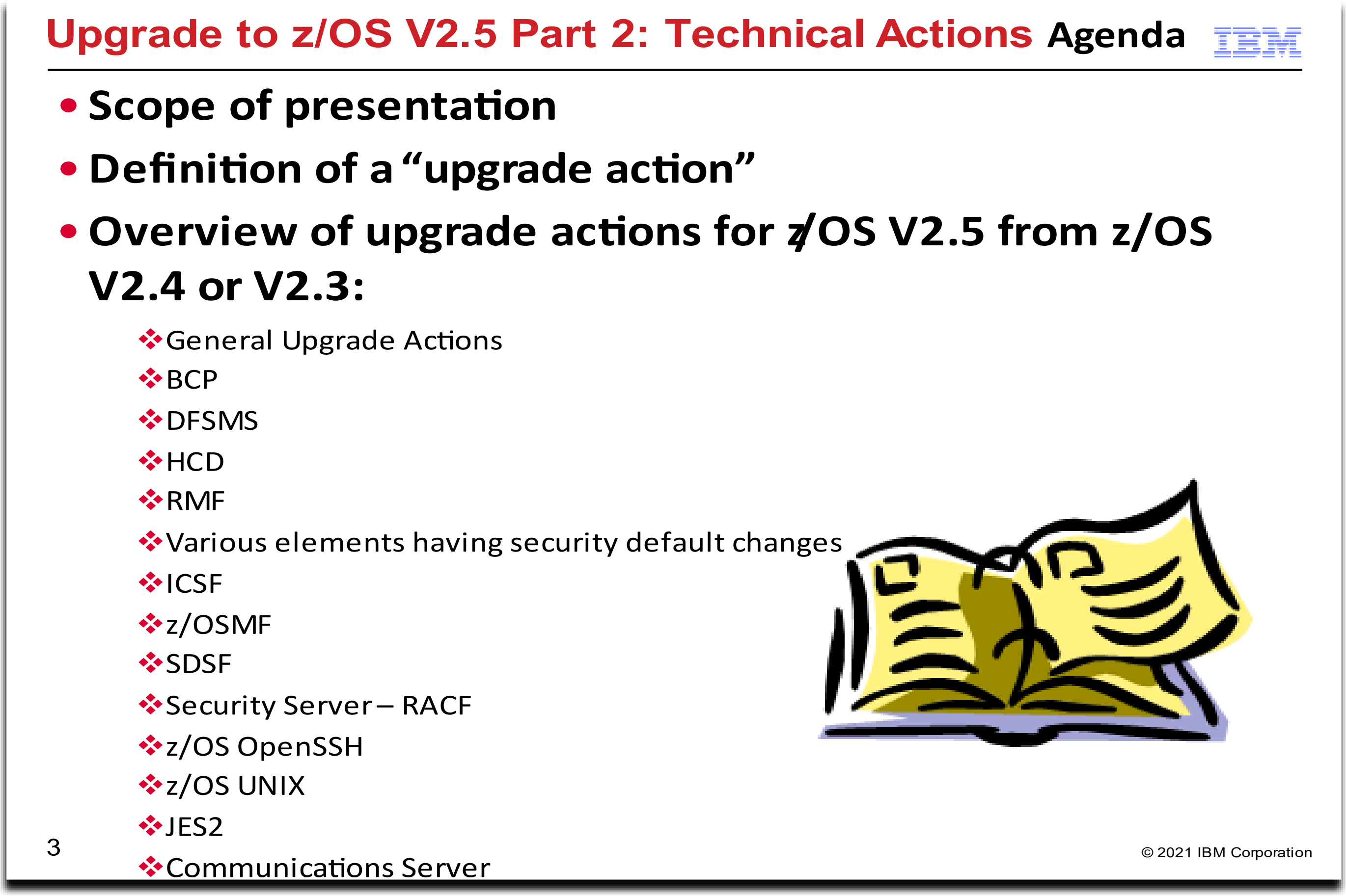
Any information contained in this document regarding Specialty Engines ("SEs") and SE eligible workloads provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g., zIIPs, zAAPs, and IFLs). IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the "Authorized Use Table for IBM Machines" provided at www.ibm.com/systems/support/machine_warranties/machine_code/aut.html ("AUT").

No other workload processing is authorized for execution on an SE.

IBM offers SEs at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.

2

© 2021 IBM Corporation

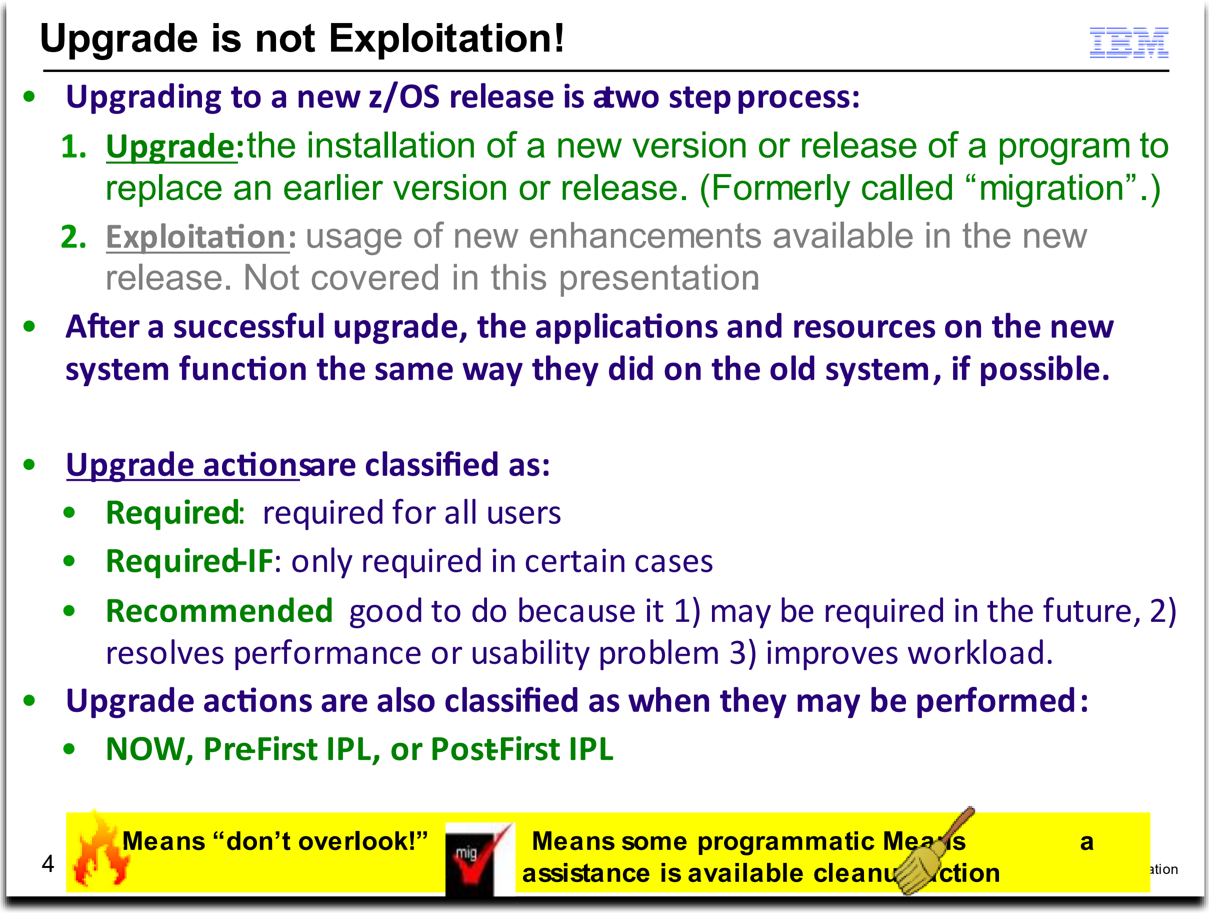


Upgrade to z/OS V2.5 Part 2: Technical Actions Agenda

- Scope of presentation
- Definition of a "upgrade action"
- Overview of upgrade actions for z/OS V2.5 from z/OS V2.4 or V2.3:
  - ❖General Upgrade Actions
  - ❖BCP
  - ❖DFSMS
  - ❖HCD
  - ❖RMF
  - ❖Various elements having security default changes
  - ❖ICSF
  - ❖z/OSMF
  - ❖SDSF
  - ❖Security Server – RACF
  - ❖z/OS OpenSSH
  - ❖z/OS UNIX
  - ❖JES2
  - ❖Communications Server

3

© 2021 IBM Corporation



Upgrade is not Exploitation!

- Upgrading to a new z/OS release is atwo step process:
  1. Upgrade: the installation of a new version or release of a program to replace an earlier version or release. (Formerly called “migration”.)
  2. Exploitation: usage of new enhancements available in the new release. Not covered in this presentation
- After a successful upgrade, the applications and resources on the new system function the same way they did on the old system, if possible.

- Upgrade actionsare classified as:
  - Required: required for all users
  - Required-IF: only required in certain cases
  - Recommended good to do because it 1) may be required in the future, 2) resolves performance or usability problem 3) improves workload.
- Upgrade actions are also classified as when they may be performed:
  - NOW, Pre-First IPL, or Post-First IPL

Means “don't overlook!” Means some programmatic assistance is available Means a cleanup action

4

Upgrade Definitions and Classifications

Upgrade (formerly, migration) is the first of two stages in upgrading to a new release of z/OS. The two stages are:

- **Stage 1: Upgrade.** During this stage you install your new system with the objective of making it functionally compatible with the previous system. After a successful upgrade, the applications and resources on the new system function the same way (or similar to the way) they did on the old system or, if that is not possible, in a way that accommodates the new system differences so that existing workloads can continue to run. Upgrade does not include exploitation of new functions except for new functions that are now required.
- **Stage 2: Exploitation.** During this stage you do whatever customizing and programming are necessary to take advantage of (exploit) the enhancements available in the new release. Exploitation follows upgrade.

Upgrade Requirement Classification and Timing

The upgrade actions are classified as to their requirement status:

- ***Required***. The upgrade action is required in all cases.
- ***Required-IF.*** The upgrade action is required only in a certain case. Most of the actions in this presentation are in this category.
- ***Recommended.*** The upgrade action is not required but is recommended because it is a good programming practice, because it will be required in the future, or because it resolves unacceptable system behavior (such as poor usability or poor performance) even though resolution might require a change in behavior.

To identify the timing of upgrade actions, this presentation uses three types of headings:

- ***Now.*** These are upgrade actions that you perform on your current system, either because they require the current system or because they are possible on the current system. You don't need the z/OS V2.5 level of code to make these changes, and the changes don't require the z/OS V2.5 level of code to run once they are made. Examples are installing coexistence and fallback PTFs on your current system, discontinuing use of hardware or software that will no longer be supported, and starting to use existing functions that were optional on prior releases but required in z/OS V2.5.
- ***Pre-First IPL.*** These are upgrade actions that you perform after you've installed z/OS V2.5 but before the first time you IPL. These actions require the z/OS V2.5 level of code to be installed but don't require it to be active.

That is, you need the z/OS V2.5 programs, utilities, and samples in order to perform the upgrade actions, but the z/OS V2.5 system does not have to be IPLed in order for the programs to run. Examples are running sysplex utilities and updating the RACF data base templates.

It is possible to perform some of the upgrade actions in this category even earlier. If you prepare a system on which you will install z/OS V2.5 by making a clone of your old system, you can perform upgrade actions that involve customization data on this newly prepared system before installing z/OS V2.5 on it. Examples of such upgrade actions are updating configuration files and updating automation scripts.

- ***Post-First IPL.*** These are upgrade actions that you can perform only after you've IPLed z/OS V2.5. You need a running z/OS V2.5 system to perform these actions. An example is issuing RACF commands related to new functions. Note that the term "first IPL" does not mean that you have to perform these actions after the very first IPL, but rather that you need z/OS V2.5 to be active to perform the task. You might perform the task quite a while after the first IPL.

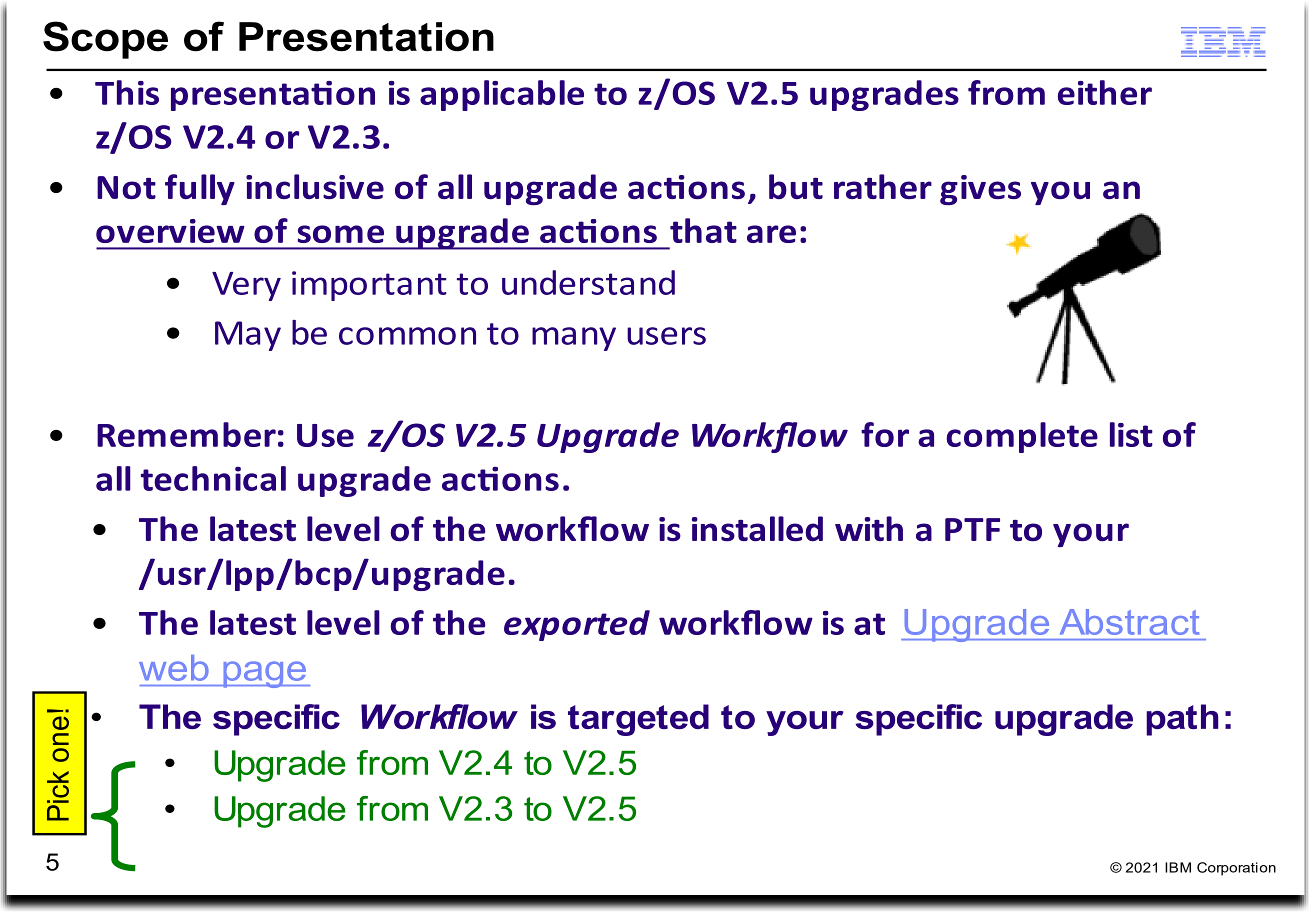
Icons used in this presentation:

means that you shouldn't overlook this upgrade action.

means that an IBM Health Check (using the IBM Health Checker for z/OS function) can help you with this upgrade action.

means that this is a cleanup item or contains a portion that is a cleanup item. It is associated with something that is obsolete. It may cause confusion if someone thinks it does something. It is best to perform this

action to avoid any confusion, since it is not needed anymore.



Scope of Presentation

- **This presentation is applicable to z/OS V2.5 upgrades from either z/OS V2.4 or V2.3.**
- **Not fully inclusive of all upgrade actions, but rather gives you an overview of some upgrade actions that are:**
  - Very important to understand
  - May be common to many users
- **Remember: Use *z/OS V2.5 Upgrade Workflow* for a complete list of all technical upgrade actions.**
  - **The latest level of the workflow is installed with a PTF to your /usr/lpp/bcp/upgrade.**
  - **The latest level of the *exported* workflow is at** Upgrade Abstract web page
  - **The specific *Workflow* is targeted to your specific upgrade path:**
    - Upgrade from V2.4 to V2.5
    - Upgrade from V2.3 to V2.5

Pick one!

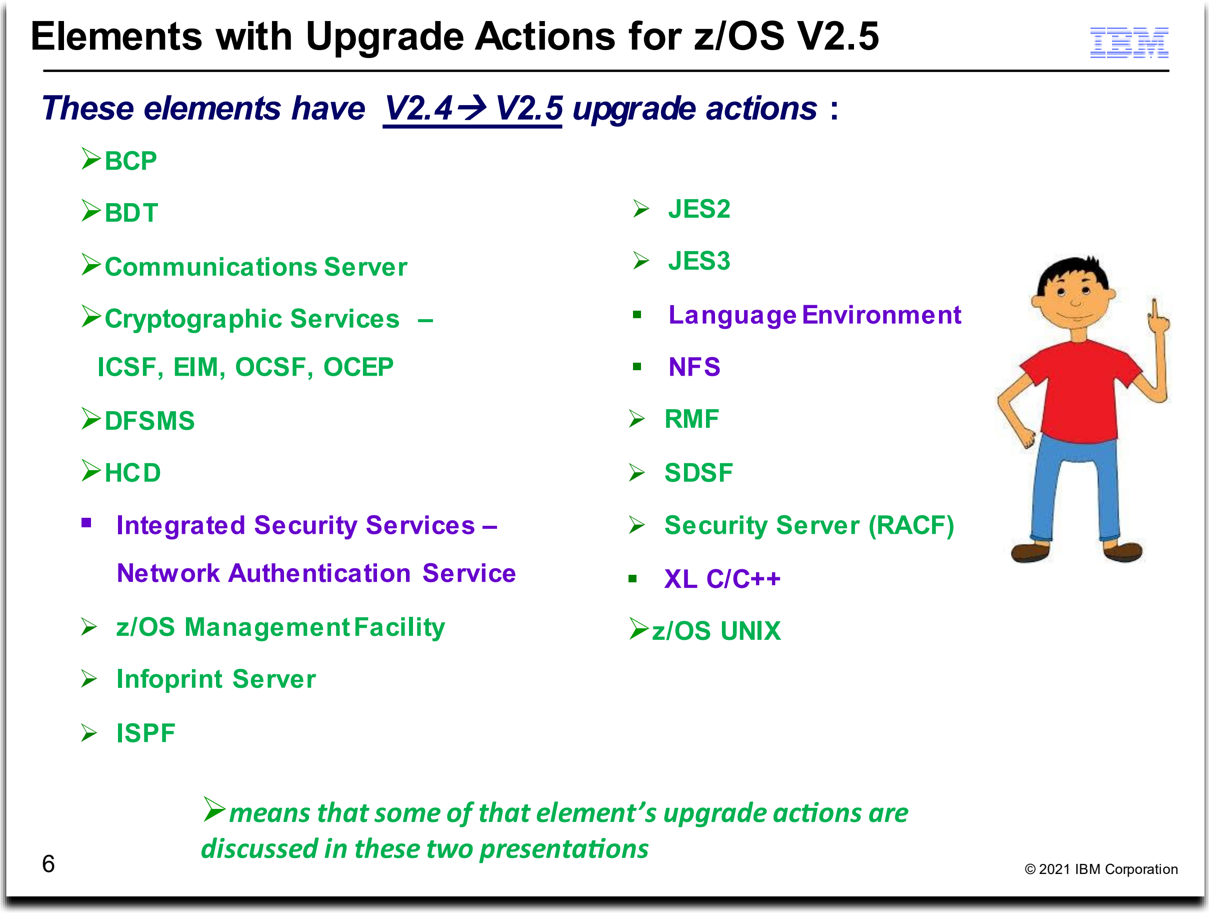
5

To use the latest version of the *z/OS V2.4 Upgrade Workflow*, retrieve it from this Github location: https://github.com/IBM/IBM-Z-zOS/tree/master/zOS-Workflow/zOS%20V2.4%20Upgrade%20Workflow

To use the latest version of the *z/OS V2.5 Upgrade Workflow*, it is available on z/OS V2.4 and z/OS V2.3 with a PTF marked with the FIXCAT IBM.Coexistence.z/OS.V2R5. Once the PTF is installed, you will find the workflows in your /usr/lpp/bcp/upgrade path.

IBM strongly recommends you use the z/OS Upgrade Workflow from z/OSMF in order to have a customized upgrade of your applicable steps to take.

However, if you wish to use the exported version of any z/OS Upgrade Workflow, you can see it here (at the bottom of the page): https://www.ibm.com/support/knowledgecenter/SSLTBW_2.4.0/com.ibm.zos.v2r4.e0zm100/abstract.htm



Elements with Upgrade Actions for z/OS V2.5

These elements have V2.4→ V2.5 upgrade actions :

- ➢BCP
- ➢BDT
- ➢Communications Server
- ➢Cryptographic Services – ICSF, EIM, OCSF, OCEP
- ➢DFSMS
- ➢HCD
- ▪ Integrated Security Services – Network Authentication Service
- ➢ z/OS Management Facility
- ➢ Infoprint Server
- ➢ ISPF
- ➢ JES2
- ➢ JES3
- ▪ Language Environment
- ▪ NFS
- ➢ RMF
- ➢ SDSF
- ➢ Security Server (RACF)
- ▪ XL C/C++
- ➢z/OS UNIX

➢means that some of that element's upgrade actions are discussed in these two presentations

6

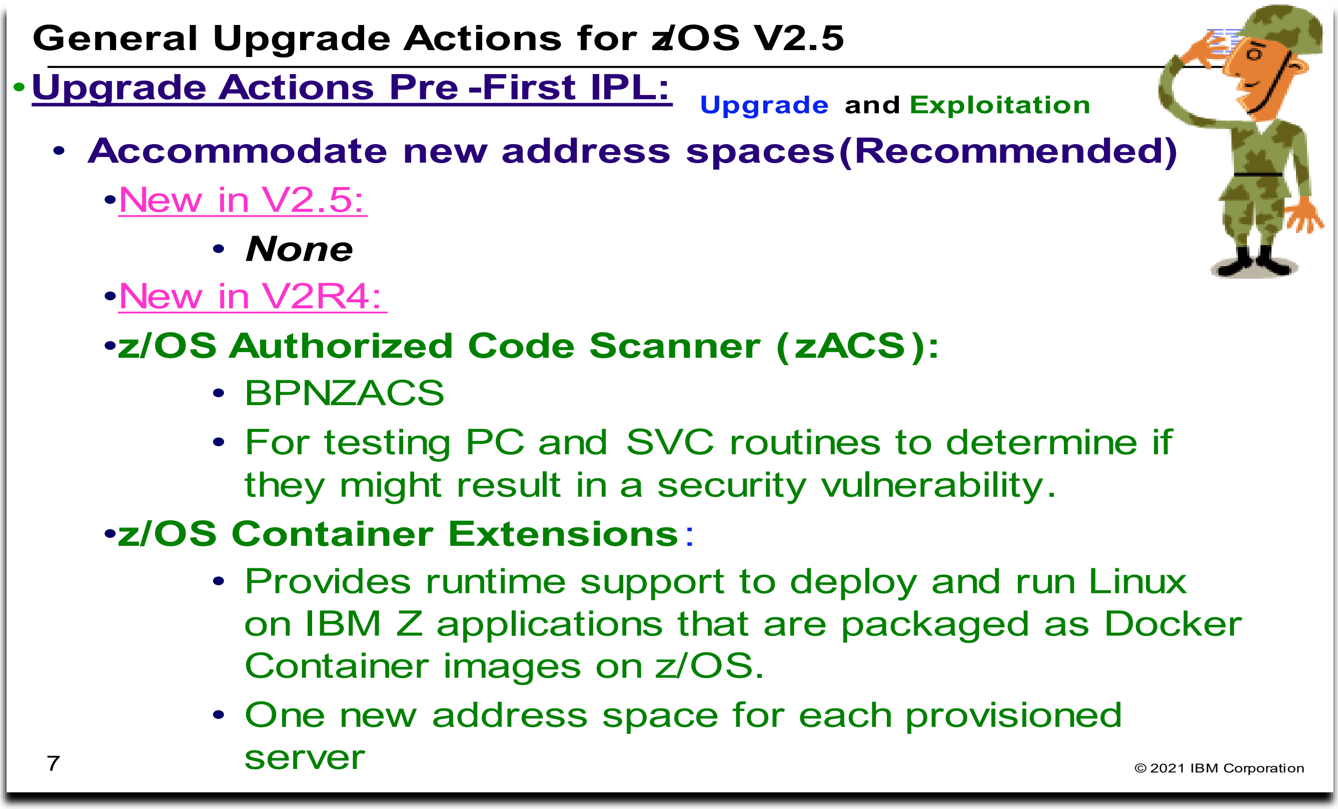
© 2021 IBM Corporation

Upgrade Actions for Elements in z/OS V2.5

When upgrading from z/OS V2.4 to z/OS V2.5, the specified elements in the slide above have new or usual upgrade actions.

If you are upgrading from z/OS V2.3, use the *z/OS V2.5 Upgrade Workflow* for the z/OS V2.3 path to see the upgrade actions which were introduced in V2.4. Alternatively, if you wanted to see the upgrade actions, you can also see the exported workflow on the IBM Documentation website (go to the bottom to click on which upgrade path you are doing). https://www.ibm.com/docs/en/zos/2.4.0?topic=level-zos-upgrade-workflow

Some upgrade actions for selected elements follow in this presentation. This presentation does not cover all possible upgrade actions.



General Upgrade Actions for z/OS V2.5

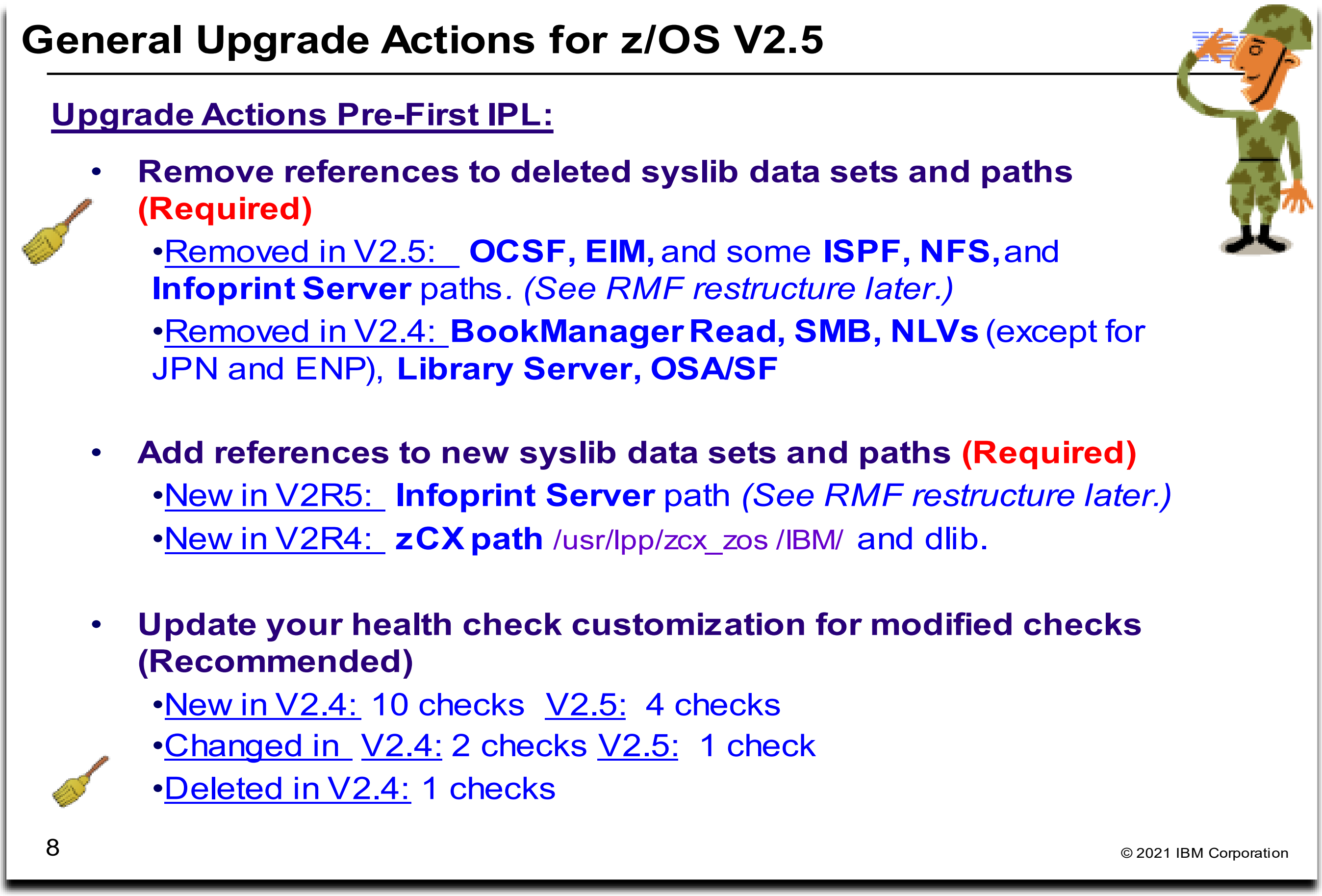
- Upgrade Actions Pre -First IPL:

Upgrade and Exploitation

- Accommodate new address spaces(Recommended)
  - New in V2.5:
    - *None*
  - New in V2R4:
  - z/OS Authorized Code Scanner (zACS):
    - BPNZACS
    - For testing PC and SVC routines to determine if they might result in a security vulnerability.
  - z/OS Container Extensions:
    - Provides runtime support to deploy and run Linux on IBM Z applications that are packaged as Docker Container images on z/OS.
    - One new address space for each provisioned server

7

© 2021 IBM Corporation



General Upgrade Actions for z/OS V2.5

Upgrade Actions Pre-First IPL:

- Remove references to deleted syslib data sets and paths (Required)
  - Removed in V2.5: **OCSF, EIM,** and some **ISPF, NFS,** and **Infoprint Server** paths. *(See RMF restructure later.)*
  - Removed in V2.4: **BookManager Read, SMB, NLVs** (except for JPN and ENP), **Library Server, OSA/SF**
- Add references to new syslib data sets and paths (Required)
  - New in V2R5: **Infoprint Server** path *(See RMF restructure later.)*
  - New in V2R4: **zCX path** /usr/lpp/zcx_zos /IBM/ and dlib.
- Update your health check customization for modified checks (Recommended)
  - New in V2.4: 10 checks V2.5: 4 checks
  - Changed in V2.4: 2 checks V2.5: 1 check
  - Deleted in V2.4: 1 checks

8

© 2021 IBM Corporation

General Upgrade Actions For z/OS V2.5

These upgrade actions were taken from *z/OS V2.5 Upgrade Workflow.* Some descriptions and actions have been shortened for inclusion in this presentation. Not all upgrade actions have been included. For the complete descriptions and actions, refer to *z/OS V2.5 Upgrade Workflow.*

General Upgrade Actions You Can Do Now

Install coexistence and fallback PTFs (Required)

Upgrade action: Install coexistence and fallback PTFs on your systems to allow those systems to coexist with z/OS V2.5 systems during your upgrade, and allow back out from z/OS V2.5 if necessary. Use the SMP/E REPORT MISSINGFIX command in conjunction with the FIXCAT type of HOLDDATA as follows:

1. Acquire and RECEIVE the latest HOLDDATA onto your pre-z/OS V2.5 systems. Use your normal service acquisition portals (recommended) or download the HOLDDATA directly from http://service.software.ibm.com/holdata/390holddata.html. Ensure you select **Full** from the Download NOW column to receive the FIXCAT HOLDDATA, as the other files do not contain FIXCATs.
2. Run the SMP/E REPORT MISSINGFIX command on your pre-z/OS V2.5 systems and specify a Fix Category (FIXCAT) value of **"IBM.Coexistence.z/OS.V2R5**". The report will identify any missing coexistence and fallback PTFs for that system. For complete information about the REPORT MISSINGFIX command, see *SMP/E Commands*.
3. Periodically, you might want to acquire the latest HOLDDATA and rerun the REPORT MISSINGFIX command to find out if there are any new coexistence and fallback PTFs.

Use SOFTCAP to identify the effect of capacity changes (Recommended)

Not required, but is recommended to help in assessing processor capacity and available resources when upgrading to new software levels, and when upgrading to z/Architecture.

Upgrade action:

- Download SoftCap from one of the following Web sites:
  - Customers: http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS268
  - Business partners: http://partners.boulder.ibm.com/src/atsmastr.nsf/Web/Techdocs. Note that this requires an ID on PartnerWorld®.Run SoftCap to determine your expected increase in CPU utilization (if any) and to identify your storage requirements, such as how much storage is needed to IPL.

Reference information: *SoftCap User's Guide*, which is provided with the tool.

General Upgrade Actions Pre-First IPL

Migrate /etc /global, and /var system control files (Required)

Upgrade action: The /etc, /global, and /var directories contain system control files: the /etc directory contains customization data that you maintain and the /global and /var directory contains customization data that IBM maintains. During installation, subdirectories of /etc , /global, and /var are created. If you install z/OS using ServerPac, some files are loaded into /etc /global, and /var due to the customization performed in ServerPac. You have to merge the files in /etc /global, and /var with those on your previous system. If you install z/OS using CBPDO, you should copy the files from your old system to the z/OS V2.5 /etc and /var subdirectories.

Copy files from your old system to the z/OS V2.5 /etc and /var subdirectories, and then modify the files as necessary to reflect z/OS V2.5 requirements. If you have other files under your existing /var directory, then you will have to merge the old and new files under /var. The easiest way to do this is to create a copy of your current /var files and then copy the new /var files into the copy.

The following elements and features use /etc:

- BCP (Predictive Failure Analysis).
- CIM.
- Communications Server (IP Services component).
- Cryptographic Services (PKI Services and System SSL components).
- DFSMSrmm.
- IBM HTTP Server.
- IBM Tivoli Directory Server (TDS). The LDAP server component uses /etc/ldap.
- Infoprint Server.
- Integrated Security Services. The Network Authentication Service component uses /etc/skrb.
- z/OS UNIX.

The following elements and features use /global:

- IBM Knowledge Center for z/OS
- IBM z/OS Management Facility (z/OSMF).

The following elements and features use /var:

- Cryptographic Services (OCSF component). See OCSF: Migrate the directory structure.
- DFSMSrmm.
- IBM Tivoli Directory Server (TDS). The LDAP server component uses /var/ldap.
- Infoprint Server.
- Integrated Security Services. The Network Authentication Service component uses /var/skrb.

Back virtual storage with real and auxiliary storage (Required)

Upgrade action: As you exploit additional virtual storage by defining additional address spaces or by exploiting memory objects, ensure that you have defined sufficient real and auxiliary storage. Review real storage concentration indicators via an RMF report to evaluate if additional real or auxiliary storage is needed:

- Check UIC and average available frames.
- Check demand page rates.
- Check the percentage of auxiliary slots in use.

Reference information: For more information about memory objects, see *z/OS MVS Programming: Extended Addressability Guide* and Washington Systems Center flash 10165 at http://www.ibm.com/support/techdocs. (Search for “flash10165”.)

Remove references to deleted data sets and path (Required)

Upgrade action: Using the tables in *z/OS Upgrade Workflow* as a guide, remove references to data sets and paths that no longer exist. Remove the references from the following places:

- Parmlib
- Proclib
- Logon procedures
- Catalogs
- Security definitions, including program control definitions
- DFSMS ACS routines
- /etc/profile
- SMP/E DDDEF entry (if you installed with CBPDO)
- Backup and recovery procedures, as well as any references to them in the table, the high-level qualifiers in the data set names are the default qualifiers.

Note: Do not remove any data sets, paths, or references that are needed by earlier-level systems until those systems no longer need them, and you are sure you won’t need them for fallback.

Reference information: *z/OS Upgrade Workflow* contains the list of all removed data sets and paths in z/OS V2R.5 and V2.4.

Add references to new data sets (Required)

Upgrade action: For z/OS V2.5, RMF and z/OS Data Gatherer, had several data sets restructured. Follow the RMF upgrade action to make the necessary parmlib and SYSPROC changes.

For z/OS V2.4, the following element had a DLIB data set and a path (with a file system) that were added:

- z/OS Container Extensions

Accommodate new address spaces (Recommended)

Not required, but recommended to keep interested personnel aware of changes in the system and to ensure that your MAXUSER value in parmlib member IEASYSxx is adequate.

The following elements adds new address spaces for z/OS V2.4, which are exploitation support, and are not upgrade actions:

- **z/OS Authorized Code Scanner (zACS)** This new priced feature, added post-GA of z/OS V2.4 adds one new address space, BPNZACS. zACS provides the capability of testing PC and SVC routines to determine if they might result in a security vulnerability.
- **z/OS Container Extensions**. This a new element in z/OS V2.4. It provides the runtime support to deploy and run Linux on IBM Z applications that are packaged as Docker Container images on z/OS. zCX creates one address space for each provisioned server that is started by the user.

The MAXUSER value in parmlib member IEASYS*xx* specifies a value that the system uses to limit the number of jobs and started tasks that can run concurrently during a given IPL. You might want to increase your MAXUSER value to take new address spaces into account. (A modest overspecification of MAXUSER should not hurt system performance. The number of total address spaces is the sum of M/S, TS USERS, SYSAS, and INITS. If you change your MAXUSER value, you must re-IPL to make the change effective.)

Update your check customization for modified IBM Health Checker for z/OS checks (Recommend)

Not required, but recommended to ensure that your checks continue to work as you intend them to work.

Changes that IBM makes to the checks provided by IBM Health Checker for z/OS can affect any updates you might have made.

The following health checks are new in z/OS V2R5:

- RACF_ADDRESS_SPACE
- RACF_ERASE_ON_SCRATCH
- RACF_PROTECTALL_FAIL
- RACF_PTKTDATA_CLASS
- RACF_SYSPLEX_COMMUNICATION

The following health checks are changed in z/OS V2R5:

- RACF_SENSITIVE_RESOURCES

The following health checks were added by IBM in z/OS V2R4:

- IBMCS,ZOSMIGV2R4_NEXT_CS_OSIMGMT
- IBMCS,ZOSMIGV2R4PREV_CS_IWQSC_tcpipstackname
- IBM_JES2,JES2_UPGRADE_CKPT_LEVEL_JES2
- IBMICSF,ICSF_PKCS_PSS_SUPPORT
- IBMINFOPRINT,INFOPRINT_CENTRAL_SECURE_MODE
- IBMINFOPRINT,ZOSMIGV2R3_NEXT_INFOPRINT_IPCSSL
- IBMISPF,ISPF_WSA
- IBMRSM,RSM_MINIMUM_REAL
- IBMSDSF,SDSF_CLASS_SDSF_ACTIVE
- IBMVSM,ZOSMIGV2R3_NEXT_VSM_USERKEYCOMM

The following health checks were changed by IBM in z/OS V2R4:

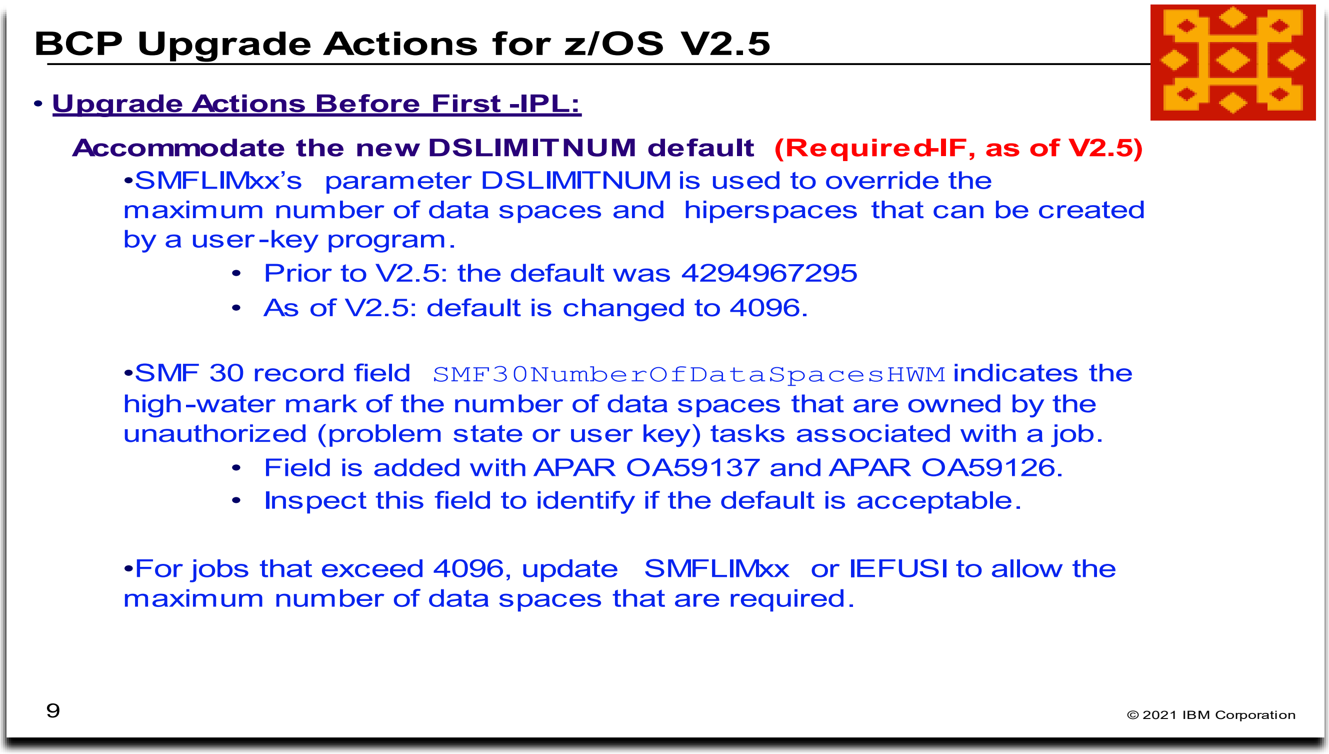
- IBMUSS,ZOSMIGV2R3_NEXT_USS_SMB_DETECTED
- IBMCS,CSVTAM_CSM_STG_LIMIT

The following health checks were deleted by IBM in z/OS V2R4:

- ZOSMIGV1R12_INFOPRINT_INVSIZE

Upgrade action:

1. Look at the updated checks in *IBM Health Checker for z/OS: User's Guide*.
2. Review changes you made for those checks, in HZSPRM*xx* parmlib members, for example.
3. Make any further updates for the checks to ensure that they continue to work as intended.

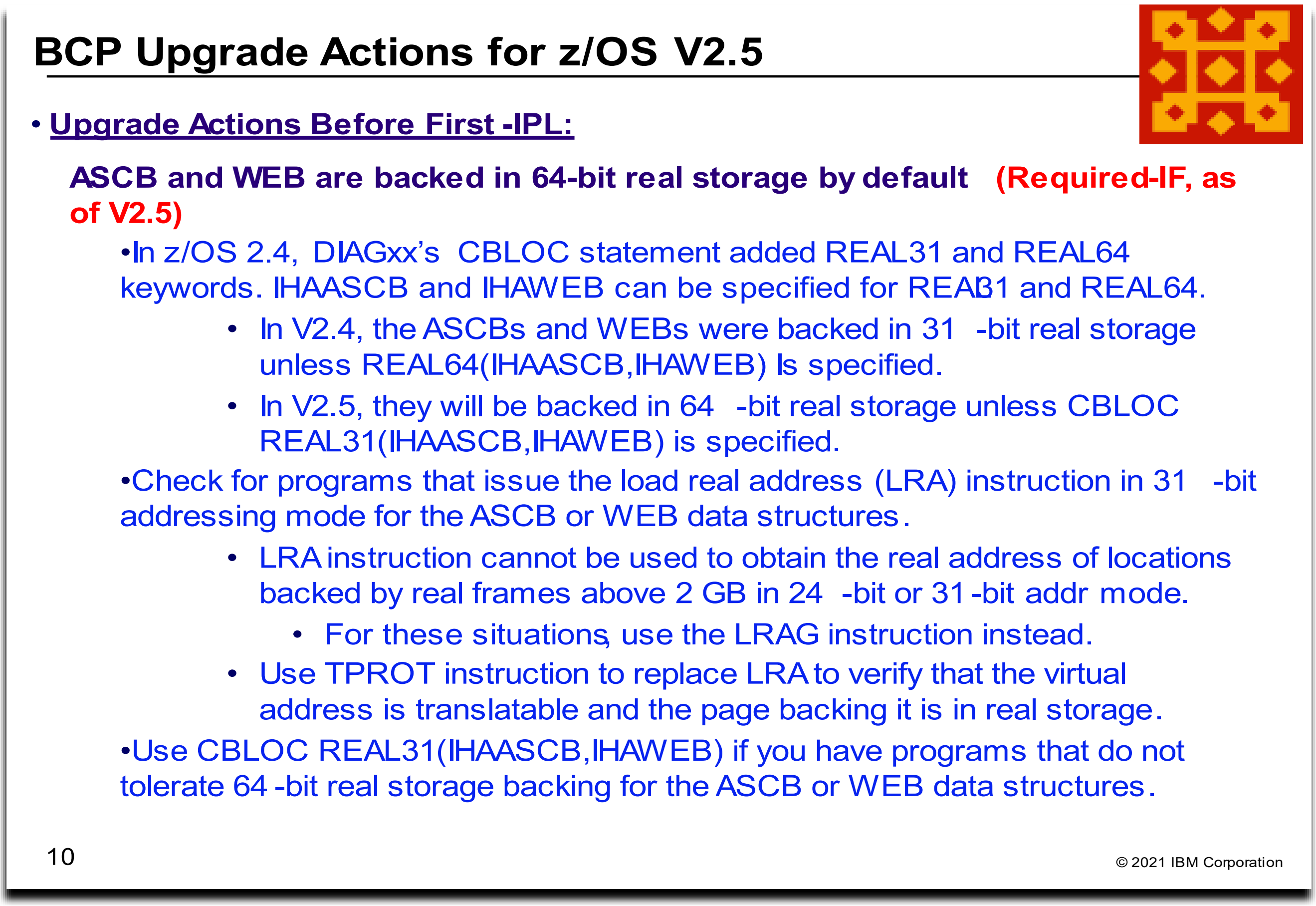


BCP Upgrade Actions for z/OS V2.5

- **Upgrade Actions Before First -IPL:**

Accommodate the new DSLIMITNUM default (Required-IF, as of V2.5)

- SMFLIMxx's parameter DSLIMITNUM is used to override the maximum number of data spaces and hiperspaces that can be created by a user-key program.
  - Prior to V2.5: the default was 4294967295
  - As of V2.5: default is changed to 4096.
- SMF 30 record field `SMF30NumberOfDataSpacesHWM` indicates the high-water mark of the number of data spaces that are owned by the unauthorized (problem state or user key) tasks associated with a job.
  - Field is added with APAR OA59137 and APAR OA59126.
  - Inspect this field to identify if the default is acceptable.
- For jobs that exceed 4096, update SMFLIMxx or IEFUSI to allow the maximum number of data spaces that are required.

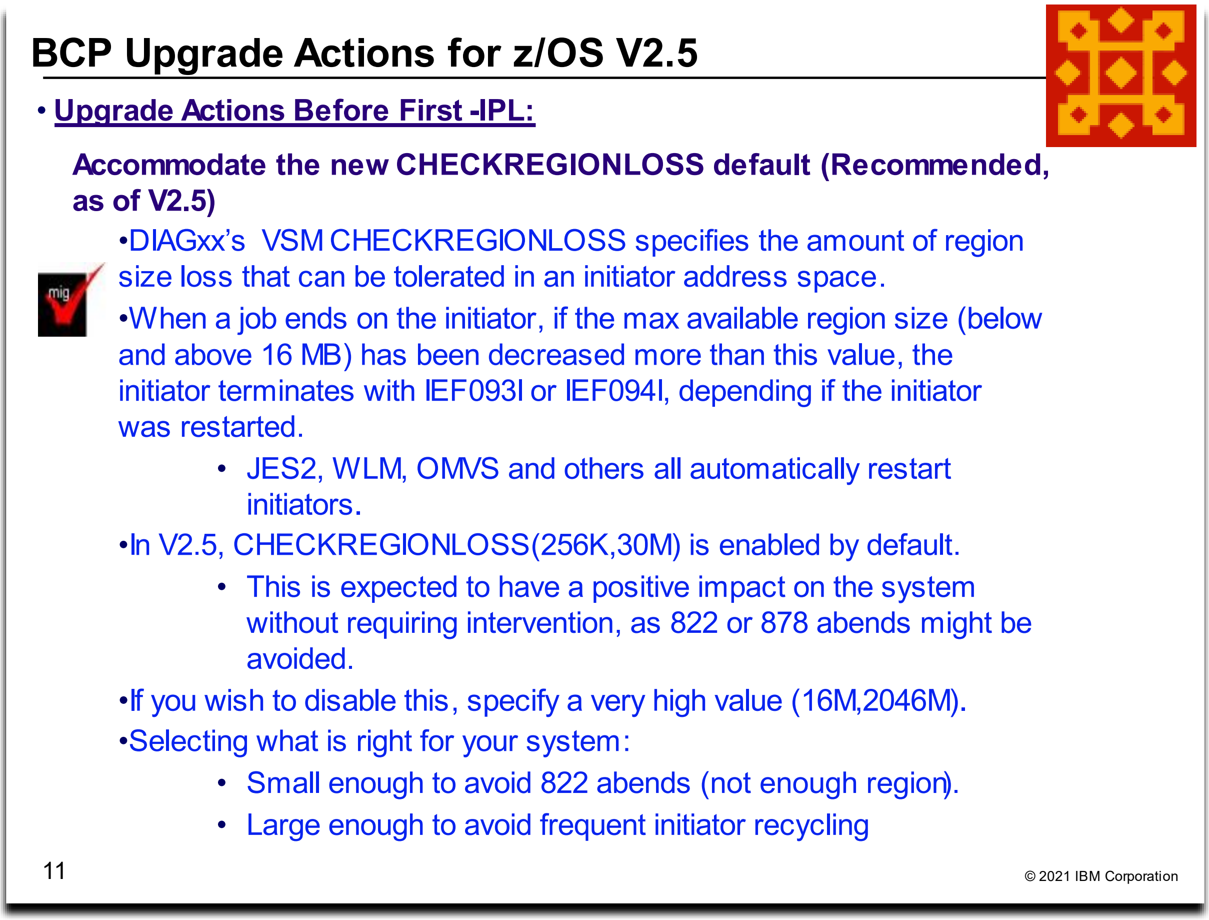


BCP Upgrade Actions for z/OS V2.5

- **Upgrade Actions Before First -IPL:**

ASCB and WEB are backed in 64-bit real storage by default (Required-IF, as of V2.5)

- In z/OS 2.4, DIAGxx's CBLOC statement added REAL31 and REAL64 keywords. IHAASCB and IHAWEB can be specified for REAL31 and REAL64.
  - In V2.4, the ASCBs and WEBs were backed in 31 -bit real storage unless REAL64(IHAASCB,IHAWEB) Is specified.
  - In V2.5, they will be backed in 64 -bit real storage unless CBLOC REAL31(IHAASCB,IHAWEB) is specified.
- Check for programs that issue the load real address (LRA) instruction in 31 -bit addressing mode for the ASCB or WEB data structures.
  - LRA instruction cannot be used to obtain the real address of locations backed by real frames above 2 GB in 24 -bit or 31 -bit addr mode.
    - For these situations, use the LRAG instruction instead.
  - Use TPROT instruction to replace LRA to verify that the virtual address is translatable and the page backing it is in real storage.
- Use CBLOC REAL31(IHAASCB,IHAWEB) if you have programs that do not tolerate 64 -bit real storage backing for the ASCB or WEB data structures.



BCP Upgrade Actions for z/OS V2.5

- Upgrade Actions Before First -IPL:

Accommodate the new CHECKREGIONLOSS default (Recommended, as of V2.5)

- DIAGxx's VSM CHECKREGIONLOSS specifies the amount of region size loss that can be tolerated in an initiator address space.
- When a job ends on the initiator, if the max available region size (below and above 16 MB) has been decreased more than this value, the initiator terminates with IEF093I or IEF094I, depending if the initiator was restarted.
  - JES2, WLM, OMVS and others all automatically restart initiators.
- In V2.5, CHECKREGIONLOSS(256K,30M) is enabled by default.
  - This is expected to have a positive impact on the system without requiring intervention, as 822 or 878 abends might be avoided.
- If you wish to disable this, specify a very high value (16M,2046M).
- Selecting what is right for your system:
  - Small enough to avoid 822 abends (not enough region).
  - Large enough to avoid frequent initiator recycling

11

© 2021 IBM Corporation

BCP Upgrade Actions For z/OS V2.5

These upgrade actions were taken from *z/OS V2.5 Upgrade Workflow.* Some descriptions and actions have been shortened for inclusion in this presentation. Not all upgrade actions have been included. For the complete descriptions and actions, refer to *z/OS V2.5 Upgrade Workflow.*

BCP Upgrade Actions Pre-First IPL

Accommodate the new DSLIMITNUM default (Required-IF, as of V2.5)

Required if the default is not acceptable on your system.

In the SMFLIMxx parmlib member, the parameter DSLIMITNUM is used to override the maximum number of data spaces and hiperspaces that can be created by a user-key program. In z/OS V2R5, the default for DSLIMITNUM is changed to 4096. In previous releases, the default was 4294967295.

Applications that invoke DSPSERV CREATE, especially those applications that loop erroneously, might fail with the more restrictive DSLIMITNUM default in effect.

Upgrade action: SMF 30 record field SMF30NumberOfDataSpacesHWM indicates the high-water mark of the number of data spaces that are owned by the unauthorized (problem state and user key) tasks that are associated with a job. This field is added when you apply APAR OA59137 and APAR OA59126.

If your installation runs jobs that rely on the default for SMFLIMxx DSLIMITNUM or IEFUSI word 7 subword 3, inspect the SMF 30 record field SMF30NumberOfDataSpacesHWM fields for values that exceed 4096. For jobs that exceed 4096, update SMFLIMxx or IEFUSI to allow the maximum number of data spaces that are required.

ASCB and WEB are backed in 64-bit real storage by default (Required-IF, as of V2.5)

Required if you have an application that relies on the ASCB or WEB to be backed in 31-bit real storage.

In z/OS 2.5, the address space control block (which is mapped by IHAASCB) and the work element block (which is mapped by IHAWEB) are backed in 64-bit real storage by default. Previously, these data structures were backed in 31-bit storage, unless your DIAGxx parmlib member specified CBLOC REAL31(IHAASCB,IHAWEB).

In z/OS 2.4, the keywords REAL31 and REAL64 were added to the CBLOC statement of parmlib member DIAGxx. With these keywords, you can specify which data structures are backed in 31-bit real storage or 64-bit real storage.

Upgrade action: Check for programs that issue the load real address (LRA) instruction in 31-bit addressing mode for the ASCB or WEB data structures. The LRA instruction cannot be used to obtain the real address of locations backed by real frames above 2 gigabytes in 24-bit or 31-bit addressing mode. For those situations, use the LRAG instruction instead of LRA. The TPROT instruction can be used to replace the LRA instruction when a program is using it to verify that the virtual address is translatable and the page backing it is in real storage. If you have programs that do not tolerate 64-bit real storage backing for the ASCB or WEB data structures, update the DIAGxx parmlib member to specify CBLOC REAL31(IHAASCB,IHAWEB).

Accommodate the new CHECKREGIONLOSS default (Recommended, as of V2.5)

Recommended. Enabling the CHECKREGIONLOSS option causes initiator address spaces to be recycled when the maximum obtainable region size is reduced below a threshold. This change is expected to have a positive impact on the system without requiring any intervention

In the DIAGxx parmlib member, the parameter VSM CHECKREGIONLOSS specifies the amount of region size loss that can be tolerated in an initiator address space. The initiator remembers the initial maximum available region size (below and above 16 MB) before it selects its first job. Whenever a job ends in the initiator, if the maximum available region size (below or above 16MB) is decreased from the initial value by more than the CHECKREGIONLOSS specification, the initiator ends with message IEF0931 or IEF094A, depending on whether the subsystem automatically restarts the initiator.

When CHECKREGIONLOSS is enabled, your installation can avoid encountering 822 abends or 878 abends in subsequent jobs that are selected by the initiator. These abends can occur when the available region size decreases because of storage fragmentation or problems that prevent storage from being freed.

In z/OS V2R5, CHECKREGIONLOSS is enabled by default with a value of (256K,30M). This change means that when the 24-bit region size decreases by 256K or more, or when the 31-bit region size decreases by 30M or more, the initiator is ended and restarted, with message IEF0931 or IEF094A.

Upgrade action: Verify that the CHECKREGIONLOSS option is specified in your active DIAGxx parmlib member:

- If the CHECKREGIONLOSS option is not specified in your active DIAGxx parmlib member, determine whether you want the option to be disabled on your z/OS V2R5 system. If so, you can set the CHECKREGIONLOSS to a very high value such as (16M,2046M), which will effectively disable the option.
- If the CHECKREGIONLOSS option is specified in your active DIAGxx parmlib member, and you want to continue using your current setting, you have no action to take. Consider using the IBM default setting CHECKREGIONLOSS(256K,30M).

Stop referencing the ETR parmaters in CLOCKxx (Recommended, as of V2.4)

In z/OS V2R4, the default values of the CLOCKxx parmlib member ETRMODE and ETRZONE parameters are changed from YES to NO.

The IBM z10 was the last IBM mainframe to support the ETRMODE and ETRZONE parameters in CLOCKxx. Because z/OS V2R4 requires a zEC12 or later processor to run, the ETRMODE and ETRZONE parameters are now obsolete. They are deactivated (set to NO) by default.

It is recommended that you set these parameters to NO, or remove them from CLOCKxx. Specifying YES can cause unexpected behavior if you also specify STPZONE NO. For details, see APAR OA54440.

Upgrade action: Review the CLOCKxx member that you use to IPL your system, and take one of the following actions:

- If CLOCKxx does not specify ETRMODE or ETRZONE, you have no action to take.
- If CLOCKxx specifies ETRMODE YES or ETRZONE YES, set these parameters to NO, or remove them so that they default to NO.
- If CLOCKxx specifies ETRMODE NO and ETRZONE NO, you have no action to take.

Evaluate the changed default for system logger’s use of IBM zHyperwrite (Required-IF, as of V2.4)

Required if you want system logger to use IBM zHyperwrite data replication.

With the installation of APAR OA57408, the use of IBM zHyperWrite data replication by system logger is changed from enabled to disabled by default.The IBM zHyperWrite function was originally provided by APAR OA54814.

In parmlib member IXFCNFx, this option is specified, as follows:

```
MANAGE . . . HYPERWRITE ALLOWACCESS(YESNO)
```

When IBM zHyperwrite is enabled for use with system logger, it provides data replication for the following types of log stream data sets:

- Staging data sets for DASDONLY type log streams
- Offload data sets for both the DASDONLY type and Coupling Facility structure-based type log streams.

System logger does not use zHyperwrite for the staging data sets for Coupling Facility structure-based type log streams.

Upgrade action: If you do not want system logger to use IBM zHyperwrite data replication, you have no action to take. When you install APAR OA57408, the use of IBM zHyperWrite data replication by system logger is disabled by default. To determine whether system logger on your system uses IBM zHyperwrite data replication, you can query the current setting by entering the following command:

```
DISPLAY LOGGER,IXGCNF,MANAGE
```

In response, message IXG607I identifies the current setting. To enable system logger use of IBM zHyperwrite data replication, you can do either of the following:

- Enter the command SETLOGR MANAGE,HYPERWRITE,ALLOWUSE(YES)
- Update the IXGCNFxx parmlib member with ALLOWUSE(YES).

Prepare for the removal of support for user key common areas (Required, as of V2.4)

IBM strongly recommends that you eliminate all use of user key common storage. Allowing programs to obtain user key (8-15) common storage creates a security risk because the storage can be modified or referenced, even if fetch protected, by any unauthorized program from any address space. Therefore, without the restricted use common service area (RUCSA) optional priced feature, the obtaining of user key (8-15) storage is not supported in z/OSV2R4.

RUCSA is more secure because it can be managed as a SAF resource. However, it does not prevent two or more different SAF-authorized applications from altering or referencing another application's RUCSA storage. RUCSA became available as a part of the BCP base element with APAR OA56180 on earlier z/OS releases, but it is only available as a priced feature in z/OS V2R4.

Related to this change:

- Support to change the key of common ESQA storage to a user key (via CHANGKEY) is removed regardless of RUCSA exploitation.
- NUCLABEL DISABLE(IARXLUK2) is no longer a valid statement in the DIAGxx parmlib member. (Note: This statement only exists in z/OS V2R3.)
- Support of user-key (8 - 15) SCOPE=COMMON data spaces is removed regardless of RUCSA exploitation.
- YES is no longer a valid setting for the following statements in the DIAGxx parmlib member: VSM ALLOWUSERKEYCSA - controls the allocation of user key CSA. ALLOWUSERKEYCADS - controls the allocation of user key SCOPE=COMMON data space

Upgrade action:

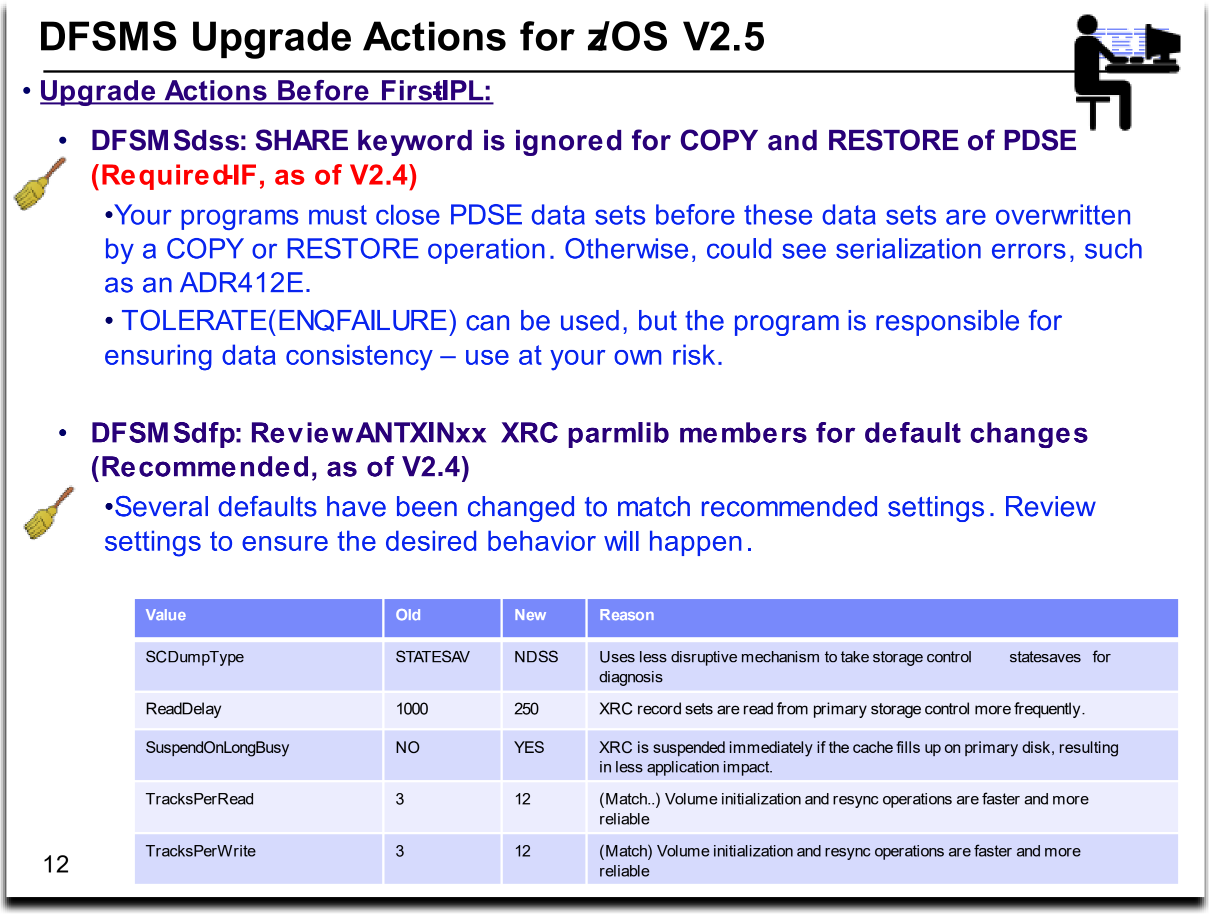
- See Part 1 (Planning) information for the details on this removal.

Review the list of WTORs in parmlib member AUTOR00 (Required)

As of z/OS V1R12, the DDDEF'd PARMLIB provides an AUTOR00 member. This member should be found in your parmlib concatenation during IPL and will result in auto-reply processing being activated. If the WTORs listed in AUTOR00 are automated by your existing automation product, ensure that the replies in AUTOR00 are appropriate.

Upgrade action: Examine the WTOR replies in the AUTOR00 parmlib member. If the replies or delay duration are not desirable, you can create a new AUTORxx parmlib member and make corresponding changes. Also compare the replies to what your automation product would reply to these WTORs. Make sure that the AUTOR00 replies are in accordance with the replies from your automation product. IBM does not recommend making updates to AUTOR00, because updates to AUTOR00 might be made by the service stream or in new z/OS releases.

There were no updates to AUTOR00 for z/OS V2.5.
There were updates to AUTOR00 for z/OS V2.4.



DFSMS Upgrade Actions for z/OS V2.5

- **Upgrade Actions Before First IPL:**
  - **DFSMSdss: SHARE keyword is ignored for COPY and RESTORE of PDSE (Required-IF, as of V2.4)**
    - •Your programs must close PDSE data sets before these data sets are overwritten by a COPY or RESTORE operation. Otherwise, could see serialization errors, such as an ADR412E.
    - • TOLERATE(ENQFAILURE) can be used, but the program is responsible for ensuring data consistency – use at your own risk.
  - **DFSMSdfp: Review ANTXINxx XRC parmlib members for default changes (Recommended, as of V2.4)**
    - •Several defaults have been changed to match recommended settings. Review settings to ensure the desired behavior will happen.

Value	Old	New	Reason
SCDumpType	STATESAV	NDSS	Uses less disruptive mechanism to take storage control statesaves for diagnosis
ReadDelay	1000	250	XRC record sets are read from primary storage control more frequently.
SuspendOnLongBusy	NO	YES	XRC is suspended immediately if the cache fills up on primary disk, resulting in less application impact.
TracksPerRead	3	12	(Match..) Volume initialization and resync operations are faster and more reliable
TracksPerWrite	3	12	(Match) Volume initialization and resync operations are faster and more reliable

12

DFSMS Upgrade Actions For z/OS V2.5

These upgrade actions were taken from *z/OS V2.5 Upgrade Workflow.* Some descriptions and actions have been shortened for inclusion in this presentation. Not all upgrade actions have been included. For the complete descriptions and actions, refer to *z/OS V2.5 Upgrade Workflow.*

DFSMS Upgrade Actions You Can Do Now

DFSMSdfp: Increase storage for SMS ACDS data sets (Required-IF, as of OA52913)

Required if you use the ACDS and it is reaching full capacity.

With APAR OA52913, the length of the management class definition (MCD) in the SMS active control data set (ACDS) was increased from 328 to 760 bytes. This change was made in support of automatic migration support for transparent cloud tiering (TCT). With this change, the values that are used to estimate the size of storage that is needed for an active control data set are out of date.

If the ACDS data set is full, the follow errors could occur:

- `IEC070I 203: Extend was attempted but no secondary space was specified`
- `IGD058I 6068 (X'17B4’): Problem could be caused by insufficient space to extend the data set`

Check your utilization of the ACDS. To prevent the ACDS from reaching full, consider reallocating the ACDS to allow for more space. When you allocate the SCDS and ACDS, specify secondary space allocations. This action helps to ensure that extends can be performed when:

- New classes, groups, and other structures are added
- Sizes of these structures increase in size.

DFSMS UpgradeActions Pre-First IPL

DFSMSdss: SHARE keyword is ignored for COPY and RESTORE of PDSE (Req-IF, as of V2.4)

Required if your programs open PDSE data set when DFSMSdss is writing to them.

Starting in z/OS V2R4, your programs must close PDSE data sets before these data sets are overwritten by a DFSMSdss COPY or RESTORE operation. Otherwise, the DFSMSdss COPY or RESTORE operation encounters serialization errors, such as an ADR412E.

Note: This behavior occurs regardless of whether the SHARE keyword is specified.

For programs that cannot close the PDSE data sets while a COPY or RESTORE operation is in progress, these programs can specify the TOLERATE(ENQFAILURE) keyword. If so, the program is responsible for ensuring data onsistency. IBM recommends against using the TOLERATE(ENQFAILURE) keyword; use it at your own risk.

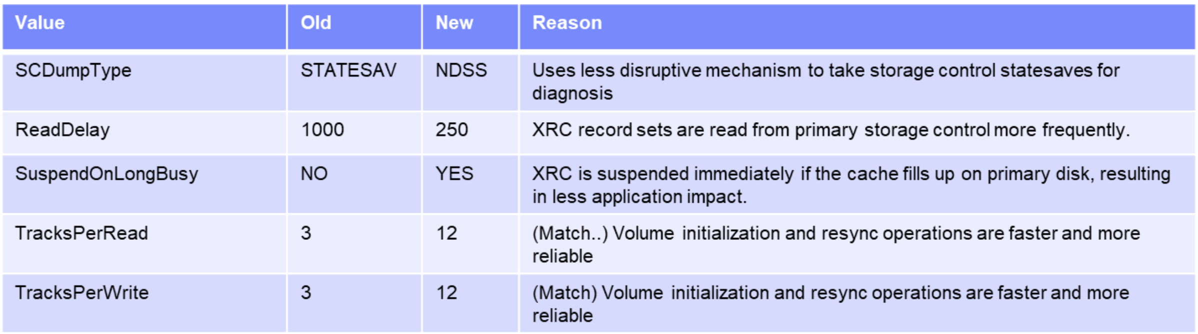
Upgrade action: Applications must now close PDSEs before a copy or restore is to overwrite it. If you do not close down the application, serialization errors such as an ADR412E occurs on the DFSMSdss copy or restore.

Note: Changing DFSMSdss to ignore the SHARE keyword for output data sets ensure integrity and prevent DFSMSdss from restoring a PDSE that an application has open. It also prevents an application from opening a PDSE that DFSMSdss is restoring.

DFSMSdfp: Review XRC parmlib members for use of default values (Recommended, as of V2.4)

Required if your programs open PDSE data set when DFSMSdss is writing to them.

In z/OS V2R4, some XRC (Extended Remote Copy, aka Global Mirror), default settings are changed to match IBM recommendations. If you depend on the old default, you must explicitly specify the old values in the appropriate parmlib members.

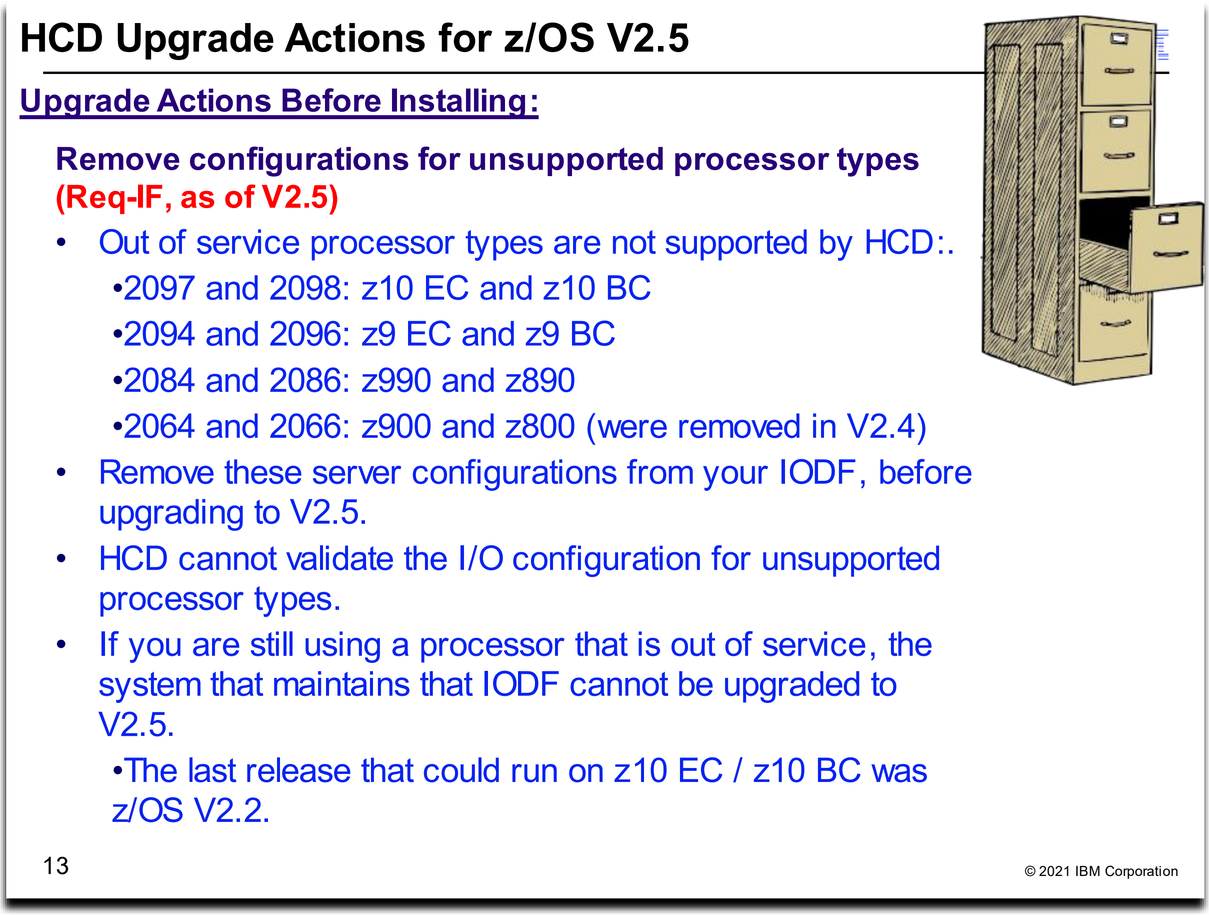


Value	Old	New	Reason
SCDumpType	STATESAV	NDSS	Uses less disruptive mechanism to take storage control statesaves for diagnosis
ReadDelay	1000	250	XRC record sets are read from primary storage control more frequently.
SuspendOnLongBusy	NO	YES	XRC is suspended immediately if the cache fills up on primary disk, resulting in less application impact.
TracksPerRead	3	12	(Match..) Volume initialization and resync operations are faster and more reliable
TracksPerWrite	3	12	(Match) Volume initialization and resync operations are faster and more reliable

Upgrade action: Examine parmlib members that are related to XRC for settings with changed defaults:

If the setting is not specified in any of the XRC-related parmlib members, determine whether the old default value needs to be retained according to the following table. If the value needs to be the old default, it must be specified in the member. Otherwise, the new default takes effect when XRC is started on the new z/OS release.

If the setting is specified in an XRC-related parmlib member (with any value, but especially with the old default value), consider whether the new default value is appropriate to use.



HCD Upgrade Actions for z/OS V2.5

Upgrade Actions Before Installing:

Remove configurations for unsupported processor types (Req-IF, as of V2.5)

- Out of service processor types are not supported by HCD:.
  - 2097 and 2098: z10 EC and z10 BC
  - 2094 and 2096: z9 EC and z9 BC
  - 2084 and 2086: z990 and z890
  - 2064 and 2066: z900 and z800 (were removed in V2.4)
- Remove these server configurations from your IODF, before upgrading to V2.5.
- HCD cannot validate the I/O configuration for unsupported processor types.
- If you are still using a processor that is out of service, the system that maintains that IODF cannot be upgraded to V2.5.
  - The last release that could run on z10 EC / z10 BC was z/OS V2.2.

13

HCD Upgrade Actions For z/OS V2.5

These upgrade actions were taken from *z/OS V2.5 Upgrade Workflow.* Some descriptions and actions have been shortened for inclusion in this presentation. Not all upgrade actions have been included. For the complete descriptions and actions, refer to *z/OS V2.5 Upgrade Workflow.*

HCD Upgrade Actions You Can Do Now

Remove configurations for unsupported processor types (Required-IF, as of V2.5)

Required if you unsupported processors are still defined in your IODF.

In z/OS V2R5, HCD removes support for processor types that are out of service. Specifically, HCD no longer supports the following processors types:

- IBM z10 EC, processor type 2097, models E12, E26, E40, E56, and E64
- IBM z10 BC, processor type 2098, model E10
- IBM z9 EC, processor type 2094, models S08, S18, S28, S38 and S54
- IBM z9 BC, processor type 2096, models R07 and S07
- IBM z990, processor type 2084, models A08, B16, C24, and D32
- IBM z890, processor type 2086, model A04

z/OS V2R5 does not run on these servers. z/OS V2.3 runs on EC12, BC12 or higher.

Previously, in z/OS V2R4, support was withdrawn for the IBM z900 (processor type 2064) and IBM z800 (processor type 2066).

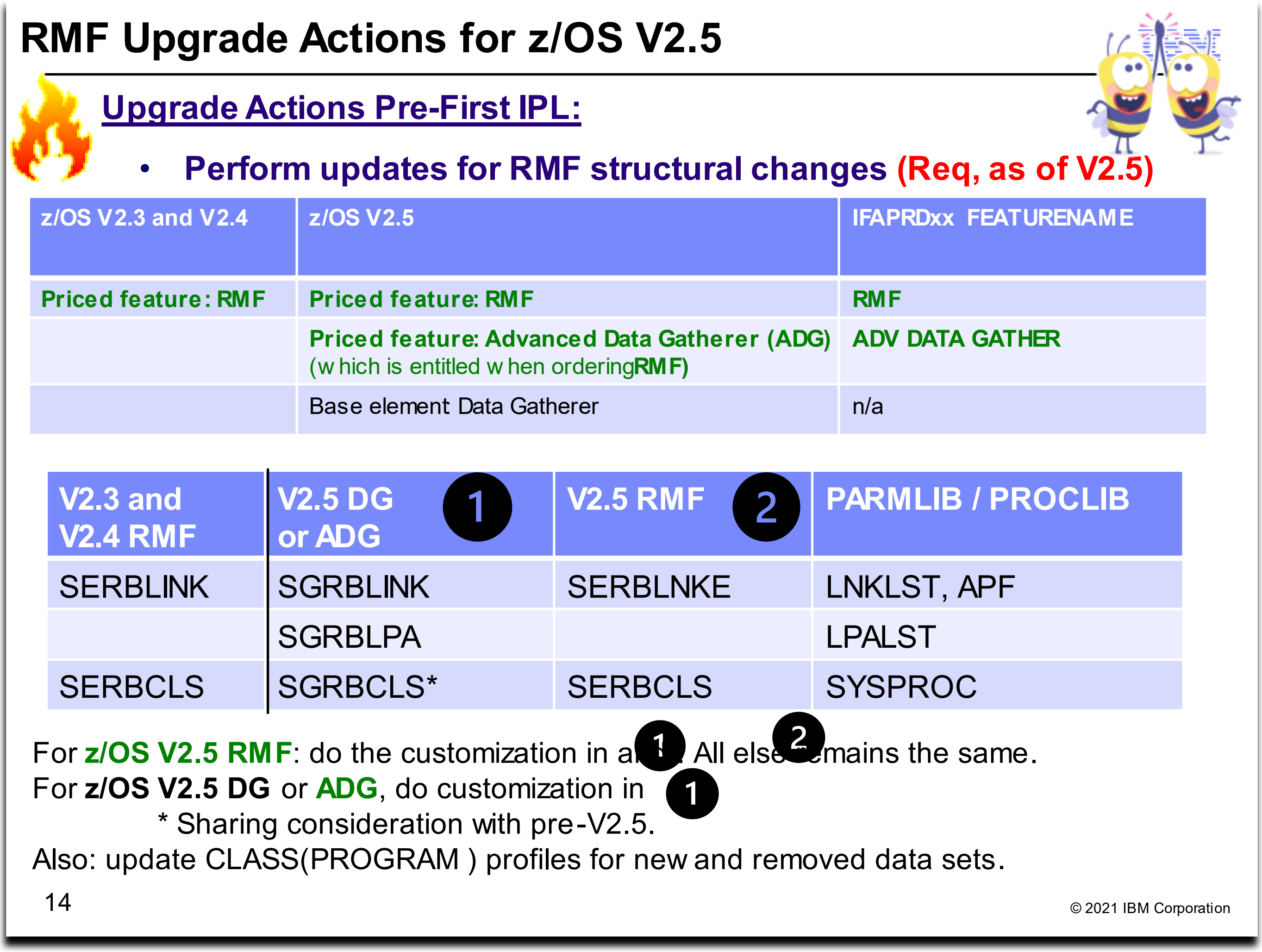
If your I/O definition file (IODF) contains definitions for these servers, and you use HCD to maintain your configuration, you must delete the old definitions before moving to z/OS V2R5. HCD cannot validate the I/O configuration for unsupported processor types.

Steps to take: Check your currently active IODFs to determine whether you have any saved processor configurations for these out-of-service processors. Foillow these steps:

1. Start HCD.
2. Select option 1 “Define, modify, or view configuration data”
3. Select option 3 “Processors” to see the list of defined processor configurations.
4. Check the Type column for any of the out-of-service processor types.

5. If you still have any processor configuration for one or more of the out-of-service processor types, determine whether the processor is still in use. If not, delete the configuration.

Otherwise, if the processor it is still in use, the system that maintains the IODF cannot be upgraded to z/OS V2R5.



RMF Upgrade Actions for z/OS V2.5

Upgrade Actions Pre-First IPL:

- **Perform updates for RMF structural changes (Req, as of V2.5)**

z/OS V2.3 and V2.4	z/OS V2.5	IFAPRDxx FEATURENAME
Priced feature: RMF	Priced feature: RMF	RMF
	Priced feature: Advanced Data Gatherer (ADG) (which is entitled when ordering RMF)	ADV DATA GATHER
	Base element Data Gatherer	n/a

V2.3 and V2.4 RMF	V2.5 DG or ADG ❶	V2.5 RMF ❷	PARMLIB / PROCLIB
SERBLINK	SGRBLINK	SERBLNKE	LNKLST, APF
	SGRBLPA		LPALST
SERBCLS	SGRBCLS*	SERBCLS	SYSPROC

For **z/OS V2.5 RMF**: do the customization in a❶. All else ❷remains the same.
For **z/OS V2.5 DG** or **ADG**, do customization in ❶
* Sharing consideration with pre-V2.5.
Also: update CLASS(PROGRAM) profiles for new and removed data sets.

14

© 2021 IBM Corporation

RMF Upgrade Actions For z/OS V2.5
This upgrade action was taken from *z/OS V2.5 Upgrade Workflow.* Some descriptions and actions have been shortened for inclusion in this presentation. Not all upgrade actions have been included. For the complete descriptions and actions, refer to *z/OS V2.5 Upgrade Workflow.*

RMF Upgrade Actions Pre-First IPL

Determine updates for RMF structural changes (Required, as of V2.5)
When the PTFs for APARs OA58281 and OA58759 are applied to z/OS V2.3 or V2.4, the RMF product is restructured into the Data Gatherer and Reporter components. In z/OS V2.5, the Data Gatherer component is packaged and delivered as separate FMID, and a priced feature of Advanced Data Gatherer is added..

With the z/OS Data Gatherer now included in the z/OS base, the RMF installation procedure and licensing model are changed. RMF consists of two components that work together to provide performance management capabilities, as follows:

z/OS Data Gatherer
  Collects performance measurements from the hardware and operating system and provides access to these measurements across the sysplex.
RMF Reporter
  Uses the collected measurements to report performance statistics in tabular and graphical reports
  The term RMF refers to the RMF Reporter component. When you are entitled to RMF, you are also entitled to the Advanced Data Gatherer priced feature.

In z/OS V2.5, the Data Gatherer base z/OS component (566527401) is shipped within the same FMID as the z/OS Advanced Data Gatherer priced feature, FMID HRG77D0. The RMF Reporter component (566527404) remains in the priced RMF feature and is packaged in the existing FMIDs HRM77D0 and JRM77DJ.

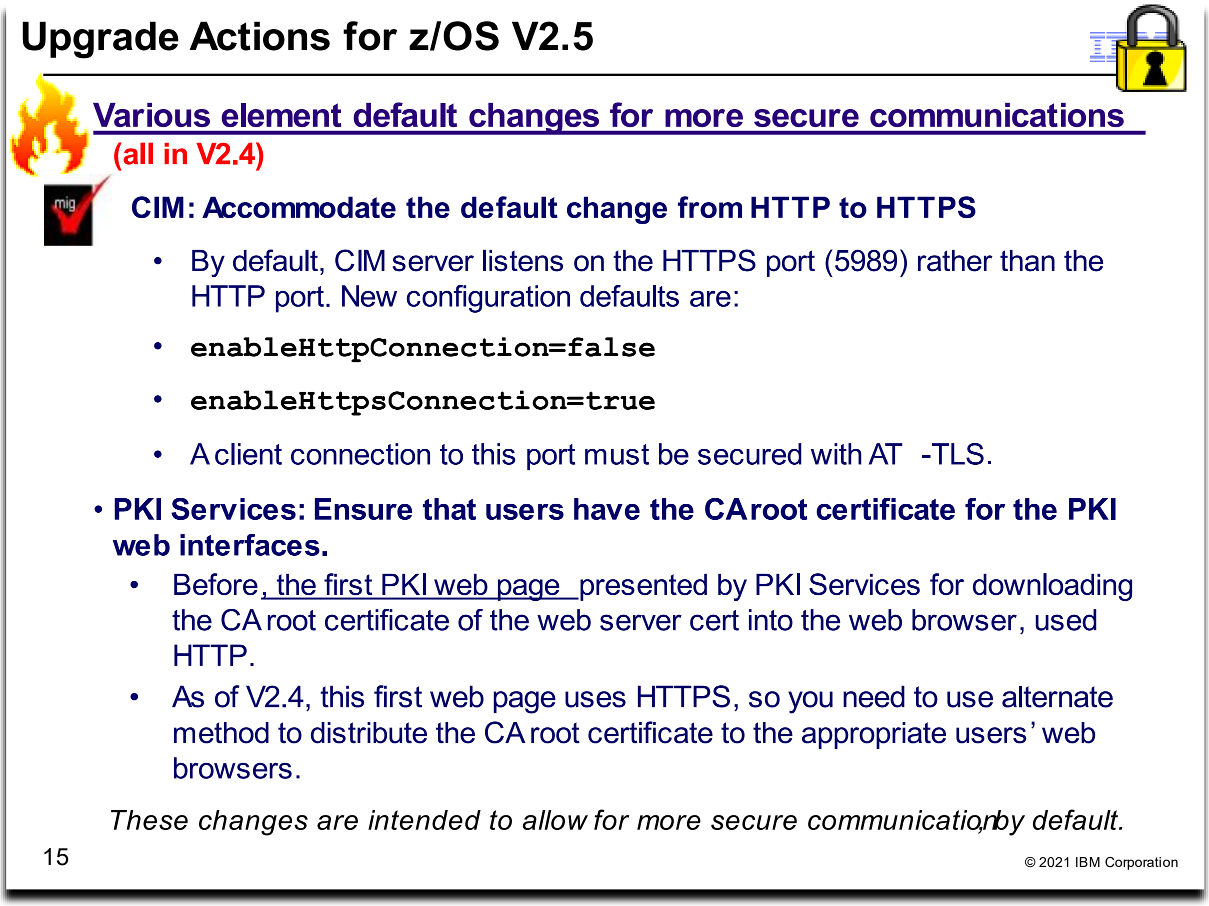
The new RMF feature provides the same capabilities as the RMF feature. The RMF feature entitles you to use both RMF Reporter and z/OS Advanced Data Gatherer.

Upgrade action:

- z/OS Data Gatherer product libraries SYS1.SGRBLINK must be added to the link list and APF list. SYS1.SGRBLPA must be added to the LPA list.
- RMF users must change SERBLINK to SERBLNKE in the link list.
- IBM supplied procedures RMF and RMFGAT are installed into SYS1.PROCLIB (as in previous releases), but are part of z/OS Data Gatherer.
- IBM supplied procedures RMFCSC, RMFM3B, GPMSERVE, GPM4CIM are installed into SYS1.PROCLIB and are owned by RMF, as in previous releases.
- IBM supplied CLISTs ERBS2V, ERBV2S, and REXX execs ERBSCAN, ERBSHOW, ERBVSDEF, are installed into SYS1.SGRBCLS during z/OS Data Gatherer installation. Make it available to your SYSPROC. If you use RMF, make SERBCLS available in your SYSPROC.
- Make the follow updates to your RACF program profiles:

```
RALT PROGRAM ERB* DELMEM('SYS1.SERBLINK’ //NOPADCHK)
RALT PROGRAM GPM* DELMEM('SYS1.SERBLINK’ //NOPADCHK)

RALT PROGRAM ERB* ADDMEM('SYS1.SERBLNKE’ //NOPADCHK)
RALT PROGRAM GPM* ADDMEM('SYS1.SERBLNKE’ //NOPADCHK)
RALT PROGRAM ERB* ADDMEM('SYS1.SGRBLINK’ //NOPADCHK)
RALT PROGRAM GRB* ADDMEM('SYS1.SGRBLINK’ //NOPADCHK)
```



Upgrade Actions for z/OS V2.5

Various element default changes for more secure communications (all in V2.4)

CIM: Accommodate the default change from HTTP to HTTPS

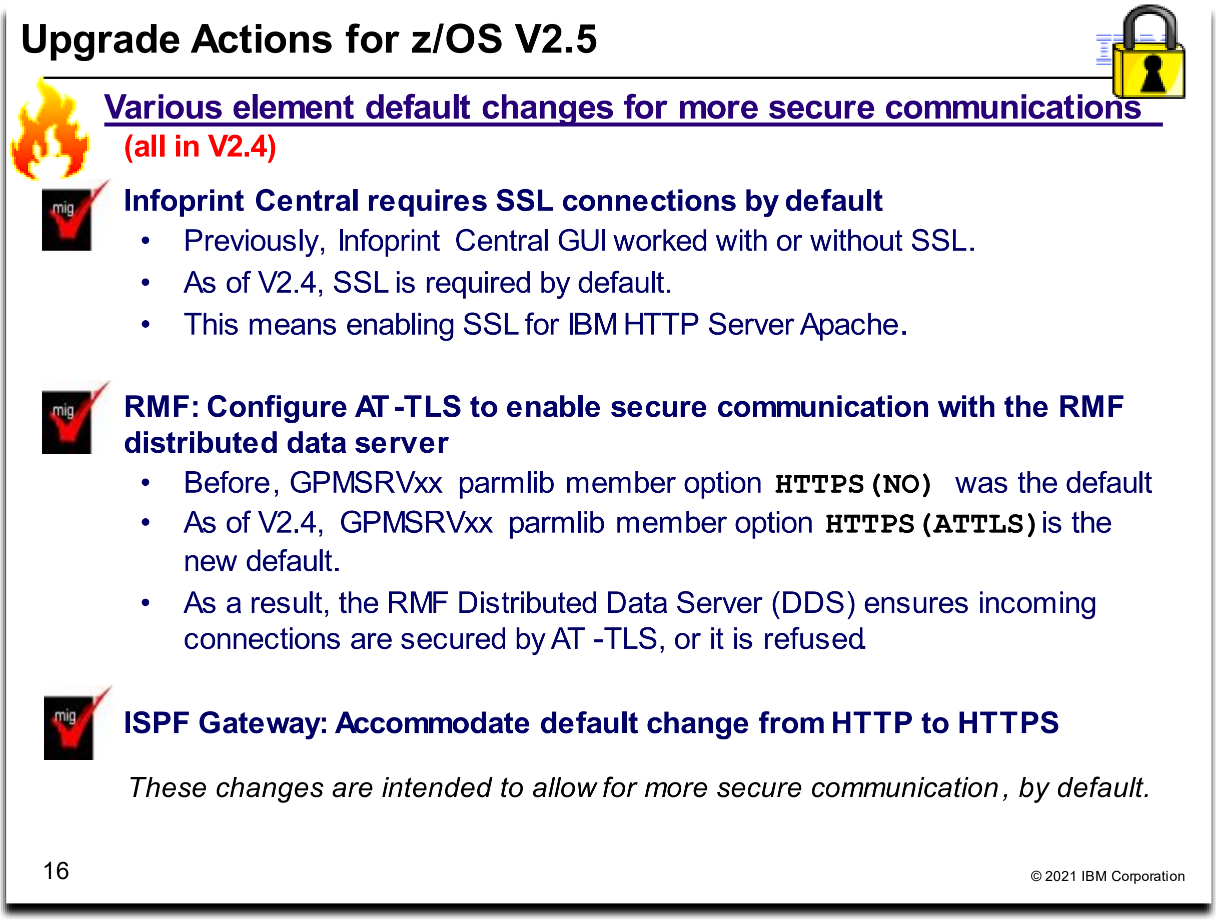
- By default, CIM server listens on the HTTPS port (5989) rather than the HTTP port. New configuration defaults are:
- `enableHttpConnection=false`
- `enableHttpsConnection=true`
- A client connection to this port must be secured with AT -TLS.

- **PKI Services: Ensure that users have the CA root certificate for the PKI web interfaces.**
  - Before, the first PKI web page presented by PKI Services for downloading the CA root certificate of the web server cert into the web browser, used HTTP.
  - As of V2.4, this first web page uses HTTPS, so you need to use alternate method to distribute the CA root certificate to the appropriate users' web browsers.

These changes are intended to allow for more secure communication, by default.

15

© 2021 IBM Corporation



Upgrade Actions for z/OS V2.5

Various element default changes for more secure communications (all in V2.4)

Infoprint Central requires SSL connections by default

- Previously, Infoprint Central GUI worked with or without SSL.
- As of V2.4, SSL is required by default.
- This means enabling SSL for IBM HTTP Server Apache.

RMF: Configure AT -TLS to enable secure communication with the RMF distributed data server

- Before, GPMSRVxx parmlib member option **`HTTPS(NO)`** was the default
- As of V2.4, GPMSRVxx parmlib member option **`HTTPS(ATTLS)`** is the new default.
- As a result, the RMF Distributed Data Server (DDS) ensures incoming connections are secured by AT -TLS, or it is refused.

ISPF Gateway: Accommodate default change from HTTP to HTTPS

These changes are intended to allow for more secure communication, by default.

16

© 2021 IBM Corporation

Various element default changes for more secure communications

These upgrade actions were taken from *z/OS V2.5 Upgrade Workflow.* Some descriptions and actions have been shortened for inclusion in this presentation. Not all upgrade actions have been included. For the complete descriptions and actions, refer to *z/OS V2.5 Upgrade Workflow.*

There were no secure communications default changes in z/OS V2.5.

CIM: Accommodate the default change from HTTP to HTTPS (Required, as of V2.4)

In z/OS V2R4, the common information model (CIM) server is changed to use HTTPS connections by default. On start-up, the CIM server listens on the HTTPS port, rather than the HTTP port, as was done in previous releases. The change from HTTP to HTTPS is intended to allow for more secure communication with the CIM server. The following CIM server configuration defaults are affected:

- `enableHttpConnection=true`
- `enableHttpsConnection=false`

In z/OS V2R4, these defaults are changed to:

- `enableHttpConnection=false`
- `enableHttpsConnection=true`

Based on this change, the CIM server opens a listener on port 5989 by default. If a client connection on this port is not secured by AT-TLS, the connection is closed and an appropriate error message is issued on the operations console.

It is recommended that you use HTTPS instead of HTTP, which allows the CIM server to use Application Transparent Layer Security (AT-TLS) functions. Here, the communication between the CIM client and the CIM server is encrypted.

You must also configure the CIM client applications to use HTTPS. Ensure that the applications run as CIM clients connected to the CIM server on HTTPS port 5989.

Fall back to HTTP is possible, though it is not secure and therefore not recommended. If you need the CIM server to use the HTTP protocol on start-up, follow these steps:

- Start the CIM server with the following settings specified in the configuration properties file:
  - `enableHttpConnection=true`
  - `enableHttpsConnection=false`
- Alternatively, you can dynamically change the enableHttpConnection value and restart the CIM server by entering either of these commands on the operations console:
  - `cimconfig -s enableHttpConnection= true -p`
  - `F CFZCIM,APPL=CONFIG,enableHttpConnection=true,PLANNED`

PKI Services: Ensure that users have the CA root certificate for the PKI web interfaces (Required-IF, as of V2.4)

Required if you a first-time user of PKI Services web page interfaces. A web browser must have the root CA of the web server, otherwise, the user cannot access the PKI page.

As of z/OS V2R4, the PKI Services component of z/OS uses the HTTPS protocol for its web page interfaces. In previous releases, PKI Services presented the first web page by using the HTTP protocol. Doing so allowed the user to use the link on this page to download the certificate authority (CA) root certificate of the web server certificate into the web browser. Thereafter, all the subsequent web pages used HTTPS.

To help ensure strong security, web pages should use HTTPS rather than HTTP. To use HTTPS, the CA root certificate of the web server must be preinstalled in the user’s web browser.

Starting with z/OS V2R4, the PKI page that previously used HTTP is now updated to use HTTPS. The link that is used to deliver the CA root certificate on the first page is removed. Therefore, you must use an alternative method to distribute the CA root certificate to the appropriate users at your installation.

Upgrade action: For any web browser that is planned to be used to access the PKI web page interface for the first time, your PKI administrator must distribute the CA root certificate of the web server (HTTP server, WebSphere, or WebSphere Liberty) to users who require access to the PKI web page interfaces. A possible method is to distribute the CA root certificate is by using the same communication channel that you use to provide users with the URI of the PKI web page. For example, if you send email, you can

1. Add the CA root certificate as an attachment or include it as Base64 encoded text in the first email.
2. Send a separate email with the root certificate fingerprint to help users ensure that the correct CA certificate was received in the previous email.

Refer to *PKI Services Guide and Reference* topic "Steps for accessing the user web pages" for more options to distribute the CA root certificate.

Infoprint Central requires SSL connections by default (Required, as of V2.4)

Required if you are running Infoprint Central

Starting with z/OS V2R4, SSL connection is required by default for the Infoprint Central web browser GUI. In previous releases, the GUI worked with or without SSL.

This change requires your installation to specify enabled SSL for your IBM HTTP Server (IHS) powered by Apache 31-bit configuration. Doing so causes the **httpd.conf.updates** file to be updated with a rewrite directive that converts the HTTP links to HTTPS links. This action saves users from having to update their Infoprint Central bookmarks.

For users who do not want to change their IHS configurations to use SSL, an Infoprint Server configuration attribute and new ISPF field are provided. The new option has an attribute name of use-unencrypted-connection and an ISPF panel field name of “Use unencrypted connection”. Note that this connection type is less secure than HTTPS.

You are encouraged to set up SSL before upgrading to z/OS V2R4.

Upgrade action: If SSL is not enabled in IHS and you are using Infoprint Central, follow these instructions. To use an SSL connection for Infoprint Central, do the following:

1. Follow the instructions to enable SSL in *IBM HTTP Server on z/OS Migrating from Domino-powered to Apache-powered*, which is available online:http://www.redbooks.ibm.com/redpapers/pdfs/redp4987.pdf.
2. Uncomment the Rewrite directive in the httpd.conf.updates file provided by Infoprint Server before copying the Infoprint Central directives to the httpd.conf file.
3. Test an Infoprint Central link or bookmark to ensure that Infoprint Central loads in the browser.

If you need to use an unencrypted connection, do the following:

1. Use the Infoprint Server System Configuration ISPF panel or PIDU to set the use-unencrypted-connection attribute to yes in the printer inventory.
2. Test an Infoprint Central link or bookmark to ensure that Infoprint Central loads in the browser.

RMF: Configure AT-TLS to enable secure communication with the RMF distributed data server (Required, as of V2.4)

Required if you rely on the current default of HTTPS(NO).

With RMF V2R4, the GPMSRVxx parmlib member option HTTPS(ATTLS) is specified by default. As a result, the RMF distributed data server (DDS) ensures that incoming connections are secured by AT-TLS. If an incoming connection is not secured by AT-TLS, the connection is refused.

Upgrade action: To allow insecure communication for the DDS, you can specify the option HTTPS(NO) in the GPMSRVxx parmlib member. However, this setting is not recommended because it allows the DDS to accept insecure connections.

Before you can configure the DDS, you must enable the Policy Agent for AT-TLS. Information about how to set up AT-TLS communication is provided in *z/OS Communications Server: IP Configuration Guide* and *z/OS Security Server RACF Security Administrator's Guide*. For other security management products, refer to the corresponding security product documentation.

The following example shows a rule that enables secure communication with the DDS:

```
# RMF Distributed Data Server Rule TTLSRule DDSServerRule { LocalPortRange 8803
Jobname GPMSERVE Direction Inbound Priority 1 TTLSGroupActionRef DDSServerGRP
TTLSEnvironmentActionRef DDSServerENV } TTLSGroupAction DDSServerGRP { TTLSEnabled On
Trace 1 } TTLSEnvironmentAction DDSServerENV { HandshakeRole Server TTLSKeyringParms
{ Keyring DDSServerKeyring } TTLSEnvironmentAdvancedParms { ServerCertificateLabel
RMFDDS } }
```

The example rule is described, as follows:

TTLSRule: Jobname

The name value specifies the job name of the application. GPMSERVE is the job name of the DDS

TTLSRule: LocalPortRange

The local port the application is bound to for this rule's action to be performed. 8803 is the default HTTP Port of the DDS.

TTLSRule: Direction

Specifies the direction from which the connection must be initiated for this rule's action to be performed. In this example, Inbound is specified, which means that the rule applies to connection requests that arrive inbound to the local host.

TTLSRule: Priority

An integer value in the range 1 -2000000000 represents the priority that is associated with the rule. The highest priority value is 2000000000. If you use multiple rules for the DDS server, the more specific a rule is, the higher its priority should be. Generic rules without detail specifications of the incoming connections should have a low priority.

TTLSEnvironmentAction: HandshakeRole

Specifies the SSL handshake role to be taken for connections in this AT-TLS environment. In this example, Server is specified which means that the SSL hand shake is performed as a server.

TTLSKeyringParms: Keyring

Specifies the path and file name of the key database z/OS� UNIX file, the ring name of the SAF key ring, or the name of the z/OS PKCS #11 token. In this example, the RACF key ring DDSServerKeyring is specified.

TTLSEnvironmentAdvancedParms: ServerCertificateLabel

Specifies the label of the certificate for a server application to authenticate the server. In this example, the DDS Server certificate with the label RMFDDS is used.

ISPF: Accommodate the ISPF Gateway access change from HTTP to HTTPS (Required-IF, as of V2.4)

Required if you use ISPF Gateway through the HTTP protocol.

Starting in z/OS V2R4, the ISPF Gateway uses HTTPS connections by default. The change from HTTP to HTTPS is intended to allow for more secure communication with the ISPF Gateway. One example of a program that accesses the ISPF Gateway is the installation verification program (IVP) that is included with ISPF.

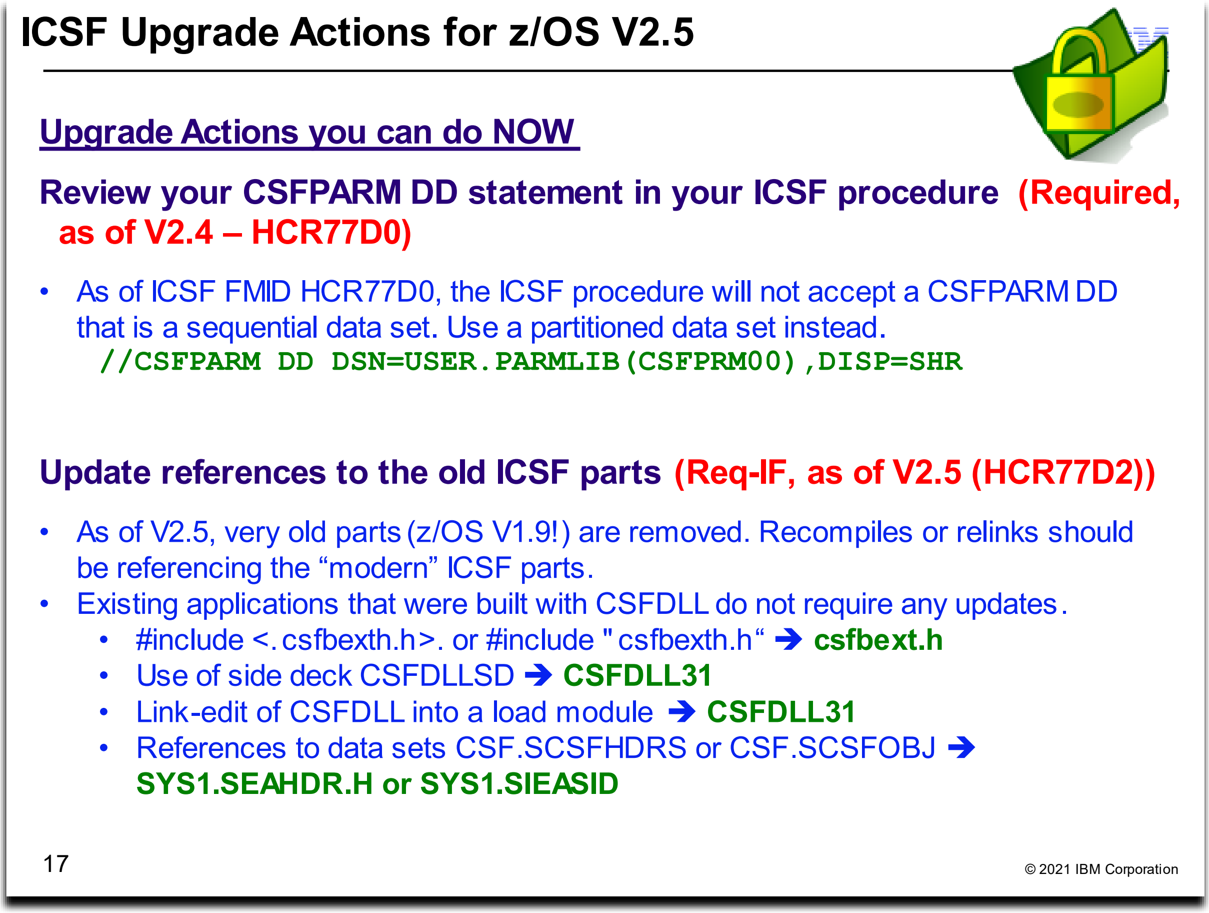
If you use the ISPF Gateway through the HTTP protocol, you must update your configuration to enable SSL for your ISPF gateway traffic.

Although not recommended, a configuration option is provided to allow you to override the default, for fall back to non-secure HTTP if needed.

Upgrade action: Determine whether the ISPF Gateway is being accessed on your system through non-secure HTTP. To do so, use IBM health check IBMISPF,ZOSMIGV2R3_Next_ISPF_GW_HTTPS. This health check is available for z/OS V2R3 with the PTFs for APARs OA58151 and OA58450 applied.

Update your configuration to enable SSL for your ISPF gateway traffic, as described in the topic “Customizing IBM HTTP server powered by Apache” in *ISPF Planning and Customizing*.

Although not recommended, you can override the default by adding environment variable CGI_SECURECONN to your HTTP configuration and setting it to FALSE.



ICSF Upgrade Actions for z/OS V2.5

Upgrade Actions you can do NOW

Review your CSFPARM DD statement in your ICSF procedure (Required, as of V2.4 – HCR77D0)

- As of ICSF FMID HCR77D0, the ICSF procedure will not accept a CSFPARM DD that is a sequential data set. Use a partitioned data set instead.

```
//CSFPARM DD DSN=USER.PARMLIB(CSFPRM00),DISP=SHR
```

Update references to the old ICSF parts (Req-IF, as of V2.5 (HCR77D2))

- As of V2.5, very old parts (z/OS V1.9!) are removed. Recompiles or relinks should be referencing the “modern” ICSF parts.
- Existing applications that were built with CSFDLL do not require any updates.
  - #include <.csfbexth.h>. or #include "csfbexth.h“ ➔ **csfbext.h**
  - Use of side deck CSFDLLSD ➔ **CSFDLL31**
  - Link-edit of CSFDLL into a load module ➔ **CSFDLL31**
  - References to data sets CSF.SCSFHDRS or CSF.SCSFOBJ ➔ **SYS1.SEAHDR.H or SYS1.SIEASID**

17

© 2021 IBM Corporation

ICSF Upgrade Actions For z/OS V2.5

These upgrade actions were taken from *z/OS V2.5 Upgrade Workflow.* Some descriptions and actions have been shortened for inclusion in this presentation. Not all upgrade actions have been included. For the complete descriptions and actions, refer to *z/OS V2.5 Upgrade Workflow.*

ICSF Upgrade Actions You Can Do Now

Review your CSFPARM DD statement in your ICSF procedure (Required, as of V2.4)

Required, as of HCR77D0 which is z/OS V2.4.

As of z/OS V2.4 ICSF, sequential data sets will no longer be accepted on the CSFPARM DD statement in the ICSF procedure.

Upgrade action:

Check for the specification of any sequential data sets specified on the CSFPARM DD statement.

Consider using a partitioned data set in place of a sequential data set on the CSFPARM DD statement, for example:

```
//ICSF PROC PRM=XX
//ICSF EXEC PGM=CSFINIT,TIME=NOLIMIT,MEMLIMIT=NOLIMIT
//CSFPARM DD DSN=SYS1.ICSFLIB(CSFPRM&PRM),DISP=SHR
```

You can find a sample ICSF procedure in SYS1.SAMPLIB(CSF), which is:

```
//*  Licensed Materials - Property of IBM
//*  5650-ZOS Copyright IBM Corp. 2009, 2018
//CSF PROC
//CSF EXEC PGM=CSFINIT,REGION=0M,TIME=1440,MEMLIMIT=NOLIMIT
//* When using CSFPARM DD, the installation options data set must be
//* a partitioned data set on systems running HCR77D0 or later.
//CSFPARM DD DSN=USER.PARMLIB(CSFPRM00),DISP=SHR
```

Update references to the old ICSF parts (Required-IF, as of V2.4)

Required, if an application that uses the old library, header, or side deck, must be recompiled or relinked. Or, if an application dynamically loads CSFDLL. Existing application that were built with CSFDLL do not require any updates.

As of z/OS V2R5, ICSF no longer provides:

- CSFDLL module in CSF.SCSFMOD0
- C header file CSFBEXTH in CSF.SCSFHDRS
- Side deck CSFDLLSD in CSF.SCSFOBJ

Also, the data sets CSF.SCSFHDRS and CSF.SCSFOBJ are no longer created at installation time.

These parts were functionally replaced in z/OS V1R9 by the C header file CSFBEXT in SYS1.SIEAHDR.H, the library CSFDLL31 in SYS1.SIEALNKE, and the side deck CSFDLL31 in SYS1.SIEASID.

Existing executable load modules that are already link-edited with CSFDLL will continue to run unchanged.

Upgrade action: Check your applications on your system for the use of any of the following:

- #include <.csfbexth.h>. or #include "csfbexth.h"
- Use of side deck CSFDLLSD
- Link-edit of CSFDLL into a load module
- References to data sets CSF.SCSFHDRS or CSF.SCSFOBJ

To use the supported interfaces, make the following changes:

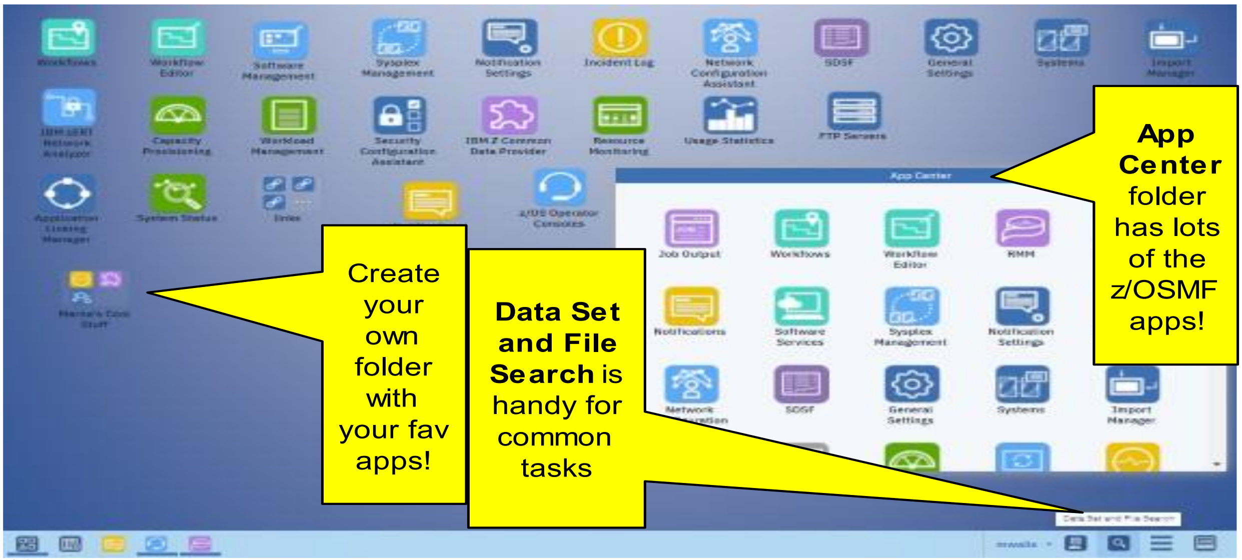
- #include <.csfbexth.h>. or #include "csfbexth.h"
  - Replace with csfbext.h (note the removed 'h' in the include name) and ensure that the standard header location SYS1.SIEAHDR.H or ICSF-specific location /usr/lpp/pkcs11/include is in the include path
- Use of side deck CSFDLLSD
  - Replace with CSFDLL31 from the standard side deck location SYS1.SIEASID
- Link-edit of CSFDLL into a load module
  - Replace with CSFDLL31 from the standard library location SYS1.SIEALNKE
- References to data sets CSF.SCSFHDRS or CSF.SCSFOBJ
  - Replace with SYS1.SIEAHDR.H or SYS1.SIEASID, if not already present in the relevant data set concatenations

z/OSMF Upgrade Actions for z/OS V2.5

Upgrade Actions you can do NOW:

Use the z/OSMF Desktop interface (Required-IF, as of V2.5)

- More modern and personalized UI than the tree-style interface.



Create your own folder with your fav apps!

Data Set and File Search is handy for common tasks

App Center folder has lots of the z/OSMF apps!

z/OSMF Upgrade Actions for z/OS V2.5

Upgrade Actions you can do NOW:

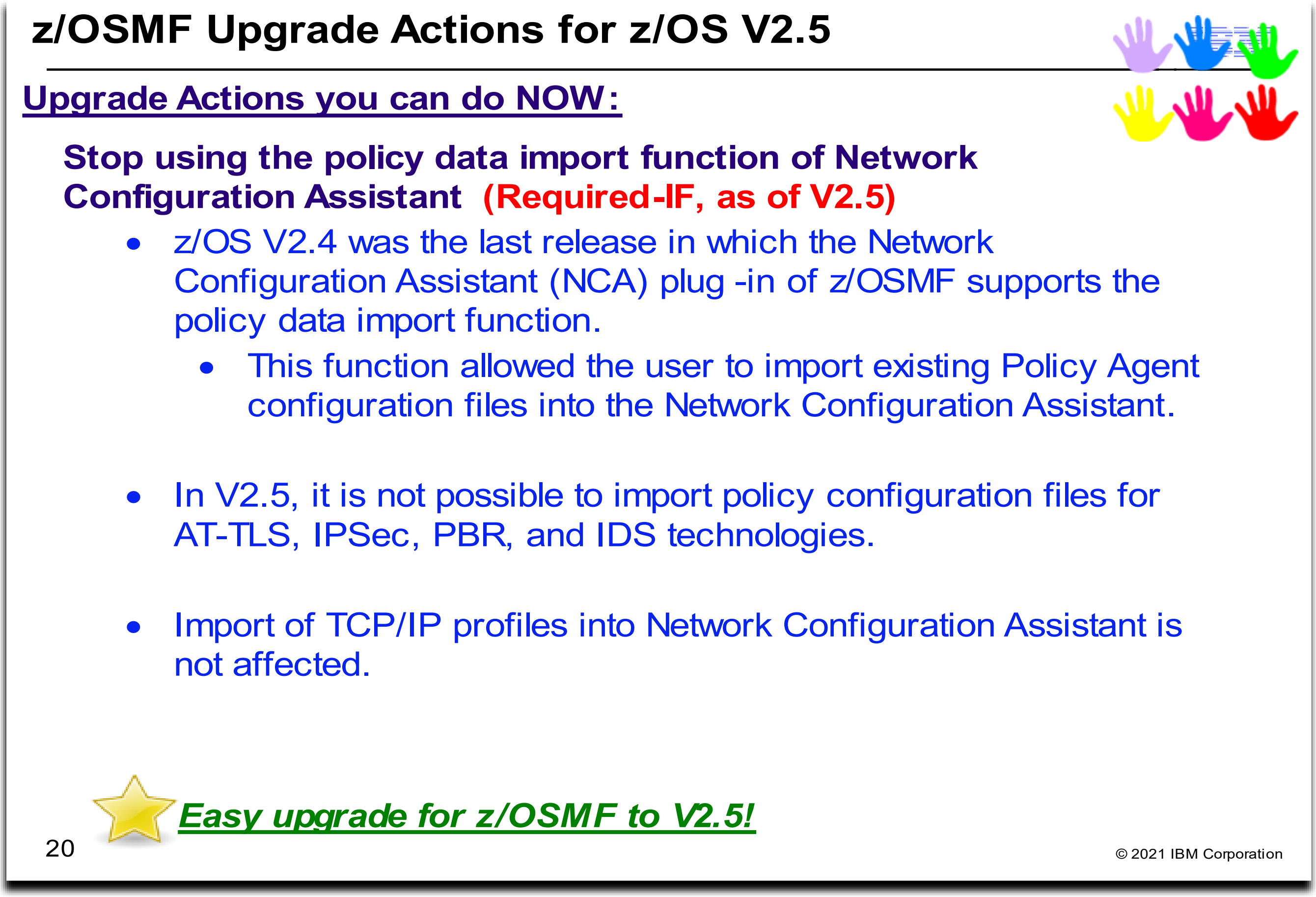
Remove references to z/OSMF mobile notification service (Required-IF, as of V2.5)

- REST API removed: `POST /zosmf/notifications/new`
- Other notification services, including the Notifications task and the email notification services remain available

Use the Diagnostic Assistant to collect diagnostic data about z/OSMF (Required-IF, as of V2.3/V2.4 with PH18776)

- Diagnostics page is removed from z/OSMF General Settings task.
- Replaced with the even better z/OSMF Diagnostic Assistant, added by APAR PH11606. Requires user authorization to use.

Easy upgrade for z/OSMF to z/OS V2.5!



z/OSMF Upgrade Actions for z/OS V2.5

Upgrade Actions you can do NOW:

Stop using the policy data import function of Network Configuration Assistant (Required-IF, as of V2.5)

- z/OS V2.4 was the last release in which the Network Configuration Assistant (NCA) plug -in of z/OSMF supports the policy data import function.
  - This function allowed the user to import existing Policy Agent configuration files into the Network Configuration Assistant.
- In V2.5, it is not possible to import policy configuration files for AT-TLS, IPSec, PBR, and IDS technologies.
- Import of TCP/IP profiles into Network Configuration Assistant is not affected.

Easy upgrade for z/OSMF to V2.5!

20

© 2021 IBM Corporation

z/OSMF Upgrade Actions For z/OS V2.5

These upgrade actions were taken from *z/OS V2.5 Upgrade Workflow.* Some descriptions and actions have been shortened for inclusion in this presentation. Not all upgrade actions have been included. For the complete descriptions and actions, refer to *z/OS V2.5 Upgrade Workflow.*

z/OSMF Upgrade Actions You Can Do Now

Use the z/OSMF Desktop interface (Req-IF, as of V2.5)

Required because importing Policy Agent configuration files into Network Configuration Assistant is not supported in V2.5.

The z/OSMF desktop is the primary user interface for interacting with z/OSMF. In z/OS V2R5, the older classic or tree-style interface is removed from z/OSMF.

The z/OSMF desktop provides all of the functions of the classic interface in a more modern and personalized UI. The z/OSMF desktop includes task icons, a taskbar, and other desktop elements that can be customized by the user. With the z/OSMF desktop, users can interact with z/OS through a familiar interface that is similar to other operating environments. The z/OSMF desktop offers additional capabilities, such as:

- Search for z/OS data sets and files
- Ability to group tasks in a folder.

The z/OSMF desktop is displayed to users when they access the z/OSMF welcome page. If the classic interface was saved as a user preference in a previous release, the z/OSMF desktop is displayed instead.

Remove references to z/OSMF mobile notification service (Req-IF, as of V2.5)

Required if you use the z/OSMF mobile notification service.

z/OS V2R5 removes support for z/OSMF mobile notification service. The other z/OSMF notification services, including the Notifications task and the email notification services remain available, and can be used in place of the mobile notification service. Specifically, the following functions are removed from z/OSMF:

- In the z/OSMF graphical user interface (GUI), the following pages are removed from the Notification Settings task: Mobile Configuration page, and z/OSMF mobile application entry in the User page.
- REST API that was used for z/OSMF mobile notifications: POST /zosmf/notifications/new

- The following request body properties are removed from the z/OSMF notifications REST API:
  - "product"
  - "eventGroup"
  - "data"
  - "alert"

The change is related to the removal of the IBM zEvent mobile application and the Bluemix based push services.
Upgrade action: Determine whether any of your users or programs use the z/OSMF mobile notification service. If so, use the z/OSMF Notifications task or the z/OSMF email notification service as a replacement.

Use the Diagnostic Assistant to collect diagnostic data about z/OSMF (Req-IF, as of V2.3/V2.4 with PH18776)

Required because importing Policy Agent configuration files into Network Configuration Assistant is not supported in V2.5.
APAR PH18776 removes the diagnostics page from the z/OSMF General Settings task. The diagnostic page is made obsolete with the addition of the new z/OSMF Diagnostic Assistant, which is added by APAR PH11606. The new plug-in provides additional functions for collecting diagnostic data that were not availabe in the older diagnostics page.

Using the z/OSMF Diagnostic Assistant might require you to create user authorizations in your external security manager (ESM). This workflow step includes a sample RACF definition that you can use as a model for creating the user authorizations.
Upgrade action: Verify that APARs PH18776 (for z/OS V2R3 and V2R4) and PH11606 (for z/OS V2R3) are installed on your system. z/OS V2R4 included PH11606. If so, the z/OSMF Diagnostic Assistant is available and the older diagnostic page is removed from General Settings. To see the service level of the z/OSMF plug-ins, check the z/OSMF server "About page." Verify that APARs PH18776 and PH11606 are installed.

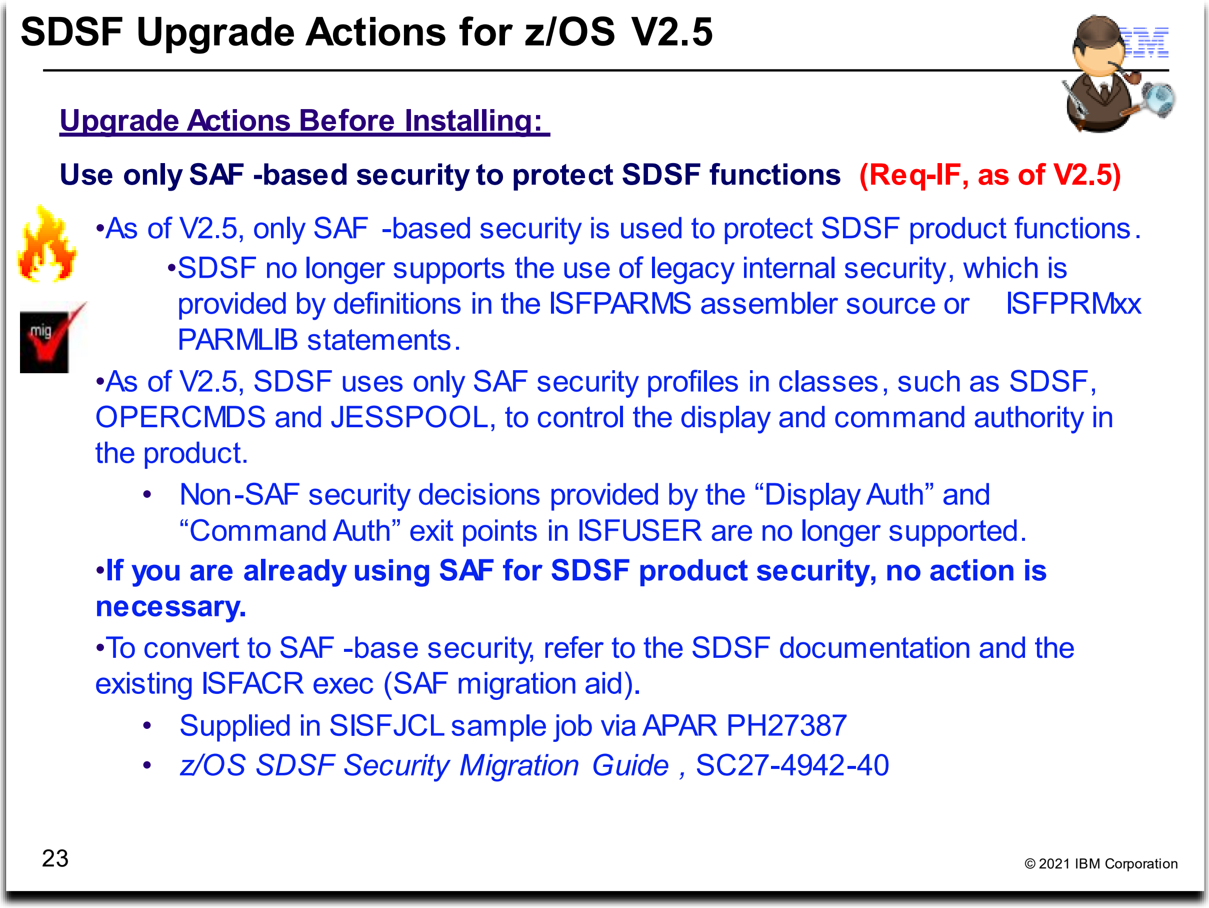
In your external security manager, create the authorizations for users of the z/OSMF Diagnostic Assistant task. The following example shows sample RACF statements for defining the resource profile and granting authorization to the z/OSMF administrators group (IZUADMIN):

- `RDEFINE ZMFAPLA IZUDFLT.ZOSMF.ADMINTASKS.DIAGNOSTIC_ASSISTANT UACC(NONE)`
- `PERMIT IZUDFLT.ZOSMF.ADMINTASKS.DIAGNOSTIC_ASSISTANT CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)`
- `SETROPTS RACLIST(ZMFAPLA) REFRESH`

Stop using the policy data import function of Network Configuration Assistant (Req-IF, as of V2.5)

Required because importing Policy Agent configuration files into Network Configuration Assistant is not supported in V2.5.
z/OS V2.4 was the last release in which the Network Configuration Assistant (NCA) plug-in of z/OSMF supports the policy data import function. This function allowed the user to import existing Policy Agent configuration files into the Network Configuration Assistant.
In z/OS V2.5, it is not be possible to import policy configuration files for AT-TLS, IPSec, PBR, and IDS technologies. Import of TCP/IP profiles into Network Configuration Assistant is not affected.

Upgrade action: If you plan to import Policy Agent configuration files into the Network Configuration Assistant, perform this work prior on a pre-V2.5 release of z/OS (V2.3, or V2.4). Otherwise, you have no action to take.



SDSF Upgrade Actions for z/OS V2.5

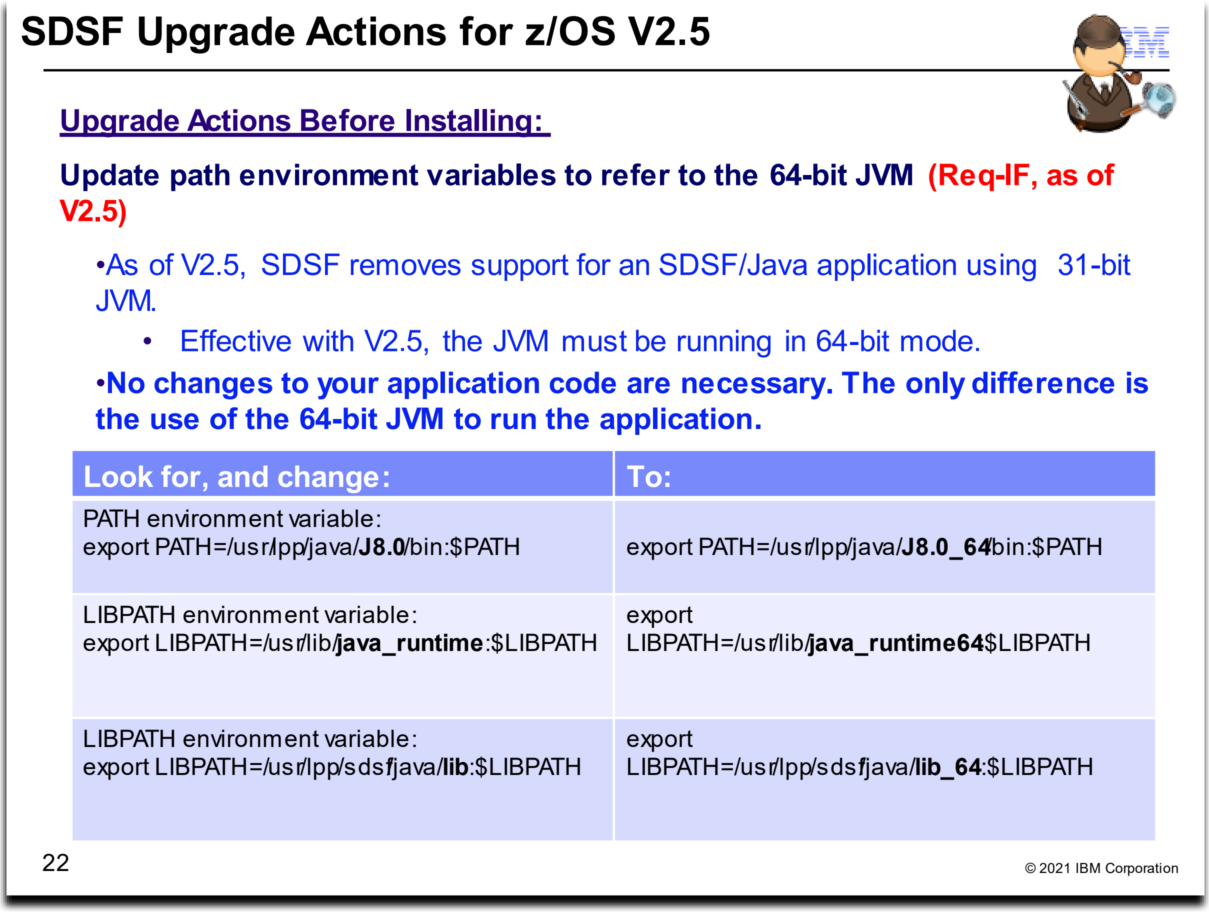
Upgrade Actions Before Installing:

Use only SAF -based security to protect SDSF functions (Req-IF, as of V2.5)

- As of V2.5, only SAF -based security is used to protect SDSF product functions.
  - SDSF no longer supports the use of legacy internal security, which is provided by definitions in the ISFPARMS assembler source or ISFPRMxx PARMLIB statements.
- As of V2.5, SDSF uses only SAF security profiles in classes, such as SDSF, OPERCMDS and JESSPOOL, to control the display and command authority in the product.
  - Non-SAF security decisions provided by the “Display Auth” and “Command Auth” exit points in ISFUSER are no longer supported.
- **If you are already using SAF for SDSF product security, no action is necessary.**
- To convert to SAF -base security, refer to the SDSF documentation and the existing ISFACR exec (SAF migration aid).
  - Supplied in SISFJCL sample job via APAR PH27387
  - *z/OS SDSF Security Migration Guide* , SC27-4942-40

23

© 2021 IBM Corporation



SDSF Upgrade Actions for z/OS V2.5

Upgrade Actions Before Installing:

Update path environment variables to refer to the 64-bit JVM (Req-IF, as of V2.5)

- As of V2.5, SDSF removes support for an SDSF/Java application using 31-bit JVM.
  - Effective with V2.5, the JVM must be running in 64-bit mode.
- **No changes to your application code are necessary. The only difference is the use of the 64-bit JVM to run the application.**

Look for, and change:	To:
PATH environment variable: export PATH=/usr/lpp/java/**J8.0**/bin:$PATH	export PATH=/usr/lpp/java/**J8.0_64**/bin:$PATH
LIBPATH environment variable: export LIBPATH=/usr/lib/**java_runtime**:$LIBPATH	export LIBPATH=/usr/lib/**java_runtime64**$LIBPATH
LIBPATH environment variable: export LIBPATH=/usr/lpp/sdsfjava/**lib**:$LIBPATH	export LIBPATH=/usr/lpp/sdsfjava/**lib_64**:$LIBPATH

22

© 2021 IBM Corporation

SDSF Upgrade Actions For z/OS V2.5

These upgrade actions were taken from *z/OS V2.5 Upgrade Workflow.* Some descriptions and actions have been shortened for inclusion in this presentation. Not all upgrade actions have been included. For the complete descriptions and actions, refer to *z/OS V2.5 Upgrade Workflow.*

SDSF Actions You Can Do Now

Use only SAF-based security to protect SDSF functions (Required-IF, as of V2.5)

Required if SDSF on your system uses security definitions in the ISFPARMS assembler source or ISFPRMxx PARMLIB statements.

Starting in z/OS V2R5, only SAF-based security is used to protect SDSF product functions. SDSF no longer supports the use of legacy internal security, which is provided by definitions in the ISFPARMS assembler source or ISFPRMxx PARMLIB statements.

The system authorization facility (SAF) is an interface defined by z/OS that enables programs to use system authorization services to control access to resources, such as data sets and MVS commands. SAF either processes security authorization requests directly or works with RACF, or other security managers, to process them.
As of z/OS V2R5, SDSF uses only SAF security profiles in classes, such as SDSF, OPERCMDS and JESSPOOL, to control the display and command authority in the product.
Non-SAF security decisions provided by the “Display Auth” and “Command Auth” exit points in ISFUSER are no longer supported.

Upgrade action: If you are already using SAF for SDSF product security, no action is necessary. If you are using SDSF internal security or the ISFUSER exit to enforce local security decisions, you must upgrade to SAF security for SDSF before using z/OS V2R5. Converting to SAF security for SDSF can be performed on any currently supported release of z/OS. For information about how to convert to the SAF interface, see SDSF Security Migration Guide, SC27-4942.

Update path environment variables to refer to the 64-bit JVM (Required-IF, as of V2.5)

Required if your installation uses SDSF programs that rely on 31-bit Java.

In z/OS V2R5, SDSF removes support for running an SDSF/Java application using the 31-bit Java virtual machine (JVM). SDSF/Java applications can run unchanged using the 64-bit JVM.
SDSF supplies Java classes (referred to as SDSF/Java) that allow access to SDSF panels and functions through applications written in Java. Such applications are typically invoked under the z/OS UNIX System Services shell by running Java and specifying a main class that references the SDSF/Java classes.
In previous releases, an SDSF/Java application could run using either the 31-bit or 64-bit version of the Java JVM. Effective with SDSF V2R5, the JVM must be running in 64-bit mode.

Upgrade action:

1. Check the PATH environment variable for a reference to the Java 31-bit JVM, such as the following:

```
export PATH=/usr/lpp/java/J8.0/bin:$PATH
```

If so, change the PATH environment variable to refer to the 64-bit JVM:

```
export PATH=/usr/lpp/java/J8.0_64/bin:$PATH
```

2. Check the LIBPATH environment variable for a reference to the 31-bit SDSF DLLs, such as the following:

```
export LIBPATH=/usr/lib/java_runtime:$LIBPATH
```

or

```
export LIBPATH=/usr/lpp/sdsf/java/lib:$LIBPATH
```

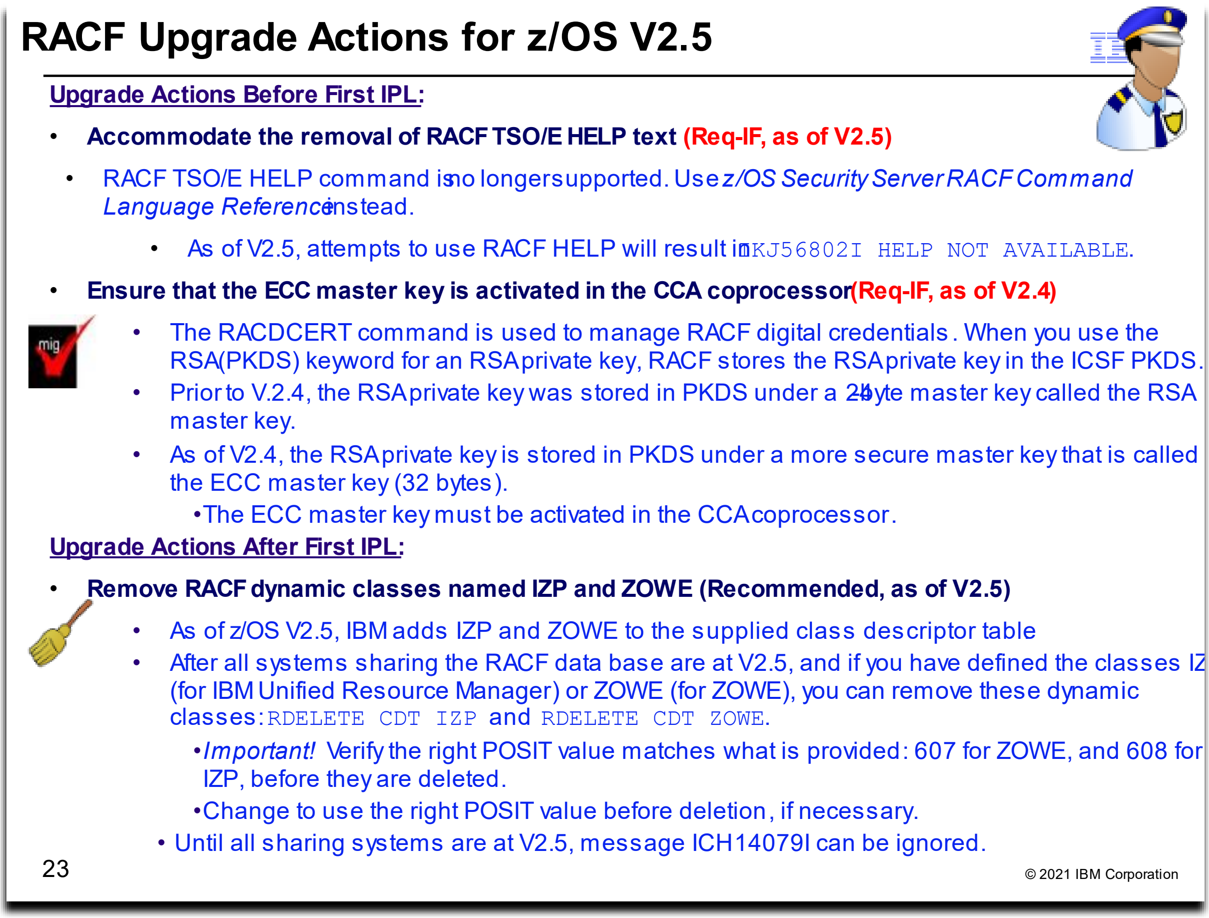
If so, change your LIBPATH environment variable to refer to the SDSF 64-bit DLL:

```
export LIBPATH=/usr/lib/java_runtime64:$LIBPATH
```

or

```
export LIBPATH=/usr/lpp/sdsf/java/lib_64:$LIBPATH
```

Note that no changes to your application code are necessary. The only difference is the use of the 64-bit JVM to run the application.



RACF Upgrade Actions for z/OS V2.5

Upgrade Actions Before First IPL:

- **Accommodate the removal of RACF TSO/E HELP text (Req-IF, as of V2.5)**
  - RACF TSO/E HELP command is no longer supported. Use *z/OS Security Server RACF Command Language Reference* instead.
    - As of V2.5, attempts to use RACF HELP will result in `IKJ56802I HELP NOT AVAILABLE`.
- **Ensure that the ECC master key is activated in the CCA coprocessor (Req-IF, as of V2.4)**
  - The RACDCERT command is used to manage RACF digital credentials. When you use the RSA(PKDS) keyword for an RSA private key, RACF stores the RSA private key in the ICSF PKDS.
  - Prior to V.2.4, the RSA private key was stored in PKDS under a 24-byte master key called the RSA master key.
  - As of V2.4, the RSA private key is stored in PKDS under a more secure master key that is called the ECC master key (32 bytes).
    - The ECC master key must be activated in the CCA coprocessor.

Upgrade Actions After First IPL:

- **Remove RACF dynamic classes named IZP and ZOWE (Recommended, as of V2.5)**
  - As of z/OS V2.5, IBM adds IZP and ZOWE to the supplied class descriptor table
  - After all systems sharing the RACF data base are at V2.5, and if you have defined the classes IZ (for IBM Unified Resource Manager) or ZOWE (for ZOWE), you can remove these dynamic classes: `RDELETE CDT IZP` and `RDELETE CDT ZOWE`.
    - *Important!* Verify the right POSIT value matches what is provided: 607 for ZOWE, and 608 for IZP, before they are deleted.
    - Change to use the right POSIT value before deletion, if necessary.
  - Until all sharing systems are at V2.5, message ICH14079I can be ignored.

23

© 2021 IBM Corporation

RACF Upgrade Actions For z/OS V2.5

These upgrade actions were taken from *z/OS V2.5 Upgrade Workflow.* Some descriptions and actions have been shortened for inclusion in this presentation. Not all upgrade actions have been included. For the complete descriptions and actions, refer to *z/OS V2.5 Upgrade Workflow.*

RACF Action Pre-First IPL

Accommodate the removal of RACF TSO/E HELP text (Required-IF, as of V2.5)

Required if you use the TSO/E HELP command for information about RACF command syntax.

As of z/OS V2R5, the RACF TSO/E HELP command is no longer supported. Entering the command "help *racf keyword*" in TSO/E results in the message "IKJ56802I HELP NOT AVAILABLE." For information about RACF command syntax, see the IBM publication z/OS Security Server RACF Command Language Reference.

Upgrade action: Stop using the TSO/E HELP command for information about RACF command syntax.

Ensure that the ECC master key is activated in the CCA coprocessor (Required-IF, as of V2.4)

Required if your installation uses the RACF RACDCERT command with the RSA(PKDS) keyword and you did not activate the ECC master key in the CCA coprocessor.

In RACF, the RACDCERT command is used to manage RACF digital certificates. When you specify RACFDCERT with the RSA(PKDS) keyword for an RSA private key, RACF stores the RSA private key in the ICSF PKA key data set (PKDS).

Starting in z/OS V2R4, the RSA private key is stored in PKDS under a more secure master key that is called the ECC master key (32 bytes). In previous releases, the RSA private key was stored in PKDS under a 24-byte master key called the RSA master key. With this change, you must ensure that the ECC master key is activated in the CCA coprocessor. Otherwise, the RACDCERT command that attempting to store an RSA key in PKDS fails with an error.

This change is intended to help maintain strong security in your enterprise. It also supports the generation of a new signature algorithm on certificates that are used for TLS1.3, which is introduced in z/OS V2R4.

To detect an active ECC master key and the availability of a coprocessor CCA-5.3 or above, use health check IBMICSF,ICSF_PKCS_PSS_SUPPORT. Based on this status, the health check indicates whether PKCS-PSS algorithms can be used under current conditions. This health check is available with APAR OA56837.

Upgrade action:
Look for uses of the RACDCERT command specified with the RSA(PKDS) keyword. For example:

```
RACDCERT GENCERT...RSA(PKDS(...))
RACDCERT REKEY...RSA(PKDS(...))
RACDCERT ADD ...PKDS(...)
```

If so, verify that the ECC master key is activated before these commands are used on a z/OS V2R4 system. You can use either of the following approaches:

- Open ICSF panel option 1 and check the CCA coprocessor ECC master keys status.
- Run the ICSF ECC master key health check.

Failure to do this upgrade action will result in RACDCERT command failures with reason code x'00002B08' and the following message:

```
IRRRD117I Unexpected ICSF CSNDPKG return code x'00000008 ' and reason code
x'00002B08'. The request is not processed.
```

RACF Action Post-First IPL

Remove RACF dynamic classes named IZP and ZOWE (Recommended, as of V2.5)

Not required, but recommended to avoid messages that indicate a conflict between the IBM classes and the dynamic classes.
If your installation uses IBM Zowe, its documentation directed you to add the ZOWE class to RACF. In z/OS V2R5, this class can be deleted after all of the systems that share the RACF database are upgraded to z/OS V2.5.

If your installation uses IBM Unified Resource Manager, its documentation directed you to add the IZP class to RACF. In z/OS V2R5, this class can be deleted after all of the systems that share the RACF database are upgraded to z/OS V2.5. Despite issuing message ICH14079I, RACF functions normally using the IBM-defined class.

In z/OS V2.5, RACF adds the IZP and ZOWE classes in the supplied class descriptor table.

> Warning: If the RACF database is shared with any z/OS release earlier than V2R5, the deletion of the class will make the profiles in that class unusable on the downlevel system

Otherwise, after you upgrade to z/OS V2R5, RACF identifies the conflict between the dynamic class and the IBM class by issuing message ICH14079I during IPL and with every subsequent SETROPTS RACLIST(xxx) REFRESH for the class.

For a list of the new classes that are shipped with RACF, see the topic “Supplied resource classes for systems” in the IBM publication *Security Server RACF Security Administrator's Guide*.
Upgrade action: Check for message ICH14079I or the existence of the IZP and ZOWE classes in the RACF class descriptor table (CDT). For example:

- RLIST CDT IZP CDTINFO
- RLIST CDT ZOWE CDTINFO

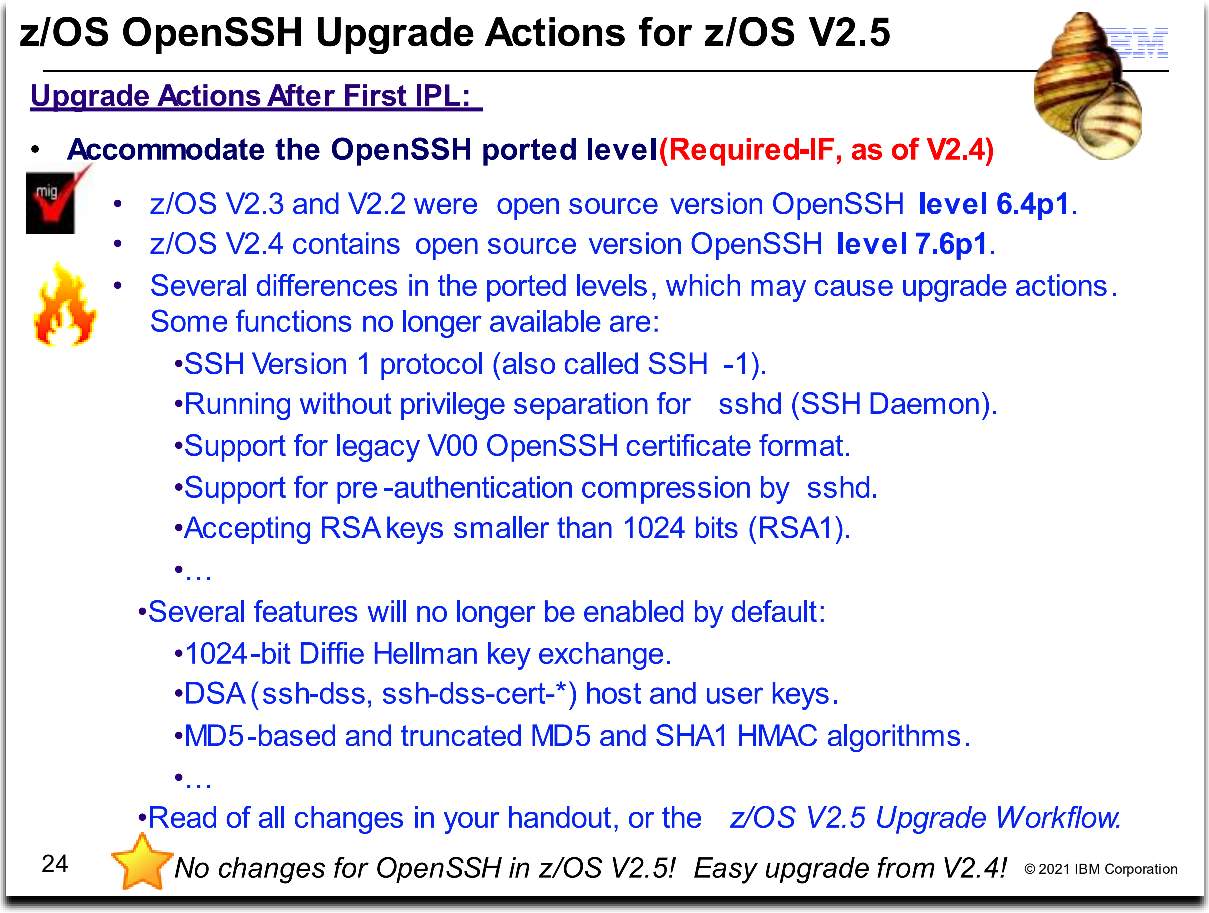
Important: Ensure that the dynamic class was defined compatibly with the IBM class, as documented by Zowe or IBM Unified Resource Manager. Specifically, verify that the POSIT value matches what is documented for the class in *z/OS Security Server RACF Macros and Interfaces* (607 for ZOWE, 608 for IZP). If not, change the POSIT value on your current release before upgrading to V2.5. The *Security Administrator's Guide* contains instructions on changing a POSIT number in the topic titled "Changing a POSIT value for a dynamic class."

When all the systems that share the RACF database are upgraded to z/OS V2.5, delete the classes as follows:

- RDELETE CDT IZP
- RDELETE CDT ZOWE

- SETROPTS RACLIST(CDT) REFRESH

In the interim, the ICH14079I messages can be ignored. After the classes are deleted from the RACF CDT class and the RACF CDT class is refreshed, the message is no longer issued. There is no need to alter any profiles in the IZP or ZOWE class.



z/OS OpenSSH Upgrade Actions for z/OS V2.5

Upgrade Actions After First IPL:

- **Accommodate the OpenSSH ported level(Required-IF, as of V2.4)**
  - z/OS V2.3 and V2.2 were open source version OpenSSH **level 6.4p1**.
  - z/OS V2.4 contains open source version OpenSSH **level 7.6p1**.
  - Several differences in the ported levels, which may cause upgrade actions. Some functions no longer available are:
    - SSH Version 1 protocol (also called SSH -1).
    - Running without privilege separation for sshd (SSH Daemon).
    - Support for legacy V00 OpenSSH certificate format.
    - Support for pre-authentication compression by sshd.
    - Accepting RSA keys smaller than 1024 bits (RSA1).
    - …
  - Several features will no longer be enabled by default:
    - 1024-bit Diffie Hellman key exchange.
    - DSA (ssh-dss, ssh-dss-cert-*) host and user keys.
    - MD5-based and truncated MD5 and SHA1 HMAC algorithms.
    - …
  - Read of all changes in your handout, or the *z/OS V2.5 Upgrade Workflow.*

24 *No changes for OpenSSH in z/OS V2.5! Easy upgrade from V2.4!* © 2021 IBM Corporation

z/OS OpennSSH Upgrade Actions For z/OS V2.5

These upgrade actions were taken from *z/OS V2.5 Upgrade Workflow*. Some descriptions and actions have been shortened for inclusion in this presentation. Not all upgrade actions have been included. For the complete descriptions and actions, refer to *z/OS V2.5 Upgrade Workflow.*

z/OS OpenSSH Upgrade Action Post-First-IPL

Accommodate the OpenSSH ported level (Required-IF, as of V2.4)

Required if you reliant upon any of the changes in the newer ported level..

With z/OS V2.4, OpenSSH is upgraded to include a new level of open source version OpenSSH 7.6p1. (The last change was in z/OS V2.2 for open source version OpenSSH 6.4p1. With z/OS OpenSSH V2R4, significant new features are included:

- Elliptic-curve DSA keys are now supported in Key Rings and FIPS.
- Support new key algorithms: ssh-ed25519, ssh-ed25519-cert-v01@openssh.com
- Support new key exchange algorithms: diffie-hellman-group14-sha256, diffie-hellman group16-sha512, diffie-hellman-group18-sha512, curve25519-sha256 and curve25519-sha256@libssh.org.
- Support new cipher algorithms: chacha20-poly1305@openssh.com
- The SMF Type 119 subtype 94 and 95 (ssh / sshd connection started) records will include a section that identifies the IP addresses and ports for the connection.
- A new command ssh-proxyc is added, which can be used by the ssh client to connect through SOCKS5 proxy servers.

Also with z/OS OpenSSH V2R4, following features are no longer available (since they are deprecated by the Open Source community in OpenSSH 7.6p1). This had been previously announced as a Statement of Direction in the

4Q2017 z/OS V2.3 Enhancement Announcement (https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=an&subtype=ca&appname=gpateam&supplier=897&letternum=ENUS217-536):

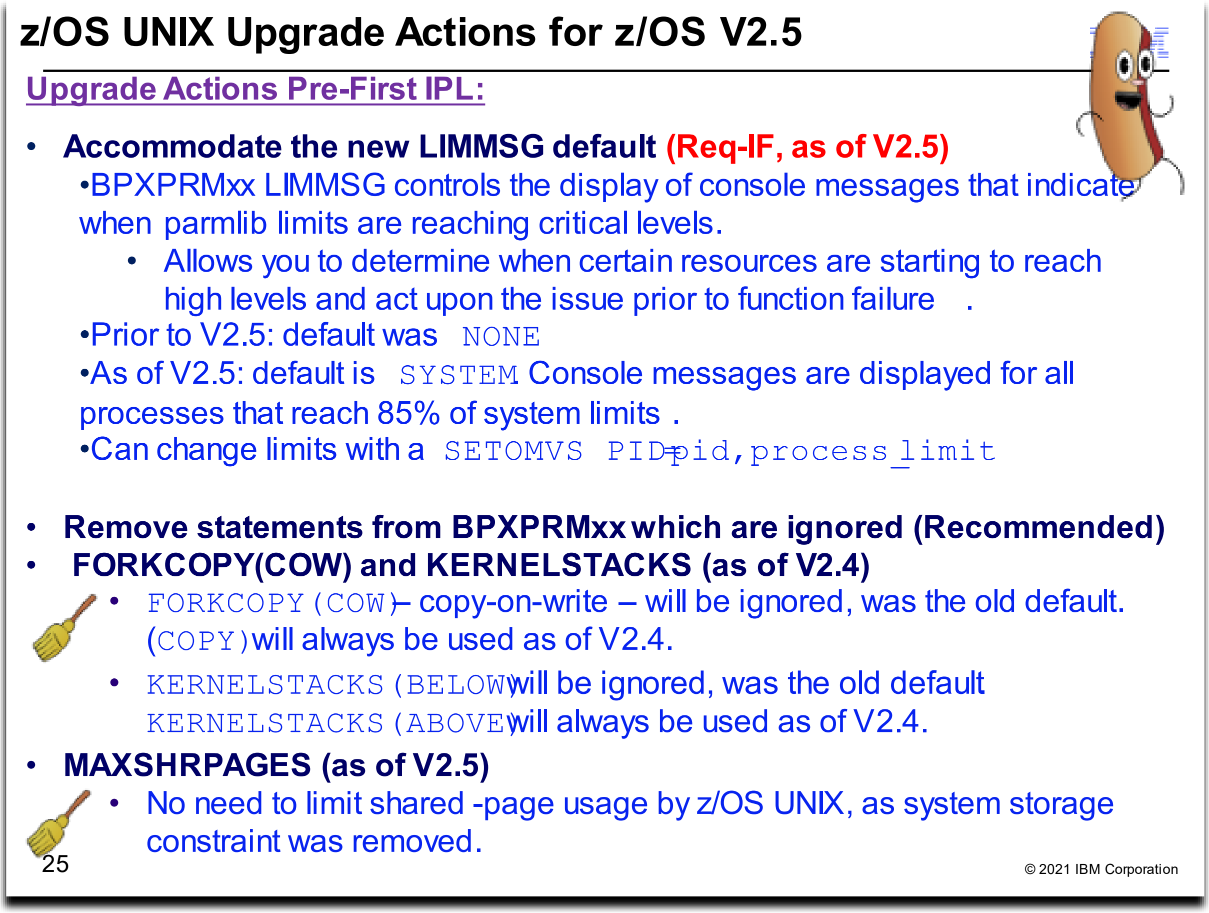
- SSH Version 1 protocol (also referred to as SSH-1).

  These options from **ssh_config** have been removed: Cipher, CompressionLevel, RhostsAuthentication, RhostsRSAAuthentication, RSAAuthentication.

  These options from **sshd_config** have been removed: KeyRegenerationInteval, RhostsAuthentication, RhostsRSAAuthentication, RSAAuthentication, ServerKeyBits, UseLogin and PAMAuthenticationViaKbdInt.
- Running without privilege separation for sshd (SSH Daemon).
- Support for the legacy v00 OpenSSH certificate format.
- Support for pre-authentication compression by sshd (SSH Daemon). SSH clients will either need to support delayed compression mode or otherwise compression will not be negotiated.
- Support for Blowfish and RC4 ciphers and the RIPE-MD160 HMAC (Hash Message Authentication Code), specifically: blowfish-cbc, cast128-cbc, arcfour, arcfour128, arcfour256, hmac-ripemd160, hmac-ripemd160@openssh.com, and hmac-ripemd160-etm@openssh.com.
- Accepting RSA keys smaller than 1024 bits. (RSA1)

With z/OS OpenSSH V2R4, the following features will no longer be enabled by default. This had been previously announced as a Statement of Direction in the 4Q2017 z/OS V2.3 Enhancement Announcement (https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=an&subtype=ca&appname=gpateam&supplier=897&letternum=ENUS217-536):

- Support for the 1024-bit Diffie Hellman key exchange, specifically diffie-hellman-group1-sha1
- Support for DSA (ssh-dss, ssh-dss-cert-*) host and user keys
- Support for MD5-based and truncated MD5 and SHA1 HMAC algorithms, specifically: hmac-md5, hmac-md5-96@openssh.com, hmac-sha1-96, hmac-sha1-96@openssh.com, hmac-md5-etm@openssh.com, hmac-md5-96-etm@openssh.com, hmac-sha1-96-etm@openssh.com,
- Support for the Triple DES cipher and cbc cipher, specifically 3des-cbc, aes128-cbc, aes192-cbc and aes256-cbc.



z/OS UNIX Upgrade Actions for z/OS V2.5

Upgrade Actions Pre-First IPL:

- **Accommodate the new LIMMSG default (Req-IF, as of V2.5)**
  - BPXPRMxx LIMMSG controls the display of console messages that indicate when parmlib limits are reaching critical levels.
    - Allows you to determine when certain resources are starting to reach high levels and act upon the issue prior to function failure .
  - Prior to V2.5: default was `NONE`
  - As of V2.5: default is `SYSTEM` Console messages are displayed for all processes that reach 85% of system limits .
  - Can change limits with a `SETOMVS PID=pid,process_limit`
- **Remove statements from BPXPRMxx which are ignored (Recommended)**
- **FORKCOPY(COW) and KERNELSTACKS (as of V2.4)**
  - `FORKCOPY(COW)`– copy-on-write – will be ignored, was the old default. `(COPY)`will always be used as of V2.4.
  - `KERNELSTACKS(BELOW)`will be ignored, was the old default `KERNELSTACKS(ABOVE)`will always be used as of V2.4.
- **MAXSHRPAGES (as of V2.5)**
  - No need to limit shared -page usage by z/OS UNIX, as system storage constraint was removed.

25

© 2021 IBM Corporation

z/OS UNIX Upgrade Actions For z/OS V2.5

These upgrade actions were taken from *z/OS V2.5 Upgrade Workflow.* Some descriptions and actions have been shortened for inclusion in this presentation. Not all upgrade actions have been included. For the complete descriptions and actions, refer to *z/OS V2.5 Upgrade Workflow.*

z/OS UNIX Actions Pre-First IPL

Accommodate the new LIMMSG default (Required-IF, as of V2.5)

Required if you use the LIMMSG parameter to limit the display of console messages. .

In the BPXPRMxx parmlib member, the parameter LIMMSG is used to control the display of console messages that indicate when parmlib limits are reaching critical levels. This option allows you to determine when certain resources are starting to reach high levels and act upon the issue prior to function failure.

Additional messages might be seen with the new LIMMSG default. The messages are informational only; no system function or processing is changed.

In z/OS V2R5, the default setting for the parameter LIMMSG is changed from NONE to SYSTEM. With this change, console messages are displayed for all processes that reach 85% of system limits.

In addition, messages are displayed for each process limit if either of the following conditions are true:

- The process limit or limits are defined in the OMVS segment of the owning user ID
- The process limit or limits are changed with a SETOMVS PID=pid,process_limit command.

Upgrade action: Examine the LIMMSG setting in your active BPXPRMxx parmlib member:

- If the LIMMSG option is not specified, you are using the old default (NONE). If you want to continue using the old default, you must add LIMMSG(NONE) to the BPXPRMxx member.
- If the LIMMSG option is specified, and you want to continue using the current setting, you have no action to take. If LIMMSG is set to SYSTEM, you are already using the new default behavior.

Remove references to the MAXSHAREPAGES option in BPXPRMxx (Recommended, as of V2.5)

Not required, but recommended if you use MAXSHAREPAGES in BPXPRMxx.

In the BPXPRMxx parmlib member, the option MAXSHAREPAGES is used to limit the combined UNIX System Services usage of shared pages to avoid system storage constraints. Recently, the system storage constraint associated with shared pages was removed, which eliminates the need to limit shared-page usage by z/OS UNIX System Services.

In z/OS V2R5, the MAXSHAREPAGES parmlib option will be processed for compatibility reasons, but the setting is ignored. For clarity, IBM recommends removing the MAXSHAREPAGES option from BPXPRMxx parmlib members.

z/OS UNIX System Services does not track shared pages or limit their overall usage. MAXSHAREPAGES is no longer included when options are displayed (DISPLAY OMVS,OPTIONS) or in any LIMMSG output, including displaying limits (DISPLAY OMVS,LIMITS).

Upgrade action: Remove the MAXSHAREPAGES specification from any BPXPRMxx parmlib members that include it.

Optionally delete the FORKCOPY(COW) option of BPXPRMxx (Recommended, as of V2.4)

Not required, but recommended for clarity in the BPXPRMxx parmlib member because FORKCOPY(COPY) will always be used even if FORKCOPY(COW) is specified.

Previously, with the FORKCOPY option in the BPXPRMxx parmlib member, copy-on-write (COW) mode could be specified for fork processing. The default was FORKCOPY(COW). In z/OS V2R4, the COW option is disabled. FORKCOPY(COPY) will always be used even if FORKCOPY(COW) is specified.

Upgrade action:

Determine whether your BPXPRMxx parmlib member specifies FORKCOPY(COW) mode. If so, remove it. FORKCOPY(COPY) is always used, even when FORKCOPY(COW) is specified.

Use of FORKCOPY(COPY) avoids any additional ESQA use in support of fork. Use of FORKCOPY(COW) caused the system to use the ESQA to manage page sharing.

Optionally delete the KERNELSTACKS option of BPXPRMxx (Recommended, as of V2.4)

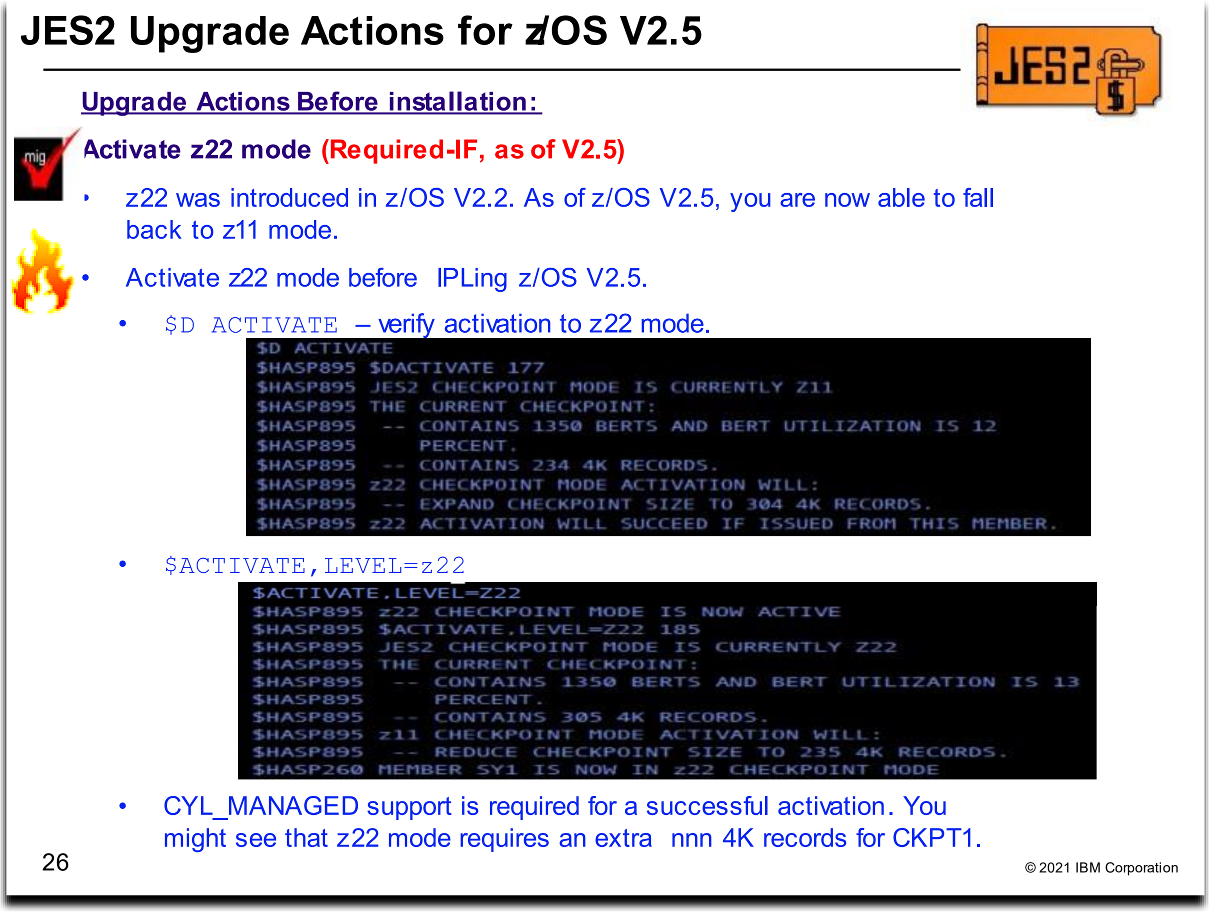
Not required, but recommended for clarity in the BPXPRMxx parmlib member because KERNELSTACKS(BELOW) will not be used.

Previously, with the KERNELSTACK option in the BPXPRMxx parmlib member, stacks could be allocated either above or below the bar. The default was KERNELSTACKS(BELOW). As of z/OS V2R4, stacks are always allocated above the bar. If KERNELSTACKS(BELOW) is specified, it is ignored and the stacks are allocated above the bar.

Upgrade action:

Determine whether your BPXPRMxx parmlib member uses the KERNELSTACK option. If so, remove it. The stacks will always be allocated above the bar.

When the kernel stacks were allocated from kernel private storage that is below the bar, the number of threads running in the kernel was limited to about 30,000. KERNELSTACKS(ABOVE) increases thread limit to a maximum of 500,000; the actual amount will vary, depending on work load and system configuration. Usage of real storage in the kernel address space is also increased.



JES2 Upgrade Actions for z/OS V2.5

Upgrade Actions Before installation:

Activate z22 mode (Required-IF, as of V2.5)

- z22 was introduced in z/OS V2.2. As of z/OS V2.5, you are now able to fall back to z11 mode.
- Activate z22 mode before IPLing z/OS V2.5.
  - `$D ACTIVATE` – verify activation to z22 mode.

```
$D ACTIVATE
$HASP895 $DACTIVATE 177
$HASP895 JES2 CHECKPOINT MODE IS CURRENTLY Z11
$HASP895 THE CURRENT CHECKPOINT:
$HASP895  -- CONTAINS 1350 BERTS AND BERT UTILIZATION IS 12
$HASP895     PERCENT.
$HASP895  -- CONTAINS 234 4K RECORDS.
$HASP895 z22 CHECKPOINT MODE ACTIVATION WILL:
$HASP895  -- EXPAND CHECKPOINT SIZE TO 304 4K RECORDS.
$HASP895 z22 ACTIVATION WILL SUCCEED IF ISSUED FROM THIS MEMBER.
```

  - `$ACTIVATE,LEVEL=z22`

```
$ACTIVATE,LEVEL=Z22
$HASP895 z22 CHECKPOINT MODE IS NOW ACTIVE
$HASP895 $ACTIVATE,LEVEL=Z22 185
$HASP895 JES2 CHECKPOINT MODE IS CURRENTLY Z22
$HASP895 THE CURRENT CHECKPOINT:
$HASP895  -- CONTAINS 1350 BERTS AND BERT UTILIZATION IS 13
$HASP895     PERCENT.
$HASP895  -- CONTAINS 305 4K RECORDS.
$HASP895 z11 CHECKPOINT MODE ACTIVATION WILL:
$HASP895  -- REDUCE CHECKPOINT SIZE TO 235 4K RECORDS.
$HASP260 MEMBER SY1 IS NOW IN z22 CHECKPOINT MODE
```

  - CYL_MANAGED support is required for a successful activation. You might see that z22 mode requires an extra nnn 4K records for CKPT1.

26

© 2021 IBM Corporation

JES2 Upgrade Actions For z/OS V2.5

These upgrade actions were taken from *z/OS V2.5 Upgrade Workflow.* Some descriptions and actions have been shortened for inclusion in this presentation. Not all upgrade actions have been included. For the complete descriptions and actions, refer to *z/OS V2.5 Upgrade Workflow.*

z/OS UNIX Actions Before Installation

Activate z22 mode (Required-IF, as of V2.5)

Required if you are use the z11 level for checkpoint data sets.

Starting with z/OS V2R5, JES2 no longer supports the z11 level for checkpoint data sets. z22 mode was introduced in z/OS V2R2. Activate JES2 in z22 mode, if you have not done so. When you switch to z22 mode, the system upgrades the JES2 checkpoint. You are not able to fall back to z11 mode.

Upgrade action: Follow these steps:

- On all of the systems in your MAS, determine your z22 checkpoint activation readiness, as follows:
  - Enter the $D ACTIVATE command to verify that activation to z22 mode can succeed.
  - If you enter the $ACTIVATE,LEVEL=z22 command, activation of CYL_MANAGED support is required.
  - You might see that z22 mode requires an extra nnn 4K records for CKPT1.

- Enter the JES2 $ACTIVATE command to verify non-configuration changes that must be accommodated before you go to z22, and to activate z22 mode. See the considerations for this command in *z/OS JES2 Commands.*

By default, JES2 restarts in the same mode as the other members of the MAS (if any are active) or the mode of the last active JES2 member when it was shut down. On a cold start, JES2 starts in z22 mode, unless overridden by the OPTSDEF COLD_START_MODE or UNACT parameter.

z/OS UNIX Actions Pre-First IPL

Accommodate the changed default for the EXECUTABLE keyword on $GETMAIN (Required-IF, as of V2,4)

Required if you have any affected JES2 exit routines or user modifications.

z/OS V2R3 added the EXECUTABLE= keyword on the $GETMAIN macro to indicate whether the obtained storage is marked as executable for systems that run on an IBM z14 server or later. For more information about non-executable memory, see the description of the EXECUTABLE= keyword on the STORAGE macro.

When the EXECUTABLE= keyword was added to the $GETMAIN macro in z/OS V2R3, the default was YES. Starting with z/OS V2R4, the default on $GETMAIN is changed to NO. This change implies that, by default, any storage that is obtained in a supported subpool does not support executable code on a z14 server. Any attempt to run code in the storage results in an 0C4 abend.

Upgrade action:

Review your exits for instances of the $GETMAIN macro that obtains storage for executable code. In particular, check for DCB exit stubs that might be obtained and pointed to by the EXLST area. When appropriate to do so, convert the $GETMAIN and its associated $FREMAIN to specify EXECUTABLE=YES. On a z/OS V2R3 system, you can perform this change before you upgrade to z/OS V2R4.

If in doubt, you can change all $GETMAIN and $FREMAIN macros to specify EXECUTABLE=YES.

Checkpoint versions are moving to 64-bit storage (Required-IF, as of V2,4)

Required if your JES2 exit routines or applications use the IAZDSERV macro with an SSI call 71 or the $DSERV macro.

Applications and exits that do not run in the JES2 address space can access checkpoint version data from the IAZDSERV data area, which provides a stable copy of the data. To access the IAZDSERV data area, applications can use subsystem interface call (SSI) 71, subfunction SSJIFOBT, and JES2 exits can use the $DSERV macro.

Before z/OS V2R4, the data returned by these services was in a 31-bit storage data space. Starting in z/OS V2R4, the returned data might reside in 64-bit storage.

z/OS V2R4 adds version 10 of the IAZDSERV data area, which supports 64-bit pointers and ALETs for use in accessing the checkpoint version data. Version 10 is the only IAZDSERV version that is supported by z/OS V2R4.

Upgrade action:

Check for applications and exits that access checkpoint version data from the IAZDSERV data area. Determine whether this code must access the checkpoint data blocks directly.

As an alternative to using the IAZDSERV data area directly, your code can use an SSI call to access checkpoint version data. IBM recommends that you evaluate the use of SSI calls, such as SSI 80 (extended status) or SSI 82 (JES property SSI). Determine whether you can use these services to obtain the data that you require. Otherwise, you must upgrade your code to accept the 64-bit data pointers that are returned in the version 10 IAZDSERV data area.

If you use the $DSERV macro in an exit, be aware that the IAZDSERV data area it returns is at the version 10 level and therefore contains 64-bit pointers. All JES2 services that use the $DSERV macro as input are upgraded in z/OS V2R4 to accept the version 10 of the IAZDSERV data area.

In general, unless your code must reference individual fields in the $DSERV mapping, it should not require changes. However, it your code references fields in the $DSERV, you must upgrade your code to use the 64-bit fields and run in 64-bit addressing mode.

Accommodate changes in the NJE input phase processing for multi-object job streams (Required-IF, as of V2,4)

Required if you have JES2 exit routines or processes that are impacted.

Before z/OS V2R4, if an NJE job stream contained more that one job or job group, the stream and all jobs within it would fail input phase processing. Starting with z/OS V2R4, JES2 now supports multiple job and job group objects in an NJE job transmission stream. This is done by keeping all the jobs in the stream busy in the INPUT phase of processing until the job trailer (end of the job stream) is received. When received, the jobs complete input phase processing and are queued to the next phase. If an error occurs on the connection and the job trailer is not received, all of the jobs are purged from the receiving system. When the NJE connection is reestablished, the entire job stream is sent again.

This change implies a number of subtle changes in how input phase processing works:

- Multiple jobs and job groups can be marked busy on a job receiver at the same time
- Final processing for the jobs is delayed until the job trailer is received. This includes exits 20 and 50 (end of input exits) and exit 51 (queue change). As a result, the end of input exit for the first job in the stream is not given control until all other input exits (job statement, accounting string, JCL statement) are called for all of the jobs. The environment in which the end of input exit is called is the same as in prior releases, however, the order is changed.
- When a connection drops, because multiple jobs can exist on the NJE job receiver, all of these jobs must be purged. Prior releases would only have at most one job that needed to be purged.

Upgrade action: Review these changes to NJE input phase processing and evaluate suitable changes to your system. For example, if you have any exits or procedures that rely on only one job or job group being active on a particular NJE job receiver at a time, review and update those exits and procedures. Similarly, if you have an end of input exit or a queue change exit that relies on being called immediately after other input exits for a particular job, review those exits and change them appropriately.

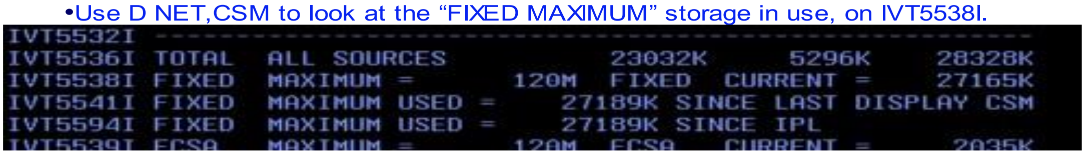
Communications Server Upgrade Actions for z/OS V2.5

Upgrade Actions Before Installing:

IP Services: Upgrade TLS/SSL support for the FTP server to AT -TLS (Required-IF, as of V2.5)

- As of V2.5, FTP server support for using IBM System SSL for TLS/SSL is removed.
- You must configure the FTP server to use AT-TLS policies.
  - Error messages are issued for any of the removed configuration keywords or parameters.

- **IP Services: Decide whether to accept the new FIXED CSM default (Required-IF, as of V2.4)**
  - As of V2.4, the default for CSM fixed storage for buffers is increased to 512M.
    - Review your HVCOMMON setting in IVTPRM00.
  - Use D NET,CSM to look at the “FIXED MAXIMUM” storage in use, on IVT5538I.



```
IVT5532I ------------------------------------------------------------
IVT5536I TOTAL   ALL SOURCES          23032K      5296K     28328K
IVT5538I FIXED   MAXIMUM =      120M  FIXED   CURRENT =     27165K
IVT5541I FIXED   MAXIMUM USED =    27189K SINCE LAST DISPLAY CSM
IVT5594I FIXED   MAXIMUM USED =    27189K SINCE IPL
IVT5539I ECSA    MAXIMUM =      120M  ECSA    CURRENT =      2035K
```

  - A brief history of this default change: V2.1→ 100M, V2.2→ 200M, V2.4→ 512M.

Don’t forget about the Communication Server removal items in Part 1 !

27

© 2021 IBM Corporation

Communications Server Upgrade Actions for z/OS V2.5

Upgrade Actions Before Installing:

- **IP Services: Ensure storage availability for IWQ IPSec traffic (Recommended, as of APAR PI77649 on V2.3)**
  - The processing of IPAQENET and IPAQENET6 INTERFACE statements is enhanced when you us OSA-Express6S (running in QDIO mode on z14).
    - If you enabled QDIO inbound workload queuing (WORKLOADQ) and you have IPSec traffic, an additional ancillary input queue (AIQ) is established for IPSec inbound traffic.
    - Additional storage is allocated for this input queue.
  - Each ancillary input queue increases storage utilization in both: ECSA by approx. 36KB, and 64KB CSM HVCOMMON for READSTORAGE.
  - Extensive instructions on how to do the calculation are provided in handout, and in the *z/OS Upgrade Workflow.* Use the workflow for some assistance.
- **IP Services: Determine the storage impact if QDIOSTG=126 is in effect (Req-IF, as of V2.4)**
  - If you specify QDIOSTG=126 in your VTAM start options, each OSA-Express QDIO interface that uses the default READSTORAGE setting of GLOBAL on the INTERFACE or LINK statement gets 8MB of fixed CSM for read storage.
  - In z/OS V2.4: For any OSA-Express QDIO interfaces that have a bandwidth of at least 10 GbE and use 8MB or read storage, an additional fixed CSM of 4K HVCOMMON is allocated for work element processing.
  - See Additional fixed storage for OSA interfaces using 8 MB of read storage in *z/OS Communications Server: IP Configuration Guide* to understand how much additional storage z/OS V2.4 allocates for work element processing.
  - If you do not want the system to allocate this extra storage for a specific interface, update your INTERFACE or LINK statement to specify a READSTORAGE value other than GLOBAL

28

© 2021 IBM Corporation

Communications Server Upgrade Actions For z/OS V2.5

These upgrade actions were taken from *z/OS V2.5Upgrade Workflow.* Some descriptions and actions have been shortened for inclusion in this presentation. Not all upgrade actions have been included. For the complete descriptions and actions, refer to *z/OS V2.5 Upgrade Workflow.*

Communications Server Actions You Can Do Now

IP Services: Upgrade TLS/SSL support for the FTP server to AT-TLS (Req-IF, as of V2.5)

Required if you are using native TLS/SSL support for the FTP server (TLSMECHANISM FTP).

As of z/OS V2R5, FTP server support for using IBM System SSL for TLS/SSL is removed. You must configure the FTP server to use AT-TLS policies. FTP configuration error messages are issued if any of the removed configuration keywords or parameters are configured for FTP servers.

Upgrade action: See the *z/OS V2.5 Upgrade Workflow for details* – the overview steps are provided here:

1. Configure AT-TLS and Policy Agent.
2. Configure the FTP server to use AT-TLS by coding TLSMECHANISM ATTLS in FTP.DATA.
3. If TLSRFCLEVEL CCCNONOTIFY is configured in FTP.DATA, update TLSRFCLEVEL to have a valid value for AT-TLS. If your FTP server uses TLSRFCLEVEL CCCNONOTIFY, change it to TLSRFCLEVEL RFC4217.
4. Migrate existing FTP server configuration to AT-TLS.
5. Migrate existing ciphers coded on CIPHERSUITE statement in FTP.DATA to AT-TLS TTLSCipherParms statements.
6. ATTLS supports more secure TLS versions and ciphers. Consider enabling TLSv1.2 or TLSV1.3 on the TTLSEnvironmentAdvancedParms or TTLSConnectionAdvancedParms statement.

IP Services: Ensure storage availability for IWQ IPSec traffic (Recommended, as of APAR PI77649)

Not required, but recommended if you have the WORKLOAD parameter that is specified on the OSA IPAQENET and IPAQENET6 INTERFACE statements, you have IPSec traffic and you have concerns about using additional ECSA or real (fixed) storage.

As of z/OS V2R3 with TCP/IP APAR PI77649, or z/OS V2R2 with TCP/IP APAR PI77649 and SNA APAR OA52275, the processing of IPAQENET and IPAQENET6 INTERFACE statements is enhanced when you use OSA-Express6S. If you enabled QDIO inbound workload queuing (WORKLOADQ) and you have IPSec traffic, an additional ancillary input queue (AIQ) is established for IPSec inbound traffic. Additional storage is allocated for this input queue.

Each AIQ increases storage utilization in the following two areas:

- Approximately 36 KB of fixed ECSA
- 64-bit CSM HVCOMMON for READSTORAGE

If you are using IPSec, when the first IPSec tunnel is activated (protocols ESP or AH), the new AIQ is backed with 64-bit CSM HVCOMMON fixed storage. The amount of HVCOMMON storage that is used is based on the specification of the INTERFACE READSTORAGE parameter.

If you configured QDIO inbound workload queuing (WORKLOADQ), ensure that sufficient fixed ECSA and fixed (real) 4 KB CSM HVCOMMON storage is available for the AIQ for IPSec traffic.

This upgrade action concerns OSA-Express6S Ethernet features or later in QDIO mode running on IBM z14 and ZR1. To determine whether sufficient fixed storage is available for IWQ IPSec enabling, use the following IBM health checks:

- IBMCS,ZOSMIGV2R4PREV_CS_IWQSC_tcpipstackname issues a message if the TCP/IP stack has inbound workload queuing (IWQ) and IPSec enabled, but the OSA does not support IWQ for IPSec. Only OSA-Express6S and later support IWQ for IPSec. This health check is shipped INACTIVE and set to run once.
- IBMCS,CSTCP_IWQ_IPSEC_tcpipstackname issues a message if the TCP/IP stack has IWQ and IPSec enabled, and the OSA does support IWQ for IPSec. This health check is shipped ACTIVE and is set to run once.

These health checks are available with PH11837 and OA57525 for V2R3, and PH12005 and OA57560 for V2R4.

Upgrade action:

1. If you are using or plan to use OSA-Express6S or later, verify that the following conditions are true:
    a. WORKLOADQ is specified on the IPAQENET and IPAQENET6 INTERFACE statements.
    b. Have IPSec traffic; protocols ESP or AH.
2. If step 1 is applicable, IWQ IPSec uses additional storage. Continue with step 3 - 6. Otherwise, there is no increase in storage usage, and no further action is required.
3. To calculate the total storage increase, count the total number of IPAQENET and IPAQENET6 INTERFACE statements that are coded with the WORKLOADQ parameter that are associated with OSA-Express6S or later. Make a note of the number.
4. Verify that sufficient ECSA is available. To calculate this, multiply the total INTERFACE statements that are counted in step 3 by 36 KB. The resulting number indicates how much additional ECSA is required.
   To determine whether sufficient ECSA is available to enable this function, verify the following ECSA definitions:
    a. D CSM usage (PARMLIB member IVTPRM00, ECSA MAX value)
    b. VTAM (Start Options CSALIMIT and CSA24)
    c. TCPIP (GLOBALCONFIG ECSALIMIT statement in the TCPIP PROFILE)
5. Verify that sufficient real (fixed) storage is available. 64-bit fixed (CSM HVCOMMON) storage is used for the IPSec AIQ read buffers. To calculate this value, multiply the total number of INTERFACE statements that are counted in step 3 by your configured READSTORAGE value (for example, 4 MB). You can verify how much storage is being used for READSTORAGE by using the D NET, TRLE command. The resulting number indicates how much additional fixed (64-bit) storage is required. To verify that the additional fixed storage is not a constraint for your system, take the following actions:
    a. Use the DISPLAY CSM command to verify that sufficient fixed storage is available (CSM FIXED MAXIMUM defined in IVTPRM00).
    b. Verify the actual amount of real storage available to this z/OS system by using D M=STOR or D M=HIGH.
6. If sufficient ECSA or real storage is not available, increase the available real storage or consider defining some of the OSA-Express6S (or later) INTERFACE statements with the NOWORKLOADQ parameter. If your CSM FIXED MAXIMUM is too low, increase this value in IVTPRM00.

Communications Server Actions Pre-First IPL

mig

IP Services: Decide whether to accept the new FIXED CSM default (Required-IF, as of V2.4)

Required if you use the default CSM FIXED MAX value of 200M and you do not want to use the new default of 512M.

In z/OS V2R4, the default amount for communications storage manager (CSM) fixed storage for buffers is increased from 200 MB to 512 MB. Your installation can specify a value for the CSM fixed storage amount on the FIXED statement in the IVTPRM00 parmlib member.

Upgrade action: Review your HVCOMMON setting in IVTPRM00 and determine whether you need to increase this value to account for the fact that the system reserves a larger portion of this storage by default for CSM buffers.

If you did not previously code a value for FIXED in IVTPRM00 and you do not want the new default, specify FIXED MAX(200M) in your IVTPRM00 parmlib member to retain the value as formerly defaulted.

Tip: You can use the D NET,CSM command to display the "FIXED MAXIMUM" storage specification in message IVT5538I.

A brief history of FIXED CSM defaults, for those interested: V2.1 – 100M, V2.2 – 200M, V2.4 – 512M.

IP Services: Determine the storage impact if QDIOSTG=126 is in effect (Required, as of V2.4)

If you specify QDIOSTG=126 in your VTAM start options, each OSA-Express QDIO interface that uses the default READSTORAGE setting of GLOBAL on the INTERFACE or LINK statement gets 8 MB of fixed CSM for read storage. For any OSA-Express QDIO interfaces that have a bandwidth of at least 10 GbE and use 8 MB of read storage, z/OS V2R4 allocates additional fixed CSM 4K HVCOMMON storage for work element processing.

The system allocates additional fixed CSM HVCOMMON storage for work element processing for each OSA-Express QDIO interface that is using 8 MB of read storage.

Upgrade action: See *Additional fixed storage for OSA interfaces using 8 MB of read storage* in z/OS Communications Server: IP Configuration Guide to understand how much additional storage z/OS V2R4 allocates for work element processing.

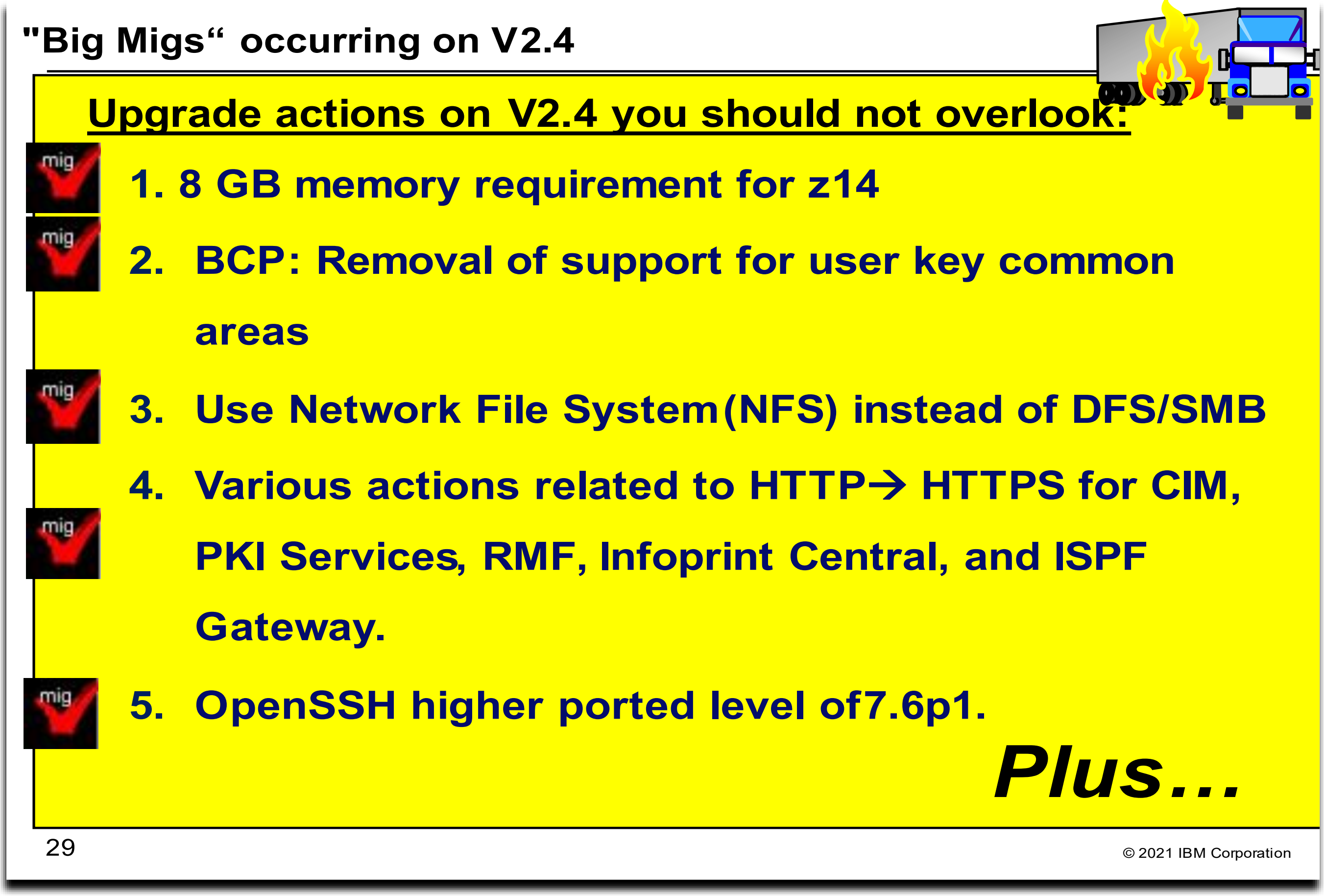
If you do not want the system to allocate this extra storage for a specific interface, update your INTERFACE or LINK statement to specify a READSTORAGE value other than GLOBAL.

IP Services: Update /etc configuration files (Required-IF)

Required if you have customized a configuration file that IBM has changed.

Some utilities provided by Communications Server require the use of certain configuration files. You are responsible for providing these files if you expect to use the utilities. IBM provides default configuration files as samples in the /usr/lpp/tcpip/samples directory. Before the first use of any of these utilities, you should copy these IBM-provided samples to the /etc directory (in most cases). You can further customize these files to include installation-dependent information. An example is setting up the /etc/osnmpd.data file by copying the sample file from /usr/lpp/tcpip/samples/osnmpd.data to /etc/osnmpd.data and then customizing it for the installation.

If you customized any of the configuration files that have changed, then you must incorporate the customization into the new versions of the configuration files.



"Big Migs“ occurring on V2.4

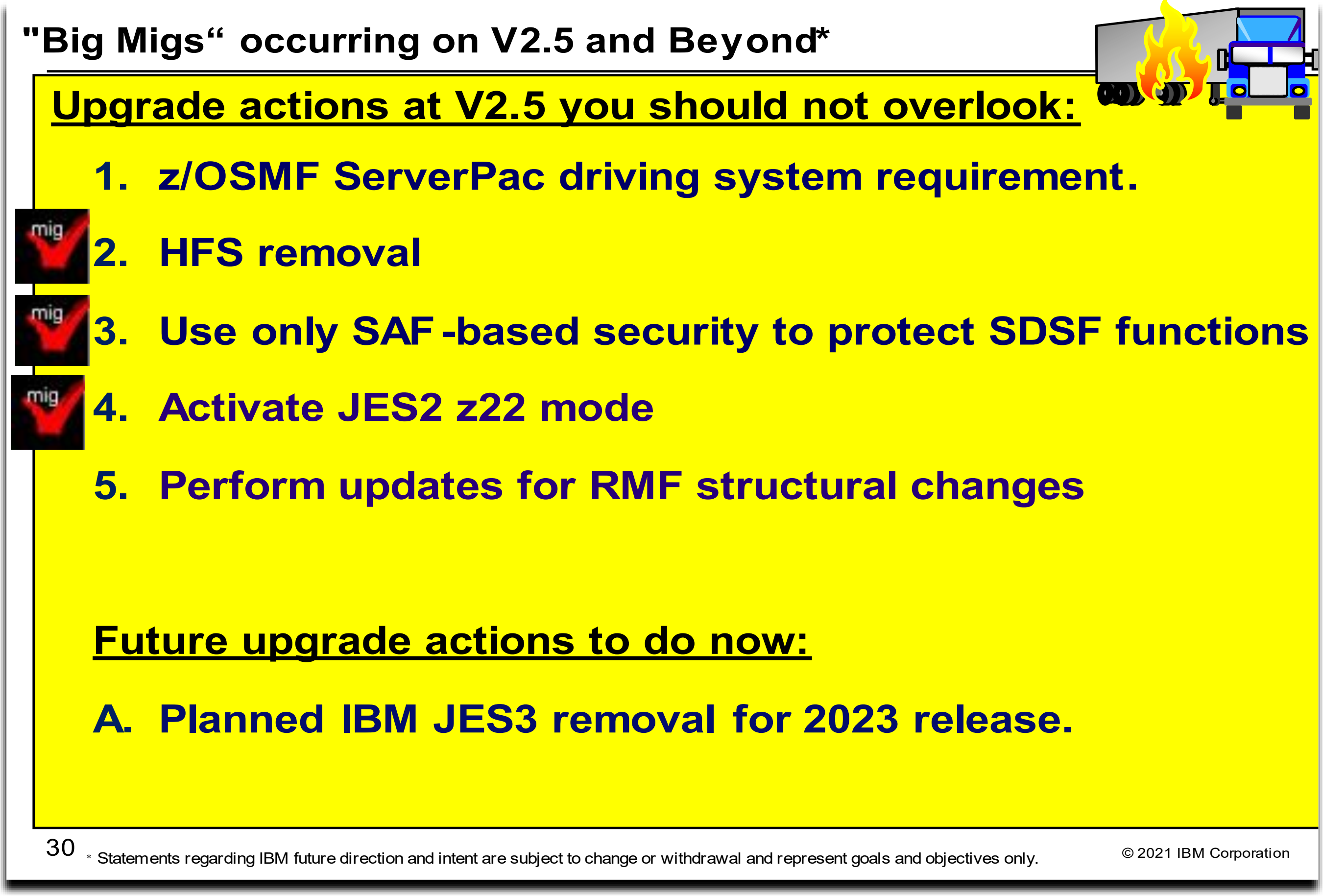
Upgrade actions on V2.4 you should not overlook:

1. 8 GB memory requirement for z14
2. BCP: Removal of support for user key common areas
3. Use Network File System(NFS) instead of DFS/SMB
4. Various actions related to HTTP→ HTTPS for CIM, PKI Services, RMF, Infoprint Central, and ISPF Gateway.
5. OpenSSH higher ported level of7.6p1.

Plus…

29

© 2021 IBM Corporation



"Big Migs“ occurring on V2.5 and Beyond*

Upgrade actions at V2.5 you should not overlook:

1. z/OSMF ServerPac driving system requirement.
2. HFS removal
3. Use only SAF-based security to protect SDSF functions
4. Activate JES2 z22 mode
5. Perform updates for RMF structural changes

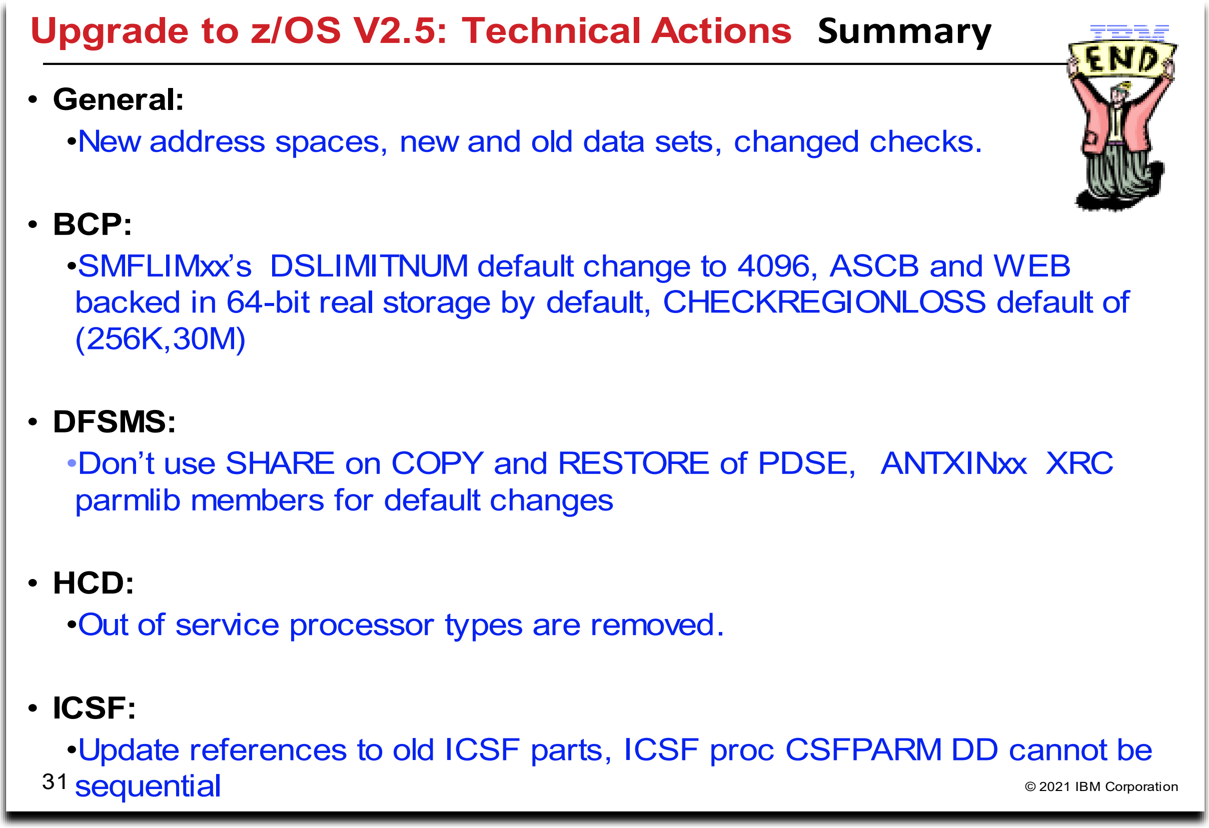
Future upgrade actions to do now:

A. Planned IBM JES3 removal for 2023 release.

30

* Statements regarding IBM future direction and intent are subject to change or withdrawal and represent goals and objectives only.

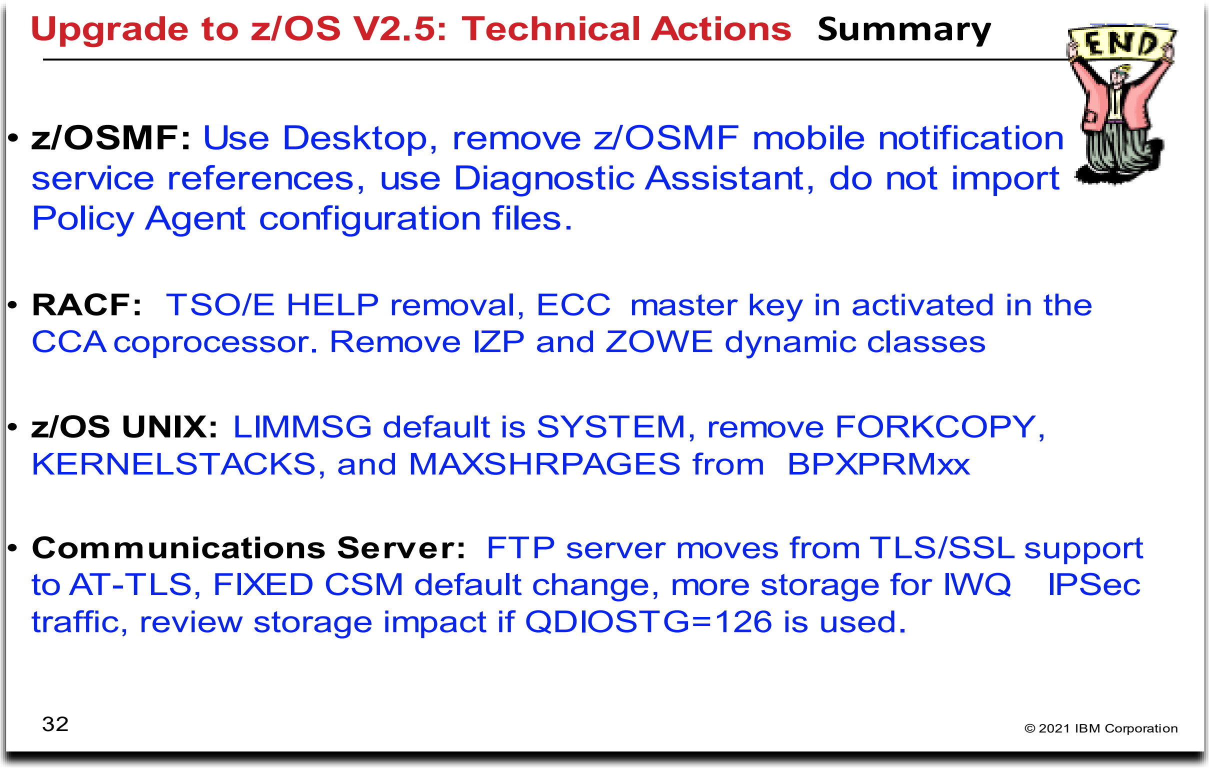
© 2021 IBM Corporation



Upgrade to z/OS V2.5: Technical Actions Summary

- **General:**
  - New address spaces, new and old data sets, changed checks.
- **BCP:**
  - SMFLIMxx's DSLIMITNUM default change to 4096, ASCB and WEB backed in 64-bit real storage by default, CHECKREGIONLOSS default of (256K,30M)
- **DFSMS:**
  - Don't use SHARE on COPY and RESTORE of PDSE, ANTXINxx XRC parmlib members for default changes
- **HCD:**
  - Out of service processor types are removed.
- **ICSF:**
  - Update references to old ICSF parts, ICSF proc CSFPARM DD cannot be sequential

31



Upgrade to z/OS V2.5: Technical Actions Summary

- **z/OSMF:** Use Desktop, remove z/OSMF mobile notification service references, use Diagnostic Assistant, do not import Policy Agent configuration files.
- **RACF:** TSO/E HELP removal, ECC master key in activated in the CCA coprocessor. Remove IZP and ZOWE dynamic classes
- **z/OS UNIX:** LIMMSG default is SYSTEM, remove FORKCOPY, KERNELSTACKS, and MAXSHRPAGES from BPXPRMxx
- **Communications Server:** FTP server moves from TLS/SSL support to AT-TLS, FIXED CSM default change, more storage for IWQ IPSec traffic, review storage impact if QDIOSTG=126 is used.

32