SHARE
EDUCATE • NETWORK • INFLUENCE

Upgrading to z/OS 3.2; Technical Actions, Part 2

Marna Walle
z/OS System Install
z/OS Development
mwalle@us.ibm.com

1

Abstract:

z/OS 3.2 is the latest release of our flagship operating system. Come to this session to learn the highlights on how to upgrade to z/OS 3.2, from either z/OS 3.1 or V2.5.

The general availability date for z/OS 3.2 was September 30, 2025.

Trademarks

Notice Regarding Specialty Engines (e.g., zIIPs 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 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

Agenda Upgrading to z/OS 3.2 TECHNICAL ACTIONS

- Where to find all the upgrade information for z/OS 3.2
- Highlight of Technical Actions for z/OS 3.2:
  - BCP
  - DFSMS
  - zCX
  - OpenSSH
  - JES2
  - SDSF
  - HCD
  - RACF
  - Communications Server

- "Big Migs" for z/OS V2.5-> 3.2 and 3.1-> 3.2

❖ *Bonus topic, if there is time! Customer configuration collection request*

3

Finding the latest z/OS 3.2 Upgrade Workflow

- The z/OS 3.2 Upgrade Workflow is part of z/OS!!
  - Not supplied via GitHub anymore.
  - IBM Service will also support this workflow
  - We still welcome any feedback or comments to zosmig@us.ibm.com.
- The files needed to create your workflow can be found in the directory **/usr/lpp/bcp/upgrade**
  - zOS_3.2_from_3.1_Upgrade_Workflow.xml
  - zOS_3.2_from_V2.5_Upgrade_Workflow.xml
  - z17_zOS_Upgrade_Workflow.xml
  - z16_zOS_Upgrade_Workflow.xml

  HW info not included in z/OS info anymore
  - When creating your workflow, choose the appropriate file for the system you are upgrading from.
- The initial workflows are shipped back to z/OS V2.5 and 3.1 with a PTF, and found with the FIXCAT **IBM.Coexistence.z/OS.3.2**
- Updates to the z/OS 3.2 Upgrade Workflow, will also have the same FIXCAT.
  - Use “Create new based on existing” to pick up updates.

4

Very Important Links:
Exported version (HTML) of the z/OS 3.2 Upgrade Workflow is available on IBM Documentation for z/OS 3.2, under “System Level” category.

Content Solution webpage for learning in an easy way about ServerPac packaged as a z/OSMF Portable Software **Continuing the advancement in z/OS upgrade assistance!** https://www.ibm.com/support/z-content-solutions/serverpac-install-zosmf/

We have two z/OS Management Facility (z/OSMF) z/OS Upgrade Workflow versions, one for the n-1, and one for the n-2 path. Using the z/OSMF workflow, you can go through a z/OS 3.2 upgrade as an interactive, step-by-step process. Depending on your z/OS 3.2 upgrade path, you select the file you will need.

In z/OS 3.2, the z/OS Upgrade Workflow has the capability to invoke IBM health checks directly from the step, and also provides the optional capability to give feedback on your upgrade experience. The z/OS 3.2 Upgrade Workflow is supported by the IBM Service organization, and provided in PTF(s). We also do welcome suggestions or comments to email zosmig@us.ibm.com.

The z/OS 3.2 Upgrade Workflow has the ability to discover used z/OS priced features (continuing what was introduced in V2.3), and some other features, on your system. This is very helpful, because if you are not using a certain feature, then why have to manually skip those steps yourself? The z/OSMF Workflow can identify many features that you might not be using, and automatically skip them in the Workflow for you, giving you less steps to perform. In z/OS 3.2, is the ability to reduce the number of applicable steps by seeing if PTFs that included HOLD ACTIONs were already performed. In addition, coexistence PTF verification can be done from the Workflow, via an included SMP/E REPORT MISSINGFIX step.

If you would like to see a short demo on using the z/OS V2.1 migration workflow, visit the IBM Media Center for an older, but yet still valuable, video on what the migration workflow looks like, and how to use it.

Upgrade Workflow Usage Tips

1. If you have performed part of any Workflow, and there has been an updated version of that Workflow that has been issued, you can update your partially completed Workflow by using the action “Create new based on existing”. This can “merge” the two Workflows together such that unchanged steps that you have completed, stay completed.
2. The URL links to the documentation in the workflow cannot go to an anchor in the web page. The URLs will just bring you to the web page, not content that may be further down in the page. You may have to scroll down on the web page to find the information that you need.
3. For each upgrade action and for the entire upgrade, you can optionally provide your feedback to IBM. Just follow the instructions you see in z/OSMF. You do not need to provide feedback to complete each step of the workflow.
4. When searching for something in the Workflow, use the Search capability in the upper right corner. This strong capability can look “inside” all the steps to find the string you are looking for.

z/OS Upgrade Workflow

Starting in z/OS V2.4, IBM no longer provides the z/OS Migration publication, GA32-0889, in its current format. Since z/OS V2.2, the preferred method for learning about upgrade actions has been the z/OS Upgrade Workflow. Discovering, performing, and verifying many upgrade actions through the z/OSMF Workflow function instead of a more traditional book format allows for a tailored and specific upgrade path associated with a particular system.

Starting with the z/OS V2.4 release and later, IBM provides upgrade tasks in a z/OSMF Workflow, as well as a single exported file. By providing the z/OS upgrade materials in both formats, users still can enjoy the advantages of a z/OSMF Workflow as well as being able to search, browse, and print in a more traditional format. Notice that the exported format of the z/OS upgrade materials that can be easily read or printed for those without any z/OSMF capabilities will not be tailored for any environment.

Elements with Upgrade Actions for z/OS 3.2

These elements have 3.1 → 3.2 upgrade actions:

- ➢ BCP
- ➢ Communications Server
  - Cryptographic Services – System SSL
  - Integrated Security Services - NAS
- ➢ DFSMS
- ➢ HCD
  - Infoprint Server
- ➢ JES2
  - Language Environment
- ➢ MICR/OCR
  - Network File System (NFS)
  - RMF
- ➢ SDSF
- ➢ Security Server (RACF)
  - XL C/C++
- ➢ z/OS Container Extensions (zCX)
  - z/OS Management Facility

➢ ***means that some of that element's upgrade actions are discussed in this presentation.***

ALWAYS use the z/OS 3.2 Upgrade Workflow to know all the upgrade actions!

5

BCP Upgrade Actions for z/OS 3.2

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

Ensure that the sysplex uses SSD-capable sysplex couple data sets
(Required-IF, as of 3.1)

- A basic or parallel sysplex requires a couple data set formatted to support System Status Detection (SSD) protocol.
- Failure to use the required level of sysplex CDS could result in:
  - z/OS 3.1 cannot initialize a sysplex containing a downlevel sysplex CDS.
  - z/OS 3.1 cannot join a running sysplex that contains a downlevel sysplex CDS.
- Use the XCF_SYSSTATDEF_PARTITIONING health check or enter D XCF,COUPLE,TYPE=SYSPLEXand check that "SYSTEM STATUS DETECTION PROTOCOL IS SUPPORTED" for both primary and alternate sysplex CDS's.
  - If the sysplex CDS is not formatted with the SSD protocol, format two replacement SSD-capable sysplex CDS's, with the input to the utility ITEM NAME(SSTATDET) NUMBER(1).
  - Introduce the primary and alternate CDS to the sysplex using the usual SETXCF commands (new alternate, switch, new alternate).

6

BCP Upgrade Actions for z/OS 3.2

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

Accommodate the changed default value of the OPT parameter CPENABLE

(Required-IF, as of 3.2)

- Starting in z/OS 3.2, the default value of the OPT parameter CPENABLE is changed from (0,0) to SYSTEM.
- The new default value, CPENABLE=SYSTEM, automatically applies low and high threshold values recommended by IBM.
- This value removes the need to update the parameter when there is a hardware migration.
- In contrast, the previous default CPENABLE=(0,0) causes all logical processors to be enabled for I/O interrupts.

7

DFSMS Upgrade Actions for z/OS 3.2

Upgrade Actions Before Installing:

DFSMSdfp: Accommodate change to SAF checking during VSAM OPEN of data sets (Req-IF, as of 3.2)

- Pre-3.2, VSAM OPEN routines automatically bypassed SAF authorization checking if the program that issued the OPEN request was running in supervisor state or protection key zero.
- In z/OS 3.2, programs no longer bypass the SAF authorization check for VSAM OPEN requests by default if they are running in supervisor state or key zero.
- Use the FACILTIY class STGADMIN.IGG.AUTO.BYPASS.LOG, collect SMF 80 for that FACILITY class resource, run workloads, and then use SMF 80 records to determine which jobs are opening VSAM data sets and bypassing SAF authorization checks.

DFSMSdfp: Define and permit copy services related facility class profiles (Req-IF, as of 3.2)

- Starting in z/OS 3.2, DFSMS system data mover (SDM) will fail TSO/E commands and ANTRQST functions if the requested service does not have a matching FACILITY class resource profile, or the user lacks READ access to the matching profile.
- Determine whether any programs on your system use SDM TSO commands and ANTRQST calls.
  - If these services are being used, determine whether profiles are defined for the related FACILITY class resources. If needed, define matching profiles and permit users before trying to use the associated commands on z/OS 3.2.

8

zCX Upgrade Actions for z/OS 3.2

Upgrade Actions you can do NOW:

Prepare existing zCX workflow instances (Required-IF, as of V2.5 OA64231)

- zCX Workflows was impacted by the z/OSMF Workflow upgrade action ("Check workflow definition files for undeclared referenced entities").
- Correction was provided in OA64231 for the affected workflows, with workflow version 1.1.4.
  - If your zCX Workflow instances are at least 1.1.4, you are not affected.
- If you have any zCX Workflow instances that are 1.1.3 or earlier, you are impacted. Prior to IPLing 3.1, you must:
  - Complete, export, or delete any zCX workflow instances on your system
  - Install the PTF for OA64231.
- After 3.1 has been IPLed, you can no longer access the zCX workflows that are levels prior to 1.1.3.

zCX: Ensure that all zCX appliance levels are at least 1.26.0 (Required-IF, as of 3.2)

- Prior to upgrading to z/OS 3.2, ensure that your existing zCX appliances are upgraded to the zCX maintenance level 1.26.0 or later. This minimum level is needed to maintain the serviceability of your zCX appliances for subsequent upgrades in the future.
- Important: You must perform this work on your existing z/OS 3.1 or 2.5 system. Failure to do so can result in zCX instance failures on the z/OS 3.2 system and require you to re-provision your zCX instances and container deployments.

9

z/OS OpenSSH Upgrade Actions for z/OS 3.2

Upgrade Actions Pre-First IPL:

- **Accommodate the OpenSSH ported level (Required-IF, as of 3.1)**
  - Pre-3.1 was open source version OpenSSH **level 7.6p1**.
  - 3.1 and 3.2 contains open source version OpenSSH **level 8.4p1**.
  - Several differences in the ported levels, which may cause upgrade actions.
  - Less-secure algorithms are either deprecated or removed as defaults:
    - Diffie-hellman-group14-sha1 is removed from the default KexAlgorithms list.
    - If ssh-keygen is used to create new OpenSSH certificates with an RSA key, the rsa-sha2-512 algorithm is used by default.
    - The ssh-rsa (sha1) key algorithm is still supported as a default key algorithm, but is deprecated. It will be removed as a default in a future release.
  - Changes to these might require a potential upgrade action:
    - ssh_config file
    - sshd_config file
    - ssh_config file in /samples/
    - sftp command
    - ssh-keygen command
  - Use the health check, and read of all changes in the *z/OS 3.2 Upgrade Workflow.*

10

JES2 Upgrade Actions for z/OS 3.2

Upgrade Actions Before installation:

Review applications that create, modify, or delete JES2 system data sets (Required-IF, as of 3.2)

- In z/OS 3.2, JES2 obtains shared SYSDSN ENQs for the following JES2 system data sets:
  - CKPT1
  - CKPT2
  - NEWCKPT1
  - NEWCKPT2
  - SPOOL data sets
- JES2 obtains shared SYSDSN ENQs on these data sets when they are allocated.
  - This change is intended to protect against the accidental modification or deletion of system data sets that are necessary for JES2 function.
- It is possible that your installation might have applications that intentionally modify or delete JES2 system data sets. If so, these applications are affected by this change. Ensure that a viable method is in place to accommodate the new system data set ENQ protection.
  - This protection can be temporarily toggled off.

11

SDSF Upgrade Actions for z/OS 3.2

Upgrade Actions Before Installing:

Use dynamic statements for SDSF configuration, not assembler macros (Req-IF, as of 3.1)

- As of 3.1, assembler macros for defining ISFPARMS are not allowed.
  - Usage of the parmlib member ISFPRMxx is required.
- ISFPRMxx was introduced in 1995 and is easier to use, less error prone, and more dynamic than assembling ISFPARMS.

- In addition, when ISFPRMxx is used, the SDSF server creates a log that lists all ISFPRMxx statements processed and the values that were used.
- **If you are already using ISFPRMxx, no action is necessary.**
- To convert from assembler format to ISFPRMxx, use conversion tool ISFACP.

Update the Java CLASSPATH and LIBPATH references in your scripts (Req-IF, as of 3.2)

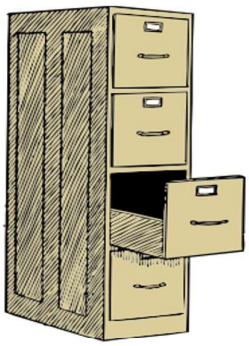
- As of 3.2, the SDSF Java API is enhanced to use the FasterXML Jackson JSON parser. To support this change, the jar files that the Jackson JSON parser uses must reside on the same class path that your scripts use to invoke the SDSF Java API.
- To accommodate this change, you might need to update the Java CLASSPATH and LIBPATH variables for any of your scripts that invoke the SDSF Java API. (Symlinks previously provided to SDSF jar files and DLLS are removed.)
- Use CLASSPATH variable of **/usr/lpp/sdsf/java/classes/isfjcall.jar**
- Use LIBPATH variable of **/usr/lpp/sdsf/java/lib_64**

12

HCD Upgrade Actions for z/OS 3.2

Upgrade Actions Before Installing:

Remove configurations for unsupported processor types (Req-IF, as of 3.2)



- Out of service processor types are not supported by HCD:
  - 2964 and 2965: z13 and z13s
  - 2827 and 2828: zEC12 and zBC12
  - 2817 and 2818: z196 and z114
  - 2097 and 2098: z10 EC and z10 BC
  - 2094 and 2096: z9 EC and z9 BC
  - 2084 and 2086: z990 and z890
- Remove these server configurations from your IODF, before upgrading to 3.2.
- 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 3.2.

13

RACF Upgrade Actions for z/OS 3.1

Upgrade Actions Before First IPL:

Security Server: Change RVARY passwords to use KDFAES encryption (Req-IF, as of V2.4 with OA65905)

- With the SETROPTS command, the security administrator can set the password the operator must supply in order for RACF to complete an RVARY command that changes RACF status or changes the RACF databases.
  - As of APAR OA65905, RVARY passwords are protected using the KDFAES algorithm. Previously, RVARY passwords were protected with Data Encryption Standard (DES), an earlier and less secure method of data encryption.
  - Install the PTF for APAR OA65905 on **all** systems which share the RACF database. Take a database backup prior to the KDFAES conversion.
  - Follow the HOLD ACTION in the PTF for APAR OA65905, which requires you to change your RVARY passwords using the new KDFAES keyword.
- Important: If the upgrade action is not performed, and an installation -defined RVARY password is in effect, the password will not correctly evaluate on 3.2.
  - Therefore, critical RACF database maintenance functions that use the RVARY command will not work, unless the RVARY command is entered from a console with master authority.
  - The condition can be avoided by changing the RVARY passwords on 3.2, but you must do so prior to encountering a situation that requires RVARY for its resolution, such as switching to the backup database.

14

Communications Server Upgrade Actions for z/OS 3.2

IP Services: Prepare for more secure TLS defaults in System SSL and AT-TLS (Req-IF, as of 3.2)

- Default **TLS protocol** change: The defaults for TLS V1.0, TLS V1.1, and TLS V1.2 are changed. Only TLS V1.2 is enabled by default.
- Default **cipher suites** change: SHA1 ciphers are removed from the default list.
- Default **signature algorithms changes for X.509 certificates and handshake messages**: SHA1, SHA224 and DSA are removed from the default signature algorithms that are used by X.509 certificates and TLS handshake messages.
- Default **signature algorithms change for certificate revocation**: SHA1, SHA224 and DSA are removed from the default signature algorithms that is used for OCSP, HTTP and LDAP CRL revocation checking.
- Default **client elliptic curves list order** change: secp224r1 is moved later in the order of the client's list of supported elliptic curves/supported groups.

IP Services: Prepare for more secure TLS defaults for the FTP client (Req-IF, as of 3.2)

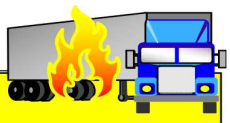
- TLSv1 is no longer enabled unconditionally. A configuration statement is added to FTP to control whether TLSv1 is enabled. **By default, TLSv1 is disabled**.
- If the CIPHERSUITE statement is configured, FTP uses 4-character cipher specifications when it calls System SSL. Otherwise, FTP does not pass a default value, which allows System SSL to use its new 4-character default ciphers in z/OS 3.2.

IP Services: Prepare for more secure TLS defaults for the Policy Agent client(Req-IF, as of 3.2)

- Parameters are added to control whether TLSv1, TLSv1.1, and TLSv1.2 are enabled. **By default, TLSv1 and TLSv1.1 are disabled** and TLSv1.2 is enabled.
- Various defaults in System SSL are updated. These changes can impact ciphers, client elliptic curves, and hash and signature algorithms for the policy agent client, if default values are used

15

"Big Migs“ occurring on 3.1



Upgrade actions at 3.1 you should not overlook:

1. IBM JES3 removal
2. Use dynamic statements for SDSF configuration, not assembler macros.
3. Sysplex couple data sets are System Status Detection (SSD) capable
4. OpenSSH new ported level, 8.4p1
5. z/OSMF Workflow definition files for undeclared referenced entities, before 3.1 IPL.
6. zCX Workflow instances should be completed, before 3.1 IPL.

Plus…

16

"Big Migs“ occurring on 3.2

Upgrade actions at 3.2 you should not overlook:

1. Update your z/OS functional dependency to Semeru 21 (verify JAVA_HOME)
2. zCX: Ensure that all zCX appliance levels are at least 1.26.0
3. IP Services: Prepare for more secure TLS defaults in System SSL and AT-TLS, Prepare for more secure TLS defaults for the FTP client, and Prepare for more secure TLS defaults for the Policy Agent client.

17

Summary Upgrading to z/OS 3.2 TECHNICAL ACTIONS

- **BCP:**
  - •IEAOPTxx CPENABLE default change from (0,0) to SYSTEM.
- **DFSMS**
  - •Accommodate change to SAF checking during VSAM OPEN of data sets.
  - •Define and permit copy service related facility class profiles, use a matching FACILITY class resource profile.
- **JES2:**
  - •Prepare for shared SYSDSN ENQs for several JES2 system data sets. Default usage of new job level resource limits and actions, truncation of blanks which affects some printing products. Investigate exit 2 and 52 changes.
- **SDSF:**
  - •Use Java CLASSPATH and LIBPATH variables for any of your SDSF JAVA scripts.
- **HCD:** Out of service processor types are removed.
- **RACF:**
  - •Change RVARY passwords to use the new KDFAES keyword.

18

The Process to Participate In First or Second Round:

To participate, please reach out to zos@ibm.com with the email subject line: **Z Configuration Collection Program**

If you participated in First round, Thank You! Come back to the website for additional collection programs!

1. **Sign up** to receive an invitation to the Early Release Program site. (click to agree to access)
2. **Download and run** the provided scripts on each system.
3. **Review and scrub** the output data to remove any information you do not wish to share with IBM.
4. **Upload** the files to IBM.

22

